Research on the Security Technologies of Power Grid EMS Based On SOA

Zhiyong Lu*, Yijun Zhang, Luan Yang, Shiping Xu ,Yuanyou Chen
Luoyang Electronic Equipment Test Center of China (LEETC) ,Luoyang, China ,471003
*e-mail: Luzhiyong2002@sohu.com

***Abstract*—This article analyzes the accidents of power grid in some domestic region to discuss the security problems existing in the power grid Energy Management Systems (EMS). Combined with the security requirements of EMS, the method of improving EMS security based on SOA is proposed and the involving key technologies are studied as follows: the loosely coupled EMS based on SOA, the graded and modularity security configuration, the management of security configuration based on Concurrent Version System (CVS) and the mirror of Real-Time Databases (RTD) based on cloud computing. All the above technologies proposed in this paper greatly improve the security of EMS.**

Keywords- EMS Security; SOA; CVS; Cloud Computing

I. INTRODUCTION

At present, with the increasingly complex of power grid structure, more close of power grid interconnection, increasing volume of trading power, gradually smaller of transmission margin, more security and reliability requirements are put forward for the power grid[1][2]. But, it is extremely easy to neglect the security of EMS, which is an important base of power grid. So, it is an urgent need to develop new technologies to improve the security of EMS. At present, a lot of researches have been made in this respect at home and abroad [3][4][5]. They mainly focus on the EMS disaster recovery, but the security configuration of EMS itself is still a "short plank" of power grid security. SOA provides reusable, scalable and open system architecture for the new generation of EMS, which can not only adapt to the modern IT technology, but also bring greater benefits to EMS companies[6][7][8][9]. The plug and play is realized for EMS modules between different providers by SOA, so it solves the monopoly of company due to the tight coupling of EMS and lays the foundation for the further development of EMS. Against this background, combined with many years of actual working experience, the importance of EMS security configuration is discussed by analyzing specific accidents in some domestic region. The method of improving EMS security based on SOA is proposed and involving supporting technologies are studied. The remaining sections are organized as follows. Section 2 analyzes and summarizes the common faults of EMS based on many years of actual working experiences. Section 3 proposes the method of improving EMS security based on SOA and studies the involving technologies. Conclusions are made in section 4.

II. THE FAULT ANALYSIS OF EMS

The EMS is an integrated power network automation system. It involves automation, dispatching, protection, operation, etc., and also covers the monitoring, control and dispatching management of all links of power grid [10]. With the increasing requirements on the security and stability of the power grid, it promotes the constant development of power grid automation technologies. The specialists in different areas study them from different angles and develop a large number of systems to ensure the safety and stability of the power grid [3][4][5], which leads to the functions of EMS more and more complex. In order to ensure that the EMS operates stably and efficiently, it is necessary to need extensive security measures. So combined with many years of experience in using EMS, by analyzing the common faults of EMS, the main reasons are summarized as following:

- **Incomplete test**

The EMS companies may have better software development standards, and do a lot of tests to ensure the EMS security. However they mainly focus on whether the functionality and performance requirements can be met and ignore the disaster recovery capability to deal with emergencies. Moreover, it is difficult to simulate the scenes of emergencies so the function of disaster recovery cannot be test completely, especially software exceptions caused by hardware failures, for example, the loss of memory data.

- **The abnormity exit of main program caused by exceptions of sub programs**

The exceptions of sub programs can cause the main program to exit abnormally. For example, in some domestic region, when the analog quantity array index in the telecontrol information table of the SCADA is out of bounds, the SCADASERVER process exits for the prevention mechanism. The SCADASERVER is a kernel process of SCADA, so its exit will lead to the SCADA function unavailable. Therefore it is necessary to develop the corresponding counter measures to ensure that the exceptions of sub programs will not affect the normally running of the main program.

- **The key configurations mistakenly modified due to no authority control**

People used to do everything by superuser in the use of Windows XP， so that most users still directly use the superuser to do operation in the use of Linux, Unix, which is inevitable to pose a great threat to the security of the system. So, it is necessary to assign an account for each application. Every user must use the assigned account to do operation so

Published by Atlantis Press, Paris, France.

as to limit the authority in the application. The authority of EMS should also be divided to ensure that the key business configuration will not be mistakenly modified. For example, it is found that the function 1 + N do not start after EMS failure, but it is normal during the Systematic Acceptance Test (SAT) of the whole system. Finally, the finding reason is that the key configuration is mistakenly modified by the synchronization procedure of maintainer, which leads to the function 1 + N failure. Moreover, this critical configuration cannot be viewed in the operator interface and the error configuration couldn't be found until finding the EMS failure and the function 1+N unavailable. Therefore, some measures must be taken to ensure that the critical configuration cannot be mistakenly modified.

- **The failure of warning mechanism based on passive waiting**

Although a lot of tests have been done, but it is possible that errors will still occur during the program's running. Therefore, it is needed to be sure that the warning is timely generated when the program throws exceptions and is about to collapse. At present, most of the works adopt the mechanism of receiving warning messages passively. When a program is abnormal, it will generate a warning message and send it to the warning notification service. Then the warning notification service will parse the message and alert the operator by warnings such as emails, short message, sound, etc. But this mechanism has a fatal problem. If the main process of EMS exits abnormally and does not generate a warning, the EMS tends to be still regarded as normal by the warning notification service. Therefore, the warning mechanism fails. For example, the SCADA cannot generate a warning after the collapse of SCADA key process because the warning itself is generated by the SCADA. Consequently the maintainer cannot yet receive a warning message, which delays the opportunity of finding the accident.

Based on the common fault reasons of EMS summarized above, this paper puts forward the following improvement measures. First, the functions of EMS are modularly divided so as to improve the test. Second, the standard interface based on service is provided so as to implement loosely coupling. Third, the security grade of each module and service is determined and the corresponding invoking and managing authority is allocated. It is ensured that the exceptions of lower grade authority service will not affect the running of higher grade authority service, but the higher grade authority service can stop the lower one. The maintainer can't do managing and maintenance by using the superuser and can only use the corresponding user. Forth, the warning, as an independent service, and the EMS operate respectively on two different servers. They monitor each other based on heartbeat mechanism, so that once one party is checked no response, the other party will warn.

To complete the above improvements, it needs to adjust the EMS architecture. Combined with the loose coupling characteristics of SOA, the improvement of EMS security based on SOA is proposed and further discussed below.

III. THE IMPROVEMENT OF EMS SECURITY BASED ON SOA

A. The Loosely Coupled EMS Based on SOA

In SOA, every function unit of an application is encapsulated as a service. The relation between services is specified by the well-defined interface. The interface is in a neutral form, independent of the specific hardware platform, operating system and programming language, so that all services can interact in a unified and general form[11][12][13]. In SOA, the application is constructed by service orchestration not by coding, so that it can response quickly to the changes of markets. Consequently, the EMS based on SOA is proposed as Figure 1 shows. It realizes the loosely coupling of each EMS function module. The EMS function modules are classified into the legacy EMS service, the standard EMS service, the basic EMS service. The legacy EMS service needs a service adapter to convert into the standard interface protocol to connect to the service bus. The standard EMS service can directly connect to the service bus. It mainly includes SCADA、AVC、PAS/DTS. The basic EMS service often has stability functions and won't be affected by business data, so it can be deployed independently. It is not only convenient for other systems to call but also can prevent the impact from the collapse of the business system. The basic EMS service mainly includes warning, log, rights management, etc.

The EMS based on SOA decouples the client and the remote provider by the message mechanism and thus to realize the loose coupling of the whole system. The communication between the client and the provider is managed by the message framework. As long as the message conforms to the standard, the client or provider can make any changes as needed, while it won't bring any influence to the other party. The loose coupling brings many advantages to the EMS, for example, decreasing the dependency between the client and the provider. Although the tight coupling has the advantage of performance, it is not necessary for the security configuration.

The data bus provides high-speed access services for all kinds of data information including files, relational databases (RD) and real-time databases (RTD). The data bus is deployed by cloud computing in order to ensure that data can be barrier-free accessed when some failure occurs. Files, relational databases, real-time databases and all other data information will be deployed on the cloud server. When an exception happens, the deployment server will drifting to other nodes autonomously.

Published by Atlantis Press, Paris, France.

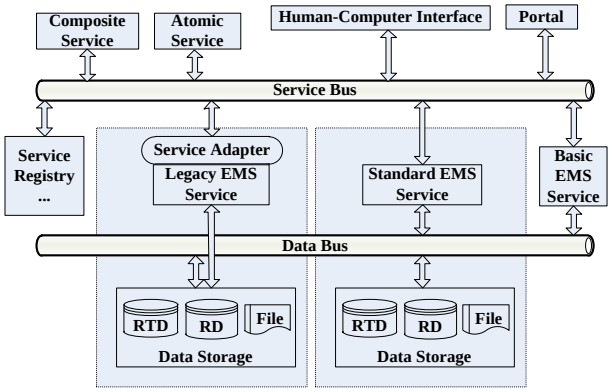

Figure 1. The architecture of EMS based on SOA

B. *The Graded and Modularity Security Configuration of EMS*

For the EMS based on SOA, each functional module is invoked in the form of independent service, but the invoking power of service is assigned by the EMS security configuration.

All the EMS security configurations are graded according to the importance and function category as follows. First grade, the platform core security configuration. It will directly affect the stability of the whole EMS platform. If there is any error setting the whole platform will collapse or become unavailable. This kind mainly includes SCADA, pre-function, real-time database, network. Second grade, the important function security configuration. It will directly affect some important function or the stability of partly platform. If there is any error setting some important function will become unavailable or partly platform will collapse. This kind mainly includes AVC, remote workstation, agency, PAS/DTS, etc.

Because each EMS sub module shares the same computing resources and network resources, the modules of the same kind are encapsulated in a separate partition. All partitions are isolated from each other in order to prevent errors spread between modules of different grade. This partition management technology greatly improves the EMS's capability of fault tolerance and makes the upgrading and maintenance of the EMS easier.

C. *The Management of EMS Security Configuration Based On CVS*

Based on the graded and modularity security configuration, EMS must need strict version control. In this paper, we propose security configuration framework of EMS based on CVS (Concurrent Version Systems). CVS is a version control system which provides code version maintenance in a collaborative development environment [14]. It adopts Copy-Modify-Merge model to support access and modify code concurrently. It clearly separates the source code and the users' workspace and makes them operate parallelly. CVS can support multi-users based on client/server network architecture, which makes it to become the first choice for collaborative development in a distributed environment. However, it is not only limited to the code maintenance, but also can be used to maintain the development and use of any document, for example, the editing and modifying of shared files.

Combined with EMS security configuration, the management process is designed as shown in Figure 2. When the system operations online, any changes must be first checked out by CVS. Then the editor can modify the security configuration. Only when the modified security configuration is registered can they get the CVS version number. As soon as having a new CVS version number, it means that the security configuration will probably change. The CVS trigger will send a warning message to the corresponding manager and developer, so as to ensure that any change pass audits. If the EMS of this accident domestic region has this management process, the mistakenly modified configuration of 1+N function would not happen, and thus avoid the accident.

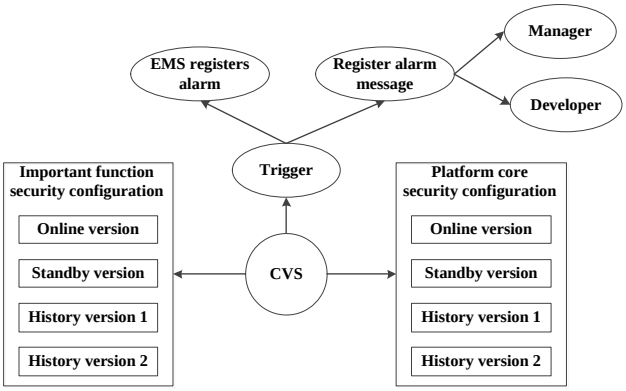

Figure 2. The management process of EMS security configuration based on CVS

D. *The Mirror of Real-Time Databases Based on Cloud Computing*

At present, most EMS uses the distributed real-time database technology and most of its databases are deployed in different SCADA servers. In accordance with settings, the distributed real-time databases automatically keep the consistency between all the databases, which provides a solution for maintaining the consistency of databases on each node. At present it is usually constructed according to the Client/Server model. For a distributed real-time database, only one database node acts as reference point (Server) in the whole system and all other database nodes act as replication point (Client). The databases on the replication points automatically keep the consistent with the database on the reference point so that the consistency of all the databases nodes is achieved. The distributed real-time database achieves disaster tolerance by dynamic switching between the same databases on different nodes. If some database has one or more real-time mirroring databases which are available to switch, then it can avoid the EMS accident to certain extent.

Published by Atlantis Press, Paris, France.

Cloud computing, as a new type of shared infrastructure, supports physical server and virtual server. With the intense research and continuous development of cloud computing, the virtualization of operation and management will gradually realize [15]. As Figure 3 shows, EMS is deployed on the cloud computing platform built by IBM cloud computing software. The virtual machines can dynamic migration between different physical hosts by monitoring their running state. The running virtual real-time database can drift to other physical hosts in milliseconds and also the front end active hardware can quickly switch to the standby hardware, so that the EMS is always protected and shows the high satisfactory performance.

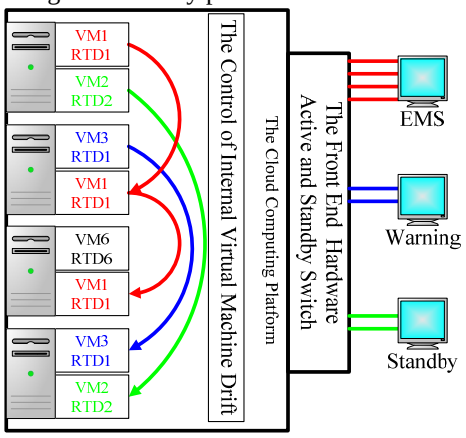

Figure 3. The deployment of EMS based on cloud computing platform

IV. CONCLUSIONS

In this paper, based on long-term actual working experience, the typical power grid accident in some domestic region is analyzed, and the fundamental problems are found that the tight coupling of EMS and the lacking of systematic design and management of EMS security configurations. EMS as the core of the power dispatching automation system, whose failure will cause the failure of analysis capabilities and most advanced applications. Against this problem, the improvement of EMS security based on SOA is proposed. The loosely-coupled EMS is realized based on SOA. The graded and modularity security configuration is put forward and the security configuration management based on CVS is designed. The mirror of real-time databases is realized by deploying on cloud computing platform. All of the above technologies significantly improve the EMS security.

ACKNOWLEDGMENT

The authors wish to thank the anonymous referees of this paper for their invaluable comments and useful suggestions.

REFERENCES

[1] Iyer, G., Smart Power Grids, Proceeding of 42nd Southeastern Symposium on System Theory (SSST), Tyler, pp. 152-155, 2010.

[2] Mcdonald J., The next-generation grid, IEEE Power & Energy Magazine, Vol 7, No. 3, PP. 26-32, 2009.

[3] Shi Li, Ming Zeng, Lingyun Li, A novel Electricity Marketing Model Integrating Intelligent Disaster-Recovery System, Systems Engineering Procedia, Vol 4, pp. 133-142, 2012.

[4] Fallara, P., Disaster recovery planning, IEEE Po-tentials, Vol 22, No. 5, pp. 42–44, 2009.

[5] Feng Ding, Hong Zhu, Leng Jun, Construction of SCADA backup system in case of disaster for district network dispatching, Automation of Electric Power Systems, Vol 29, NO. 6, pp. 105–107, 2009.

[6] Pagani, G. and Aiello, M., Service Orientation and the Smart Grid state and trends, Service Oriented Computing and Applications, Vol 6, No. 3, pp. 267-282, 2012.

[7] Mercurio, A., Giorgio, A., Cioci, P., Open-source implementation of monitoring and controlling services for EMS/SCADA systems by means of web services, IEEE Trans Power Deliv, Vol 24, No. 3, PP. 1148–1153, 2009.

[8] Pagani, A., Aiello, M., Towards a service-oriented energy market: current state and trend, Proceedings of the 2010 international conference on Service-oriented computing, pp. 203–209, 2011.

[9] Postina, M., Rohjans, S., Steffens, U., Uslar, M., Views on service oriented architectures in the context of Smart Grids, Proceedings of the first IEEE international conference on Smart grid communications, pp. 25–30, 2010.

[10] Maghsoodlou, R., Masiello, R., Energy management systems. IEEE Power and Energy Magazine, Vol 2, No. 5, pp. 49–57, 2004.

[11] Laskey, K.B. and Laskey, K., Service oriented architecture, Wiley Interdisciplinary Reviews: Computational Statistics, Vol 1, No. 1, pp. 101-105, 2009.

[12] Draheim, D., Service-Oriented Architecture, in Business Process Technology, Springer Berlin Heidelberg, pp. 221-241, 2010.

[13] Perrey, R. and Lycett, M., Service-oriented architecture. Proceedings of Applications and the Internet Workshops, pp. 116-119, 2003.

[14] http://www.nongnu.org/cvs/

[15] Tsai, W., Sun, X., Balasooriya, J., Service-oriented cloud computing architecture, Proceedings of Seventh International Conference on Information Technology: New Generations (ITNG), Las Vegas, 684-689, 2010.

[16] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[17] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[18] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[19] K. Elissa, “Title of paper if known,” unpublished.

[20] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[21] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[22] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[23] Electronic Publication: Digital Object Identifiers (DOIs):

Article in a journal:

[24] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.