Increasing Security of Remote Control of Circuit Breakers from Intentional Destructive Impacts

Vladimir Gurevich

Central Electric Laboratory, Israel Electric Corp. POB10, Haifa 31000, Israel

gurevich.iec@gmail.com

***Abstract*-The article is a continuation of the author's previous article: "Device of Protection of Relay Protection"[1] and describes a new way for increasing immunity of remote control of circuit breakers from intentional destructive electromagnetic impacts and cyber attacks.**

***Keywords*- Remote Control; Circuit Breaker; Cyber-Security; Digital Protective Relays; Electromechanical Relays**

I. INTRODUCTION

The previous article [1]***"Device of Protection of Relay Protection"***, concentrates on the necessity to protect digital protective relays (DPR) from cyber attacks and intentional destructive electromagnetic impacts (IDEI), offers a protection device with the starting unit (SU) included and employs the principle of by-passing the sensitive input terminals of DPR by electromechanical reed relays (RR4-RR6) with a simultaneous breaking of their trip circuit by quickly operating electromechanical relay (RR7) with reed switch, as shown in Fig. 1.

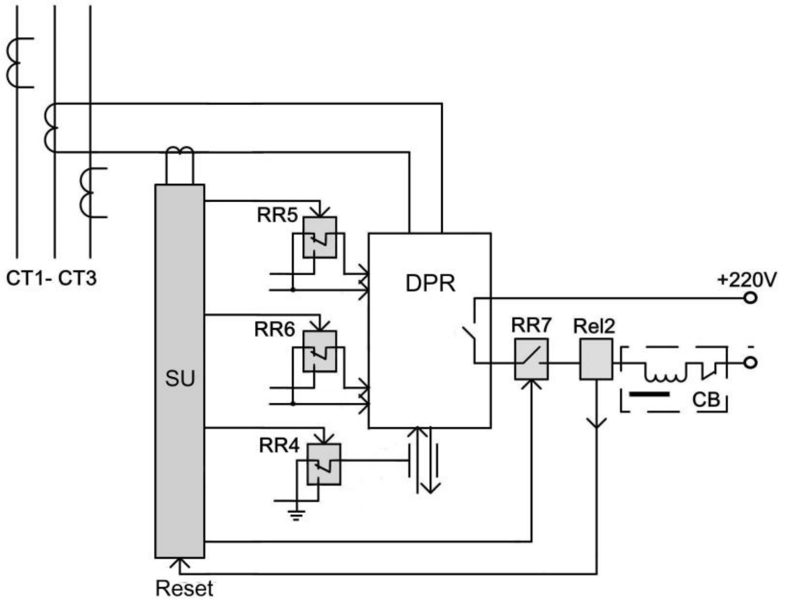

Fig. 1 Principle of protection of digital protective relays (DPR) suggested in [1]

However, due to a negative trend of adding extra functions to DPRs, which have nothing to do with relay protection functions (this issue was touched upon earlier [2]), implementation of the suggested protection principles of DPR will be complicated in some instances. I am referring to the wide usage of DPR for remote control of circuit breakers (RCCB) [3 - 5]. Obviously, usage of the DPR in this way has nothing to do with functions of relay protection, but rather remote control of DPR via communication channels in order to change the circuit breakers position is difficult to be distinguished from a cyber attack by means of hardware.

As mentioned before, the problem of increasing the reliability of relay protection cannot be solved when DPR functions are combined with those that have nothing to do with relay protection, such as power equipment on-line monitoring, remote control of circuit breakers, etc. DPR should be used to fulfil objectives of relay protection only. A fortiori, in order to solve other problems, such as monitoring of power equipment's many specialized devices (from simple relays, for supervision continuity of trip coils circuit of a circuit breaker to sophisticated complexes, which provide real-time control of the composition of gases dissolved in transformers oil or the level of partial discharges in insulation) are available in the market. It is considered that RCCB should also be separated from relay protection and performed by separate hardware. This is the only way to increase the reliability of relay protection and ensure its efficient protection from intentional remote destructive impacts.

This separation will not only allow providing highly efficient protection of DPR, but also allow implementing a protected remote control of circuit breakers (PRCCB).

II. SOLUTION FOR THE PROBLEM

The suggested PRCCB system (see Fig. 2) is a hybrid, which combines both a digital controller with a network channel of data transfer and a cable channel with an electromechanical relay. The main purpose of the system is to prevent an unauthorized change of circuit breaker position during a cyber attack and failures of electronic devices incorporated in the system. The secondary objective of the system is to increase its survivability and maintain its working capacity after IDEI. The overall idea of the system is that any command for changing the circuit breaker position is transferred via a computer network and should be confirmed by short pick-ups of an electromechanical relay at a substation by energizing its coil via an ordinary control cable. Why is it necessary to use the electromechanical relay and why can't we use a communication channel based on fiber-optic communication system (FOCS) for the confirmation command?

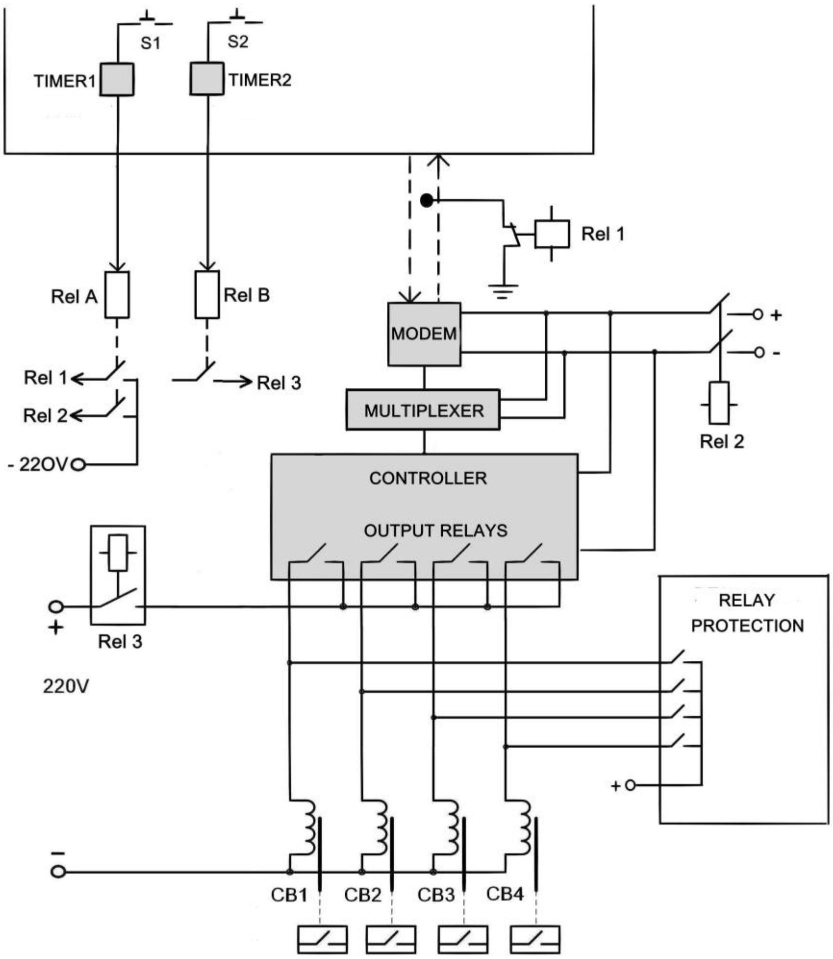

Fig. 2 The offered structure of protected remote control system of CB. Power supply circuits and CB trip coils are shown provisory to simplify the diagram

The problem is that FOCS does not provide protection from IDEI, since they are equipped with complex digital multiplexor switches on both sides, which can translate electric signals into light signals on one end of FOCS and restore electric signals on the other end. Our studies on several types of multiplexor switches show [6] that they cannot bear even a standard high voltage impulse as required by electromagnetic compatibility standards. If the internal microelectronic components of the FOCS are broken under IDEI, the condition of their output circuits will be unpredictable. If a broken FOCS is not able to send a remote command for the CB, there will be no disaster, but if its output circuits are actuated, the problems will be inevitable. The same is applicable to all other components of a PRCCB system (modem, controller, etc).

Besides, since fiber-optic communication channels with all mating equipment is rather expensive, there is a tendency to refuse the use of dedicated FOCS and use the existing computer network channels based on twisted-pair wires instead. Moreover, in order to further reduce the costs of control systems, relay protection and automatics even more, a transition to WiFi technology is under thorough investigation now. In any event, many of the world leading manufacturers of DPR already produce them with built-in WiFi modems. In fact, the idea of converting all power electric equipment to communicate over standard computer networks, including wireless, is a central idea of the Smart Grid concept. In connection with this, the development of special hardware (which is not connected with computer networks and is highly resistant to IDEI) for increasing security of relay protection and CB remote control system from intentional remote destructive impacts, including electromagnetic impacts and cyber attacks [7] has become relevant. This is why electromechanical relay controlled by auxiliary voltage via control cables to act as elements of such protection is selected. In order to protect the additional communication channel from malicious external connection and unauthorized actuation of electromechanical relays, the wires of different control cables are used in addition to two relays, namely RelA and RelB, instead of one (see Fig. 2). Of course, the coils of these relays and current leading cable wires through which the relays are powered should be protected (e.g., by means of variable voltage resistors) from high voltage impulse events, which can be applied to these wires under powerful electromagnetic impulse of IDEI. In addition, it is recommended that these relays should be powered by alternating current of industrial frequency with a capacitor connected in series and a splitting transformer can be used on the side of a substation. These measures will allow preventing actuation of RelA and RelB from current of extremely low frequency applied to underground cables under electromagnetic impulse’s E3 component’s effect [7].

In the suggested system, any command for changing the CB position transferred via a network channel of any type should be accompanied by a short-term, remote turn-on of RelA and RelB via the control cable. The contacts of these relays energize local electromechanical auxiliary relays: Rel1 (unblocks the network communication channel), Rel2 (supplies power to electronic devices of the system) and Rel3 (turns on the power supply circuit of CB trip coils). These local relays can be different in terms of their characteristics. For example, Rel1 is a high-frequency relay; Rel3 is a relay with powerful contacts designed for switching the inductive load on direct current. The availability of two control relays – RelA and RelB – with separate control channels increases the protection of the system from unauthorized access.

The first to pick-up is RelA; after the necessary information about the changing position of a certain circuit breaker is transferred to the controller and the closing of contacts of a corresponding output controller’s relay, RelB will be pick-ups and energize Rel3 by its contacts. The time during which RelA and RelB remain energized is controlled by timers in order to prevent continuous engagement of these relays because of human error. In fact, this is a short period of time during which it is almost impossible to undertake an effective cyber attack. The blocking of the communication channel and disconnection of the controller’s power supply beyond this short time period eliminates the danger of preliminary actuation of output controller’s relays as a result of a cyber attack with the further unauthorized changing of CB position when electromagnetic relay RelB is energized. The same measures will dramatically reduce the probability of failures of sensitive electronic equipment (modem, multiplex and controller) as a result of IDEI.

After a registered cyber attack or electromagnetic impulse, the remote control of the circuit breakers should be prohibited until a special check, since the condition of the controller after such impacts is not known.

The output controller’s relays can be standard and low voltage; this type is usually installed on controllers. However, Rel3 should have contacts that can be compatible with switching powerful inductive load (CB trip coils) at direct current 230V.

Analysis of specifications of widely spread electromagnetic relays shows that the majority of them are not designed for the switching (and even turn-on) of inductive loads at 230VDC [8]. Specially designed relays are used for this purpose: they ensure multiple series breaks in a switched circuit (Fig. 3) or they accommodate a continuous magnet near the contacts, designed to push out the electric arc from the inter-contact gap (Fig. 4). There are also relays with triple series breaks per contact, Fig. 5, which can control trip coils of old-style high voltage circuit breakers consuming high-ampere current.

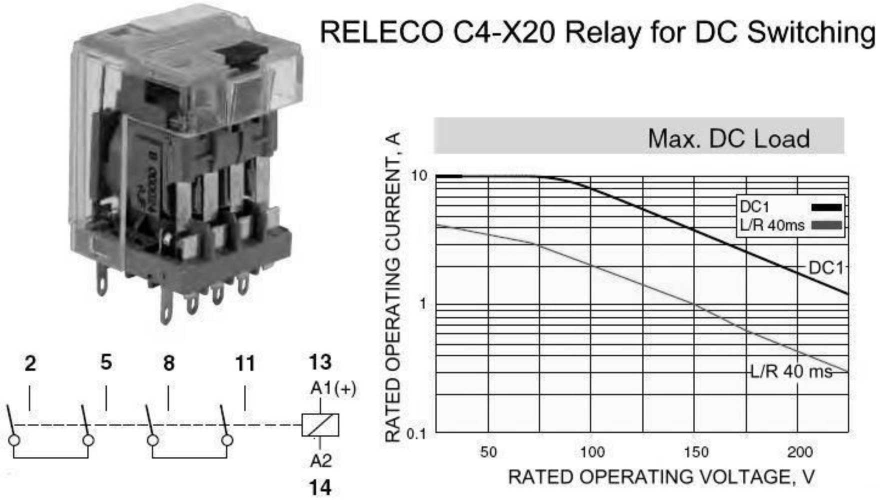

Fig. 3 The C4-X20 (RELECO) relay type (with partially removed casing) with two double break contacts and high switching ability at DC

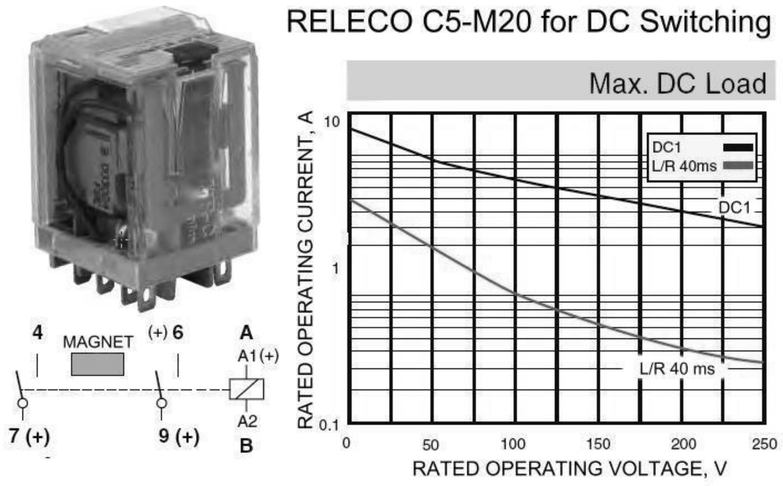

Fig. 4 The C5-M20 (RELECO) relay type with two make contacts and a blowout magnet for increasing switching ability for inductive load

Fig. 5 The RMEA-FT-1 (RELEQUICK S. A.) relay type with one triple make contact, capable of switching currents up to 3A in an inductive load at 220VDC

In those cases where the use of a control cable to control RelA and RelB is not possible due to the remoteness of a control station from a substation, it is possible to use FOCS as a permitting communication channel. However, the decrease of the system’s protection level from IDEI should be kept in mind. In order to prevent the occurrence of spontaneous commands for changing CB position due to the failure of electronic equipment of the system, they should be equipped with a self-diagnostic feature: the FOCS channel should be equipped with a continuous monitoring of its own soundness as well as the position of RelA and RelB, whereas the controller should be equipped with a self-diagnostic system, which is automatically actuated immediately after Rel1 and Rel2 actuation and including a status scan of output relays (they should be off) and the validity of the operation of the communication channel.

When a failure is detected, the self-diagnostic system should block further operation of the controller. The use of the system for remote control of circuit breakers should only be allowed when the control station receives information about operating efficiency of all the elements of the system.

III. CONCLUSION

The suggested system will dramatically increase the security of remote control of circuit breakers from intentional destructive electromagnetic impacts and cyber attacks. You can see that in both cases, i.e., for DPR protection [1] and for RCCB protection, electromechanical relays are used. However, the use of these relays is different due to the different operating algorithms of DPR and PRCCB. In the first case, the command to the circuit breakers is sent automatically when the controlled operation mode of power network or utilities equipment is changed, whereas in the latter case, the command is sent manually by operators working at the control station. This results in different principles of implementation of protection. In the first case, it is important to protect the DPR continuously working in the automatic mode from unauthorized changes of its settings or internal logic, which induces actuation of output relays, and it is impossible to check the validity of commands before actuation of the relays. Besides, it is impossible to send a sort of a permission signal to the DPR in case of an emergency mode in the control circuit. This permission signal should be generated on the spot as a result of the power network emergency mode.

However, in the latter case, when the protected object (PRCCB) is not operated in the automatic mode, the task becomes much easier, making it possible to use an external permission signal. In addition, in critical situations, the PRCCB can be cancelled completely. These natural differences in principles of implementation of protection from intentional destructive impacts justify splitting of tasks of relay protection and remote control of circuit breakers.

Obviously, specific circuit configurations can be different from those described in this article. However, the suggested solution will definitely increase the reliability of PRCCB.

The simplicity of the described device makes it possible to quickly arrange its production at any enterprise manufacturing electronic devices.

REFERENCES

[1] Gurevich V. I. Device for Protection of Relay Protection. - Scientific Journal of Electrical Engineering, June 2013, Vol. 3, Iss. 3, pp.52-57.

[2] Gurevich V. I. Technological Advantages in Relay Protection: Dangerous Tendencies. - Electrical Engineering & Electromechanics, 2012, No. 2, pp.33-37.

[3] MRI(K)3-C – Digital time overcurrent relay with control function and auto reclosing – Woodward SEG GmbH & Co. KG, p.77.

[4] Circuit Breaker Controller - with Arc Flash Mitigation. - PAC World, 2007, Autumn 2007 Issue, p.79.

[5] Relion® protection and control. Generation, transmission and sub-transmission. ABB AB Substation Automation Products, 2013.

[6] Gurevich V. I. Actual Problems of the Relay Protection: Alternative View. - “Electric Power’s News”, 2010, N 3, pp.30 – 43.

[7] Gurevich V. I. Digital Protective Relays: Problems and Solutions. - CRC Press (Taylor & Francis Group), Boca Raton – New York – London, 2010, p.404.

[8] Gurevich V. Peculiarities of the Relays Intended for Operating Trip Coils of the High-Voltage Circuit Breakers. - Serbian Journal of Electrical Engineering, 2007, v. 4, N 2, pp.223 – 237.

Vladimir I. Gurevich was born in Kharkov, Ukraine in 1956, received the PhD in 1986 from National Technical University “Kharkov Polytechnical Institute”, Ukraine.

His employment experience includes: teacher, assistant professor and associate professor at Kharkov National Technical and Agricultural University (electrical engineering disciplines); head of research laboratory in the same university; chief engineer and director of Inventor, Ltd (Kharkov, Ukraine). From 1998 he has worked as Managing director of Elprocom Ltd (Israel) and today at Israel Electric Corp. as an Engineer-Specialist and Head of the section of the Central Electric Laboratory. In 2006 he became an Honorable Professor.

Dr. V. Gurevich is author of 10 books, more than 160 articles and more than 100 patents.