http:d2cigre.org
http://cigregroups.org/display/SCD2

CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2017 Colloquium
September 20th to 22nd 2017
Moscow – RUSSIA

PS2-13

ABOUT CYBER PHYSICAL MODEL FOR CYBERSECURITY RESEARCHES IN POWER INDUSTRY.

by

Fedor Ivanov(EnLAB),
Oleg Arkhangelsky (RTEC).
Aleksandr Voloshin (MPEI),
RU

SUMMARY

Large-scale implementation of modern communications, information technologies and computing techniques at power facilities acutely raises the issue of cyber security and safety within the oil and gas as well as electric power systems. However, object’s cybersecurity assessment based only on information and telecommunication system’s operation analysis can’t give a full understanding of the real consequences of possible cyberattacks.

For a complete analysis and assessment of the consequences severity it is necessary to analyze various scenarios of operational disorder for the electric power systems (PS) caused by cyberattacks on information and telecommunications infrastructure as well as on protection, automation and control systems. This requires the establishment of specialized cyber-physical simulator (CPS) of power systems where automated control systems, information and telecommunication infrastructure together with PS are modeled simultaneously for operation in real time. Using such type of CPS allows us to evaluate and analyze possible consequences of cyberattacks on different objects within the energy industry (for example, result of cyberattacks can be follows: interruptions in the electricity supplying to consumers, violation of the PS stability, equipment’s outage, etc.).

For this purpose, Russian Telecom Equipment Company (RTEC) creates a large CPS, which is unique for Russian Federation. A distinctive feature of the developed CPS is that in addition to the virtual model of the primary power system equipment, performed on the basis of the software-hardware RTDS (Real Time Digital Simulator), testbed also contains real physical relay protection, control and other intelligent devices, together with SCADA servers integrated into a single model, which simulates in real time the operation of a complex electric power system.

Main technical solutions of CPS design and its possible application for cybersecurity investigations are considered in this report.

KEYWORDS

Cyber physical simulators, large power system simulator, cybersecurity of control and networks communications systems.

* JSC EnLAB, Nizhegorodskaya st., Cheboksary, Russia, 428018
Fax: + 7 8352 406626 e-mail: mail@ennlab.ru

1. INTRODUCTION

Data acquisition and data transmission systems, as well as communication equipment and automated control systems at various levels of the operational dispatch management hierarchy have become integral elements of modern PSs. The modern power management system is built based on information and telecommunications systems and SCADA, so an increasing amount of electrical substation equipment is connected to communication networks [1]. Along with increasing efficiency of operational and dispatch management, the active introduction of information technologies and the concept of remote control at the fuel and electric power complexes have several drawbacks: many power facilities become vulnerable to intruders; possible cyber-attacks on the infrastructure of such objects can have serious consequences for cities and even whole regions [2].

Thereby the problem of cybercrime in general and cyberattacks on important infrastructure facilities in particular becomes increasingly actual in the modern world. In connection with this, a special attention is dedicated at present time to the information security within the complete energy industry including the risks reduction for possible cyber-attacks in the Russian Federation at the state and corporate level.

To prevent attacks on the infrastructure objects and to analyze attack vectors, it is necessary to identify the most critical (vulnerable) elements of the system and evaluate severity of consequences from a possible attack. The severity of potential cyber-attacks consequences and their impact on the operation sustainability of the PS depend on a current mode of the power system operation: availability of power reserves, reserve transformers and power lines; changes in the network topology (switching), equipment’s damage, etc. It is obvious that it is impossible to verify the PS stability for different scenarios of cyber-attacks in real functioning power system for many organizational and economic reasons. Instead, it is suggested to use the method of real time simulation of PS with secondary equipment included in the simulation loop (hardware-in-the-loop simulation). The testbeds developed under this approach are called cyber-physical simulators [3]. To create such models, Real Time Digital Simulator (RTDS) with RSCAD software is connected to real relay protection devices or any other IEDs by analog, discrete and different interface signals, see Figure 1.

Nowadays CPS are the most effective tool for information security of electric power systems researches providing the most complete opportunities for modeling and research. The CPS with the RTDS simulator was demonstrated in September 2016 in Innopolis city at the conference about SCADA cybersecurity [4]. The same CPS was also used for the final stage of CTF tournament, where cybersecurity experts examined power system’s equipment for various unauthorized influences. Similar tournaments were held earlier and their results were consistently disturbing: having the ability to connect to the internal network of the company, hackers caused several times false operation of simulated power equipment, which can lead in real PS to serious consequences [5].

The successful development of real time simulation systems has led to the creation of CPS which include top-level dispatching management systems: SCADA, EMS systems, etc. in addition to relay protection, automation, data collection and transmission systems. Such augmented CPS allow conducting detailed researches of interaction between the substations and the control center. Testbeds also allows to study the modeled part of PS for sustainability and security against attacks on various information assets, etc.

The laboratory created in the RTEC based on CPS is the first Russian testbed, specifically oriented to conducting researches in the domain of electric power system's information security. The use of the RTDS in this CPS makes it possible to flexibly expand the capabilities of the tested system as new tasks and research goals arise.

The developed CPS consists of the following main parts (see Fig.1):

1. Workstation with RSCAD software; it allows to create new projects with different power system infrastructure, manage and monitor the simulation process;
2. RTDS cubicle with processor cards and different Input / Output modules;
3. Amplifiers cubicle, intended to amplify low-level analog signals from RTDS. Amplifiers used to generate current and voltage signals for the tested protection relays and other secondary equipment;
4. Cabinets with the investigated protection relay and automation equipment, SCADA devices and other IEDs.

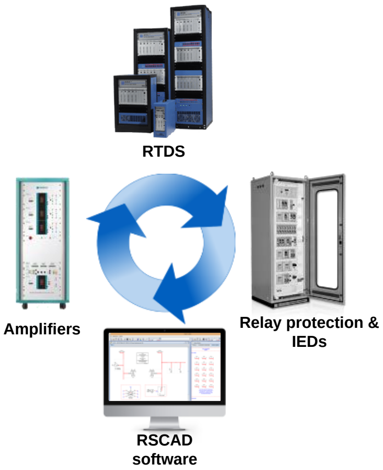

Figure 1: Main parts of the developed CPS

The application of the developed CPS allows to improve level of conducted research of PS's information security by the ability to simulate individual features of real electrical networks and complete power systems. CPS also allows to take into account infrastructural redundancy, reservation, work of emergency control systems (SIPS), relay protection, different auxiliary and measuring systems, etc.

The main goals and tasks of the RTEC's laboratory are as follows:

1. Developing different approaches and methods for the detection of cyber-attacks, prompt response measures and incident management.
2. Substations and electrical networks cybersecurity researches.
3. Analysis of critical substations elements.
4. Assessment of the PS facilities protection and their components.
5. Analysis of power grid infrastructure vulnerabilities, development threat models for power grid facilities based on testing and scenario tests.
6. Conducting researches with manufacturers of protection, automation, control devices and SCADA systems to detect vulnerabilities in equipment, listed above.

7. Support in the elaboration and further development of the normative base (national standards, guidelines and best practices) to provide information security of critical infrastructure facilities.
8. Advanced training in information security.

2. Description of CPS

As it was shown above, the CPS is based on the RTDS simulator which allows to use RSCAD software (see Fig.2) to perform real-time simulation and interact with relay protection devices and SCADA by analog and digital signals, as well as digital interfaces IEC61850 (GOSSE, SV), PMU, MMS, 104, DNS – all what is important for simulating "digital substations" and simulating the interaction of the substation and the control center.

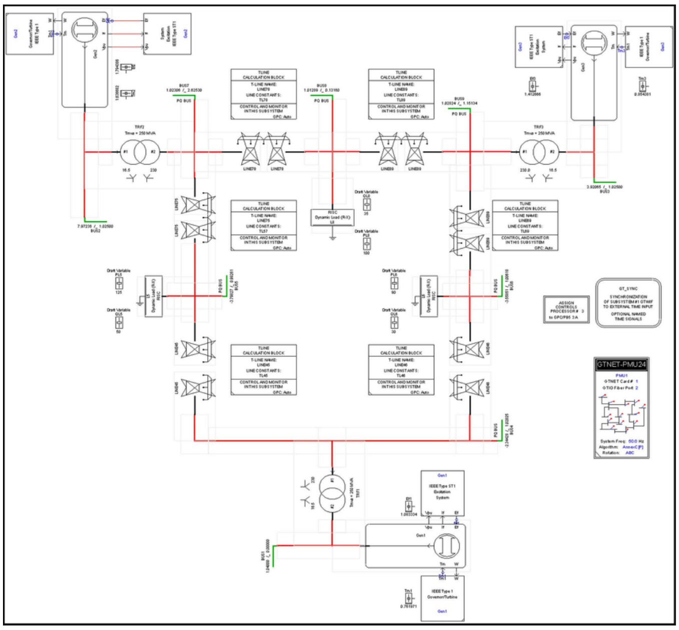

Figure. 2. Example of simulated power system part with 9-bus scheme

The logical scheme of the CPS can be represented as several interacting levels, each of them containing certain equipment, software, etc., corresponding to the tasks of this level. In general, it is convenient to use a representation in the form of 4 infrastructure levels: (see Figure 3):

- **PS layer**: the physical infrastructure of power systems simulated on the RTDS which simulates generation, transmission and distribution of electric energy. It includes primary and secondary equipment of power plants, substations and transmission lines;
- **IED’s layer**: intelligent devices (IEDs) i.e. sensors, connection controllers, etc. At the same time, for the realizing of secondary equipment in CPS, both real devices of relay protection and automation devices and automated control systems are used as well as their virtual models created in RSCAD software;
- **Communication layer**: data and communication infrastructure including substation and control center communication equipment, providing at the same time data collection from the SCADA and transfer of this information to top-level dispatching systems;
-
- **Applications layer**: at this level, there are interacting systems of operational-dispatching and technological management of PS.

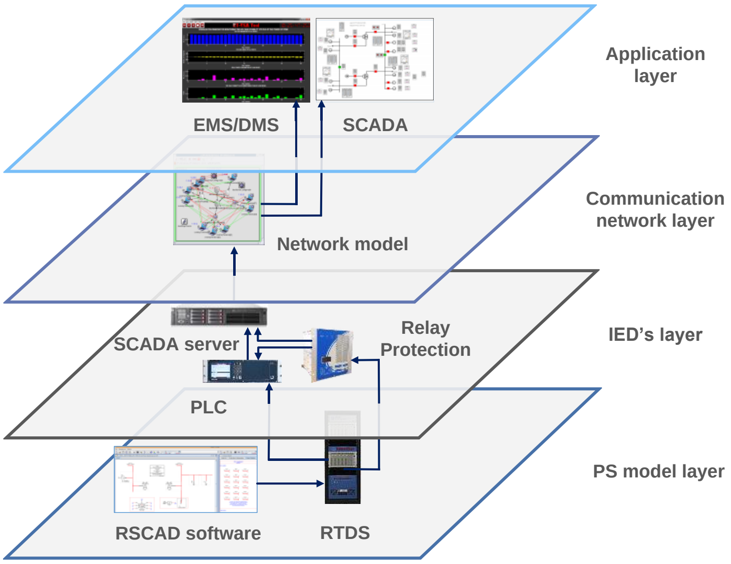

Figure. 3. The architecture of the CPS model

The main condition for obtaining a real picture in simulation is the availability of models of PS components that accurately reflect the parameters of real devices. The RSCAD library includes all types of equipment used in the PS, which allows to successfully fulfill the following tasks on the CPS:

1. Management of the virtual PS under simulation with the realization of the information exchange with the real relay protection and SCADA equipment according to the protocols: IEC 61850 (GOOSE and SV), IEC 60870-5-104, DNP;
2. Management of PS characteristics, multi run of the examples with different values;
3. Management of sets of the relay protection and of the Ethernet network switches by protocols IEC 61850 (GOOSE, SV, MMS), DNP, 104, Telnet, SNMP;
4. Implementation of custom scripts for conducting experiments, including optimization tasks of the model data or the testing equipment with the use of genetic algorithms.
5. Conservation of test results in the database;
6. Automatic generation of test reports.

The developed CPS is a unique testbed for Russia, which allows testing various information security tools and provide certification tests. Today there are several main areas of research conducted or planned to be conducted at the laboratory:

1. *Relay protection testing*. The real-time simulator generates signals that are close to the real signals of the PS. Their closed loop operation provides the interaction of the relay protection devices with the simulated PS by traditionally analogue signals or by the IEC 61850 protocol.
2. *Testing of PS's control systems.* In the frames of this direction correctness of automated control systems functioning in various conditions (including some of the system's functions lost as a result of cyber-attack) is being conducted. On the virtual PS specifies the objects to which the control signal can be issued. These include switches, disconnectors and earthling switch, specialized control devices for generator, SVC, HVDC and FACTS.
3. *Phasor measurement units testing*. Test the correctness of phasor measurement systems operation in violation of the integrity or availability of information, received from PMUs compliant with the IEEE C37-118 protocol.

4. *Smart networks and distributed generation.* Research of information security of the IEDs, provided within the concept of Smart Networks, Distributed Generation and Industrial Internet of Things.

CONCLUSIONS

In connection with increased cybersecurity level in the complete energy industry in general and in the electric power industry in particular, the RTEC has created a laboratory for the research of safety of the relay protection, control, and automation devices together with SCADA systems and conducting at the same time cyber security researches of PS facilities. The uniqueness of the developed cybersecurity laboratory is in the fact that besides the relay protection devices also SCADA system and other IEDs together with different subsystems are also included in the testbed's circuit (hardware-in-the-loop concept). Thus, testbed simulates in real time operation of an electrical network, also considering the functioning of different intelligent devices, automated and automatic control systems. This allows conducting comprehensive researches of cybersecurity for these systems, assessing the severity of the possible consequences of cyber-attacks on different information resources.

REFERENCES

1. Организация телеуправления подстанциями без постоянного присутствия обслуживающего персонала. Комплексный подход / Федоров О.А., Небера А.А., Литвинов П.В., ЗАО «РТСофт» // С.5. - 4 CIGRE
2. SCADA Security in a Post Stuxnet World / Eric Byres, P. Eng // Byres Security Inc - 2007.
3. Khaitan S.K., J.D. McCalley "Cyber physical system approach for design of power grids" IEEE Power and Energy Society General Meeting, 2013;
4. "Наша киберфизическая модель на конференции Кибербезопасность АСУ ТП 2016" http://ennlab.ru/rus/news/92
5. "Кто взломал электрическую подстанцию: разбор конкурса Digital Substation Takeover " https://www.phdays.ru/press/news/41185/

BIBLIOGRAPHY

Alexander Voloshin Ph.D. Head of the department relay protection of MPEI.
Fedor Ivanov. Since 2011 he has been working as a Deputy of Technical Director at ENLAB and is engaged in technical support of RTDS and PSCAD simulators
Oleg Arkhangelsky Graduated Moscow Power Energetic Institute in 2015, . Now working at CJSC Russian Telecom Equipment Company as a Project Manager.