Advances in Intelligent Systems Research, volume 169
VIth International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security' (IWCI 2019)

Problems of Cyber Security of Digital Substations

Irina Kolosok
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
kolosok@isem.irk.ru

Elena Korkina
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
korkina@isem.irk.ru

***Abstract*— Digital substation is a substation with a highly automated control, where almost all processes of information exchange between substation components, communication with external systems, and control of the substation operation are carried out digitally based on IEC 61850 protocols. The high importance of substations for the operation of power systems places unconditional requirements for their cyber security. Data transfer on Ethernet through the process bus and substation bus leads to an increased vulnerability of the digital substation to cyber attacks. The most common cyber attacks and their consequences influencing digital substation operability during cyber attacks, and also countermeasures are analyzed. A tree of threats and attacks to analyze digital substation capability to resist cyber attacks and restore operability after their exposure**.

Keywords*— Digital substation, cyber-attacks, tree of threats and attacks, recovery measures

I. INTRODUCTION

At present Russia is implementing a Concept of an intelligent energy system, which entails an ideology, basic technologies and mechanisms for developing the next-generation intelligent energy system, and features a hierarchy of control of the Unified Power System (UPS), transmission and distribution networks [1]. The paper focuses on a digital substation as a facility of the next-generation UPS that relies on advanced digital protection and control devices [2].

Substation is an essential element of technological control in UPS. Substations control power flows, and perform dispatch control of the system. Their main functions are data acquisition and transfer from primary equipment, emergency control (EC), relay protection (RP), computerized process control system (CPCS), electricity and power metering (EPM).

The high importance of substations for the operation of **power systems** places unconditional requirements for their cyber security. The most common cyber intrusions in the substation operation are created by insufficiently skilled personnel (the notorious human factor): anyone, who can access the substation and has basic skills in working with the relay protection terminal, can change the terminal settings and gain access to the switch control and diddle the power meter data. This attack qualifies as unauthorized control using a human-machine interface, and the probability of this attack grows with the use of public communication networks such as GSM, the Internet, etc. [3].

Until recently, substation protection and control systems have been based on the isolation and closed nature of the facility, the reliability of communications within the substation, and the use of internal protocols. The process of **energy** system "digitization", the use of intelligent technologies, sophisticated technical, information and communication equipment have increased the risks related to cyber security of energy facilities, including digital substations.

Digital substation is a substation with a highly automated control, where almost all processes of information exchange between substation components, communication with external systems, and control of the substation operation are carried out digitally based on the IEC 61850 protocols [4]. Data transfer on Ethernet using the process and substation buses leads to an increased vulnerability of the digital substation to cyber attacks, because in addition to the security threats of the “classic” substation there appear the threats of intrusion into operation of the process bus and time synchronization.

The information-technological protection of a digital substation can be ensured, if it possesses such properties as stability, adaptability, restorability, which can be developed based on deep analysis of the cyber security problem of digital substations.

The paper proposes a tree of threats and attacks to analyze digital substation capability to resist cyber attacks and restore operability after their exposure. The most common cyber attacks and their consequences influencing digital substation operability during cyber attacks, and also countermeasures are analyzed.

Control system of the Unified Power System has a hierarchical structure. All facilities of electric power industry are controlled by corresponding centers of the dispatch control: the lower control level – regional dispatch center (RDC) that is subordinated to the interregional dispatch center (IDC), and the whole power system of the country is controlled by the central dispatch center (CDC).

Data acquisition and processing systems SCADA are installed in the computerized control systems of the whole dispatch system and connect control centers with subsystems. The SCADA equipment includes workstations, servers, communication processors and communication links of the center with energy facilities. Communication protocols traditionally used in the SCADA system are not protected from malicious intrusion into enterprise network, this being one of the vulnerabilities at the local network entry of the substation. If there is no firewall at the local network entry of the substation, the malware easily penetrates into the network and decreases or interrupts performance of the information system of substation. If the firewall is adjusted properly, then part of the unknown information is blocked and some malware is revealed. Cyber security can be enhanced by creation of a perimeter network with an intrusion detection system along with the firewall. Servers of the perimeter network exchange information with the external network, and the firewall allows an external network to receive requested data solely.

II. Cyber Vulnerabilities And Cyber Threats At Digital Substations

Substations differ in structure, levels of automation and security. However, cyber threats and vulnerabilities for most substations are typical.

Some of the well-known cyber attacks – denial of service" (DoS-attack); injection of viruses and software with "bugs"; spoofing of GPS signals/stream of sampled values (SV-stream)/MMS and GOOSE-messages; traffic overflow, etc.- are direct threats to operability of the digital substation. The attacks, their consequences, and possible measures to counteract them are listed in the Table below.

TABLE Cyber Threats At Digital Substations

Cyberattack	Effects	Countermeasures
1.DoS–attack	Delay in control; failure of tripping/operation	Backup of IED-devices
2.Malware code injection, malware injection	Undesirable tripping/operation; failure of tripping/operation	User authorization; detection and prevention of attack; installation of anti-virus software; prohibition to use memory sticks, their replacement with CD; disconnection of automatic data download from external media
3.Specialized malware	Intrusion into operating system Windows	Hardware removal because of unavailability of developed anti-virus software
4.Packet transfer delay due to route change	Delay in control commands	Closing of ports; hardening of protection of switchers/routers/ NMS ("network control system")
5.GPS spoofing	Desynchronization	Use of VLAN (virtual local area network); antenna tracking; backup of GPS receivers
6.Spoofing of SV-stream, MMS- and GOOSE-messages	Undesirable tripping/ operation; failure of tripping/operation	Message authentication
7.Scanning of ports; network monitoring; eavesdropping	Object configuration data theft	Encryption
8.Inlet of repeated cyber or physical attacks	Overflow of transit traffic	Construction of a cryptographic authentication system
9.Intrusion into corporate network by Internet (by web- or FTP-server)	Intrusion into the local network of substation with subsequent information distortion	Proper configuration of network operating systems and security tools
10.Intrusion into the local network of substation with subsequent information distortion	Impact on the Human-Machine-Interface Most HMI vulnerabilities are divided into 4 categories: memory corruption; management of user credential; lack of authentication/ authorization; insecure default values.	All these errors can be prevented using the safe techniques of code development.
11.Impact on the Human-Machine-Interface	If you successfully attack the HMI vulnerabilities, you can do anything with the infrastructure itself, including physical damage to the equipment: Formation of false commands to control network, electronic equipment, to trip network elements	Strict rules for network access, correct configuration of firewall
12.Fuzzing – bad data feed		Invitation of certified experts only
13.Notorious human factor	Access to control devices, switching of relay protection to substation and RTU of neighboring substations	Strict rules for network access, correct configuration of firewall
14.Electromagnetic interference	Impact on transmission lines	Filters, coaxial cable, twisted pair

Analyzing the listed attacks, it can be noted that some of them are interconnected - the implementation of one attack leads to the immediate implementation of another attack. The 7th attack initiates the 8th one, the 9th attack initiates the 10th one, the 10th attack initiates the 11th one. Such cases are marked with ⇩ (see Table).

In case of large volumes of information the use of the Table, however, is not the most convenient way to analyze. The emerging problem of cyber security of energy facilities makes it necessary to create easily implementable means of analysis and prevention of cyber threats.

III. Tree Of Threats And Attacks.

In order to generate the measures to counteract possible malicious attacks it is necessary to identify vulnerabilities on the substation territory and potential cyber security threats. To this end, the fault tree technology used in the theory of reliability of complex technical systems was applied [5]. The Fault Tree Analysis technology applied by expert systems in military aviation, then in nuclear power, and in some other industries [6]. The method of fault tree is proposed to describe the consequences of cyberattacks on the state estimation procedure.[7]. Carefully thought over tree of the attacks lowers the level of vulnerabilities and risks [8].So, a tree of threats and attacks was constructed to analyze the cyber security of the digital substation (Fig. 1) that shows vulnerabilities for possible cyber attacks.

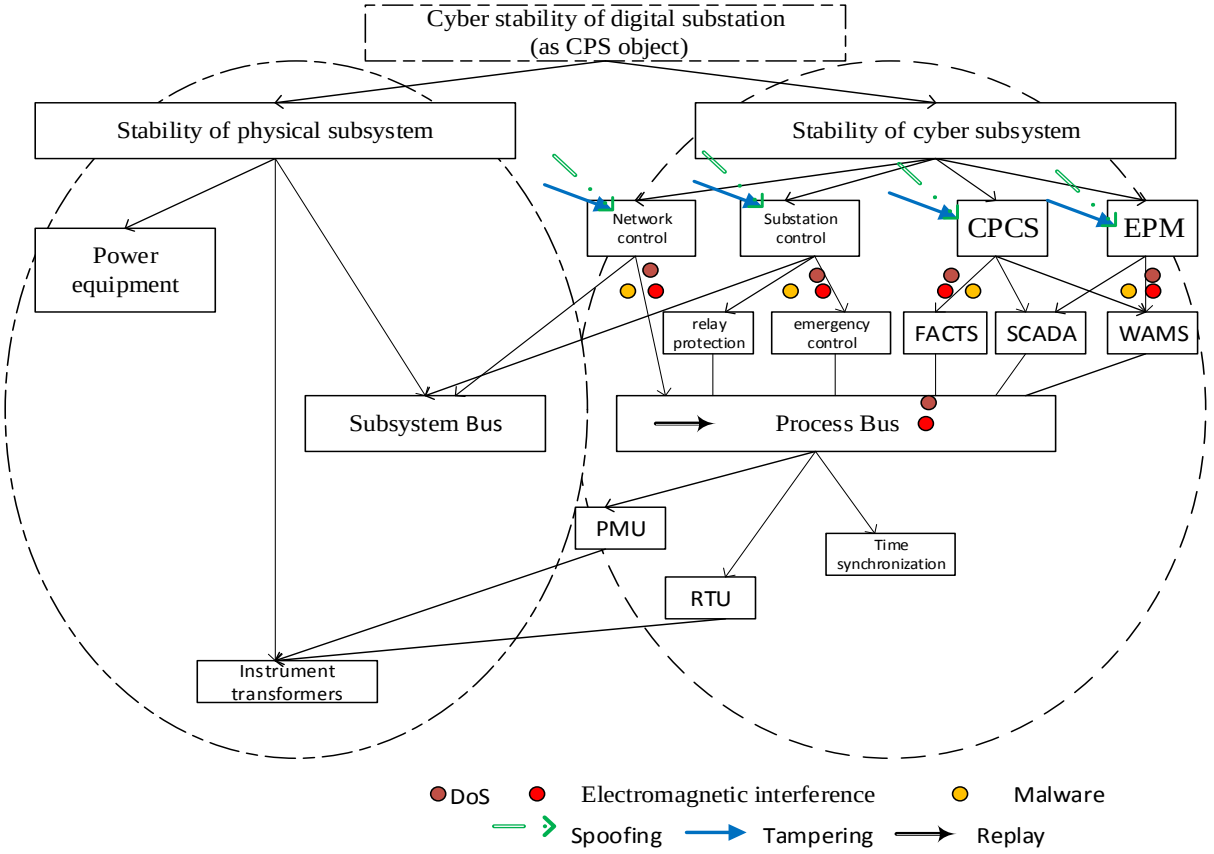

Fig.1. Tree of threats and attacks of digital substation

A tree of threats and attacks can be constructed for each substation in an understandable form. Such a tree will make it possible to analyze the information-communication system of the digital substation for availability of vulnerabilities, to audit available protective cyber measures and to plan further steps on cyber security development at the considered energy facility.

The results of the study have shown that the statistical methods of measurement information processing at the digital substation also play an important role along side with technical and organizational measures to improve its cyber stability [9]. Combination of all measures will reduce the risk of errors in power system control at cyber attacks on digital substations.

In the future, at the substation level it is planned to implement algorithms of the generalized state estimation [10,11] for joint estimation of operating parameters and communication hardware state, since the measurements - logical (i.e. telesignals, TS) and analog (i.e. telemetry, TM) – are made synchronously, collected in a single place and digitized by the standard protocols. The applied process bus and substation bus offer access to a great amount of measurement information fixed at the substation. Implementation of computational algorithms of the local generalized state estimation at the substation level will provide high-quality

verification of TS on the state of network elements and telemetry, which will reduce the risks of errors because of measurement information distortion at the digital substation as a result of cyber attacks during power system control.

IV. CONCLUSIONS.

At present, the cyber threats of malicious intrusion becomes ever more obvious in electric power and many other industries that apply information resources for production process control. Due to the increasing problem of cyber security for industrial facilities, the use of easily implementable tools to analyze and prevent cyber threats is indispensible. The tree of threats and attacks that was developed on the basis of the fault tree technology from the reliability theory of complex technical systems.is one of these tools.

The developed tree of threats and attacks includes all basic components of the information-technological system for digital substation control. The tree diagram vividly displays the most probable vulnerabilities of digital substations. Probable cyber threats and cyber attacks are enumerated for each vulnerability, the countermeasures to prevent cyber attacks or reduce their adverse effect on digital substation operability are worked out for each case of intrusion.

ACKNOWLEDGMENT

This study is supported by the Siberian Branch of the Russian Academy of Sciences (Project III.17.4.2) of the Federal Program of Scientific Research (No. AAAAA-A17-117030310438-1) and partial by RFBR grant №19-07-00351 A.

REFERENCES

[1] Fortov, V., and Makarov, A. (2012). A concept of Russia's intelligent power system with active-adaptive network. Moscow JSC "NTC FSC EES». 235p.

[2] ‑A. Epifanov. We see great potential in digital substations,. Electricity // Transmission and Distribution. No 1 (34), 2016 pp. 6-9.

[3] Alymov I.S. Problems of information security of substation and ways of their decision / I.S. Alymov//Digital substation [an electronic resource] – 2016. – Access mode:
http://digitalsubstation.com/blog/2016/02/17/problemy-informatsionnoj-bezopasnosti-podstantsii-i-sposoby-ih-resheniya/

[4] Definition of DSP and priority technologies of DSP // Digital Substation. No. 9, 2018, pp. 10-20.

[5] Yu.B. Guk.Computing the energy facility reliability. (Leningrad.: EnergoAtomIzdat, 1988 – 224 p.

[6] Ericson C.A. Fault tree analysis http://www.eecs.ucf.edu/~hlugo/cop4331/ericson-fta-tutorial.pdf

[7] Kolosok I., Korkina E., Tikhonov A. A Reliability Analysis of State Estimation Software Based on SCADA and WAMS // Energy Systems Research, Vol. 1, No. 1 (2018): pp.100-107.

[8] Vidhyashree Nagaraju, Lance Fiondella, and Thierry Wandji. A Survey of Fault and Attack Tree Modeling and Analysis for Cyber Risk Management. International Symposium on Technologies for Homeland Security. IEEE, 2017.

[9] Kolosok I.N., Korkina E.S Role of the State Estimation in Ensuring Cyber-Physical Security of Electric Power System.// *Proc. 88th Int. Scientific Workshop on Methodological Problems in Reliability Study of Large Energy Systems, 2014*, Issue 67, Syktyvkar: Komi RC UB RAS, 2016, pp. 386-395.

[10] G.N. Korres, P.J. Katsikas, G.E. Chatzarakis. "Identification of analog and topological measurements errors in generalized state estimation", *Journal of Materials Processing Technology*, vol. 161, pp. 121-127, 2005.

[11] A. Simoes Costa, E.M. Lourenco, L. Colzani. "Reduced anomaly zone determination for topology error processing in generalized state estimation", *Proceedings of IEEE Power Tech conference*, Lausanne, pp. 137-142, 2007.