ATLANTIS PRESS
Advances in Intelligent Systems Research, volume 158
Vth International workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-based, Cloud Computing and Cyber Security" (IWCI 2018)

Cyber Resilience of SCADA at the Level of Energy Facilities

Irina N. Kolosok, Elena S. Korkina

Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences,
Lermontov str., 130
Irkutsk, Russia
E-mail: korkina@isem.irk.ru

Abstract

SCADA systems are widespread in the energy industry: the automated dispatch control of electric power systems is supported by SCADA along with the automatic control. Today, the consequences of cyberattacks on the information subsystem of the control system are especially dangerous. SCADA, being an information-technical system that plays the most important role in the control system of a power facility, should be resilient to different cyber threats.

Keywords: SCADA, cyberattacks, resilience, power facility.

1. Introduction

Nowadays, in any type of production (metallurgy, aircraft and machine building, manufacturing industry, etc.), where a continuous technological process is controlled by a computer technology, SCADA (Supervisory Control And Data Acquisition) systems are widely used for collection and processing of technological information. Undoubtedly, SCADA systems are widespread in the energy industry as well: on the basis of information coming to industrial controllers from sensors installed at buses and outgoing lines, as well as at various connections, certain commands are developed to control the equipment of the power facility. Initially, SCADA was used only for automatic control of individual power plants of electric power systems (EPS). Over time, however, a human-machine interface (HMI) was created in the SCADA environment for the efficiency and convenience of operators, technologists, and dispatchers. This interface enabled the duty personnel to see the scheme of the power facility, messages and alarms, graphs, diagrams and other technologically useful information on the screens of workstations (automated workstations). Thus, the automated dispatch control is organized along with the automatic control. The power facility information collected using RTU (remote terminal unit) undergoes primary check for meeting the technological limits and comes in the form of arrays to a real-time database located on a server. A package of SCADA-applications is also placed on one of the servers. The interaction between the information on the current state of EPS and applications is organized by the SCADA control system located on the master terminal unit (MTU).

The digitalization of the SCADA technical base, the requirement to meet international standards for information exchange, and other innovations increase the vulnerability of the EPS control system to external intrusions. Today, the consequences of cyberattacks on the information subsystem of the control system are especially dangerous.

2. Cyber Vulnerability of SCADA Systems

At one time, when the first SCADA systems were developed, there was no talk of cyberattacks, so no measures were taken to create a specialized cyber protection. Now, various types of specific cyberattacks are known in the information environment: from database hacking (when the rules for administering access to the network and directly to the database are violated) to placement of a malicious code in the texts of the process control programs (when this code gets into the computer of an IT specialist of the power facility). Even economizing on computers and software becomes a vulnerable issue of SCADA: incomplete hardware configuration, minimal application package, and untimely update of the latest software versions lead to uncontrolled maintenance of SCADA software, involving random specialists, installation of unlicensed equipment and unlicensed software. The problem of

vulnerability faces communication channels and information exchange protocols. Such disciplinary and economic violations should be dealt with by the administration of power company. An analysis of state estimation results allows a technologist to make a conclusion on the facts of information failures, corruption of some state variables or network parameters, and probably indicate the expected place of intrusion into the information structure of the EPS facility.

3. A state estimation

State estimation is an important procedure that provides reliable and qualitative information for EPS control [1]. Solutions to the state estimation problem are the EPS steady state (current state) calculated on the basis of measurements. Until recently, the measurements of state variables and telesignals on the state of switching equipment that were obtained from SCADA system have been used as the measurements for state estimation.

The SE problem consists in solving the following basic problems [1]:

- Formation of the current network topology using the data of telesignals;
- Analysis of observability;
- Identification of gross errors in measurements or bad data detection (BDD);
- Filtering of random measurement errors, i.e. their estimation and calculation of non-measured state variables.

The main problems that arise in state estimation are related to a low quality of metering information, arriving from SCADA, and low redundancy of measurements. This leads to errors in formation of the current network topology, appearance of unobservable sections, critical measurements and critical sets, in which it is not possible to find bad data; to "smearing" of gross errors and, as a result, – to distortion of SE results and low accuracy of obtained estimates.

The state estimation procedure aims to search for such calculated values (estimates) of measured state variables $\hat{y}$ that are most close to the measured values y in the sense of some criterion, most frequently the sum of the least-weighted squares of derivations of estimates from measurements:

$$\varphi(y) = (\bar{y} - \hat{y}\ )^T R_y^{-1} (\bar{y} - \hat{y}) \quad (1)$$

and satisfy the electric circuit equations

$$w(y, z) = 0, \quad (2)$$

that relate measured y and unmeasured z state variables, R_y - a covariance matrix of measurement errors.

Traditionally, EPS state estimation is mainly based on SCADA measurements: magnitudes of nodal voltages U_i , injection of active P_i and reactive Q_i power at nodes, power flows in transformers and lines P_{ij} ,Q_{ij} and less often – magnitudes of currents at nodes I_i, and in lines I_{ij} .Thus, the vector of measurements looks as follows:

$$\bar{y} = (P_i, Q_i, P_{ij}, Q_{ij}, U_i, I_i, I_{ij}) \cdot$$

The other approaches to choosing SE criterion are possible [2].

4. A system of SCADA protection

The SCADA control system is represented by three areas –dispatch control (DC), automatic control (AC) and a system for protection of the entire SCADA software-hardware system. The traditional information protection system of any power company, normally, includes specialized software products:

1. Network firewalls,
2. Demilitarized zone,
3. System of recognition and prevention of intrusions,
4. Perimeter protection,
5. Protection of remote access, etc.

and a mandatory requirement for strict implementation of the following activities:

1. Authentication;
2. Access control;
3. Encryption;
4. Logging of events;
5. Security settings.
6. Vulnerability analysis:
    - Check for the latest updates;
    - Check for vulnerabilities;
    - Check for zero-day vulnerabilities.

At present, we know about many cyberattacks targeted directly at the SCADA system:

- Phishing - obtaining confidential data that allows access to the network;
- ICT Worm infection - isolation of the SCADA server from the rest of the network;
- DNS Poisoning - connection of the user with a fake web- or SCADA-server;
- Denial of Service – for example, overflow of network traffic;
- Fault Data Integrity –input of false data in measurements or in telecontrol;
- Replay attack - redirects data packets in the wrong direction;
- Timing attack - a kind of Replay attack;

- Desynchronization attack - a kind of Timing attack;
- Malware infection - computer infection with malicious applications;
- Man-In-The-Middle - compromising communication channels, etc

Normally, the public learns about cyberattacks at power facilities, only if the attacks cause great economic damage. Therefore, the statistics on cybercrimes at SCADA is significantly underestimated compared to the actual situation. Nevertheless, even the available official information led to a special European project [2], whose goal is cyber security of SCADA. In the period from 2009 to 2014, the number of cyberattacks in the information-management system (IMS) of SCADA increased by more than 27 times. The first steps announced within the framework of the project are:

1. Take the problem of cyber security of ICS SCADA to the level of the national cyber security strategy and efforts to protect the critical information infrastructure.
2. Develop good practices of ICS SCADA cyber security.
3. Standardize information sharing among critical sectors.
4. Build ICS SCADA security awareness.
5. Foster expertise with ICS SCADA cyber security training and educational programmes.
6. Promote and support ICS SCADA cyber security research and test beds.

Great analytical work on the investigation of SCADA vulnerabilities and development of countermeasures to cyberattacks was carried out in [3]. After the formation of the list of cyberthreats on SCADA, the authors created a special stand that allowed them to develop a number of measures to protect SCADA from the implementation of these threats. As a result, in the laboratory conditions, SCADA security characteristics were considerably strengthened against unauthorized access to the local network and servers, and against penetration into the network protocols and in the SCADA configuration settings. In [3], such measures as the increase in the level of protocol security, the creation of an integrated architecture of firewalls with intrusion detection systems, the use of encryption in conjunction with tunneling[*], "enhanced the immunity" of the SCADA system greatly.

[*] To protect the network flow, it is sufficient to insert it in an encryption tunnel between a sender and a receiver. Thus, only the receiver will be able to understand the flow content, nobody will be able to change the sent packets or use them again, because the encrypted tunnel includes time tags as well.

The developed measures to ensure cyber security of an electric power industry facility were initially based on the traditional reliability indices, i.e. the operability of the facility, time between failures, capability to restore functionality after significant and minor damages. However, cyber intrusions into the process control system significantly burden both the operating conditions and the process itself. The traditional approaches to the reliability of a facility and its functioning under cyberattack conditions are insufficient. In this regard, the term "Cyber resilience" meaning "cyber stability" was introduced.

5. Cyber resilience is a property of the cyber-physical subsystem of EPS

The term "cyber resilience" [4-9 and others] has appeared recently. It embraces all the stages of the technological process from the stage of normal operation of a facility and its subsequent functional failure, to the restoration of the facility operable state.

Various options of return to an operable state are considered for the last stage (restoration of an operable state after a failure):

(1) the state does not differ from the pre-emergency state (robust behavior),

(2) incomplete recovery with weakened state variables (flexible behavior),

(3) transition to an inoperable state (destructive behavior),

(4) the state with variables surpassing the pre-emergency state (recovery with adaptation). As evidenced by the analysis in [4], insufficiently reliable technologies applied at the facility, topological redundancy of a scheme and inaccurate forecast of the forthcoming course of events affect dramatically the deterioration of the facility state. The analysis also indicates that the restoration stage depends on the level of the control system effectiveness, on the requirement of continuous integration (Continuous Integration dependence[†]), and on the availability of resources for the restoration. Thus, if, for some reason, one node *i* connected with a number of other m nodes falls out of the process, the performance of the scheme is reduced

[†] CI- continuous integration (a development methodology used in modern software development projects, which consists in performing frequent automated project assemblies to identify and solve integration problems as quickly as possible.) In an ordinary project where different parts of the system are developed independently by individual developers, the integration stage is the final. It can unpredictably delay the completion of the project. The transition to continuous integration can reduce the complexity of integration and make it more predictable by the earliest detection and elimination of errors)

by the amount, $\Gamma_i = \sum_{j=1}^{m} n_j \tau_j$ where $n_j \tau_j$ is the disconnected node n_j, and τ_j is its idle time. Restoration of the system is the magnitude $R^{-1} \propto \Gamma_i$.

6. SCADA cyber resilience

SCADA, being a separate technical system that plays the most important role in the control system of a power facility, should be resilient. In [3], the SCADA resilience ability even in a lab environment was not studied, whereas the current situation requires CADA resilience in production conditions in real time.

Researchers in [4-9] find interesting functional and algorithmic solutions for the resilience of SCADA system that has suffered from a cyberattack. In [5], the authors consider three types of FDI (Fault Data Integrity) attacks on SCADA (Fig.1):

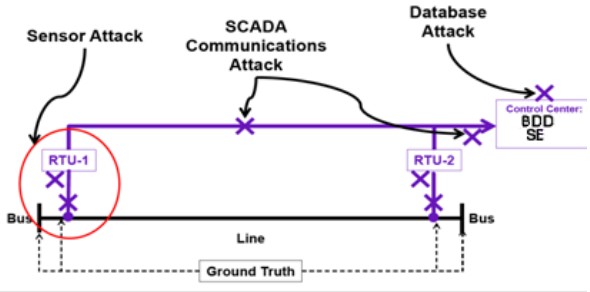

Fig. 1. Three types of Fault Data Integrity attacks on SCADA [5].

1) on a separate sensor;
2) on a communication channel;
3) on a real-time database,

and suggest the ways to enhance the SCADA resilience by creating a protective system of cyber-physical (CP) agents. Such a system can ensure the cyber resilience of SCADA: provided all sensors are covered by cyber-physical agents:

1) It is very easy to identify a FDI attack on a separate sensor;

2) The FDI attack on a separate communication channel is also easily identified, if the topology of the scheme is radial;

3) The FDI attack on a real-time DB can be identified only by using the procedures of Bad Data Detection (BDD) and distributed state estimation (SE) at the Dispatcher centre of electric power system.

Thus, the need for the state estimation procedure for solving the cyber resilience problem is coming to the fore.

An interesting approach to solving the problem of SCADA cyber resilience with the help of state estimation is proposed in [6]: for all measuring devices (RTU, MTU, etc.) (Fig. 2), a descriptive table is built with indication of a two-way connection between the devices, and their belonging to the category of the encrypted, hence, secure devices. In addition, a table is compiled with a list of all possible measurements received in the collection system, indicating which device the measurement comes from. The table thus created contributes to solving the problem of Secure Observability.

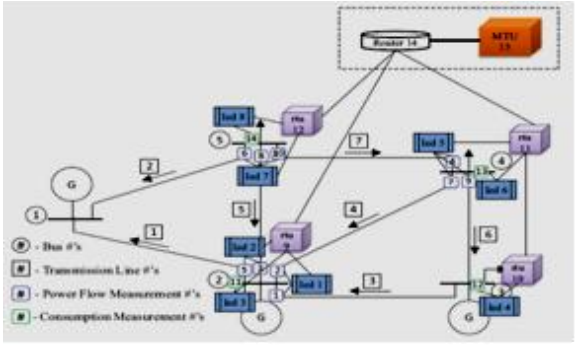

Fig. 2. A data collection structure at the energy facility [6].

Thus, in the analysis of the bad data detection procedure results, the data from such a table will allow a conclusion about a suspicious origin of the error in the data.

The approach demonstrated in [7] suggests the use of built-in software (peer-to-peer overlays). Such middleware is placed between the SCADA communications and the IP layer: the so-called SCADA listener hears the appearance of a message on the SCADA network and duplicates it. If it is impossible to send SCADA messages via the channels, SCADA-listener sends "saved" information by its "overlay" network. Interestingly, in general SCADA has a hierarchical structure, while peer-to-peer overlay network is flat. Therefore, for each section in the SCADA structure, a peer-to-peer overlay is created.

In SCADA there are some possible places of penetration by intruders who managed to bypass traditional protective measures. Some of the SCADA-system elements subject themselves to cyber threats - for example, software applications that work with the same corrupted data or erroneous commands, duplicated and distributed further.

The state estimation software is located in the SCADA control system space among "EMS Applications, etc.". The FDI (fault data integrity) attack directly affects the state estimation procedure, however, it can suffer from the consequences of almost any cyber intervention:

- Due to problems in the SCADA hardware (buffer overflow, denial of service (DoS), low transmission speed in the channel, use of

unprotected protocols), the source data may not come to the state estimation procedure;
- Due to database attacks (violation of administration rights, Phishing attacks, SQL-injection, data substitution), the reference and archive information used by the state estimation procedure can be distorted;
- Finally, the use of data from another SCADA, the functional non-isolation of applications can also affect the state estimation procedure operation.

The algorithms implemented in the state estimation software are designed to verify the original information. With their help, we can identify erroneous and doubtful data, as well as places on the scheme, that are poorly provided with measurements (in particular, due to sudden data loss). Based on the results of the state estimation software operation, specific alarms should be generated for the information subsystem. These alarms will then be delivered to the operator workstation, as well as the alarms from the automatic SCADA control system. Receiving the alarms about a disorder in the information subsystem must be immediately confirmed by the operator, in accordance with the established rules. IT specialists should respond to the received information alarm.

Existing data processing algorithms, in particular, the traditional algorithm of bad data detection by estimation residuals, are no longer sufficient to detect gross errors in the initial information. The fact is that hackers successfully introduce distortions in the state variables measurements, which are perceived by the BDD algorithms as reliable [10, 11 and others]. Therefore, the requirements for processing the data subject to cyberattacks are increasing. For example, in [8] the authors consider new algorithms for solving the cyber resilience problem:
- A resilience control algorithm that provides protection at the level of control system by increasing the application security;
- Algorithms for resistance to intrusion and detection of anomalies that can classify measurements and commands into good and bad in the sense of their application;
- Protection algorithms, that take into account the attacker's knowledge about the network functioning;
- Smart Grid control algorithms that are capable to maintain the system within stability limits during an emergency (the most critical to cyberattacks).

7. Conclusions

In the future, in order to improve the cyber resilience properties of the state estimation software, we plan to update the algorithms that process the initial information by increasing the intelligence of the verification procedure based on the analysis of statistics obtained during online operation of the software. To this end, the obtained verification results will be compared with the verification results in the previous state estimation snapshot; statistics on the occurrence and location of gross errors, critical measurements and critical groups will be gathered; the correlation between the measured values of state variables and their estimates for each significant node of the grid scheme will be monitored. These measures will also increase the cyber resilience of the SCADA system.

Acknowledgements

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 (№ AAAA-A17-117030310438-1).

References

1. A. Gamm and I. Kolosok, Test equations and their use for state estimation of electrical power system, *Power and Electrical Engineering* (Riga: RTU, 2002).
2. R. Mattioli and K. Moulinos, *Analysis of ICS-SCADA cyber security maturity levels in critical sectors.* www.enisa.europa.eu
3. I. Fovino, M. Masera, L. Guidi and G. Carpi, An Experimental Platform for Assessing SCADA Vulnerabilities and Countermeasures in Power Plants, in *Proc. of HIS* (Poland, 2010).
4. A. Tofani, S. Alessandroni, G. D'Agostino, A. Di Pietro, G. Onori, M. Pollino and V. Rosato, Operational Resilience Metrics for a Complex Electrical Networks, *CRITIS* (Italy, 2017).
5. J. Giampapa, G. Hug-Glansman, Saummia Kar, SCADA resilience via autonomous cyber-physical agents (Pittsburg, USA, 2014). *https://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_300497.pdf*
6. E. Al-Shaer, M.A. Rahman, *Security and Resiliency Analytics for Smart Grids*, (Springer-Verlag, New York 2016). *https://www.springer.com/it/book/9783319328706*
7. D. Germanus, A. Khelil, and N. Suri, Increasing the resilience of critical SCADA systems using peer-to-peer overlays *(ISARCS, Prague, Czech Republic, 2010)*, pp.161–178. *https://link.springer.com/chapter/10.1007/978-3-642-13556-9_10*
8. S. Shirazi, A. Gouglidis, K. Syeda, S. Simpson, A. Mauthe, I. Stephanakis and D. Hutchison, Evaluation of Anomaly Detection Techniques for SCADA communication resilience *(Resilience Week (RWS), 2016)* pp.140–145.
9. A. Gouglidis, Protection against cyberattacks: Introducing resilience for SCADA networks, (*Symposium on Innovative Smart Grid Cybersecurity Solutions, Austria, 2017*)
10. M. Khokhlov, A matroid theory approach to constructing the sparse attacks on power system state estimation, in *Intern. Conf. on Problems of Critical Infrastructures, 2015*) pp. 57–65.
11. I. Kolosok and E. Korkina, Decomposition of power system state estimation problem as a method to tackle cyber attacks (*IPCS, Saint-Petersburg, 2018*).