A SCADA approach for Micro-grid based on Platform as a Service (PaaS) Delivery Model of Cloud Computing

Di Zhuo, Gang Yining, Ding Yi, Sun Jianhang*
Liaoning Electric Power Energy Development Group Co., Ltd. Shenyang, 110000, China

Abstract. Based on the current development of smart grid, this paper makes an in-depth exploration on the interoperability of microgrid platforms, mainly on the interoperability among institutions. Conduct a hierarchical analysis of different requirements to study different levels of interoperability. In this paper, a private hybrid cloud based SCADA architecture is found based on the interoperability of the microgrid platform while ensuring security limitations. Because data collection and critical monitoring are limited by time in the grid, not as critical monitoring and data collection can be accessed by private cloud partners only after being selected. And the main SCADA function is still controlled by the local server, so the cloud architecture is mixed, and this communication is a service delivery model, a model based on cloud computing.

1. Introduction
With the development of smart grids, there is an increasing demand for interaction between user platforms. Interoperability allows platforms to seamlessly and independently integrate all components of power and distribution systems, and management and communication interoperability of microgrid platforms allows users to exchange and process meaningful information between systems[1].

The interactive platform is usually placed in a research center or laboratory for demonstration or as an experimental platform. At one institution application needs to use other platforms facilities, interoperability between each other is inevitable, and strengthen the platform interoperability between the connection time and occupied resources and to establish a new experiment module, compared to establish a new experiment module compared far want to spend much more time and energy, and the technology is also in the study of the multi-site project develops, more provides technical support for the project implementation [2].
Figure 1 illustrates a simple cloud-based hybrid SCADA architecture. From the top level, communication policies between the two operational agencies should be coordinated[3]. Interoperability of the functional layer is used in the mapping of experimental applications and research infrastructure, and this information is used in the planning of multi-site projects and applications, such as remote control and co-simulation. In order for the information exchanged to be understood by the other party, interoperability requires both parties to share an information model or one or more transformation interfaces from a technical perspective. For the communication layer, only when the communication protocol achieves good synchronization can the information be transmitted effectively. The physical elements of communication are involved at the constituent layer. Communication standards play a major role in the selection of these three layers, so to expand the number of partners, the choice of these three layers should be more open. Under the premise of the existing three-tier structure, it should be protected by corresponding security measures, while the integration of seamless and reliable SCADA system should be allowed.

The security of shared resources (platform control and platform data) is an issue that needs to be considered when integrating SCADA systems of partner microgrid platforms, which can be accessed remotely. The SCADA concept of the cloud allows us to be more flexible at a lower cost, but it has both advantages and disadvantages, requiring more security considerations during use.

The purpose of this paper is to solve the problem of SCADA architecture integration in the interoperability environment between microgrid platforms at the technical level. In order to solve this problem, an in-depth discussion of SCADA architecture based on hybrid cloud SCAD and platform as a service (PaaS) delivery model is proposed and targeted. The proposed architecture is expected to successfully address security and reliability risks while retaining the advantages of the cloud. This will provide an efficient communication basis for the interoperability of the microgrid platform, while also enhancing collaboration between research institutions.

2. Hybrid Cloud Computing-Based on SCADA Architecture

2.1. Cloud-based SCADA concept
The cloud is a concept that can store and process information based on servers on remote networks. This information can be accessed by a network connection. Software as a service (SaaS), platform as a service
(PaaS) and infrastructure as a service (IaaS) are three service delivery models widely used in cloud computing [4].

IaaS, PaaS, and SaaS are categorized by the level of control that users have access to. IaaS allows users to control the deployment of infrastructure and applications on the cloud. The PaaS delivery model allows users to deploy applications, to have incomplete control over the underlying infrastructure, and to have no free access to restricted data. The SaaS delivery model has a higher level of security, allowing users to use applications that run on the infrastructure, albeit on the client side, but with full control of the infrastructure by the carrier [5], such as a web browser.

SCADA systems based on cloud can be divided into three types, private, community or public, which are mainly measured according to public data exposure. When the system is a private cloud-based SCADA, the system should be fully deployed in the field and run on the Intranet. At this point, the visitor only has access at the local level, but he can grant certain collaborators permission to create communities. When SCADA applications are remotely connected to the control network and run entirely in the cloud, it is a common, common architecture that requires access to authentication. The choice of three different delivery modes SaaS, PaaS, or IaaS is based on the needs and security constraints of the operator.

After fully considering the reliability and safety of the power grid (response time, availability, etc.), the local PLC/RTU performs the key control and protection tasks, and the exchange information is given through selection and adjustment. The local network is directly connected to the application in this scenario, and data analysis can be done in the cloud. This is a cloud-based hybrid SCADA architecture.

Although cloud-based SCADA has many advantages and is more convenient, it also has some disadvantages, especially potential risks in critical data. The most important consideration is network security and reliability risks.

Data exchange between research institutions is likely to be sensitive, so the implementation of cloud SCADA needs to take such risks into particular account. In a future article, we will address the benefits of being cloud-based by tweaking the architecture, while limiting security and reliability limitations.

2.2. An architecture based on microgrid platform interoperability

In order to realize the interoperability between various application platforms of microgrid, an SCADA architecture is proposed to realize the secure interaction and information communication between various application platforms and flexibly access new application users.

The application of SCADA system in cloud computing mainly considers its security and reliability. In a cloud computing system, local SCADA servers, PLCS, or RTU are responsible for performing important SCADA tasks. Due to the use of LAN for communication and local information exchange, important tasks have low bit error rate and high security during interactive execution. Applications such as AMI, DMS, VAR optimization, and interrupt management can be delivered through the PaaS model for placement in the cloud.

Interoperability of microgrid platforms is made possible through a common cloud SCADA server, where data generated by Shared applications is uploaded from the local server to the public cloud platform. This common server can be either a physical SCADA architecture or a virtual PaaS/SaaS server that communicates with a local SCADA server on the platform over a wide area network, with the option of simple, low-cost Ethernet with TCP/IP and Webservice protocols. However, if the speed and delay of transmission are required, other methods should be considered.
Figure 2. Interoperability SCADA architecture of microgrid platform based on hybrid cloud.

In the PaaS delivery pattern architecture, SCADA applications are directly connected to the platform control network. Important functions are performed on the local SCADA server, and the transfer to the public cloud SCADA server is just some unimportant information. The public cloud SCADA server is authorized to allow users limited access to some visual, report light content, or launch some applications. The public cloud SCADA server is set up at sites agreed upon by the partners for the convenience of each user and is strictly controlled by the common committee and technical staff responsible for interoperability within the network. When applying the PaaS delivery model, users shall obtain the permission of the platform owner if they remotely apply to use a function of the platform and visualize it.

SCADA systems require high bandwidth and latency for network connections, and failure to restore platform monitoring within minutes or even seconds can cause serious damage to the platform. Therefore, when accessing important tasks from the cloud, they must go through a rigorous risk assessment. Network accessibility has an impact on performance fluctuations, latency, and latency changes of platform and data.

The cloud server, built with the hybrid cloud architecture and PaaS delivery model, is a private server owned by all users in the grid, with strict permissions on the access mechanism. Applications are not normally open to the public and can only be accessed after successful authentication. The system will automatically detect the organization and check the access rights to distinguish whether the visiting user is related to the organization.

3. Safety Risk Assessment

Because the architecture sets up two authentications, the interoperability between the microgrid platform and the research facility is always secure. When accessing a PaaS or SaaS application, only the user can be granted access to the selected public cloud SCADA server through authentication. When a user wants to access a particular platform, a second authentication is required to verify that the appropriate partner institution is authorized to access the local SCADA service.
Recently, secureDNP3 and IEC61850 implemented message authenticity verification. SCADA architecture may be vulnerable to attacks because it shares security risks with classic SCADA systems, but some risks can be handled smoothly. They will send a instruction, a lot of demand to the server is equal to the server has been in full load condition, which can lead to system can not run normally. Shared resources may become not under DoS attacks in the server resources sharing, information may be cut off communication, when using the public network, even if public server is a safe state, there is no guarantee that the middle of the communication link and intermediate server security.

4. Conclusion
With the development and investment of smart grid as the background, the interoperability of microgrid platform plays a very important role in promoting the cooperation and exchange of information between research institutions and industrial institutions, especially in research institutions. Multi-site projects are strongly supported by the interoperability of this platform.

In order to support the interoperability of research institutes and industrial institutes microgrid platform, a hybrid SCADA architecture based on cloud is proposed. This architecture demonstrates the benefits of a hybrid cloud SCADA and PaaS delivery model that can be used as a common research infrastructure for working network partners. In order to ensure data security and interoperability between the implementation platform, effective security measures should be implemented to control. In this architecture, the data exchanged by CIM on OPC-UA protocol is introduced into the semantics and used as the common information model of the partners to ensure the effective communication between the cooperation platforms.

References
[1] G. A. Council, "The modern Grid initiative," Pacific Northwest National Laboratory, Sep. 2008.
[2] S. G. T. F. E. G. European Commission, "Final Report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids," European Standardizations Organizations, May 2011.
[3] e.-e.-E. Smart Grid Coordination Group, "Smart Grid Reference Architecture v3.0," Nov. 2012.
[4] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic, "Smart power Grid and cloud computing," Renewable and sustainable Energy Reviews, pp. 566-577, 2013.
[5] M. Peter and G. Timothy, "The NTST Definition of Cloud Computing," National Institute of Standards and Technology, Recommendations of the National Institute of Standards and Technology Special Publication 800-145, Sep. 2011.