J. Basic. Appl. Sci. Res., 3(1s)558-563, 2013

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Evaluation of Existing Protocols to Improve Information Exchange Security in the Smart Grid

Sara Baghar-Nasrabadi[1], Hossein Shahinzadeh[2*]

[1] Communications Group, Department of Electrical Engineering, Najaf Abad Branch, Islamic Azad University, Najaf Abad, Iran.
[2] Department of Electrical Engineering, Islamic Azad University, Isfahan, Iran.

Received: June 5 2013
Accepted: July 2 2013

ABSTRACT

One of the main goals in smart electrical grids is optimize and enhance its capabilities through handling it. Of course, through sharing of information between the various components and network subsystems, the total system standardization is necessary. Because required to achieve to smart electrical grids, is potential of interaction and understanding of information among all the equipment and machinery, systems, available software and hardware throughout the grid. In this paper, standards used in electricity distribution networks have been studied by a suitable architecture in view of the information security and information technology.
KEYWORDS: Distribution automation, Smart grid, Standards, Protocols, Communication systems.

1. INTRODUCTION

Nowadays efficient methods in distributed systems that are unilateral, goes into smart control and by increase the visibility and monitoring system, it will be to process of handling network, because of sharing information between various components and subsystems, standardization network is gaining significant importance. Because requisite to achieving to the smart grid is ability to the mutual understand and interaction of information of all equipment and machinery. In this regard, protocol for data exchange, are defined a set of definitions, rules and terms, that seems possible to send and receive operations defined types of data by efficient manner and with diagnosis and control of common errors in communication systems. This set of rules includes hundreds defined and laws, they are associated the integral manner with each other. Yet, there are several parameters for adaptation and implementation of a protocol with a particular application that should be determined considering the conditions set out in the application and by performing the necessary calculations. And this Article is apart from cases they are noted in the issue of compatibility. Implementation considerations involve the cases they are affected optimal performance of the remote control system without harm to the adaptation protocol.

If each component of the system is not functioning properly, it damages to excellent performance of the whole system. As regards, implementation of the protocol on the both side of line can be made by different manufacturers and differently of each other, it may be lead to problems in information exchange that is said the protocol mismatch.

An important point about problems caused by incompatible protocol is that in many cases, due to involvement of compatibility issues with the system software implementation, eliminate of them needs to change the system software, even if there is a possibility to perform it, it is done with much cost and time. Therefore, it must be prevented the incidence of these problems by adopting appropriate before proceeding with the purchase of equipment. Incompatibility makes a part of the information exchange system will not work, while the lack of attention to implementation considerations makes failure to achieve desired performance. As an example of these considerations can be noted to choose the method of collecting and sending analog values. In different systems, analog values are collecting and sending by different methods they are usually one or a combination of the two methods “send periodic” or “posted by changing the amount”. This choice does not harm the adaptation protocol, but it can cause undesirable quality in Reading amounts in the control center given the amount of change in the field, limited bandwidth in communication channels (exchange rate) and link parties horsepower and other cases. So the decision in this case is one of the things that goes into implementation considerations that must be done with the calculation and based on information from the process and demands by the remote system [1,2].

2. Smart grid Architecture

Smart grid is a title which usually refers to describe elements they are connected to the power grid and include advanced telecommunications infrastructure that provide many advantages and benefits for the electricity network. Foundation for the smart grid is safety and reliable telecommunications infrastructures that Its management is based on open standards and communicate between smart grid elements. The goal of creating the smart grid is transmission of electrical energy from production to consumer using digital technology to increase energy efficiency, reduce costs, increase reliability and transparency of the production, transmission and consumption. With increasing awareness of energy and environmental, the demand for reliable and stable power grid and also need to high reliability and high quality resources make the smart grid becomes the common goal to develop the power grid across the world. Smart grid should be implemented as soon as possible to give desirable effect on the current trend of delivering power, reliability and efficiency of renewable energy. But the success in this project depends to a large number of factors as consumer’s cooperation and

Corresponding author: Hossein Shahinzadeh, Department of Electrical Engineering, Islamic Azad University, Isfahan, Iran.
Email address: ee_ieee@yahoo.com

potential of equipment for utilization of information technology development in order to adopt general standards in network and increasing the efficiency of energy transfer system [3].

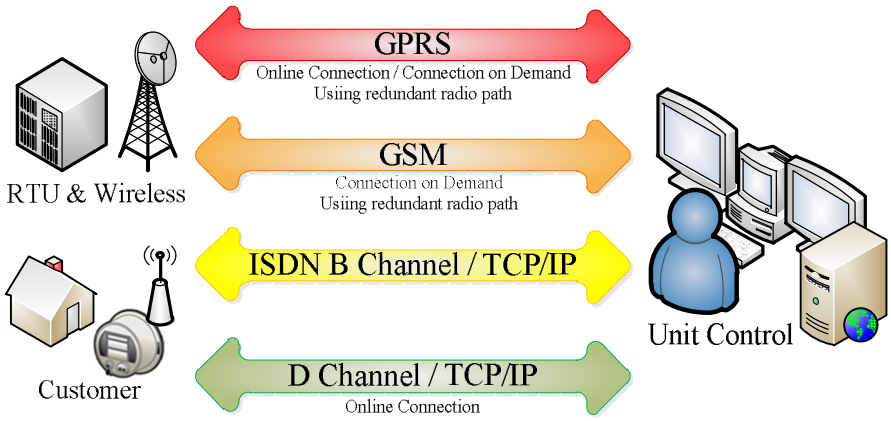

Fig. 1. Transmitting information in smart distributed network architecture

3. Investigate of existing standards in the domain of smart electricity networks

Reputable international organizations they are active in developing standards, has been established the special committee in order to improve the performance of smart grid with the aim of creating and developing standard protocols and common models. Their aim is achieving to interaction and enhances of mutual performance capabilities of smart grid equipment and other systems [4]. Existing standards in the field of smart grid are summarized as follows:

- Production standards
- Communication standards
- Communication standards of internal network
- Information Security Standards

However, these standards proceed performance of subdivisions under its control towards targets alone, but parallel or even conflicting standards is barrier of general communication systems in some cases that implies to the same argument of protocols and standards consistency. Some of these cases can be pointed to smart measurement system that focus on meters information with AMR units in the field of available protocols and standards in the data exchange IEC standard and don't include all requirements of coverage network.

4. Challenge of information transfer by wireless network

An intermediate system between distributed network and smart measuring systems must be can include building automation systems, industrial automation and distributed energy resources. Electrical Distributors are seeking economical ways for meter reading of subscribers that is achieved with the installation of a device that can be used to view and control. Meter readings device can be so programmed that if read number exceed from anticipated amount, report it. In AMR (Automatic Meter Reading) system, meter reading and tariff classification of customers is done remotely and automatically that use spread spectrum communication system with narrow bandwidth UNB (Ultra Narrow Bandwidth) and use PLC in some cases. Data is sent to the recipient in the distribution by RTU [5].

Second generation mobile (GSM) provides the standards that in it, the connection is based on the circuit (Circuit Switch). In this system communication to the meter established through the public telecommunications network and there is no need to data collection or specific senders and receivers and data communication can be done easily through any meter. Third generation mobile is UMTS that provide possibility of broadband communication (bandwidth of a few hundred kilobits per second). Advanced meters can be equipped with GSM or UMTS modems until communicate between communication networks and data collection center. Since there is no guarantee to availability of the network at the meter place, we can use this network alongside other communication media. In UMTS network, different services can be supported, that these services include voice services, Data services such as video telephony and video conference with up to 8 participants, ability to download and multimedia content of electronic mail and internet services and mobile commerce. All of these services, depending on the application and importance are required to different levels of security. UMTS includes the following sections:

- Security access
- Network domain security
- Security of user domain
- Application security
- Ability to security view and configure

For security in the voice and data services, must be provided security of access, core network domain security and user domain security. In internet services and mobile commerce, in addition, there is a need for application security to create a security through end-to-end. Security features in UMTS built based on security features of second generation (GSM), with this difference that security features have been added to it and some of available features in it, improved. GSM encryption algorithms not published generally and this is a major weakness of GSM. About UMTS, these

algorithms along with other standard parts should be designed and published. In GSM and UMTS, all users are required to use a specific encryption algorithm. About the origin authentication algorithms, this is not true, and operators can use their own algorithms. In GSM, there is no presented algorithm in the standard sample and this has led many operators use COMP-128 algorithm that was relatively weak algorithm.

Strong the algorithm so depends on the length of the key. In GSM, The actual length of encryption key was 54 bits that in current situation this key length is short according to computational power of modern supercomputers. In GSM was tried that designed algorithm for cryptographic include a 128-bit key length and thus can provide appropriate security level. In GSM, verification of authenticity was unilateral and in that network was not verification of authenticity to user. Thus it was possible to BTS cyber-attack. To eliminate this weakness in UMTS, bilateral validity was established. In GSM, confidentiality of user traffic and signaling sensitive data was applied only in the air between user and BTS. Since in many cases path between BTS and their controllers is through microwave links, at UMTS cryptography is extending a step towards back and hence the path between Node-B and RNC be protected [6].

5. Data access security

The goal of access network security is security in radio interface and access network. This is an important part of security, because due to the air interface and the lack of physical protection, many attacks such as eavesdropping and messages manipulation applies in this section. Security features in this section are four general categories:

- Confidentiality of user identity
- Mutual authentication
- Confidentiality
- Data integrity

5.1. Security problems resulting from UMTS & GSM

One of the available security problems in third generation is due to inner workings between GSM and UMTS. Due to lack of adequate regional coverage of the third generation in some areas, its users can be moving to second generation networks. Although, this subject improves performance in service of this generation, but, in fact, this is moving between networks with different security protocols. Attacks that can occur in this case, is attacking by the middle factor. This attack occurs when a UMTS user works with second generation BTS. The core network in this case is the third generation network. Authenticity verification protocols that is performed in this case, is similar to AKA protocols in the third generation, with this difference that BTS does not support integrity and hence message No. 9 in UMTS authenticity verification protocol trading without integrity and so the enemy with changing this message, can be established without encryption state or weak encryption algorithm between user and BTS and thereby hear the conversations [7].

5.2. Communication Network security

It is hard effort to analysis and management of information security. These efforts can be divided into a range of separate and independent from, and discuss about dependence as a specific topic and proceed than anticipated risks with a list of assets and their importance to the organization. After determining all the risk for any property, identified security weaknesses and threats causes. And then overcome weaknesses by having the information. So we should be documented risks, threats and vulnerabilities to able to make the right decision to deal with them by using the documentation relating to the security weaknesses to manage risks. Different security officials may choose each type of analysis, security program and security operations for their security domains or subdomains. Of course, many of these areas decrease through negotiation, but however, some of them remain that they need to information interact and exchange.

The term “network domain security” is defining to provide security for the exchange of information between network elements and not related to the mobile terminal. These elements can be both at a network or belong to two different networks. If these elements be in the two different networks, security mechanisms should be standardized. In the past, security mechanisms for communication between two network elements were not really necessary, because it was available for specific institutions and it was difficult to entry into the SS7 network for a striker. But now this is not true for two reasons: First, number of operators and service providers are increasing, and the other, many networks tend to replace No.7 signaling protocol or SS7 with IP network protocol. Although using IP protocol has great interest, but many hacking tools that exist on the Internet are applied to this network. For this reason, messages protection between signaling networks should be considered a major security target. For this purpose, in the third generation network, security mechanisms related to core network have been developed they are included MAPsec & IPsec. In Table.1, the security of data sent over the network is shown [8].

Table 1. Security of telecommunication networks

	IPsec	SSL/TLS	SSH
Type of Security	Network	Transfer	User
Account Type	Data path	Management	Control / Management
UDP security	Yes	No	No
Document user protection	Yes	Yes	Yes
Firewall	Limited	Yes	Yes
Create Network	So-so	Easy	Easy

By comparison between the listed standards they are used for distribution automation, Table.2 is achieved. If some of the above mentioned standards and guidelines are compared, we will see that applied definitions for security is different. All referred sources acknowledge that risk assessment and risk management are very important, however, none except few of them say nothing about methodology.

Table 2. Standards and communication protocols

	Tetra	IP	UMTS	GSM
Security Definition	Own	Own	Own	Own
confidentiality	Yes	Yes	Yes	Yes
Integrity	Partly	Partly	Yes	Yes
Availability	Partly	Partly	Yes	Yes
scope				
Type of organization	Communications	Data network	Communications	Communications
Type of system to protect	Communications	Communications	Communications	Communications
Risk assessment	Important	Important	Important	Important
Methodology guidance				
Security policies	Strong	Medium	Strong	Medium
Guideline	Yes	Yes	Yes	Yes
Examples	Yes	Yes	Yes	Yes
Security management				

It is very difficult to find written smart security standards and guidelines for the power industry. Table.2 shows that this document provides guidance for a security management system or risk assessment. In conclusion it must be said, since, there are no comprehensive guidelines or standards that has referenced to smart system used in power distribution network. Therefore, a power company should be trust to standards and general guidelines for its comprehensive security based on a control system, distribution and transmission when the IT management framework is created [9].

6. Definition of functional areas in electricity networks

There is strong need for information exchange between companies in the power industry. Suppose we face the situation in which two or more security domains must be interconnected and each of they have been responsible for its own security and they are in different levels of security. In a model, security areas should be noted to domain or ultra-domain definition, so that include all domain coordinate like range of domain responsibility and the policy that it can be linked fields as before. Before anything, it should be created a security unit for each domain or ultra-domain.

The first question in each network and information security project is that the security of which part should be created or improved? Therefore, the first phase in the network security project generally and security standard project particularly, is accurate and complete understanding of all available information and information systems in the organization and future needs, and classify them. Identification and classification of assets and information and communication systems will do exactly and completely based on information security management standard ISO 27003.

The biggest challenge for organizations, companies and service providers of information technology services is spend the least possible cost and best quality. It appears in different parts of the organization that among which can be mentioned to items such as increasing labor productivity, optimal use of existing and the creation of new facilities and capacity based on the real needs of business. Having advanced technology and skilled manpower was not instrumental lonely and service management processes are discussed as an important issue which is the connecting loop of people and technology. To achieve these goals, in the last two decades, many activities have taken place in the world in IT management services and it is presented various methods and recommended. ITIL is not a recommend or method proposed by an organization or institution, but it is the collection of best practices in world's largest companies during various years at IT service management. This standard has been faced very much welcome in the world and reliable statistics showing interest in various companies and organizations providing IT services to adaptation and application of ITIL procedures in IT service management [10].

ITIL is as an industry standard for IT management and a proper framework for management. ITIL identify goals and performance keys in a process and defines them. Indeed, it will be provided a map to the director to know what stage the project is now. In addition, it is a collection of thoughts and techniques for managing IT infrastructure, implementation and use of them.

This means that security policies related to it, should be implemented on a large scale in all parts of an organization and not just between a security group at IT department. In practice this means that each employee involved and responsible in the part of the information security office including data protection, support system office, computers, etc. inside the electric company, should be subject to this policy.

Therefore, establishment of organization surrounding information security will normalize over time, until information security and deal with it, be as a natural part of the organization's activities and perform such other activities within Electric Power Company as the process of operation office, maintenance, planning, construction, etc.

To support this work, comprehensive knowledge is necessary from security experts to provide necessary helps for electric companies. For a small electric company, the number of these experts may be one or two people, and use as part of the duties of the IT department within the company. For larger power companies, it may be necessary a special security department. But, also in practice, information security should be applied at all levels of organization of an electric company.

Therefore, it is better that information security be a part of daily operation of business processes. So, to restart, it is recommended that existing framework for data handling, generally, should be used in line with information security management processes, and other related processes [11].

7. New solutions for data protection

It is require to a fundamental change in the smart grid architecture system for reduce threats in the electric field. So systems future architecture should be driven to the stronger and more consistent infrastructure.

Since, for information security on a computer or internet, several methods have been used. The most common method of data protection is encryption them. It is not possible to unauthorized to access to encrypted data and only people with keys are able to open the encode and use information. Computer data encryption is based on encryption sciences. Use of cryptography has a long history and historical.

Encryption is among other strategies to improve information security. Web-based information exchanges are protected by encryption protocols such as HTTPS and SSL. AES method approved by NIST to protect stored data and send and receive secure data that can be used the key size of 128,192 or 256 bits. U.S. government knows enough last two measurements to protect classified (secret) data, and until today, despite has been tested academic attacks against AES, but no one has been able to break this algorithm. NIST organization believes all three key sizes can provide adequate protection of the data until 2031 and even then [12].

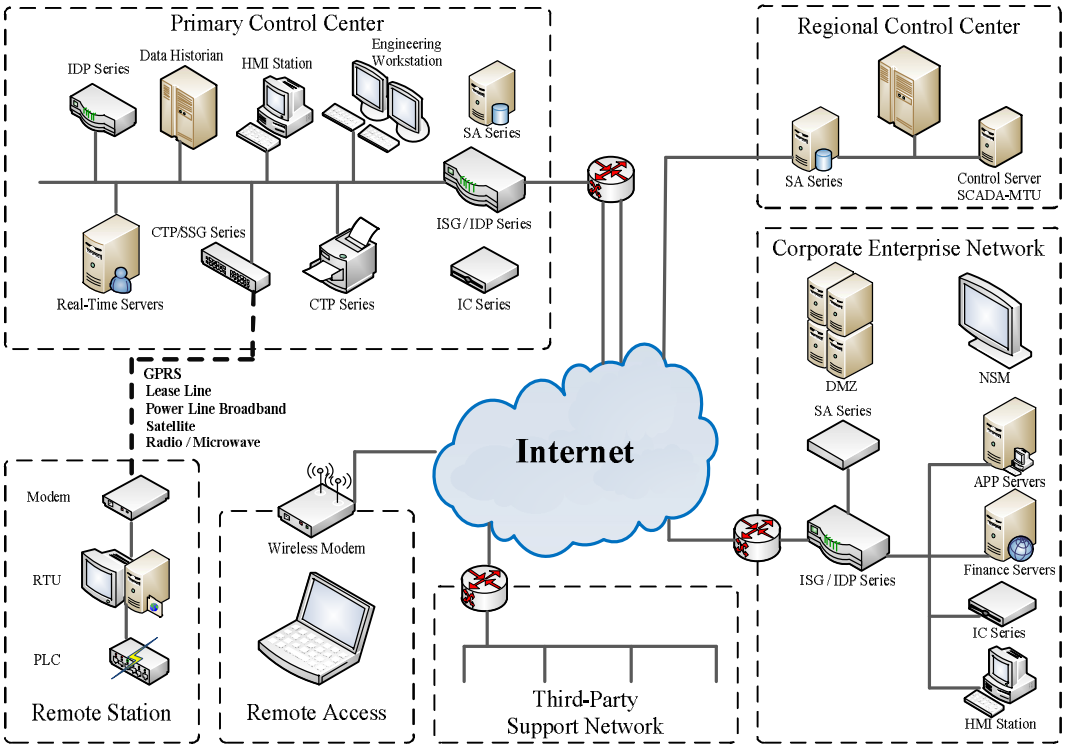

Fig. 2. Diagram block of sending and receiving data encryption in SCADA

According to some experts, low safety margin of this algorithm may be problematic in the future. But even with the best attacks, breaking this algorithm requires to 2120 act that is impossible to do this work with modern facilities. The most successful attacks against cryptographic algorithms have been attack against RC5 Sixty-four-bit key. Therefore, it seems we can be used AES for a long time for confidential and secret data encryption.

8. Conclusions

In the field of standard compilation organizations are active and in this context, the NIST and IEC are more valid. In task priority of NIST organization, we can point to response to consumer demand and energy efficiency, energy storage, electric vehicles, smart measurement systems and information security in communication networks. From ITIL standard distinctions compared to other conventional and traditional standards, it can be pointed to process-oriented in this standard approach versus task-oriented in other standards.

This standard are considered customer satisfaction in IT service and continuous improvement as two fundamental principle and based on the principle of continuous improvement provide evolution of the company gradually and under the conditions.

Another major difference that is ITIL distinct from other structures is management of continuing care in crisis which based on it, even in the event of any natural disaster, no matter can stop service in this model, and by pre-calculating the cost, investigated the effects of natural disasters and it is predicted risks and strategies specific to crisis and thus, prevent normal confusion of directors in emergencies.

Now, since information exchange between terminals and communication centers is one of the pillars of the telemetry system and its performance accuracy and speed plays a key role in dispatching system effectiveness, therefore, since purchased equipment for dispatching centers and terminals not supplied from one constructive necessarily, it is very

important due to the consistency and compatibility of protocol between terminals and center and suitable communication protocol is among strategies for optimizing the system. For this purpose, we need to knowledge of available communication protocols and infrastructure in distribution networks to develop smart electrical grid, until we can examine compatibility of communication protocols in different fields.

REFERENCES

1. Göran N. Ericsson; "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure", IEEE TRANSACTIONS ON POWER DELIVERY – , VOL. 25, NO. 3, JULY 2010; ISSN 0885-8977.
2. Hossein Shahinzadeh, Sara Baghar-Nasrabadi; "Technical Guidelines for Creating Smart Cyber Security of Information Technology in Power Systems", 1st Iranian Conference on Smart Grid, Iran, Tehran, Sharif University of Technology, October 19 - 21, 2010.
3. Hossein Shahinzadeh, Hajar Ghotb, 2012; "Load Estimation and Supporting Energy Efficiency in Smart Grids", International Journal of Scientific and Engineering Research (IJSER), Volume 3, Issue 9, September 2012; ISSN 2229-5518.
4. Miao Xin, Zhang Kai, Chen Xi, Zhang Xin, Sun Shenbo, Wu Guoliang, Zhou Zhaomao, Tian Shiming, Li Jianbo. Development Countermeasure of Constructing Smart Grid [J]. Electric Power Construction, 2009 (30): 6-10.
5. Xenakis C, "Security Measures and Weaknesses of the GPRS Security Architecture", International Journal of Network Security, Vol.6, No.2, PP.158– 169, Mar. 2008.
6. A. Hasanalizadeh Khosroshahi; "Sensor Networks in demand-side of Smart Grid", 8th International Conference on Technical and Physical Problems of Power Engineering, Norway, Fredrikstad, Ostfold University College, 5-7 September 2012.
7. The Smart Grid Interoperability Panel, Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, Volumes 1, 2, 3, National Institute of Science and Technology NISTIR 7628, Sept. 2010.
8. ISO/IEC, *"Information technology — Security techniques — Code of practice for information security management"*, International Organization for Standardization, International Electrotechnical Commission, ISO/IEC 17799:2005, 2005.
9. V. Igure, S. Laughter, and R. Williams, *"Security issues in SCADA networks"*, Computers & Security 25, (2006) 498 – 506.
10. G. Ericsson, and T. Torkilseng, "Management of Information Security for an Electric Power Utility—On Security Domains and Use of ISO/IEC17799 Standard", IEEE Transactions on Power Delivery, vol. 20, No. 2, April 2005.
11. Xenakis C, "Security Measures and Weaknesses of the GPRS Security Architecture", International Journal of Network Security, Vol.6, No.2, PP.158–169, Mar. 2008.
12. Hossein Shahinzadeh, Parastoo Azizyan, Naser Mashayekhi and Rezvan Dehkhodaei; "Evaluation of SCADA Security in smart grids", 3rd International Conference on Computer Technology and Development (ICCTD 2011), Chengdu, China, 25-27 November, 2011.