SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 11, No. 2, June 2014, 233-241

UDC: 621.316.925:004.738.5 **DOI: 10.2298/SJEE131026019G**

Susceptibility of Modern Relay Protection: Will Protection From Cyber Attacks Help?

Vladimir Gurevich[1]

Abstract: Modern trends in relay protection (RP) based on the substitution of electromechanical protection relays (EMPR) by digital protective relays (DPR) have resulted in the emergence of an absolutely new problem, which was not known before. This problem is the possibility of an intentional remote destructive impact (IRDI) on relay protection in order to put it out of action or make it perform functions that have nothing to do with the current operational mode of protected electric equipment. Traditional and well-known methods ensuring information safety cannot fully prevent unauthorized actions of RP. The article describes a new way for the problem solution.

Keywords: Relay protection, Cyber attack, Digital protective relay, Intentional electromagnetic destructive impact, Cyber security.

1 Introduction

In the modern power systems, DPR is the most critical link [1], which on one hand is the most susceptible to IRDI, while on the other hand it is directly connected to a circuit breakers influencing the state of the power system. This is why the IRDI in the form of cyber attacks [2] and intentional electromagnetic destructive impact (EMDI) [3, 4] are aimed initially at DPRs.

It is known that protection relay has two types of failures: the so called "non-operation" and the "unnecessary operation" (which in this context is similar to faulty operation). As mentioned in [1], the unnecessary (faulty) operation of RP can result in more significant damages than non-operation. This is due to the fact that non-operation of protection of a certain type is backed-up by protection of other types or more remote protection, such as protection on other levels, while the unnecessary operation of RP is almost impossible to prevent by available means. This idea is not something unexpected and has been mentioned before elsewhere [5]. At the same time, [1] mentions that this is an absolutely different situation, when an inadequately operating protection relay can generate a command for switching off a circuit breaker in the case of unnecessary operation and thus artificially prevent a power system from

[1]Central Electric Laboratory, Israel Electric Corp., POB 10, Haifa 31000, Israel;
E-mail: vladimir.gurevich@gmx.net

functioning normally. This leads not only to the disconnection of thousands of consumers and considerable damage comparable to emergency mode in a power system, but also creates the danger of a serious blackout caused by sudden overflows of power in the case of disconnection in a branched energy supply system. As mentioned in [6] 25-28% of significant blackouts known in the world were the result of protection relay failures. If we admit that 50-70% of transition of an ordinary emergency mode to a serious blackout is also caused by protection relays [6], we can conclude that protection relay is responsible for all the blackouts. ORGRES representatives (Moscow) presented interesting data, which confirm the above mentioned idea [7]:

> *In 2012 there were 53,214 events of actuation of protection relays and automatic equipment on Federal Grid Company's equipment. This includes 52,763 events (99,15%) of correct actuation; 451 events of incorrect actuations, which* ***include 213 events of unnecessary actuation, 160 faulty actuations and 76 failures to actuate…***
>
> *The index of correct operation of DPR in 2012 was 98.97%, which is lower than the generalized index of correct operation of electromechanical protection relays (99.31%).*

First of all this means that the number of faulty and unnecessary actuations (373) under general operational conditions (i.e., without intentional remote destructive impacts) is much higher than the number of non-operation (76). Secondly, it suggests that the reliability of modern digital protection relays (DPR) is lower than that of old and worn-out electromechanical protection relays (EMPR).

Special research conducted by the B5 committee of CIGRE and presented in its report confirmed the relevance of the problem and the conclusion that expansion of application of the most advanced standard IEC 61850 with its GOOSE-messages as well as modern Ethernet technologies in relay protection result in increasing its susceptibility to cyber attacks [8]. The appreciation of the problem of DPR's cyber safety has resulted in intensification of multiple investigations in the area of cyber safety all over the world. For example, in the USA this situation is dealt with by a large department, which consists of several thousand people under the supervision of the Head of National Security Agency – General A. Keith [2], while in Russia this job is performed by a special department of the Federal Security Service of Russia. There are also Edicts of the President of the Russian Federation: "About establishment of a state system of detection, prevention and liquidation of consequences of computer attacks on informational resources of RF" and "The framework of state policy of RF in the area of international information security by 2020", which are viewed as a reply to the "International Strategy for Cyberspace" adopted by the USA in 2011 [9]. It is the first time that the USA sets computer subversions on a par with traditional military actions, reserving the right to react with all available means,

up to the use of nuclear weapons. It is known from the Mass Media that the problem of cyber security of the Israeli power system is handled by a special department of Israel Security Agency (SHABAK) together with specialists of the Israel Electric Company. In 2011 Israel launches National Cyber Command (The **National Cybernetic Taskforce**) into Administration for the **Development of Weapons and Technological Infrastructure (MAFAT)** for coordination and concentration cyber R&D activities for the various branches of the Israeli defense establishment (cyber departments of Mossad, SHABAK, Ministry of Defense (**Unit 8200**) and other entitiesv) with budget of hundreds of millions of shekels in year. Recently, the major Russian Institute – All Russian Research and Development Institute of Relaying (VNIIR) – also established a special department, which is dealing with specific problems of cyber security of relay protection. According to Gartner, the volume of the international market of cyber security increased from 61.8 billion USD in 2012 to 67.2 billion USD in 2013. It is expected that it will reach 86 billion USD by 2016.

2 What "Cyber Security" Means?

This being said let us clarify what "cyber security" means? Analysis of several related publications shows that this term usually means informational security. It should be considered that "information security" may mean different things in different contexts, such meaning can be wider or narrower. The wider meaning includes the whole spectrum of organizational and technical measures of security provision. The types of information security are provisionally divided into passive and active. The passive risk of information security is aimed at illegal use of information resources and is not aimed at setting the information system out of order. This type of risk includes access to databases or listening through the data transfer channels. The active risk of information security is aimed at setting the information system out of order by an intentional attack on its components. The active threats of computer security include: physically knocking the computer out of operation or disturbance of its performance as well as intentional interference with the normal mode of operation of equipment controlled by the computer by interference with the algorithm of its operation. A typical example of the latter would be a well-known virus called Stuxnet [2]. Under information security I will mean the ways of information protection from intentional or accidental unauthorized access, which can damage the normal course of data exchange in a system as well as stealing, modification and destruction of information.

The major problems that need to be solved in the area of engineer-technical protection of information include:

– Interception of electronic emanation and electric signals;
– Forced electromagnetic irradiation (lighting) of communication lines in order to obtain a parasitical modulation of the carrier;
– Implementation of listening devices;
– Remote photography;
– Interception of acoustic irradiation and restoration of text sent to a printer;
– The copying of information carriers, breaking through protection;
– Impersonation;
– Masking under system's queries;
– Use of software traps;
– Use of drawbacks of programming languages and operating systems;
– Unauthorized connection to hardware and communication lines of specific devices, which provide access to information;
– Malicious setting of protection mechanisms out of order;
– Deciphering of encrypted information by special software;
– Informational infections, that is, different viruses, including "logical bombs", "Trojans", "worms", "password interceptors", etc.

In order to ensure information security the following measures are usually implemented:

1. Firewall - a complex of hardware or software measures, which control and filter network packets flowing through it in accordance with established rules. This means enables:
   – Filtering access to initially unprotected services;
   – Prevent obtaining closed information from protected sub-network as well as intrusion into a protected sub-network of faulty data by means of susceptible services;
   – Control access to network nodes;
   – Registering all access attempts both from external and from internal networks;
   – Regulating the order of access to the network;
   – Notification of suspicious activity, flexing or attacks to network nodes or the firewall itself.
2. Antivirus software developed to locate computer viruses as well as malicious software and restore the infected (modified) files and to prevent infecting files and/or the operating system. Location of viruses is usually based on comparison of codes browsed by the antivirus with the known codes (signature) of malicious software set up in the library of the antivirus. Recently the so called pro-active technologies of antivirus protection have started to develop. The idea behind them is that unlike reactive (signature-based) technologies they prevent infection of the system rather than searching for malicious software in the system.

3. Cryptographic methods of protection of information, in other words coding and encryption of information, access keys, special protocols of network and user authentification.

These widely known technical measures can be supplemented by some specific measures accepted in digital relay protection. One of these measures is a use of general information data buses (process buses) since the attack on such a bus is the simplest and the most efficient way, which can interfere with operation of a substation. It is possible to use several "point-to-point" links instead of these buses. This will allow using commutation protocols (including one-way data transfer), which are more resistant to attacks. These and many other specific measures of RP protection, which have more to do with protection of data transfer protocols, increasing of password cryptographic robustness, etc., are discussed in more details in [10].

3 Are Widely Known Measures of Information Security Enough to Ensure Reliable Operation of Digital Protective Relays?

The main question now is: are all of these widely known measures of information security enough to ensure reliable operation of digital protection relay? My answer is – no. Traditional and well known methods ensuring information safety cannot fully prevent unauthorized actions of RP. It doesn't mean that some methods of protection are not efficient enough yet (which is actually the case), but it means that it is not possible in principal. The analysis discussed above suggests that all the known technical measures of protection of information are designed to protect information channels from unauthorized access and information itself from being stolen and/or damaged. Of course, these information channels are widely used in digital RP and they should definitely be protected very well. But here's the question: are these channels the only way to make DPR disconnect the circuit breakers and ruin the circuit? In point of fact DPR contains a lot of so called "logical inputs" (LI) that are sensitive to voltage availability. This voltage is delivered to LI by means of contacts of external electromechanical relays. It is not possible to encrypt or encode the fact of voltage presence or absence on the LI. Moreover, the LI's design in a DPR is not suitable to receive encoded information. It is enough to modify the freely-programmable logics of DPR so that during a remote supply of voltage by means of a certain external relay to a previously selected LI there will be actuation of output DPR relays affecting the circuit breakers and it will be possible to use it to sabotage the power system. Unfortunately, none of the above measures of protection from cyber attacks will help in this situation, since in actuality there was no cyber attack to DPR. Considering the fact that besides the above impacts powerful direct ultra-broadband radio waves or a powerful electromagnetic impulse can tamper with the DPR [3, 4], I think we should

avoid using the term “cyber attack” and use the “intentional remote destructive impact” (IRDI) instead. This will include all types of intentional destructive impacts on relay protection. I think that this transition is rather substantiated, since the technical solutions that I offer result in efficient protection of DPR from all types of such impacts simultaneously.

So, what do I offer to reduce susceptibility of DPR to IRDI?

4 The New Way for Increasing Reliability of Relay Protection

As we mentioned before, the task of increasing reliability of relay protection cannot be fulfilled by combining DPR’s functions with those that have nothing to do with relay protection, such as monitoring the functionality of electric equipment, remote control of circuit breakers, etc. The DPR should be used solely to solve the problems of relay protection. Moreover, there are many specific devices on the market that can be used to solve other problems, such as monitoring the electric equipment. These devices may vary from the simplest relays that control the circuit breaker trip coil circuit to sophisticated complex units that ensure online control of gas composition dissolved in the transformer’s oil or the level of partial discharges in the insulating material. I think that remote control of circuit breakers should also be separated from DPR and should be performed by separate hardware rather than by DPR. This is the only way we can increase the reliability of RP and efficiently protect it from intentional remote destructive impacts. This separation of functions not only ensures efficient protection of DPR, Fig. 1, but also employs a remote system of circuit breakers control [11].

The general idea behind the suggested hardware-facilitated method of protecting DPR from IRDI is to use an electromechanical reed-switch operated actuator in combination with DPR and connected in series with it as well as a responsive electromechanical starting unit - SU (RR1 – RR4), which ensures blocking the sensitive terminals of DPR and disconnection of its output circuit, Fig. 1. The reset of the actuated SU is performed upon the circuit breaker’s actuation and backed-up by a RESET command at the end of a preliminary set-up time period.

Without current and/or voltage actuation of this SU, DPR will not be able to influence the operation mode of the power system, even under IRDI or a powerful electromagnetic interference impact. If the SU is actuated and DPR is enabled, nothing will interfere with using specific features and wide functional capabilities of DPR. At the same time unnecessary actuation of the SU itself does not influence the operation of relay protection and thus there are no specific requirements to the accuracy of SU actuation. The only thing that is important that it should always be actuated before DPR, i.e. it’s settings should be a little bit lower than required for the controlled parameter. If the AE

actuation was unnecessary and DPR was not actuated, the device would automatically reset. The main technical requirements to this device are its high reliability, insensitivity to short impulse (micro- and nanosecond range) and high-frequency interferences, resistance to substantial overloads, high level of galvanic separation from external circuits and high speed of response to actuation (several milliseconds).

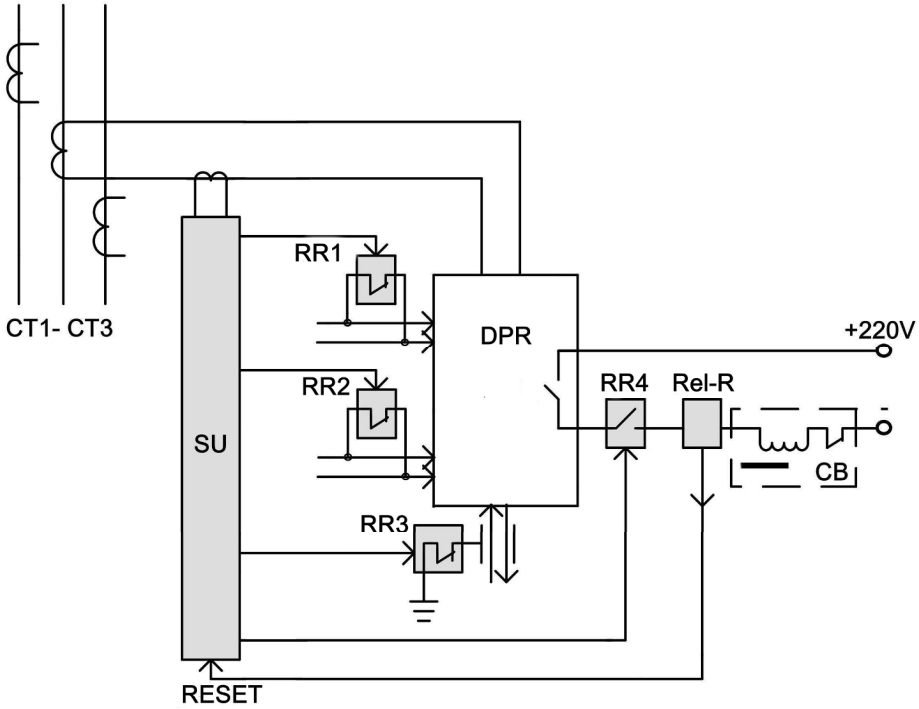

Fig. 1 – *Structural Diagram of DPR Protection from IRDI.*

The principle of operation of this device is as follows. In its initial state under the normal operation mode of the protected object, all the input reed-switches (current and voltage sensors, etc) of the SU are in released state; the coils of the control reed-switches RR1-RR4 are not powered. The normally closed contacts RR1 and RR2 are short circuited the logical inputs of DPR, the RR3 terminals are short circuited the communication channel, while the RR4 terminals are breaking the output circuit of DPR. Under these conditions the DPR is fully blocked both in inputs and in outputs and neither IRDI can result in its unnecessary actuation and unauthorized turn on of CB trip coil. By-passing of logical inputs of both DPR and communication channel increase its operational life under the impact of a powerful electromagnetic impulse.

In case of emergency mode in the protected object at least one of the controlled parameters (current, voltage or power) will drastically change. This change leads to actuation of at least one of the reed-switches of the SU within 1 ms or less and to further actuation of RR1-RR4 relays (turn off of reed-switches) takes place during 2–4 ms, while closing of powerful terminals of RR4 reed-switch on a Bestact R15U reed-switch type doesn't take longer than 5 milliseconds. Thus, the total response time of the unit to an emergency mode does not exceed 6 ms, which is rather acceptable considering the DPR's own actuation time of 30–40 ms. Under this mode of operation of DPR protection device, the DPR will be fully unblocked and returned into its normal mode of operation, retaining all its settings and features

The selection of reed-switches as basic elements of the device is based on the aggregate of their most important features, such as: air tightness, long life, high responsiveness, special gas environment or vacuum, where contact elements are located, no need to adjust or clean the terminals, high level of galvanic separation between the input (control coil) and output (reed-switch), as well as clear and consistent actuation threshold (pickup). I developed the current and voltage sensors with adjustable pickups on reed-switches long ago and were widely used in special hardware and military equipment. There is a description of some of them in [12], which can be used in the device described above. All the elements of the device can be mounted in a separate module supplied by DPR manufacturers and located close to DPR in a relay cabinet.

5 Conclusion

1. Cyber attacks are not the only threat to modern digital protection relay. This is why in order to improve reliability of relay protection conventional methods ensuring information security are not enough.
2. Instead of "cyber attack" it is suggested using the term: "intentional remote destructive impact" (IRDI). This will include all types of intentional destructive impacts on relay protection. Targeted at unauthorized interference with its operation, disturbance of its normal algorithm of operation or setting it out of order.
3. The known methods ensuring information security are not able to protect DPR from IRDI. Thus, it is necessary to develop absolutely new means of DPR protection, which will supplement the methods ensuring information security.
4. As a universal means of DPR protection from IRDI it is proposed using a separate module, containing an actuating element with responsive electromechanical current and voltage sensors with reed-switches and output control reed-switch relays, which would unblock the logical

outputs of DPR, its output circuits and the communication channel only in case of emergency or an event close to emergency in a protected unit.

5. In order to benefit from DPR protection from IRDI it is necessary to stop the malpractice of supplementing DPR with additional functions, which have nothing to do with RP; limit the scale of programmable logic use as well as separate functions designed for the remote control of CB and the relay protection, considering an independent and protected system for remote control of CB.

6 References

[1] V. Gurevich: The Issues of Philosophy in Relay Protection, Energize, May 2013, pp. 33 – 34.

[2] V. Gurevich: Cyber Weapons Against the Power Industry, Energize, Sept. 2011, pp. 40 – 42.

[3] V. I. Gurevich: Stability of Microprocessor Relay Protection and Automation Systems against Intentional Destructive Electromagnetic Impacts – Part 1, Electrical and Electromechanical Engineering, No. 5, 2011, pp. 23 – 28.

[4] V. I. Gurevich: Stability of Microprocessor Relay Protection and Automation Systems against Intentional Destructive Electromagnetic Impacts – Part 2, Electrical and Electromechanical Engineering, No. 6, 2011, pp. 21 – 28.

[5] A.I. Shalin, A.S. Trofimov: Efficiency and Reliability of a Relay Protection – Relay Protection and Substation Automation of Modern Power Systems, CIGRE 2007, Cheboksary, Russia, 09 – 13 Sept. 2007. (In Russian).

[6] N.Y. Saratova: The Analysis of Approaches to Research of Processes of System Collapses – System Researches in Power Engineering, Conference of Young Scientists, Irkutsk, Russia, 2007, pp. 31 – 39. (In Russian).

[7] V.A. Kuzmichev, S.N. Sakharov: Analysis of Functioning of Relay Protection Devices in the ENES in 2012 Year, Relavexpo-2013, Cheboksary, Russia, pp. 56 – 57. (In Russian).

[8] The Impact of Implementing Cyber Security Requirements using IEC 61850 – CIGRE Working Group the B5.38, Aug. 2010.

[9] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, Executive Office of the President, WA, USA, May 2011.

[10] S. Ward, J. O'Brien, B. Beresh, G. Benmouyal, et al: Cyber Security Issues for Protective Relays: C1 Working Group Members of Power System Relaying Committee, IEEE Power Engineering Society General Meeting, 24-28 June 2007, Tampa, FL, USA.

[11] V.I. Gurevich: Increasing Security of Remote Control of Circuit Breakers from Intentional Destructive Impacts, Power Transmission and Distribution, Vol. 3, No. 3, 2013, pp. 52 – 57.

[12] V.I. Gurevich: Reed Switch Relays with Adjusted Pickups, Components and Technologies, No. 11, 2013, pp. 30 – 33. (In Russian).