Research of Smart Grid Cyber Architecture and Standards Deployment with High Adaptability for Security Monitoring

Hu, Rui; Hu, Weihao; Chen, Zhe

Published in:
International Conference on Sustainable Mobility Applications, Renewables and Technology (SMART), 2015

DOI (link to publication from Publisher):
10.1109/SMART.2015.7399218

Publication date:
2015

Document Version
Accepted author manuscript, peer reviewed version

Research of Smart Grid Cyber Architecture and Standards Deployment with High Adaptability for Security Monitoring

Rui Hu, Weihao Hu, Zhe Chen
Department of Energy Technology, Aalborg University
rhu@et.aau.dk, whu@et.aau.dk, zch@et.aau.dk

***Abstract*—Security Monitoring is a critical function for smart grid. As a consequence of strongly relying on communication, cyber security must be guaranteed by the specific system. Otherwise, the Demand Response (DR) signals and bidding information can be easily forged or intercepted. Customers' privacy and safety may suffer huge losses. Although OpenADR specifications provide continuous, secure and reliable two-way communications in application level defined in ISO model, which is also an open architecture model for adopted security systems, no specific or proprietary technologies is restricted to OpenADR itself. It is significant to develop a security monitoring system. This paper discussed the cyber architecture of smart grid with high adaptability for security monitoring. An adaptable structure with Demilitarized Zone (DMZ) is studied. Focusing on this network structure, the rational utilization of standards is investigated to provide a smart grid communication network with better performance and higher security, whilst it avoids the extra investment of an individual security monitoring network as far as possible.**

Keywords—Smart Gird Cyber; Security Monitoring; DMZ

I. INTRODUCTION

A smart grid is a modernized electrical grid that uses analog or digital information and communication technologies to gather and act on information about the behaviors of suppliers and consumers. The analysis of bilateral information can be used to keep power consumption balance, improve the efficiency, reliability, economics, and sustainability of the production and distribution of the electricity. Using modern communication methods, more and more people can participate in power generation activities. However, it will bring security issues with strongly relying on communication technologies [1]. The interception and forgery of data packages flowing in the communication links is becoming more and more convenient to realize [2]. The network attack in smart grid not only influence users' privacy, but also threaten the grid safety, event people's life. Currently, many standards which have been proposed share a great concern on cyber network security. It is significant to develop a security monitoring system.

Security monitoring system for Smart Grid can be realized in two aspects. The first one is keeping the security of communication network, which is mainly based on the design of communication protocols. The second one is preserving the security of the whole grid, which is mainly based on analysis and management of smart grid information.

There exist requirements for smart grid cyber security as following [3]:

(1) The protocols should be able to preserve privacy of its users. Besides, participants must be able to verify the authenticity and integrity of all DR events and bid notifications.

(2) Untrusted entities must not be able to link DR bids to individual consumers and infer private information about individual consumers from the DR system.

These two main requirements are guaranteed by the security monitoring system and the relatively mature communication network design. Many references have already investigated the privacy preserving protocols. A number of security guidelines and specifications for smart grid has been developed as well, like ENISA guidelines, ISO/IEC TR 27019, NIST-IR-7628 [4][5].

In this paper, investigation of standards and protocols used in security monitoring system for smart grid has been conducted. The security monitoring architecture proposed in this paper has been modelled and analyzed in order to discuss the deployment of standards and protocols from view of security. Meanwhile, this work is a part of an EU Horizon 2020 project SmarterEMC2 [6], which aims at empowering Smart Grid Market Actors through information and communication technologies. It provides references and infrastructure of communication system for smart grid applications and guarantees the security of demand response activities.

II. THE ARCHITECTURE OF SECURITY MONITORING SYSTEM

A. Main Security Monitoring Actors

According to the requirements and threatens mentioned in Section I, the main actors related to security monitoring are imported from the definitions of project SmarterEMC2. These actors and their descriptions are listed in tabled I and their communications and exchanged data will be discussed later.

These main actors play an important role in Demand Response and cyber security monitoring. The main idea of this paper is to use concept of demilitarized zone to isolate the resources and core functions inside the smart grid cyber to protect them from attacks and provide a flexible and friendly interface for the security monitoring. Besides, by the employment of DMZ, the adaptability of the cyber could be

improved. People are developing the standards and protocols of the smart grid ceaselessly, the changes of the application level standards are faster than the lower level standards and protocols, so the monitoring system may face varying situations. By using the proposed cyber structure, the loads of security monitoring behind the DMZ is alleviated and the pressure moves to the interfaces of the DMZ with inside cyber and DMZ with outside internet. Compared to the other solutions such as distributed one which key servers are distributed inside the cyber, the proposed structure is more convenient for construction and monitoring. As DMZ is a more centralized method, it makes the security monitoring system of smart grid more adaptive to the changes of other protocols and easier to maintain.

TABLE I. MAIN ACTORS OF SECURITY MONITORING

Actor Name	Actor Type	Description
Distributed Energy Resource	Device	An energy generation device with relatively small capacity. It can be aggregated to provide power necessary to meet regular demand of the Smart Grid.
Smart Meter	Device	A device which can measure the consumption of power in predefined cycles. It sends the measured information and user habits to the Smart Meter aggregator or up level SCADA
Smart Load	Device	A Local device which is composed of EVs or energy storage systems and able to control load's power consumption. It is able to consume or generate power during a certain period according to the received signals or commands.
Distribution Management System	Computer	A system which provides many applications to monitor and control the distribution grid in centralized approaches.
Grid	System	Grid infrastructure, including substations, wires, buses and so on.
EMS	Computer	Energy Management System. EMS is a cluster of computers which provide energy management and operation plan for the smart grid.
DMZ Gateway	Device	DMZ Gateway provides access control of the Smart Grid Security Monitoring network. It rejects the untrusted and unauthorized visits from the DMZ.
Security Monitoring Network	ICT Network	Smart Grid Security Monitoring Network is a mixed communication network based on modern communication technologies like Ethernet, GPRS, Fibre-optical and so on. For local protection, in order to provide fast response and analysis, real-time Ethernet protocols may be used, i.e. Powerlink Ethernet or Ethercat. For long distance communication, WAN and Internet technologies and prototypes like TCP/IP, TLS, HTTPS and FTP are used. It is coupled with ICT networks in Smart Grid. Video surveillance is also integrated in this network.
Demilitarized Zone	ICT Network	DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to larger and untrusted network, usually the internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network; an external network node only has direct access to servers and services in the DMZ, rather than any other part of the network.

From the table we can see that the core actors of DMZ are the DMZ gateways and the servers inside the DMZ. Because of the relatively centralized feature, to improve the reliability of this structure, more than one DMZ should be configured to form the backup.

B. Cyber Structure

The cyber structure of security monitoring is shown in Fig. 1. It employs DMZ as a guard for the intranet. All the access to the internet and the visit of the resources in the intranet will be monitored by the gateways and servers inside the DMZ. Different resources will be granted with different level of authority according to the specifications and guidelines like ENISA, OpenADR. Any intended access to the resources will be recorded and verified by the monitoring software deployed on DMZ gateways. Thus, the advantages of the DMZ are fully used and the security level of the cyber is improved further.

Inside the intranet, servers which provide key services such as SCADA, EMS are distributed. The correspond DSO are responsible for the maintenances of these hosts and any access to these facilities can be easily recorded and monitored through the methods in mentioned guidelines or by video cameras. The monitoring software deployed within the intranet focuses on data flow analysis. Abnormal data flows can be used to diagnose the communication problems, invalid port access, and potential network violations. This function is significant to keep the Smart Grid communication network operating in a secure, load-balanced and high performance state. The whole cyber was modelled and analyzed using the tool SGAM-toolbox which is an extension for Smart Grid architecture modelling.

The Security Monitor Network (SMN) can be independent or coupled with the cyber according to the communication loads of the paths. In the links with less requirement of delays and bandwidth, the SMN can use the cyber directly to transfer data. However, to monitor the links with higher requirement of the bandwidth and delays, the monitor node of it should use independent communication path to analyze the monitored data and transfer it.

With this configuration, the access paths to the core resources are limited. In some degree, the SCADA system and EMS system can focus on their kernel functions without caring the security monitoring of the network. The communications which require high performance of the network are kept away from the influences of security monitoring system. Although the security monitoring pressure increased in the DMZ, we can use several DMZs to share the pressure and provide higher reliability. Meanwhile, the visits from the outside internet are not influenced, the resources are exposed transparently to the users who are authorized and verified.

III. Standards Exploration and Deployment of Security Monitoring System

With proposed cyber structure, related standards should be deployed on different dimensions. The standards can be classified into two categories, namely information standards and communication standards, according to the problems they intend to address. In this paper, rational utilization of standards and protocols in proposed cyber structure are discussed.

The Smart Grid's DR communications are assumed to be modelled and operated in OpenADR framework. OpenADR is a research and standards development effort for energy management led by North American research labs and companies. It employs the leveraging of the market to balance power generation and consumption. Usually, the implementation of OpenADR specification uses XML as a tool to define DR signals and data models. Because no specific or proprietary technologies is restricted to OpenADR itself, practical and well-designed security monitoring system becomes a critical part of Smart Grid. For example, one of the security monitoring system's functions is to protect DR data and signals from forgery and interception, making sure that the grid operates in a safe and reliable environment, this can be guaranteed by only monitoring the XML data flows without the consideration of DR level. Whilst, users' privacy should be preserved, attacks should be detected by monitoring the data flow and cyber loads, these targets can be achieved by using current security mechanisms such as described in IEC 62443. Besides, the security mechanisms employed by OpenADR 2.0 [7] are common ones without any modification. The whole use case is based on the Public Key Infrastructure certificates (PKI) whose cryptography algorithms are normally RSA and ECC with the certificate type of X.509v3.

Due to the security monitoring standards and mechanisms mentioned by OpenADR are mostly deployed in DMZ physically, the influences of the changes in OpenADR are reduced, and it will rarely block the operation of SCADA, DR, and EMS systems. While in the distributed solutions, normally the SCADA and DR are highly coupled with the security monitoring system. Thus, the changes in the mechanisms may cause the core functions of the smart grid to pause. Besides, the mechanisms should be inclined to the legality, integrity and validity of the information providers and receivers, while the correctness of the data inside the information should be guaranteed by the other applications.

Currently, the development of security approaches sometimes lags behind the development of communication technologies. Many leaks are found after the deployment of the communication system. However, it is an inevitable fact that, to improve the cyber performance, more and more novel techniques have to be utilized or verified to satisfy increasing users and enhance their experiences, such as Power Line Communication (PLC), IEEE 802.11ac, 5G, etc., although the PLC standards have been used for decades in the utility industry for remote metering and load control applications [8]. So the security monitoring must rely on the relatively matured standards and technologies like TSL, HTTPS first, whilst be adaptive for the application of novel methods. Both Information standards and communication standards in SmarterEMC2 can be divided into two categories from the view of security, namely the security technology and security mechanisms. For the communication standards, security technologies should be guaranteed by themselves, i.e. no matter PLC or Wi-Fi, they should consider their own techniques against eavesdrop, cracking, etc. when any extension is made. For information standards, the design of security mechanism is the main concern. It should be complete and leak less. However, OpenADR, one of the most applied standards in all use cases, didn't specify the concrete standards to use for addressing security issues. Mixing of different security standards due to no universal recommendation may cause safety problem.

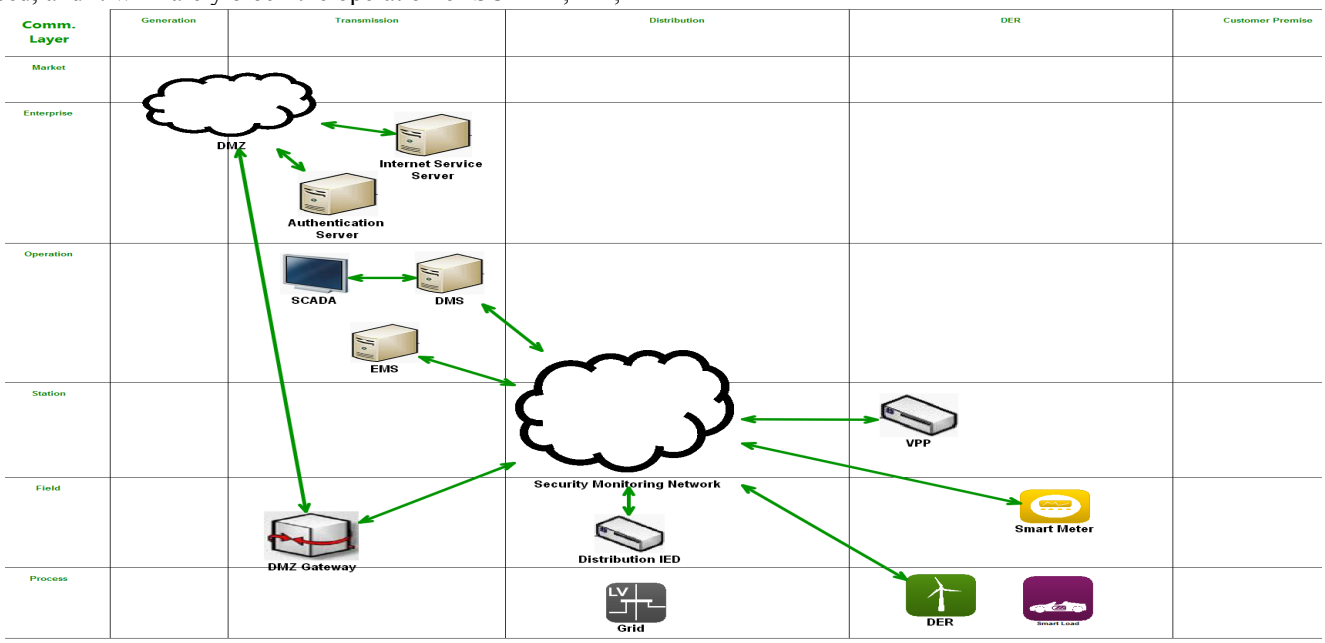

Fig. 1 The cyber structure of security monitoring system for smart grid

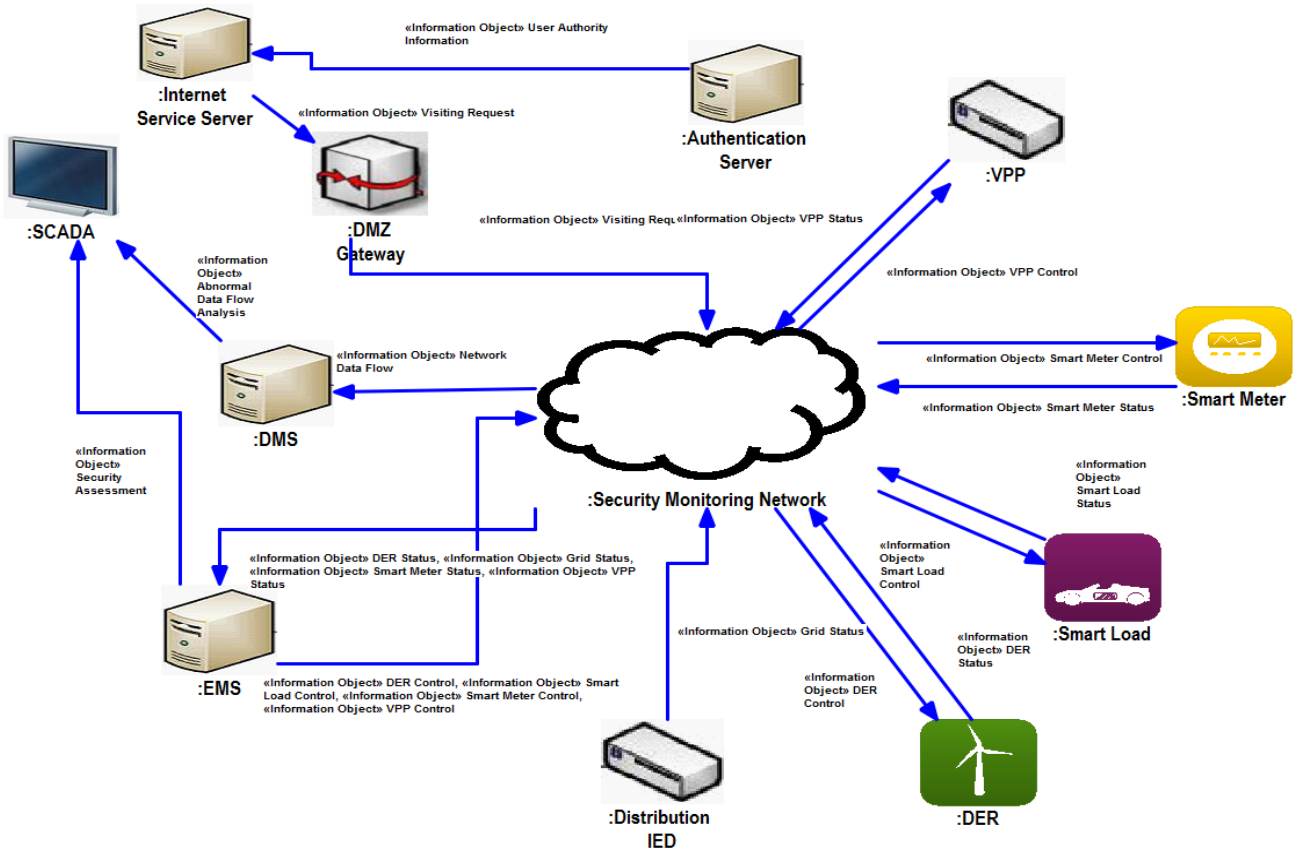

Fig. 2 Information flow of Demand Response Activities with security monitoring system

A. Deployment of Information Standards

The term "Information Standards" mainly refers to the standards which format the exchanged data and give models of communicated entities. In construction of Smart Grid network, information standards such as IEC61850, IEC 61968, IEC 61970, etc. are consulted commonly. Most of these standards are oriented to high level applications and implemented by the combination of several communication technologies like COM, XML, and SOAP. The security monitoring system is responsible for preventing these XML signals or TSL packages from intercept and forging. After designing the deployment, the information objects generated by all the related actors can be derived according to the guidelines. For instance, in this use case, the information objects to be monitored are illustrated in Fig. 2.

B. Deployment of Communication Standards

The term "Communication standards" mainly refers to the standards and protocols which define the detailed techniques and methods of communication. These kinds of standards and protocols used in Smart Grid can be diverse due to the different technique requirements of communication. Besides, these communications usually related to the operation of VPP and DER, or information from SCADA and data sampler. Thus it's better to locate these networks behind the DMZ. The sample of security information which used in security assessment relies on these standards as well.

C. Acess Sequence of the Proposed Cyber

After the standard deployment, we pick up several primary use cases to depict the functions of this structure when the user wants to have access with the resources inside the network.

TABLE II. TIME SEQUENCE OF THE INTERNET ACCESS CONTROL

Step #	Triggering Event	Description of the Activity	Information Producer	Information Receiver
1	Request resources in the security monitoring network	Request resources such as printer, server, or some services in the security monitoring network	Internet service server	DMZ Gateway
2	Verify identity	Verify identity, certificates, credential and authority	Authentication Server	DMZ Gateway
3	Log the visit	Log the visit into database	DMZ Gateway	DMZ Gateway

The Internet access is the most common requirement for the islanded cyber. Because of the employment of DMZ, the number of the access points is limited, so it is easier to monitor the internet activities than the networks whose internet access

points are distributed. Thus, in this kind of network, the sequence of the internet activity is shown in the figure 3 and table II. If the cyber is constructed without DMZ, the internet access servers or gateways may distributed in the network and become harder to cooperate with other services.

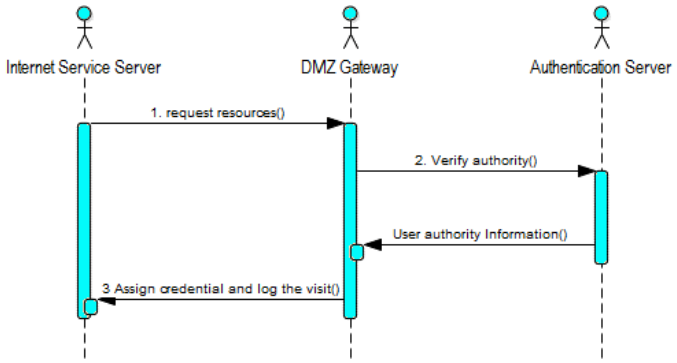

Fig. 3 Time sequence diagram of Internet access control

Besides the internet access control, the authentication control is another important part of security monitoring, all the visitors outside and inside the cyber will be authenticated by the authentication server. The progress of the authentication are listed in the table III and figure 4.

TABLE III. TIME SEQUENCE OF THE USER AUTHENTICATION CONTROL

Step #	Triggering Event	Description of the Activity	Information Receiver	Information Exchanged
1	Request Authority	Request authority from the authentication server	Authentication Server	Identity Information
2	Verify identity	Verify authority request and user identity	DMS	Authority information

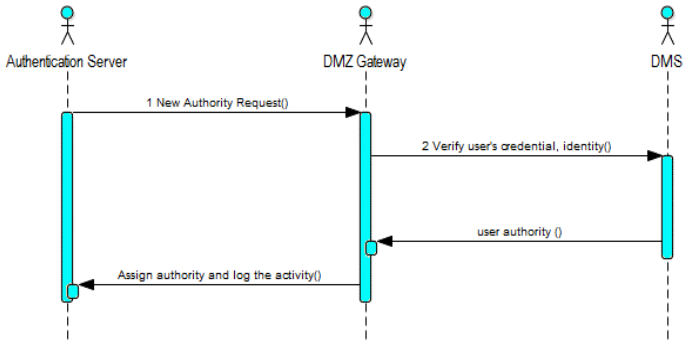

Fig. 4 Time sequence diagram of Authentication control

The last case is the security monitoring and communicatoin flow. In this case, the data of communication flows is collected by the SMN, then it will be analysied by the DMS to determine whether there are abnormal data flows and whether the cyber is suffer from port scaning or other attacks. Then the SCADA will generate the reports to the administrators. The procedures are shown in table IV and fig. 5.

TABLE IV. TIME SEQUENCE OF THE SECURITY MONITORING AND COMMUNICATION FLOW CONTROL

Step #	Triggering Event	Description of the Activity	Information Receiver	Information Exchanged
1	Receive sample data	Receive data sampled from Distribution IED, Smart Meter, VPP and Smart Load	DMS	Data load information
2	Analyze data loads	Monitor abnormal port scanning packets	DMS	Network detecting actions or DDOS attack
3	Analyze abnormal data loads	Analyze distribution of data loads	DMS	Abnormal data loads
4	Obtain attack information	Request logs from DMZ gateway to get more details	DMZ Gateway	Gateway logs
5	Generate report	Generate cyber abnormal situation report	SCADA	Abnormal situation report

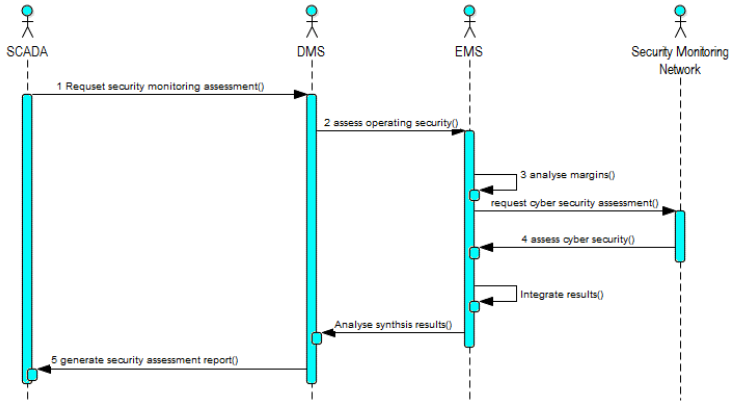

Fig. 5 Time sequence diagram of Security monitoring and communication flow control

IV. CONCLUSION

With proposed cyber structure, the Smart Grid communications are adaptable for security monitoring. The analysis in this paper shows that it also has the adaptability for the changes in both security related standards and the communication standards. Besides, due to the guard of the DMZ, construction of special network for security monitoring is minimized because the monitoring system can share the same network when particular requirements are satisfied. The employment of DMZ not only improves the security of the whole network, but also isolates the communicating load, which mitigates the influences caused by users' visits outside the DMZ. From the view of legal users, the resources inside the smart grid still remain apparent. Because most of the security monitoring mechanisms are realized inside the DMZ and the monitoring loads are undertaken by the DMZ gateways and the related servers inside the DMZ, the kernel servers behind the

DMZ can focus on their own business and consequently, the performance of them will be enhanced.

REFERENCES

[1] Heberlein L T, Dias G V, Levitt K N, et al. A network security monitor[C]//Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on. IEEE, 1990: 296-304.

[2] Paverd A, Martin A, Brown I. Security and Privacy in Smart Grid Demand Response Systems[M]//Smart Grid Security. Springer International Publishing, 2014: 1-15.

[3] Beckers K, Heisel M, Krautsevich L, et al. Determining the Probability of Smart Grid Attacks by Combining Attack Tree and Attack Graph Analysis[M]//Smart Grid Security. Springer International Publishing, 2014: 30-47.

[4] Beckers K, Heisel M, Krautsevich L, et al. Determining the Probability of Smart Grid Attacks by Combining Attack Tree and Attack Graph Analysis[M]//Smart Grid Security. Springer International Publishing, 2014: 30-47.

[5] Ejebe G C, Jing C, Waight J G, et al. Security monitor for on-line dynamic security assessment[C]//Power System Control and Management, Fourth International Conference on (Conf. Publ. No. 421). IET, 1996: 58-64.

[6] SmarterEMC2 Project, http://www.smarteremc2.eu/

[7] OpenADR 2.0 Specifications, http://www.openadr.org/specification

[8] S. Galli, A. Scaglione, and Zhifang Wang, “Power Line Communications and the Smart Grid”, 2010 First IEEE International Conference on Smart Grid Communications, October 2010, Gaithersburg, USA