Security Assessment based on SCADA Aystem: Taking Shanshan Oil Transportation Station as an example

Lian Xiao[1, a], Zhijun Bu[2,b], Chaosheng Chen[1,c] and Binxian Yuan[3,d *]

1 Production and Operation Division, PetroChina West Pipeline Company, Urumqi, China

2 Instrumental Automation Office, China Petroleum Pipeline Engineering Corporation, Langfang, China

3 Tianjin Engineering Center of Digital Manufacturing of Die & Mold, Tianjin, China

[a]mostoivi@tom.com, [b]648315965@qq.com, [c]258370403@qq.com, [d]ybx2003@163.com

Keywords: SCADA system; security; security assessment

Abstract. SCADA (Supervisory Control And Data Acquisition) system is a computer-based automation system applied in operation process control and remote scheduling. This paper introduced the principle and method of security assessment based on SCADA system. Three basic elements of security assessment, asset, threat and vulnerability, are analyzed in detail. Taking the SCADA system of Shanshan oil transportation station as an instance, the security assessment practice was carried out based on matrix method.

1 Introduction

SCADA (Supervisory Control And Data Acquisition) system is a computer-based automation system combining operation process control and remote scheduling, which has been widely applied in the oil and gas pipeline field. In the operation process of long-distance pipelines, the SCADA system can collect real-time field data, automatically control industrial filed and sequential transportation, monitor the operation situation of equipments, pipelines and transportation stations systems, pipeline leaking, carry out pipeline simulation and operation security, provide essential data of operation, scheduling and management, and so on.

The research of security assessment for SCADA system has been conducted for many years at home and abroad. United States Department of Homeland Security (DHS) has established an industrial control system security assessment laboratory to conduct related researches with a few industrial control companies. Some international standardization organizations have presented related standards, advices and guides, such as NIST800-82 and ISA/IEC 62443.

API1164 (Pipeline SCADA Security 2nd Ed) standard established by American Petroleum Institute (API) regulates SCADA system security for oil and gas pipeline from system management, physical security, system access control, information publication, network design and data exchange, etc [1]. In China, National Engineering Laboratory of Industrial Control System Information Security Technology provides a powerful technical support to solve the problem of industrial control system information security. GB/T 30976-2014 series standards provide a basis for system and product assessment in industrial control field [2-3].

The SCADA system of Shanshan/Urumqi-Lanzhou was completed and put into operation in 2007, the protective construction was not fully considered at the beginning of the design of the system. In order to fully know the security of SCADA system, PetroChina West Pipeline Company set Shanshan oil transportation station as a typical station, and conducted the security assessment of SCADA system for the first time. The assessment work was conducted on the basis of a combination of domestic and international oil and gas pipeline security assessment technology and standard of SCADA system [4-5].

2 **Security risk**

Security risk, which is man-made or natural threats, it uses vulnerability that exists in the information and management system, and leads to the possibility of a security incident and the effects on the organization.

Asset, threat and vulnerability are the basic elements of the security risk, and basic conditions for the existence of security risk, each of which is indispensable. No asset, there is no objects that threat attacks or damages. No threat, although the asset is very valuable, vulnerability is severe, security incidents will not happen. If there is no vulnerability in the system, no links that threat can use, security incidents will also not happen. The relationship between elements of security risk is shown in Fig. 1.

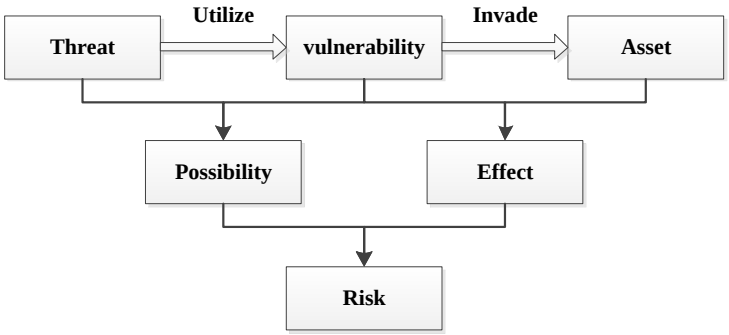

Figure 1. Relationship between elements of security risk

3 Security risk analysis

Security risk analysis involves three basic elements: asset, threat and vulnerability. Each essential element has its own property. Asset value is the property of asset. The frequency of threat is the property of threat. The severity of vulnerability is the property of vulnerability.

Security risk analysis associates these three basic elements and their properties of each element, then establish the interactions between each element. the principle of security risk analysis is shown in Fig. 2.

The basic steps of security risk analysis are as follows:

1) Identify the asset, and the value of asset.

2) Identify the threat, and assign the frequency of threat.

3) Identify the vulnerability, and assign the severity of vulnerability.

4) Calculate the possibility of security based on threat and the difficulty level that threat utilizes vulnerability.

5) Calculate the loss of security based on the severity of vulnerability and the asset value that the security can act on.

6) Calculate the risk value, that is the effect on the organization when the security happens, based on the possibility and the loss of security.

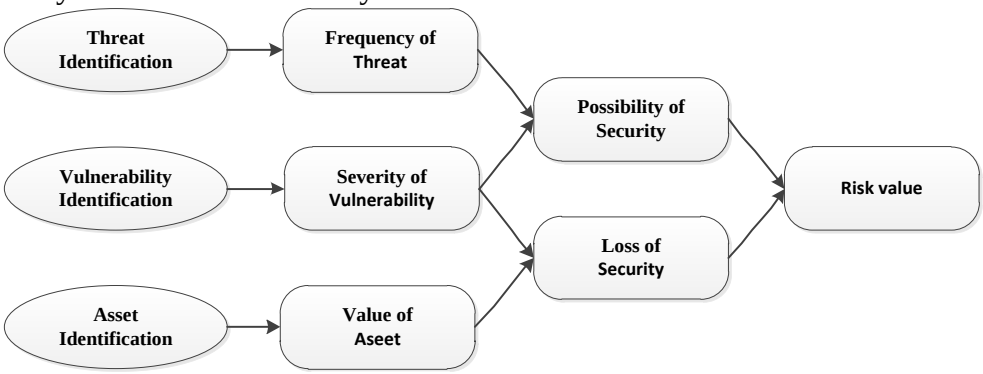

Figure 2. Principle of security risk analysis

3.1 Security assessment of SCADA system on Shanshan oil transportation station

Shanshan oil transportation station is composed of Shanshan crude oil first station, Shanshan product oil intermediate station and Shanshan crude oil reserve base. The main tasks of SCADA system on Shanshan oil transportation station are on-site process data acquisition, monitoring and controlling, sending real-time data to the control center, and accepting tasks that the control center issued.

In order to fully understand the security of SCADA system, PetroChina West Pipeline Company takes the SCADA system of Shanshan oil transportation station as an instance to conduct Security assessment of SCADA system for the first time.

3.2 Asset identification

The methods of asset identification usually include checking the design documents, interviews, on-site inspection, and so on. In this assessment, we adopted team meeting and on- site inspection of key assets.

Through on-site investigation, in this assessment the main part of SCADA system on Shanshan oil transportation station consists of process control system of product oil, ESD system of product oil, process control system of crude oil, ESD system of crude oil, process control system of reserve base, fire fighting system of reserve base, operator station, fire fighting station, station control server, switch, router, optical transceiver, and so on.

According to the actual situation of assets, we analyzed the confidentiality, integrity, and availability level of the system's assets one by one, evaluated the value of each asset comprehensively. Then, we obtained the assets' levels using the judgment criterion of assets importance degree. The higher the level is, the more important the asset is.

3.3 Threat identification

In this investigation, we got the possible threats faced by on SCADA system of Shanshan oil transportation station through the analyzing sources of the threats, the security incidents in the past, relevant industry statistics of the threats, the experiences of the evaluators and communications with the users, then assigned a value to the frequency of the threats.

3.4 Vulnerability identification

The vulnerability of SCADA system, generally includes management vulnerability and technical vulnerability. The methods of vulnerability identification mainly include document review, interview, questionnaire survey, tool testing, human verification, log analysis, and so on. According to the real-time requirements of the SCADA system's operation, it is inconvenience to use tools scanning and testing method to identify the vulnerability. In this assessment, combining with actual demand, we identified the vulnerability of the SCADA system according to the API1164 security requirements.

Through team meeting and on-site investigation, we fully investigated actual configuration and operation of security protection strategy, physical security, personnel security, network connection, and application system in SCADA system on Shanshan oil transportation station.

The items, which did not meet with requirements proposed by API1164 standard that found in the investigation, would cause security vulnerability of the SCADA system. Once utilized by the attackers, additional permission of the SCADA system could be got, and then they can access or damage the system without authorization, which can lead to security incidents of the SCADA system.According to the identified vulnerability, combining with the practical operation of SCADA system, we assigned the severity of the vulnerability.

3.5 Risk calculation

In this assessment, we used matrix method to evaluate the risk.

The possibility matrix of security incidents is shown in Table 1. According to the frequency of the threat and the severity of the vulnerability obtained in the investigation, we can determine the possibility of the security incidents in SCADA system of Shanshan oil transportation station against the matrix table.

The loss matrix of security incidents is shown in Table 2. According to the value of the asset and the severity of the vulnerability obtained in the investigation, we can determine the loss of the security incidents in SCADA system of Shanshan oil transportation station against the matrix table.

The risk matrix of security incidents is shown in Table 3. According to the possibility and loss of the security obtained in the calculation above, we can determine the risk value of the security incidents in SCADA system of Shanshan oil transportation station against the matrix table.

Table 1 Possibility matrix of security incidents

Severity of vulnerability / Frequency of threat	1	2	3	4	5
1	2	4	7	11	14
2	3	6	10	13	17
3	5	9	12	16	20
4	7	11	14	18	22
5	8	12	17	20	25

According to the user's actual risk acceptance, we know that the risk is not acceptable when its level is in Grade 4 or above. Thus, there were 31 unacceptable risks in SCADA system of Shanshan oil transportation station based on the calculated risk above.

Table 2 Loss matrix of security incidents

Severity of vulnerability / Value of asset	1	2	3	4	5
1	2	4	6	10	13
2	3	5	9	12	16
3	4	7	11	15	20
4	5	8	14	19	22
5	6	10	16	21	25

Table 3 Risk matrix

Possibility / Loss	1	2	3	4	5
1	2	4	6	10	13
2	3	5	9	12	16
3	4	7	11	15	20
4	5	8	14	19	22
5	6	10	16	21	25

For unacceptable and acceptable risks in SCADA system, we proposed specific corrective measures from the security protection of operating system and application program, security protection of database, account and password management, internal and external personnel management, SCADA computer and equipment management, protection of data and information, security protection plan, business continuity plan, configuration management, and so on.

4 Conclusions

Taking Shanshan oil transportation station as a typical station, we conducted security assessment from assets, threat and vulnerability of the SCADA system using the matrix method, which filled the domestic blank of security assessment of oil and gas pipeline SCADA system, it can effectively help users to comprehensively understand the safety of the system. According to the assessment conclusions, we took corresponding security protection measures, which can reduced the risk of the system to an acceptable degree, and provided powerful guarantee for the safety of the SCADA system.

References

[1] API STD 1164-2009, Pipeline SCADA Security Second Edition.

[2] GB/T30976.1-2014, Industrial control system security – Part 1: Assessment specification.

[3] GB/T20984-2007, Information security technology – Risk assessment specification for information security.

[4] X.Y. Guo, Y.B. Lu, J. Zheng, Technical status of long-distance pipeline SCADA system standards worldwide, Oil and Gas Storage and Tansportation. 30 (2011) 156–159.

[5] A.G. Wu, X. He, Overview on SCADA technology in long-distance oil/gas pipeline, Oil and Gas Storage and Tansportation. 19 (2000) 43–46.