RIGA TECHNICAL UNIVERSITY
Faculty of Power and Electrical Engineering
Institute of Power Engineering

Mārtiņš Silarājs
Doctoral student of the Power Engineering doctoral study programme

METHODS AND MEANS FOR TESTING RELAY PROTECTION AND AUTOMATION COMPLEXES

Summary of the Doctoral Thesis

Supervised by
A. Sauhats,
Dr. habil. sc. ing., Professor

Riga Technical University Publishing House
Riga, 2012

Silarājs M. Methods and means for testing relay protection and automation complexes.
Summary of the Doctoral Thesis. – Riga: RTU, 2012. – 34 pages.

Printed in accordance with Record No. 1 of RTU Doctorate Council P-05 (Power and Electrical Engineering) dated July 2, 2012.

THIS DOCTORAL THESIS
HAS BEEN SUBMITTED FOR THE AWARD OF A DEGREE OF DOCTOR OF ENGINEERING SCIENCES
AT RIGA TECHNICAL UNIVERSITY

This Doctoral Thesis for the Degree of Doctor of Engineering Sciences (Power Engineering) is to be defended in public on 22 November, at the Faculty of Power and Electrical Engineering of Riga Technical University, 1 Kronvalda Blvd., room 117.

OFFICIAL REVIEWERS

Professor **Vladimirs Čuvičins**, Dr.habil.sc.ing.
Riga Technical University, Faculty of Power and Electrical Engineering, Institute of Power Engineering

Lead Researcher **Diāna Žalostība**, Dr.sc.ing.
Riga Technical University, Faculty of Power and Electrical Engineering, Institute of Power Engineering

Deputy General Director of Science
Dmitry Lyubarsky, Dr.sc.ing.
JSC "Institute "Energosetproyekt"" (Russia)

DECLARATION

I hereby declare that I have worked out this Doctoral Thesis, which has been submitted for review at Riga Technical University for the award of a doctoral degree in the field of engineering. This Doctoral Thesis has not been submitted to any other university for the award of a scientific degree.

Mārtiņš Silarājs.....(signature)
Date .....

The doctoral thesis has been written in the Latvian language and consists of an introduction, four chapters, a conclusion, recommendation for future work, as well as a bibliography. The total volume of the paper is 131 pages in computer setting. The paper contains 2 tables and 58 figures. The bibliography consists of 88 used literature sources.

THE TOPICALITY OF THE SUBJECT

Over the recent 100 years, electric power has become the basis for the functioning of modern civilization. Since electric power is easy to transmit and transform, its application field is very wide as compared to other types of energy. In order to ensure consumers with electric power, power systems are set up, which consist of electric power production, distribution and transmission companies. From time to time, abnormal or emergency operation conditions emerge in power systems; many of these sets of conditions start by short circuits in a certain element of the power system. To eliminate the short circuits and disconnect the damaged elements of the system, it is necessary to set up quick-response, human-independent protection systems, the response time of which would be measurable in tenths of a second. The setting up of an independent protection system for a power system is a long and complicated [1] process, which is based on relay protection and automation (RPA) complexes with a task to, as dangerous conditions emerge, adopt a correct decision regarding the disconnection of the damaged element of the power system.

Relay protection and automation perform a very important and responsible task. Incorrect action of these devices may cause immense economic and social losses. Therefore, for many years already, accomplishment of RPA and increasing of reliability receive much attention worldwide; dedicated conferences are organized and hundreds of scientific publications are written. Significant contribution to the development of RPA and increasing their reliability was made by a number of Latvian and foreign scientists: Veniamin Fabrikant, Jānis Putniņš, Voldemārs Putniņš, Antans Sauhats, Kārlis Briņķis, Vilnis Krēsliņš, Vladimir Chuvichin, Jānis Rozenkrions, Alexei Fedoseyev, Jānis Bubenko,Goran Anderson, Mladen, Kezunovich and others. RPA hardware is produced by world-famous companies: ABB, Siemens, Alstom, General Electric, Sneider Eelectric, Hitachi, and others. Nowadays, the degree of technical accomplishment and reliability of relay protection and automation devices is very high, yet also today, as can be seen from statistics, device failures take place and consequent damages are incurred, thus the wish to increase the quality and reliability of RPA remains a topical issue.

When forming the RPA of a power system, the following peculiarities of the power system have a very important role:

1. The scale of the system encompassing millions of facilities operating jointly; besides, the territorial coverage of the system. Arguably, the number of RPA devices exceeds the number of primary devices (power transmission lines, generators, transformers, etc.). At the same time, RPA devices, similarly to the primary ones, may fail and cause large-scale emergencies.
2. Indetermination of structure and parameters, influence of random factors;
3. The dynamic nature of development. Power systems develop continuously [4]. New energy sources and power transmission lines are being built; new power consumers are connected. Therefore, relay protection and automation devices have to be able to adapt to the new working conditions;
4. The capital intensity of the power system and its control. RPA has to be reasonably cheap and capable of performing the planned functions over several decades.;
5. The operating conditions of RPA. Many power facilities that generate or transmit considerable capacities, operate in the conditions of an intensive electromagnetic field, which means that it becomes necessary to take into consideration sources of interference The operating conditions (temperature conditions, humidity, vibration, etc.) are rather severe.

As a result of the influence of the above-mentioned peculiarities, the basic requirements to RPA can be formulated:

- Reliability;
- Technical efficiency;
- Economic efficiency;
- Ability to operate at variable conditions and modes.

To ensure compliance with the requirements set for RPA devices, it is necessary to conduct their testing at the development, introduction and operation stage. Upon an analysis of the statistical data of RPA operation, it can be seen that conformance to the above-mentioned requirements is ensured in 95...98% of the cases. To ensure correct operation of relay protection, testing methods and means are developed, the task of which is to detect a relay protection failure before the emergence of an abnormal mode in the power system and to point to the faulty element as precisely as possible.

Over the last twenty years, it is generally accepted practice to use microprocessor element basis in the creation of reliable, economically efficient and technically accomplished anti-emergency systems.. The use of microprocessor equipment offers new opportunities in developing complex, technically accomplished relay protection and emergency automation devices working within a united system. Many researchers are working in this direction and thousands of publications are available. Very rapid development of hardware and software is evident. New equipment is rapidly entering the practice of power systems operation. When comparing the situation in RPA equipment in the Baltic countries and in the industrially developed countries, a considerable lag can be observed both in the applications and, especially, in the manufacturing of these systems. The world's leading electrotechnical companies (ABB, Siemens, Toshiba, General Electric) had started producing many RPA microprocessor devices on a serial basis. The advantages of this type of devices were proven by operation experience. The practical needs of the power industry of the Baltic countries, their economic situation, as well as the new opportunities to use state-of-the-art microprocessor elements served as a precondition for a practical task: to bring the research and products to a level that would ensure the production of RPA systems in Latvia, as well as their competitiveness in the power systems of Latvia and the neighbouring countries.

Ensuring of competitiveness is encumbered due to the following practical causes:

1. RPA equipment is produced by using state-of-the-art technologies, as well as the possibilities of the famous and powerful companies ;
2. A high level of hardware reliability and other technical indicators;
3. A number of additional technical means are in place to ease the operation of RPA.

At the same time, the relatively high price level of RPA terminals and the proportional share of software prices leads to a wish to try to develop and start producing microprocessor-based RPA terminals in Latvia. When planning the production, it is necessary to consider the considerable differences in the equipment prices as well as the operation and production conditions. Based on the demand in the Baltic countries, the price level of the offered equipment and the production possibilities at small-enterprise conditions, development of RPA for high-voltage lines and facilities looks more attractive. The present study is dedicated to solving some of the tasks and problems of this kind, as well as the performance of universal RPA tasks suited for high voltage (110-330 kV), the structure of the equipment and the algorithms for its testing.

THE PURPOSE OF THE PAPER AND THE SOLVED TASKS

The main goal of this doctoral paper is to increase the level of reliability and efficiency of the power systems of the Baltic countries.
To achieve the set goal, the paper solves the following main tasks:

1. An analysis of the functioning statistics of the transmission part of the Latvian power system has been conducted;
2. A review of the testing methods and hardware has been conducted;
3. An analysis of RP devices and system synthesis sections and tasks has been conducted;
4. A structure of a terminal suitable for testing and performing the relay protection tasks required in the Baltic countries;
5. A RPA virtual testing method has been developed and implemented;
6. An optical communication channels testing device has been developed and implemented for the needs of the relay protections to be used;
7. A complex relay protection and automation device of high-voltage lines has been synthesized and implemented.

THE RESEARCH METHODS USED FOR REACHING THE SET GOAL AND TASKS

1. The methods of mathematical statistics and the Monte-Carlo method.
2. To solve the tasks set by the present doctoral paper, the EUROSTAG software for simulating the electromechanical processes of power systems, recordings of the digital oscillograms of the real-life emergency processes and the protection testing devices FREJA and OMICRON.
3. A specialized relay protection terminal testing software was developed for the purposes of the reasearch.
4. The functions of a global positioning system for the purpose of synchronizing the monitoring of the geographically distant elements.

THE SCIENTIFIC NOVELTY OF THE PAPER

1. Data about the functioning of relay protections and automation in the Latvian power system have been summarized.
2. A new methodology has been developed for testing complicated relay protection and automation terminals.
3. A new structure of relay protection and automation terminals, suitable for testing, has been synthesized.
4. A device for testing relay protection devices and automation communication channels has been synthesized.
5. Testing of distance protections has been performed at the conditions of complicated electromechanical processes.

THE PRACTICAL SIGNIFICANCE OF THE PAPER

The practical significance of the promotion paper is expressed as follows:

1. The proposed structure of relay protection and automation terminals can be applied to a number of devices to be synthesized, as well as used for increasing the reliability level of terminals.
2. A terminal implementing complex protection of high-voltage lines is proposed, which has been produced and is being tested within the Latvian power system. The structure of the synthesized, tested and produced terminal ensures the solution of the complex relay protection and automation tasks of high-voltage lines. Experiments and operation experience confirm the effectiveness and correctness of the adopted solutions.
3. The developed virtual testing methodology and software can be applied for testing the reliability, speed and selectivity of the existing relay protection elements.
4. The developed virtual testing methodology has been applied to the implementation of the Europe-financed projects PEGAS and ICOEURE.
5. Hardware and software for testing the fast communication channels has been synthesized. The hardware has been produced and used at the facilities owned by JSC "Latvenergo".

THE BASIC APPROACHES FORMULATED FOR DEFENSE

1. The usefulness and the advantages of the statistical approach and the Monte-Carlo method in the testing of relay protection and automation terminals.
2. The appropriate structure of relay protection and automation terminals with an additional digital input interface for testing has been synthesized and tested.
3. The structure of a communication channel testing device using GPS functions has been synthesized and tested, the results of the communication channel tests have been collected and summarized and recommendations have been worked out for using them.
4. On the basis of the EUROSTAG software, a relay protection and automation testing hardware complex and software have been synthesized. The complex may be used for testing relay protection and automation during the electromechanical transient processes of power systems.

APPROBATION OF THE PAPER

The scientific results have been reported at the following international conferences:
1. The 2nd International Conference on ELECTRICAL and CONTROL TECHNOLOGIES ECT-2007 – from May 3 to 4, 2007, Kaunas, Lithuania.
2. The 8th IEE International Conference on DEVELOPMENTS IN POWER SYSTEM PROTECTION – from April 5 to 8, 2004, Amsterdam, the Netherlands.
3. The 11th International Power Electronics and Motion Control Conference, EPE/PEMC 2004, from September 2 to 4, Riga, Latvia.

PUBLICATIONS

The results of the doctoral paper have been described in the following articles:
1. A. Utāns, A. Sauhats, L. Leite, M. Silarājs. "Experimental Testing of the Quality of Relay Protection Communication Channels". Scientific proceedings of Riga Technical University. Riga, 2010.

2. A. Sauhats, A. Utāns, M. Silarājs. „Sarežģīta relejaizsardzības un automātikas termināla uz mikroprocesoru bāzes automatizēta pārbaude" ("Automated Testing of a Microprocessor-Based Complicated Relay Protection and Automation Terminal"). Scientific proceedings of Riga Technical University. Riga, 2007.
3. M. Silarājs, A. Utāns, L. Leite, A. Sauhats. "Multifunctional Relay Protection Device for Power Transmission Lines LIDA". The 2nd International Conference on Electrical and Control Technologies, ECT-2007, Kaunas, 2007.
4. A. Sauhats, M. Bockarjova, A. Dolgicers, M. Silarājs. "New Method for Complicated Automation Systems Simulation Test". EPE-PEMC, Riga, 2004.
5. A. Sauhats, M. Bockarjova, A. Dolgicers, M. Silarājs. "New Method for Complicated Automation Systems Simulation Test". THE IEE Developments in Power Systems Protection, Amsterdam, 2004.
6. A. Sauhats, A. Utāns, L. Leite, M. Daņilova, A. Vasiļjevs, M. Silarājs. "THE MULTIFUNCTION TERMINAL OF RELAY PROTECTION AND ANTIEMERGENCY AUTOMATION". Scientific proceedings of Riga Technical University. – 2003. – Vol. 4. – Power and Electrical Engineering No. 8. – Riga Technical University, Latvia (in Latvian).

THE STRUCTURE AND SCOPE OF THE PAPER

The doctoral thesis has been written in the Latvian language and consists of an introduction, four chapters, a conclusion, as well as a bibliography. The total volume of the paper is 131 pages in computer setting. The paper contains 2 tables and 58 figures. The bibliography consists of 88 used literature sources.

1. FAILURES OF THE STRUCTURE OF RELAY PROTECTION, METHODS AND MEANS OF TESTING

Relay protection and automation development stages and structures

The longest period of RPA equipment development, which lasted for about 170 years, is related to the electromagnetic relays as the basic elements of automation structures. The development of the element base of radioelectronics, the emergence of new elements (radioelectronic lamps, semiconductor diodes and transistors, integral circuits, operational amplifiers) resulted in attempts to use these in RPA equipment. Numerous devices and systems were created and applied in practice [5,6,7,8,9]. Yet the following may be stated:

1. Massive replacement of electromechanical RPA relays did not take place;
2. The systems created on the basis of radioelectronic lamps and semiconductor diodes did not find wide practical application. The main reason for this was the insufficient operating reliability as compared with electromechanical systems;
3. RPA semiconductor systems (integral logical microcircuits, operational amplifiers) ensured improvement of a number of technical parameters, broadened the spectrum of the functions to be performed, but also brought about a number of new problems related to the following: maintenance, operation reliability, disturbance stability, etc. This kind of systems came to be used in the automation of especially complicated facilities; individual relay protection types and automation elements became widely applied (fault locators, semiconductor time and current relays, , distance protection devices, etc.);
4. At all the above-mentioned stages, the analog signal processing method and corresponding analog elements were used. RPA devices (starting from the electromechanical ones, to devices based on operational amplifier microcircuits and other microcircuits of the middle level of integration) could be depicted in the form of a structural diagram [10].

It is interesting to point out that in order to achieve the required degree of complexity of electromechanical devices, several generations of microprocessors needed to alternate. The first attempts to use a essentially different information processing method, namely, the digital method, were undertaken in the 1960s [15]. At that time, large and powerful digital electronic machines had been developed, running at a speed of millions of operations per second [16,17]. Still, to enable practical application of the digital methods of information processing in RPA, the following was necessary:

1. Analog/ digital converters of signals. The monitored processes have always been and remain analogous by their physical nature;

2. The economic substantiation of the new solutions. The price of the large computing machines for the implementation of the functions of local automation devices was unacceptably high;

3. Ensuring an adequate level of operating reliability. The large computing machines of that time consisted of thousands of discrete elements, therefore the failure intensity of computing complexes was unacceptably high.

The absence of cheap, reliable analog/ digital converters (ADCs) with sufficiently high technical indicators, the high prices and the low operating reliability of the large computing machines did not allow to apply the new relay protection and automation setup principles. The

creation of microprocessors in the 1970s and the following rapid development of the technical parameters of those elements facilitated the creation and practical application of RPA methods and means, starting from the 1980s.
Digital RPA devices are produced by using the digital information processing methods. In order to implement them, analog/ digital conversion of signals is performed. To convert the monitored analog signals into digital form, the uniform procedure (with equal time intervals of sampling) procedure (there are also other methods of analog/ digital conversion [17], which are practically not used in the implementation of RPA devices).
The initial possibilities of microprocessor elements were considerably limited. Therefore, studies appeared that were directed at the minimization of the requirements set for these elements. Algorithms were proposed that minimized the resource input for the microprocessor elements.
Still soon it became evident that the possibilities of microprocessor equipment and its development tendencies ensure not only free implementation of the traditionally used functions, but also make it possible to implement a number of other RPA functions, which have proven to be very important in the practical application of these devices:

- Self-testing and identification of the faulty units;
- Significantly reduced load on the current and voltage instrument transformers;
- Registration of the monitored processes and the state of the elements in the internal structure;
- Convenience of the input of settings and the reflection of the recorded settings;
- Information exchange with other digital devices, including personal computers;
- Technically simple and relatively cheap connection to communication channels with the purpose of receiving and transmitting information.

The possibilities offered by the new functions were decisive for the practical spread of the devices. In the mid-1980s, their future and advantages became generally recognized and evident. Microprocessor equipment became the basis of the development of many industries and systems. Especially important changes (in terms of the development of relay protection and automation) took place in the sphere of communication and navigation systems. Optical fibre channel networks were set up, an immense speed of information transmission and a high level of reliability was achieved, which made possible a wide use of optical communication channels in RPA systems. Significantly new and important opportunities were offered by the global positioning system (GPS) [11,12,13], by means of which it became possible to synchronize geographically distant measurements.

Failures of relay protection and automation devices, their causes and consequences

Failures in the operation of protection relays leading to severe consequences take place in many of the world's power systems. In the case of any serious disturbance in a power system, an investigation is conducted to assess the causes of the event and draw conclusions. Below follows a description of an emergency where the decisive role fell to one inaccuracy in the RPA device, which resulted not only in technical problems but also in social consequences.
The world's power companies show a tendency to increase the reliability level of the power system. One of the means of increasing the reliability level is to prevent incorrect operation of RPA devices. To better understand the problem, the operation of the RPA devices of the Latvian Power system transmission company was analysed. By conducting this type of

analysis, the intensity of failures and their causes can be determined; consequently, it can be concluded which aspects need increased attention. The analysis has been conducted within the company "Augstsprieguma Tīkls" (*High Voltage Network*) of JSC "Latvenergo". JSC "Augstsprieguma Tīkls" maintains a 330 kV power transmission network with a total line length of 1247.9 km and a 110kV power transmission line with a total line length of 3953.8 km, as well as 14 330 kV substations and 115 110kV substations. The total capacity of the installed transformers is 6904.8 MVA. The 330 kV and 110 kV power transmission networks operate with a solidly earthed neutral. The study has been conducted over a time period from 1998 till 2003 (see Figure 1.10), by determining the annual intensity of RPA device failures δ as follows:

$$\delta = \left(1 - N \big/ N_S\right) \cdot 100\,, \qquad (1.1.)$$

where N – the total number of the correct RPA operations per year;
N_S – the total number of RPA operations per year.

The basis for determining N_S is an analysis of the operation of all the RPA devices involved in the short circuit event. For instance, if there has been a transient short circuit on the line, then a successful operation of the RPA is expressed as the disconnection of the fault from all the ends of the line with subsequent successful or substantiated unsuccessful autoreclosing. Within the time period over which the study was conducted, 2951 RPA device actuations took place, whereof 2874 were substantiated.

The main types of failures of relay protection and automation devices

Any failure of RPA may express itself in three ways:

1. A RPA device is actuated in such conditions (most often, in normal operating conditions) when actuation is undesirable, i.e., a superfluous actuation;

2. A RPA device is actuated in such conditions when actuation is necessary;

3. A fault of the RPA device takes place, which causes the failure of other devices that are to be used at the place of service. For instance, the device causes an overload to the operating voltage source or the measuring circuits and irradiates an increased level of electromagnetic energy. For detecting this type of fault, measurements of power consumption, insulation and radiation level are conducted. The methodology for making these measurements is well-developed and is not the subject of this study, which is dedicated to the elimination of the first two types of failure.

Types and classification of testing methods

The task to test RPA appeared together with the first relays, that is, starting from the 1830s. For solving the task, the following basic methods were used for a long time:

1. Experimental operation of the devices at real-life facilities;
2. Generation of circuits and voltages, their measurement and assessment of the correctness of the response of the tested device. To implement this method, current and voltage sources were necessary, which had to be controlled by a human operator by using corresponding measuring devices. The operator analyzed the operation of the facility to be protected, assessed the possible damage and the current and voltage levels accompanying it;

3. Imitation of fault of the facility to be protected by using physical models of the power system and the facility. Many types of models had been developed and were used. The most complicated ones thereof required dozens of operators, hundreds of square metres of space and were consequently extremely expensive in construction and operation.
4. Electronic computing machines discovered the possibility to use power systems and digital models of their facilities. Digital simulation of the power system RPA device operation processes also allowed to solve RPA testing tasks.. Simultaneously with electronic computing machines, also the fourth way of conducting RPA tests emerged, which was based only on the use of digital models. In this case, instead of testing the device, its software is tested. This approach makes it possible to simultaneously test the method to be used, the algorithms, and the implementing programme.

Before the RPA terminals are installed at the place of service, it is necessary to ensure the essential conformity of this equipment to the wishes of the customer and the standardized requirements set for RPA equipment.

For this purpose, a testing methodology is being developed and the following test types have been conducted.

1. **Development of the testing methodology**. At this stage, it is determined as to in what scope the testing is to be done for the device to be considered fit for putting into operation. In most cases, this is done when the specialist makes himself acquainted with the technical task and the functional solutions of the device. During the development of the testing methodology, the basic requirements for device operation are defined:
   - the conditions for actuation;
   - the conditions for non-actuation;
   - the possible permissible failures, or the conditions that the device in question will not be able to solve. Examples to be mentioned are the so-called “dead” zone in case of distance protection, or the possible situation when the final parameters of the process correspond to the actuation conditions but the development of the process itself contradicts the nature of short circuit.
2. **Testing of the operation algorithm**, in the course of its synthesis. The synthesis is usually performed by analyzing the processes taking place in the facility to be protected. Simplified models of facilities and the heuristic approach are used [25,26]. The majority of the algorithms can be described by equations that operate with complex and logical values:

$$If: \begin{cases} \varphi_1(\underline{X_1}, \dots \dots, \underline{X_K}) \geq 0, then\ L_1 = 1\ else\ L_1 = 0 \\ \vdots \\ \varphi_n(\underline{X_1}, \dots \dots, \underline{X_K}) \geq 0, then\ L_n = 1\ else\ L_n = 0 \end{cases} \qquad (1.2.)$$

where $\underline{X_1}$, ..., $\underline{X_K}$ – the parameters of the vectors of the industrial harmonic of the currents and voltages (the active and reactive component, or the module and the phase).

The decision as to whether or not to disconnect the facility to be protected is made based on the size of the logical values $\underline{L_1}$, ..., $\underline{L_n}$ and the time periods over which these change. In algorithms of the type (1.15.), either consciously or unconsciously, a very significant simplification is made, implying the absence of the higher harmonics and components in the current and voltage circuits . Using such a simplification may be acceptable only in two cases:

a. If a RPA device with a large inertia or a large actuation time delay is synthesized. In these cases, the electromagnetic transient processes attenuate and the

non-industrial harmonics, or exponents, practically disappear from the currents and voltages;

b. If frequency band filters are used in the input circuits.

The first case was characteristic of electromechanical devices whereas the second case, of devices implemented on the basis of integral microcircuits as well as microprocessor devices. The algorithms are tested by using mathematical modelling of the monitored facilities and protections.

3. The **conformity test is performed after the selected algorithm has been implemented in the form of an exact device**. First of all, the capability of the device to operate at the operating conditions (temperature, humidity, vibration level, pressure, insulation levels, ability to withstand overvoltages) is tested. The operating conditions are reglamented by harmonized standards of European and other countries. It is necessary to make sure that the technological production process used for the device is conformant.
4. For a standard-compliant device, a production test is conducted.. The main purpose of the production test is to make sure that the algorithm built into the device effects the selected actions at a sufficiently high degree of accuracy. The industrial test is conducted for all the possible operating conditions (voltage class of the facility to be protected, capacity, various levels of short-circuit currents, line lengths, etc.). The industrial test is usually conducted on several experimental devices rather than one.
5. **The functional test** is usually conducted with the purpose to make sure that the device is suitable to the protection of the facility in question. It can be argued that the functional test is considerably simplified, as compared to the industrial test.
6. The alignment **or technological conformity test**. This type of test is conducted at the place of service with the purpose to make sure that the introduced settings correspond to the needs of the facility in question.
7. **Periodic tests**. These tests are aimed at making sure about the operating capacity of the whole circuit — the current transformers, the voltage transformers, the RPA terminal, and the power circuit breaker. The subject of testing is not only, and not primarily, the operating capacity of the RPA terminal, but also the condition of the external circuits and the assembly. During the periodic tests, the protection settings can be modified or an essential part of the electric circuit may be changed.
8. **Testing after a failure**. This test is performed if a device failure has occurred. Particularly useful information about the operation of the device is available after a short circuit event has actually occurred. Upon a careful evaluation of the records of the processes that have taken place, in many cases it is possible to detect deficiencies in the protection or automation algorithm that are related to the operation of the system as a whole.
9. If additional measures are required, for instance, due to unclear causes of the failure, then **special** tests are conducted.

Relay protection and automation testing devices

Industrially manufactured relay protection testing devices can be divided into two major groups. The first group consists of real-time digital simulators (RTDS), which make it possible to generate processes taking place in complicated power systems.

The testing systems that belong to the second group are capable of generating a fairly limited number of currents and voltages and are foreseen only for testing the local RPA devices. We will term this type of testing systems simplified real-time simulators (SRTS).

Real-time digital simulators

RTDS replace the physical models of power systems that were used earlier, making it possible to configure the topology of a complicated power system, to make changes to it, to simulate electromechanical and electromagnetic transient processes. By using digital/ analog converters and amplifiers, processes are presented in the form of currents and voltages. The number of currents and voltages is limited only by the price of the system and the financial possibilities of the user.

RTDS ensure the following:

- The variable topology of the system to be created. Configurable and multiform models of power system elements are used;
- Simulation of complicated and complex modes is ensured;
- Data input is effected by using a graphical interface and internationally accepted designations;
- The components of the systems to be used ensure a wide range of protection device tests.

RTDS testing systems are applied for power systems with a high-voltage or super-high-voltage electric network [18].

RTDS have a number of advantages. It can be expected that their application will widen as the *Wide Area Protection* concept is turned into practice. The main drawback of the RTDS systems to be mentioned is their price, which may exceed several million euros.

Simplified real-time simulators

The high price of RTDS renders their wide application impossible. In the power systems operation practice, fairly simplified systems are applied. In fact, SRTS developed a testing direction which is based on the generation of currents and voltages with the help of an operator. The operator's work is highly automated. A very significant role in the structure of the device is played by the presence of circuit insulation, which is important when performing tests in real-life conditions. To reflect the testing results, a large number of combinations of influencing parameters are used, along with the "third dimension" — colour, to facilitate the analysis of the results. It can be seen that a full-fledged test of two distance protection zones may require tens of thousands of attempts. All in all, it can be said that SRTSs are suited to simplified conditions, first and foremost, at substations, yet they are insufficient for performing industrial, functional and special tests.

2. THE SUBSTANTIATION AND IMPLEMENTATION OF THE VIRTUAL TESTING METHOD

The essence of the virtual testing method

Summing up the above, we can say that the testing of RPA devices still remains topical and at the same time, all the known methods and the instruments for their implementation have significant drawbacks. For eliminating these drawbacks, a new testing method is proposed, which is called the virtual testing method. The essence of this method as follows:

The testing procedure is divided into two parts:

1. The binary RPA inputs and outputs are tested, along with the analog circuits and the analog/ digital converter;
2. The RPA implementation method, the selected algorithm and the algorithm implementation software as well as the hardware are tested.

To implement the testing procedure, existing, widely applicable, industrial power system simulation programmes are used. If required, the programmes are equipped with additional blocks, in order to ensure as complete a test as possible;
The implementation of the tests requires a special terminal to be made: it is necessary to ensure the replacement of analog/ digital conversions by the calculation results from a simulating programme.
The essence of the proposed method is reflected in Figures 2.1. and 2.2.

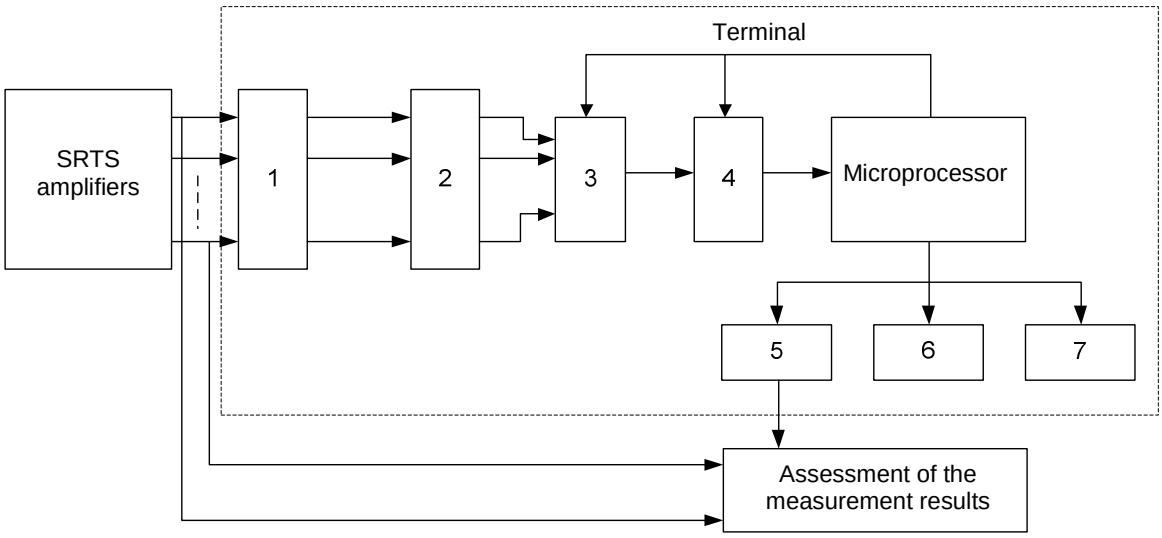

Figure 2.1. Testing the correctness of the analog/ digital conversion process. For the titles of the units, see Figure 1.2.

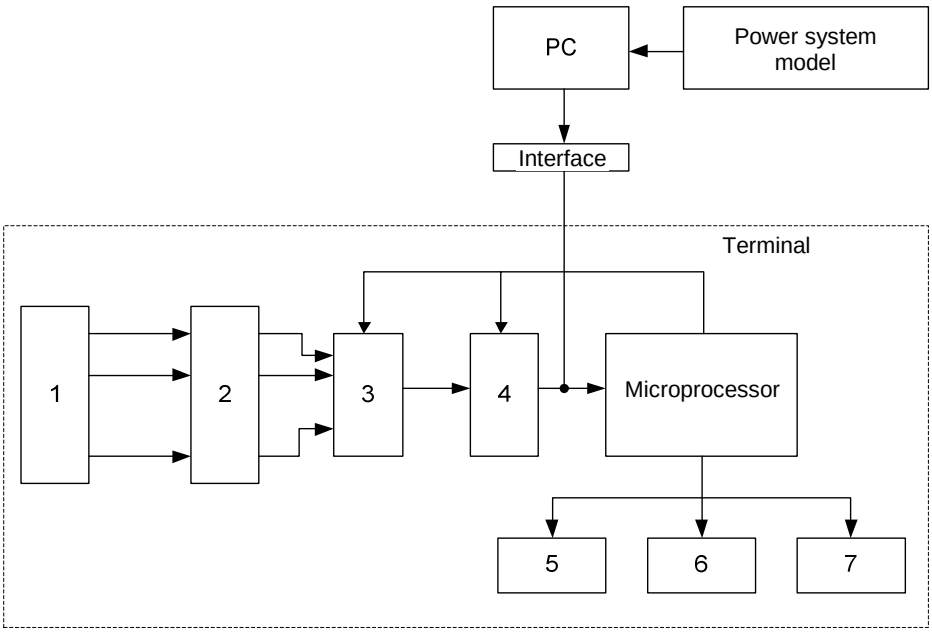

Figure 2.2. Testing the method, the algorithm software and the digital hardware.

Testing and determination of the number of tests

To determine the way the tests are conducted and their number, let us perform the mathematical formulation of the task. For this purpose, let us define a γ-dimensional function ***R***, assuming that ***R*** describes the condition of the output signal of the terminal (R can assume only two values, 0 or 1):

$$R = R(x_1,\ldots,x_n, l_1,\ldots,l_k, s_1,\ldots,s_e), \quad (2.1)$$

where $\gamma = n + k + e$,

n – the number of the analog signals to be monitored $\underline{X}$ (which in the simplest case is equal to the summary number of the current and voltage vector modules and angles);

k – the number of the signals of the logical inputs to be monitored;

e – the number of the terminal's settings $\underline{S}$.

Let us assume that the γ-dimensional complex of parameters $\underline{X}$, $\underline{L}$, $\underline{S}$ can be divided into two non-overlapping groups, which are shown on Figure 2.3:

1. The group R_1, which corresponds to the terminal's actuation,
2. The group R_2, which corresponds to the non-actuation conditions of the terminal.

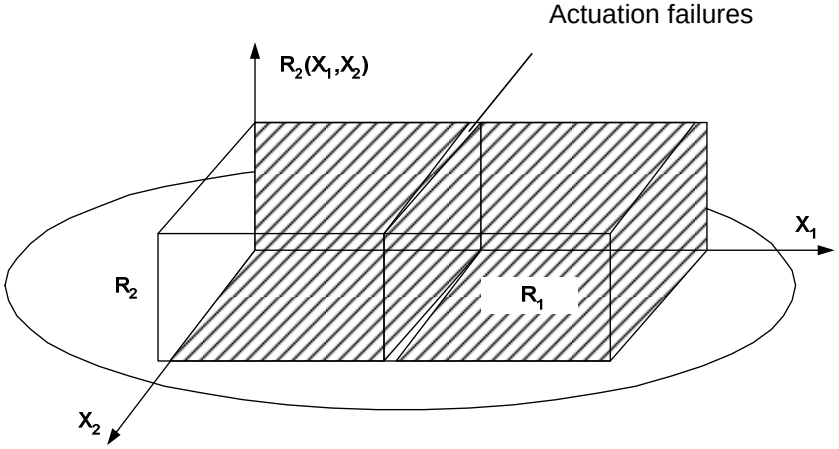

Figure 2.3. Example of a two-dimensional response function

Let us assume that the functions of the parameters $\underline{x}$, $\underline{l}$, $\underline{s}$ are known for each of the groups R_1 and R_2.

Let us also introduce the definition of the ideal terminal, by assuming that this kind of terminal is matched by the function R, which can be described in the following way:

$$\begin{aligned} &R = 1, \text{ if and only if } [\underline{x} , \underline{l} , \underline{s}] \in R_1, \\ &R = 0, \text{ ja } [\underline{x} , \underline{l} , \underline{s}] \in R_2. \end{aligned} \quad (2.2)$$

The parameters of the analog signals to be monitored X and logical signals L depend on the processes taking place in the power system, during which numerous factors of random nature occur (loads and their distribution, generated capacities, structure of the network, presence of short circuit, location and type of the short circuit, etc.). In this way, we can say that X and L are random values. If an industrial test is conducted and the exact element of the power system, for protecting which the tested terminal will be used is not known, then also the settings can be attributed to random values. It is known that for a more complete description of the random values, it is necessary to know the probability distribution function. Let us assume that two conditional distribution functions F_1 and F_2 are known:

F_1 – a distribution function, which corresponds to the conditions when the actuation of the tested device is desirable;

F_2 – a distribution function which was formed at conditions when actuation is undesirable.

Considering the expressions (2.1.) and (2.2.) and knowing the distribution functions F_1 and F_2, we can define the actuation and non-actuation probability rates for an ideal terminal:

$$P_1 = \iint_{R_1} dF_1(\underline{x}, \underline{l}, \underline{s}) = 1,$$

$$P_2 = \iint_{R_2} dF_2(\underline{x}, \underline{l}, \underline{s}) = 0, \quad (2.3)$$

where P_1 – the probability of the protection device coming into action, at the condition that the actuation conditions are fulfilled;

P_2 – the probability of the protection device not coming into action, at the condition that the non-actuation conditions are fulfilled.

If in the implementation of the tested device, errors or inaccuracies have occurred in the software or the elements used, then, in comparison to an ideal device, the response will be different $R_{RE} \neq R$. For a real-life device, it is possible, in any case, to make the following statement:

$$P_1 \leq 1,$$

$$P_2 \geq 0. \quad (2.4)$$

A protection device can be considered tested if the probability values P_1 and P_2 have been calculated. If P_1 and P_2 are sufficiently close to „1" and „0", a decision regarding the terminal operation permit can be made. According to the expression (2.4), the probabilitiesP_1 and P_2 can be determined by using the *Stieltjes-Lebesgue* integral [27]. The integrals of the expression (2.4) can be calculated by means of two approaches:

1. The classical or regular method [28], which divides the integration space into a number of equal areas. The accuracy of this method directly depends on the number of areas used.
2. The Monte-Carlo method. In this case, the accuracy directly depends on the number of attempts.

Below, it is shown how both of these methods can be used for performing relay protection and automation tests. To simplify the task, let us assume that the parameters $\underline{x}$, $\underline{s}$ are within a value range from 0 to 1. The influence of the logical parameters $\underline{L}$ will be disregarded.

As is known, the error of the classical method can be determined according to the following expression:

$$\Delta_1 \approx N^{-2/\gamma}, \quad (2.5.)$$

The error of the Monte-Carlo method can be determined according to the expression:

$$\Delta_2 \approx 1/\sqrt{N}, \quad (2.6.)$$

where N – the number of intervals to be integrated in the classical method or the number of attempts using the Monte-Carlo method, $\gamma = n + e$, assuming that the influence of the logical signals, k, is disregarded.

If the $\underline{x}$ and $\underline{s}$ parameters are assumed freely during the tests and the testing is done for a limited number of combinations of the values $\underline{X}$ and $\underline{S}$, it becomes possible to skip a failure.

Let us assume that we can afford to not find out about those existing failures of the tested device which have a sufficiently low probability Θ. Thus, in order to perform the test with a sufficiently high degree of accuracy, it is necessary to solve the above-mentioned integral equations with an acceptably high degree of accuracy, obtaining the following:

$$\Delta_1 \leq \Theta, \qquad (2.7.)$$
$$\Delta_2 \leq \Theta,$$

Figure 2.4. shows the required number of integral divisions or attempts N, by using both approaches depending on the number of γ, un, in order to obtain the required accuracy Θ.

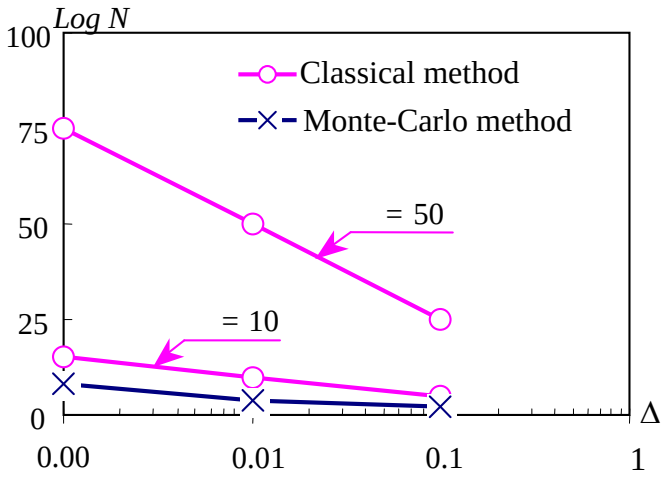

Figure 2.4. The number of attempts depending on the method used and the desirable degree of accuracy

The required accuracies Θ can be approximately determined by finding the "acceptable" probability of relay protection failure P_A. P_A over a period of one year. To determine the allowability of a failure, let us use the following average service time of this type of device until the first failure. Assuming that this time T_{aver} is similar and and using the exponential law of reliability:

$$P_A = 1 - \exp (- t / T_{aver}), \qquad (2.8.)$$

we obtain the following:

$$P_A = 1 - \exp (- t / 25) = 0.04, \qquad (2.9.)$$

Since the required accuracy is to be determined as $\Theta \leq P_A$, then it is simple to determine the number of required tests according to Figure 2.4.

Let us point out that the obtained number is quite close to the statistical data about failures quoted in Section 1.

By analysing the obtained results, it can be concluded that the application of the Monte-Carlo method, as compared to the classical method, becomes more effective, if if γ is greater than or equal to 4.

Taking into account the actually used number of voltage and current inputs, used logical signals and settings, the approach of the Monte-Carlo method is the only really usable one, because for a modern relay protection and automation device γ may be exceed a thousand. This is why the classical method proves inefficient for testing this type of devices.

Implementation of the virtual testing method

The above-described testing method is foreseen for the following relay protection and anti-emergency automation devices:

- out-of-step protection automation;
- protection and automation of high-voltage (110kV/20kV/10kV/6kV) transformers;
- a microprocessor-based high-voltage power transmission line differential protection terminal.

To concretize the testing method, an analysis will be made for the system shown on Figure 2.5., which implements the differential and distance protection of the line together.

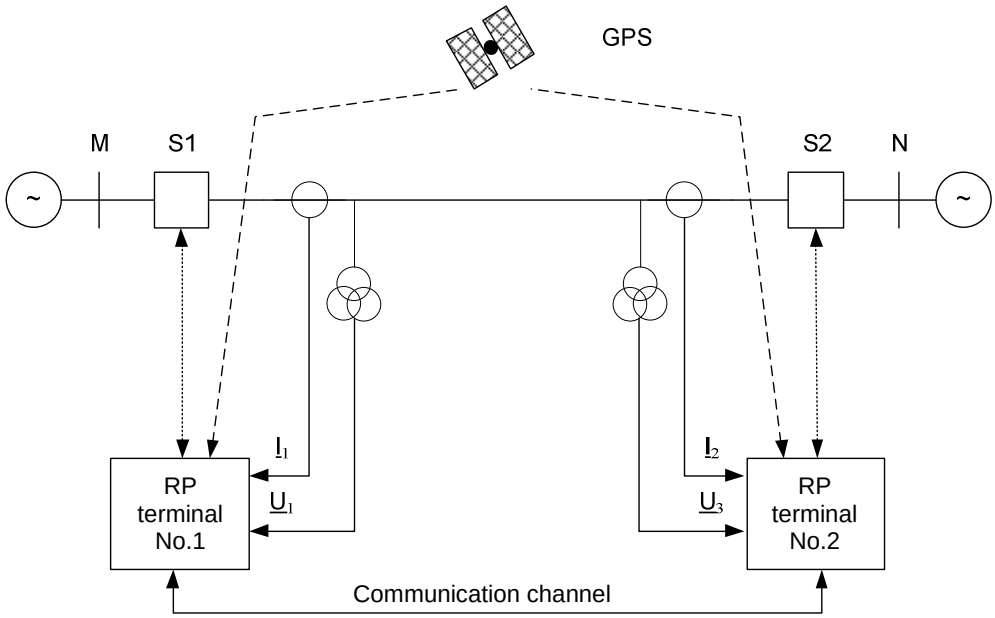

Figure 2.5. Protection diagram for a high-voltage power transmission line

At substations M and N, two RPA terminals are installed; data transmission takes place via an optical fibre channel. Synchronization of measurements is ensured by a global positioning system (GPS) [29]. The terminal comprises the line longitudinal differential protection as the base protection as well as distance protection, maximum current and directional earth fault protection as a backup protection. In addition, the terminal includes autoreclosing, fault location and other functions. Each of the terminals receives the phase currents I_A, I_B, I_C and the zero sequence current $3I_0$ as well as the phase voltages U_A, U_B, U_C and the zero sequence voltage $3U_0$ as well as synchronization voltage from the buses for autoreclosing needs. Therefore, the group of parameters, which describes the fundamental harmonic of the analog signals led to one terminal 18-dimensional (it has to be taken into account that all the parameters are complex). It can be concluded that the total amount of analog signal parameters for a system consisting of two terminals is 36-dimensional. The total number of settings that determine the operation of each RPA for each of the four groups of settings, is a matter of hundreds. Thus the coefficient γ (2.1.) reaches a value of several hundreds, in which case the number of attempts (tests) according to the expression (2.5.) becomes larger than a decimal number with a hundred decimal zeroes. Such a number of tests is neither feasible in terms of time nor in economic terms and the virtual testing method according to the Monte-Carlo principle is the only substantiated solution.

Two approaches to the performance of tests is possible:
1. Testing in the signal parameters and settings area;
2. Testing in the area of the facilities to be protected.

Testing in the signal parameters and settings area

The testing device is shown on Figure 2.6. In this case, testing means transmission of signals freely chosen by the random number generator and the storage of these values in the memory of the tested device with a subsequent response from the ideal device and comparison of responses. This approach has the following drawbacks:

- Transmission of superfluous parameter combinations is possible, which will not emerge in a real-life power system. One example is the generation of large short-circuit currents simultaneously with a voltage that is equal to the nominal voltage or larger.
- Complicated definition of the responses of an ideal device;
- The transmission of signals of an irregular form becomes more complicated (signals, which, apart from the fundamental harmonic, comprise other harmonics or exponential components).

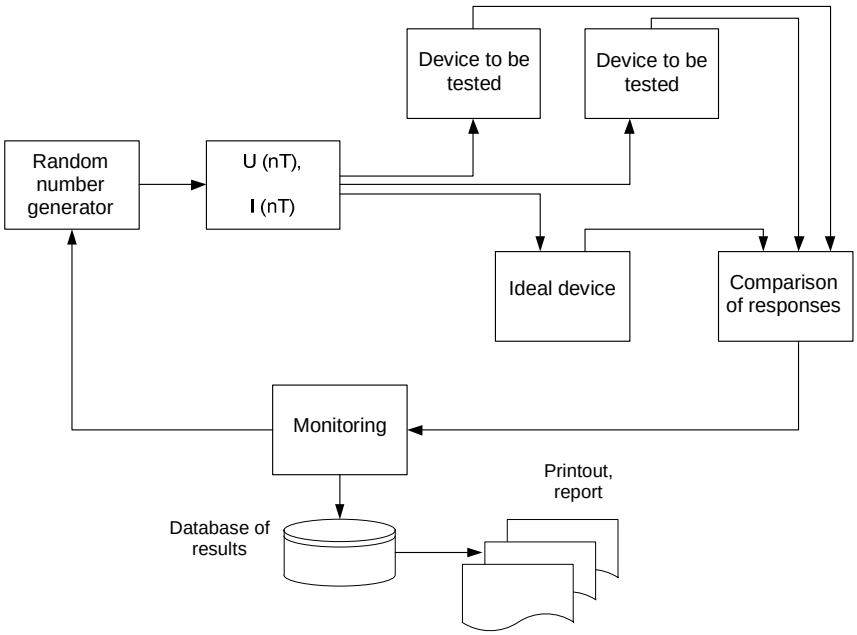

Figure 2.6. Testing a terminal by transmitting a signal into the parameter space

Testing in the parameter space of the power system

Let us look at a highly simplified diagram of the electrical network, which is shown in Figure 2.7.

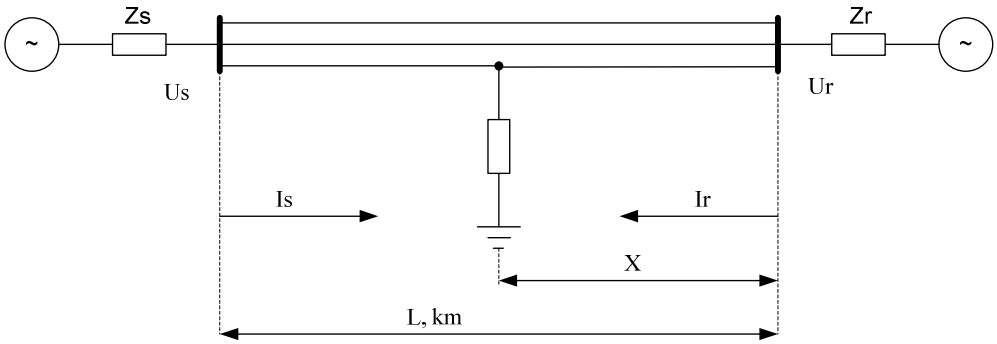

Figure 2.7. A model of a facility to be protected

Let us assume that in the power transmission line protected by device to be tested, there is a short circuit at the distance l_F via the fault transient resistance R_F. The system parameters Z_S, Z_r and the line parameters are variable. Like in real life, the distance to the fault location, the type of the short circuit, and the transient resistance at the fault location are random values. Such conditions of the power system are easy to simulate. When forming the random number generator, it is possible to use the statistical data of power system operation regarding the parameters of pre-emergency modes, short circuit distances and types. The testing procedure is shown in Figure 2.8.

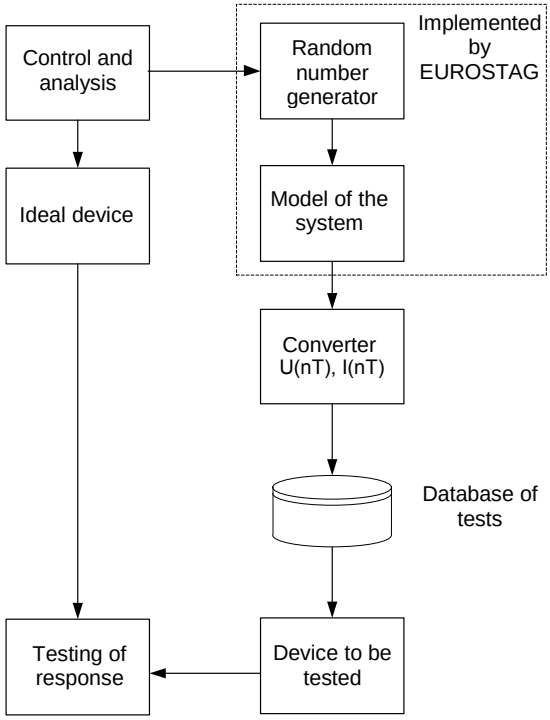

Figure 2.8. The structure of the testing system

3. SYNTHESIS OF A MULTIFUNCTIONAL RELAY PROTECTION TERMINAL FOR POWER TRANSMISSION LINES

Functions and software structure of the relay protection and automation terminal

Since a two-processor solution has been applied for implementing the RPA terminal for power transmission lines (PTL), the task to distribute the software between the processors appears. The chosen software structure is shown in Figure 3.1.

The functions of the equipment are distributed in the following way:
The first processor (CPU1) ensures the following functions:

- Control of analog-to-digital converter (ADC), processing of analog signals and logical inputs (Discrete Signal Register) and control of output relays (Output Relay Register);
- Distance protection (DP), overcurrent protection (OCP), directional and undirectional earth fault protection (EFP), overload protection (OLP) and breaker failure protection (BFP);
- Autoreclosing (AR);
- Oscillographic testing of analog and digital signals in nonvolatile memory (NVRAM) [30];
- Registration of events;
- Distance-to-fault location;
- Control of the indication display;
- Control of the settings input unit;
- Control of the oscillogram and settings reading/input interface RS-232.

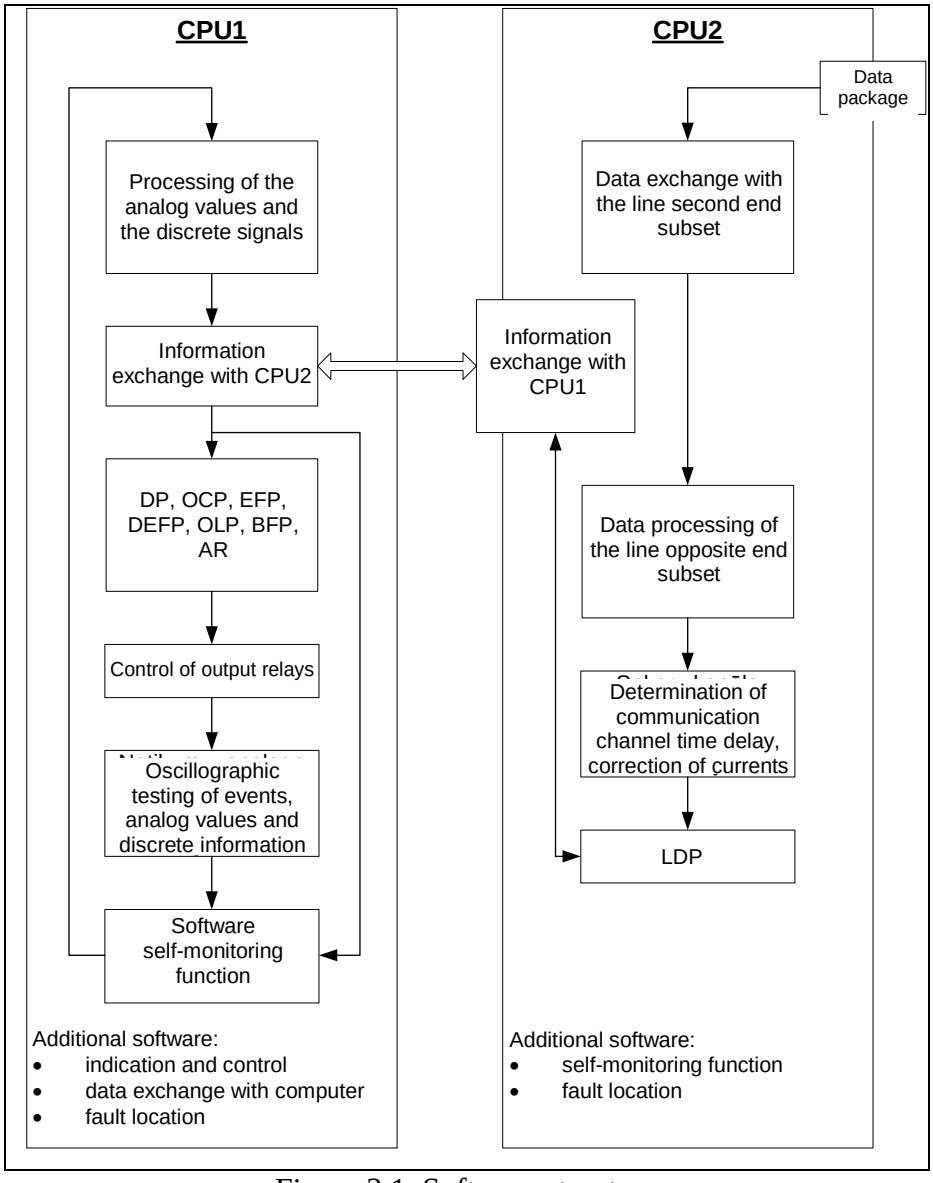

Figure 3.1. Software structure

The second processor (CPU2) ensures the following functions:

– Control of information exchange interface RS-422 for both subsets;
– Correction of the second subset angular error that emerges during data transmission;
– A GPS module control programme;
– Longitudinal differential protections (LDP);
– Distance-to-fault location by using measurements of both subsets.

A high-speed data transmission bus ensures information exchange between both processors. Both processors ensure the self-monitoring function as well as perform monitoring of each other. The programme of the first processor can be depicted as a series of separate programme units, which are run in real time with a cycle of 1 ms. As mentioned above, CPU2 ensures the LDP function. The phase current orthogonal components [31,32] of the first and second subsets are used as the calculated values. CPU1 performs data processing for the first subset every millisecond; data processing for the second subset takes place after data have been received from the opposite end of the line. This means that the LDP operate time directly depends on the speed of the communication channel. The subprogrammes performing service functions operate in the 'background' mode. The RPA terminal operates according to the classical principle [33,34] of comparing the differential current $\dot{I}_{dif} = \dot{I}_1 + \dot{I}_2$ and the braking current $I_{bremz} = \left|\dot{I}_1\right| + \left|\dot{I}_2\right|$. The exchange of data (the phase current orthogonal components) between the LDP subsets is performed in packages. The information package exchange between the subsets is ensured by a digital communication channel. When determining the amount of information in one package, the following is to be taken into account:
– by increasing the amount of information, it is possible to ensure more efficient PTL protection methods;
– by increasing the amount of information, the operate time of the protection increases.
Considering the above, the following information is transmitted in one information package:
– the phase current orthogonal components;
– information about the start-up of the subset (detection of a fault);
– information about the actuation of the subset;
– saturation/ non-saturation of current transformers;
– the state of four binary inputs, which ensure the transmission of separate commands;
– the state of external shutoff signals of differential protection;
– the readings of the internal timers, which are necessary for determining the time delay of the communication channel;
– the check information ensuring the determination of erroneous packages.
The operation principle of LDP is based on measurements conducted at geographically distant locations. Synchronization of measurements is required. Two synchronization principles are known, which are based on the following:

1. Using the possibilities of the communication channel by means of sending a signal to the opposite end of the line and receiving a response. Evidently, it is possible to calculate the time (the time delay) necessary for transmitting the signal "forward and back";
2. Using of the possibilities of the Global Positioning System (GPS). It is known that this system makes it possible to synchronize time measurements with an accuracy of microseconds. This accuracy is completely sufficient to ensure the precise operation of the differential protection.

Both measurement synchronization possibilities are provided for the synthesized terminal. Let us call the using of the GPS as the external synchronization. Taking into account the

complexity of the GPS systems, a probability of their failure should be considered. In this case, it is possible to perform the synchronization by using only communication channels.
If the external synchronization of both subsets is not used or is out of order, then the first subset current vectors $\dot{I}_1$ are synchronized with the second subset current vectors $\dot{I}_2$ by determining the time delay of the digital data transmission channel.

The unequal transmission time delay effect

For synchronizing the current measurements at both ends of the line, each subset calculates a delay time of the communication line. It is assumed that the communication channel is symmetrical. In case of the symmetrical communication channel, the delay time of the information to be transmitted is equal to the delay time of the information to be received. The asymmetry of the communication channel can affect the operating capacity of the protection. The permissible asymmetry value can be found on the basis of certain settings, which are determined by the protection actuation characteristic curve. If the transmission times in both directions, from slave to master and from master to slave, are not equal, a current measurement error will occur. In the transient mode, both amplitude and phase will change and this will cause a differential current that is larger than that in the steady-state mode. When the transmission times are not equal, the only possibility to avoid an incorrect action is to set the settings at a higher level than the expected "false" differential current.
By using the synchronization signal from the GPS module, it is possible to synchronize the LDP subset measurements, which are not affected by the time delay and asymmetry of the communication channel. A schematic diagram of the longitudinal differential protection by means of using the GPS synchronization.
The GPS module receives the information from the earth satellites by generating a synchronization pulse and standard time signals. Both differential protection subsets, LDP1 and LDP2, perform the processing of the controlled values (current and voltage) at the moment when the synchronization pulse arrives from the GPS module. In this way, both subsets exchange their phase current orthogonal components, which are time-synchronized. The GPS module sends a synchronization pulse in every 10 ms. If the information transmission delay from one subset to the other does not exceed 10 ms, this delay do not affect the operation of the differential protection. The protection continuously monitors the presence of synchronization. If the synchronization pulse fails to appear in at least one subset, the protection automatically changes over to a mode, in which the communication channel time delay is calculated. When the synchronization signals appear in both subsets again, the protection automatically changes over to the synchronized data exchange mode. In this way, the failure of the GPS synchronization device will not affect the LDP operation.

The results of the protection of microprocessor operation and their analysis

The above-described microprocessor terminal was implemented and installed for the 110 kV power transmission lines. After installing it on one of the lines, two short circuits occurred, which makes it possible to evaluate the viability of the proposed solution.

A description of the power transmission network section to be protected

The substations "Bolderāja 1" (133) and "Bolderāja 2" (136) are connected via a 1.7 km long power transmission line; the substations "Bolderāja 1" and "Imanta" (130) are connected via a 7.7 km long line. Between the substations "Bolderāja 1" and "Imanta" there is a 1.2 km long branch line to the substation "Daugavgrīva" (132). Since the lengths of the lines are not large, the longitudinal differential protection is to be used for protecting the line against faults, which will ensure quick and selective tripping of a faulty line.

Distance protection is used as the backup protection. In case of a fault in the line, quick tripping is ensured by transmitting commands between both substations.

Analysis of short circuits and the results of fault locators

On March 18, 2005, the line longitudinal differential protections "LIDA" (effecting the tripping of power breakers) were put into operation at the substations "Bolderāja 1", "Bolderāja 2" and "Imanta". Within less than a month and on April 2 and 7, earth faults occurred on the line LNr.233 "Bolderāja 1" – "Bolderāja 2". On April 2, no fault was found on the line (see Figure 3.2.). On April 7, it was found out that birds had tried to build a nest at a distance of 2.88 km from the substation "Imanta".

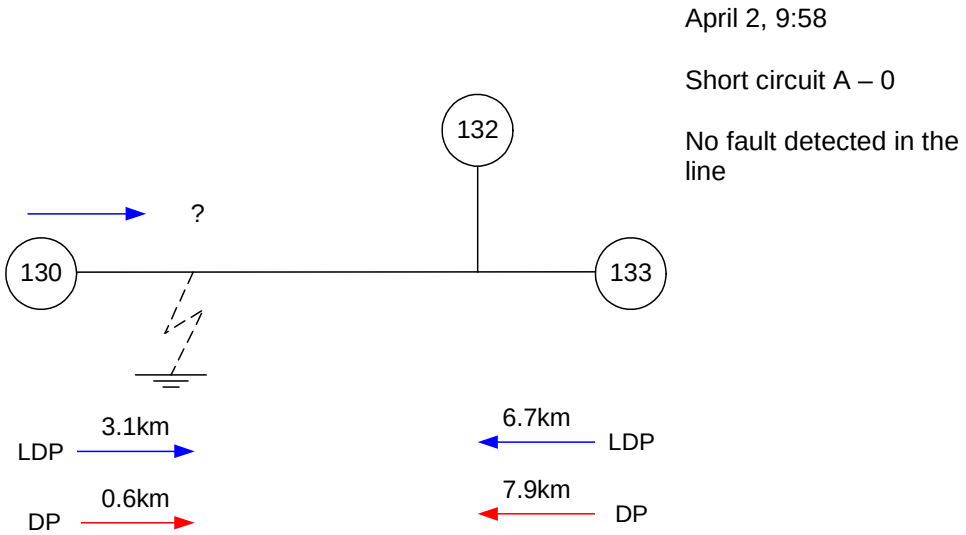

Figure 3.2. Short circuit in the 110 kV power transmission network on April 2

Note: LDP – the fault location detected by using the information from both ends of the line;
DP – the fault location detected by using the information from one end of the line

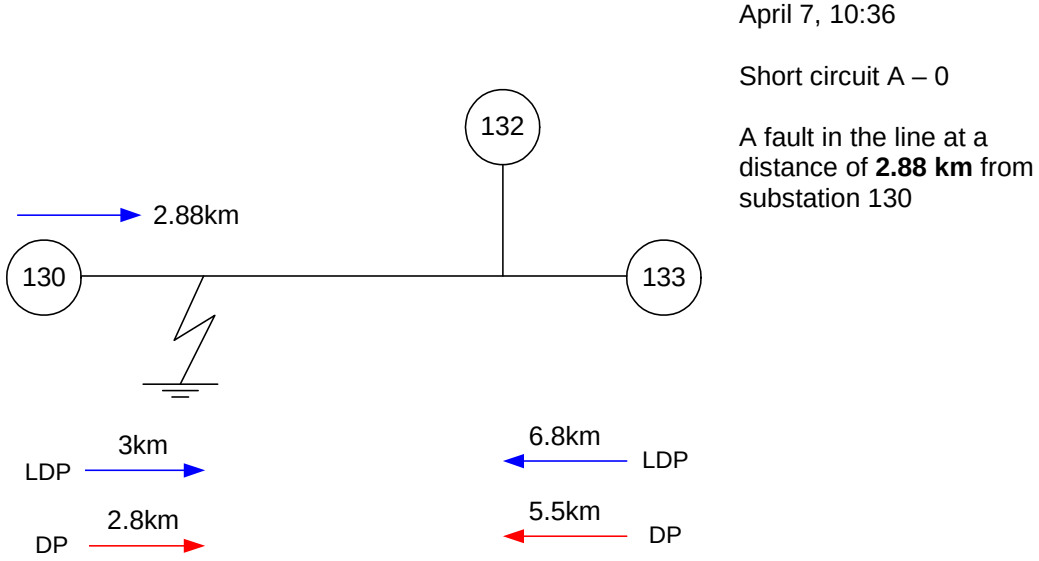

Figure 3.3. Short circuit in the 110 kV power transmission network on April 7

The short-circuit currents from the substation "Imanta" were comparatively large: 10.6 kA and 8 kA. Since the fault was transient, in both cases, the line was re-energized by means of

autoreclosing. During these short-circuit events, two fault locations were detected, since the RP sets contain two fault location algorithms. One of the algorithms for fault location uses measurements from both ends of the line. In this case, the same communication channel that ensures the operation of longitudinal differential protection is used for information exchange. The second distance-to-fault location is detected by using a "classic" algorithm developed by Riga Technical University in the 1990s, which takes into account the measurements only from one end of the line. Both algorithms are used simultaneously so as to ensure the detection of fault location if, for some reason, the communication channel is out of order.

4. INFLUENCE AND TESTING OF LINE DIFFERENTIAL PROTECTION COMMUNICATION CHANNEL

Influence of the time delay asymmetry on the differential current calculation

There is a probability that when transmitting and receiving the information, the time delays are not equal. Hence, it is impossible to correctly determine the angular error of two current vectors. When determining the differential current, the angular error $\Delta\varphi$ between the current vectors occurs. In the 50 Hz system, $\Delta\varphi$ can be found in the following way (in radians):

$$\Delta\varphi = 2\,\pi\,f\,\Delta T_a, \qquad (4.1.)$$

where ΔT_a – the time delay asymmetry, which is determined by the following formula:

$$\Delta T_a = |T_{TX}-T_{RX}|\,/2. \qquad (4.2.)$$

By using the possible angular error, $\Delta\varphi$ can determine the differential current error:

$$\Delta I = I\left(\sqrt{(1-cos\Delta\varphi)^2+(sin\Delta\varphi)^2}\right) \qquad (4.3.)$$

where I – the phase current.

By performing such a recalculation, we can determine, for example, that if the time delay asymmetry is 1 ms, the angular error of 18^0 between the current vectors of the remote terminals will occur [37]. If the telecommunication service provider is not able to ensure the monitoring and compensation of the time delay asymmetry, then additional measures are to be taken in order to prevent a superfluous actuation of the protection. The simplest measure is to raise the protection setting so as to make the protection more insensitive. In this way, we loose one of the main advantages of the longitudinal differential protection – the very high level of sensitivity. Normally, the protection setting is comparable with the line nominal current; besides, this compensation is efficient for the delay time asymmetry of up to 50 µs. If the time asymmetry is larger, then the LDP is practically unable to operate. To ensure a selective operation of the differential protection, it is necessary to set up the following additional blocking functions, which are foreseen for the quality analysis of the communication channel [38,39]:

- Blocking of the LDP function, if the total time delay exceeds the maximum possible value, which is determined by the volume of the current vector memory built in the terminal;
- Short-term blocking of the LDP, if within the certain time period, a repeated change in the total time delay occurs. The change in the time delay can be caused by the change in the path of the multiplexed communication channel. It is possible to determine a new delay time only after receiving the next information package. In

this case, there is a probability that if short circuit occurs outside the protection zone during this time, a superfluous actuation of the protection will take place;

- Blocking of the LDP, if the link with the GPS device is faulty or the synchronization pulse does not arrive in due time. The blocking is necessary, if the used communication channel has an unexpected delay time asymmetry;
- Blocking of the LDP, if the number of faulty packages exceeds a certain quantity. Packages with faulty data appear when there is disturbance in the communication channel and it cannot be used for protection needs.

The statistics of the operation of the differential protection communication channel

For collecting the statistical data, 29 power transmission lines with voltages 330 kV and 110 kV were used, in which interruption of data transmission and disturbances were recorded. Table 4.1. shows the statistics of protection blocking within a year. For collecting the statistical data, terminals with the built-in event recording function were used. A disturbance of the communication channel is recorded, if an interruption of communication occurs (T_{loop} exceeds the set value), or distortion of data is recorded (when transmitting the data, a check sum is calculated, which is transferred to the opposite subset and used for checking the operating capacity of the communication channel).

Table 4.1. Statistics of blocking the differential function of the protection devices

	Protection terminal type 7SD 3	
1	LNr.204	Up to 2 disturbances per day
2	LNr.213	No disturbances recorded
3	LNr.214	Up to 2 disturbances per day
4	LNr.215	No disturbances recorded
5	LNr.216	No disturbances recorded
6	LNr.220	More than 2 disturbances per day
7	LNr.221	More than 2 disturbances per day
8	LNr.609	Up to 2 disturbances per day
	Protection terminal type 7SD 4	
9	LNr.161	Up to 2 disturbances per week
10	LNr.162	Up to 2 disturbances per day
11	LNr.200	Up to 2 disturbances per week
12	LNr.241	Up to 2 disturbances per day
13	LNr.243	No disturbances recorded
14	LNr.244	More than 2 disturbances per day
15	LNr.245	More than 2 disturbances per day
16	LNr.246	Up to 2 disturbances per day
17	LNr.304	Up to 2 disturbances per day
18	LNr.310	Up to 2 disturbances per week
19	LNr.311	No disturbances recorded
20	LNr.313	More than 2 disturbances per day
21	LNr.314	No disturbances recorded
22	LNr.320	No disturbances recorded
23	LNr.322	No disturbances recorded
24	LNr.323	Up to 2 disturbances per week

25	LNr.451	Up to 2 disturbances per week
26	LNr.466	Up to 2 disturbances per week
	Protection terminal type LIDA	
27	LNr.233	Up to 2 disturbances per week
28	LNr.236	More than 2 disturbances per day
29	LNr.151	Up to 2 disturbances per day

As the main disturbance sources, the following have been found out:

- the change in data transmission time;
- the possible asymmetry of the communication channel;
- interruptions of communication.

From the obtained results, it can be concluded that only 28% of the observed differential protection sets was not blocked. 55% of the protection sets are blocked one or two times per week. The frequency of the cases of blocking the other protection sets is sufficiently high for their operation to be considered unreliable.

The device for testing the data transmission channel

The blocking of the LDP due to the appearance of disturbances in the communication channel or the change in the time delay decreases the total efficiency of the protection. Nevertheless, the line is not left without protection, because the back-up of the LDP is implemented by means of the distance protection or overcurrent and directional earth fault protection. Within the time period from 2000 to 2008, some cases of superfluous actuation occurred, when it was not possible to precisely determine the cause of disconnection. This means that during the fault, the oscillograms did not show any fault and any kind of tests did not indicate the possible causes of incorrect actuation. Logically, as a result of the performed analysis, it was concluded that the superfluous actuation of the protection could be caused by the short-term asymmetry of the communication channel time delay.
In order to clarify the causes of blocking the LDP sets and investigate the causes of incorrect operation of the protection, it became necessary to monitor the characteristics of the used communication channel. For implementing the real-time monitoring of communication channel parameters, a special microprocessor device, “Line Tester”, was developed, which should ensure the following:

- The testing of the stability of the communication channel;
- The monitoring of the data transmission process with the integrity check of the data packages;
- The detection, classification and registration of communication errors;
- The detection of time delays of the communication channel:
  - The determination of the total delay of the channel;
  - The determination of the transmission/ reception time unbalance of the communication channel;
- The recording of the time delay shift;
- The measuring and recording of the data transmission frequency and frequency shift of the communication channel.

The communication channel testing device, consisting of two devices (terminals), was connected to the SDH/PDH network by means of the V.35 (X.21) interface (see Figure 4.1.). The information exchange between the devices is implemented by sending the data packages

in series. The terminals operate according to the master/ slave principle. The terminal performing the master function starts the data transmission and monitors the content of the data package. The terminal performing the slave function makes predetermined changes in the data package and sends them to the master terminal. That information part, which is sent between the terminals, is suitable for monitoring the data authenticity and calculating the communication channel time delay. Based on its internal time and the time sent by the second terminal, the master terminal calculates the time delay. The master terminal sends the determined time delay to the slave terminal in every data package.

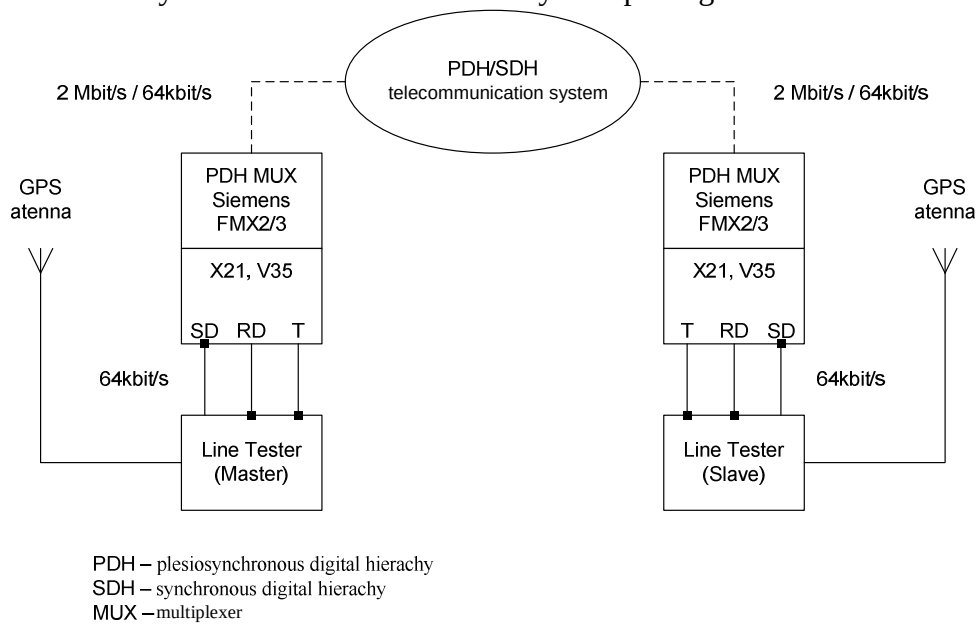

Figure 4.1. Connection diagram for the device "Line Tester"

Based on the local and received information, the total communication channel delay "T_{loop}" is calculated. If a GPS antenna is connected to each of the devices and the devices are time-synchronized, then not only the total delay "T_{loop}", but also the delays separately in both directions, "T_{forw}" and "T_{back}", are calculated. The terminals continuously monitor the time delays and compare "T_{loop}", "T_{forw}" and "T_{back}" with the pre-calculated values. If the difference exceeds the preset value (the start-up setting), the device records all the monitored signal values as an oscillogram. Each of the devices monitors the information exchange process and, in case of an error, calculates them by means of four independent counters:

- A byte error counter, which counts the number of received erroneous bytes;
- A header error counter, which counts the number of data packages transmitted erroneously;
- A CRC error counters, which count the 32-bit check sum code errors;
- A timeout counter, which counts the number of data packages that have not been sent. The data package is considered unsent, if it is delayed for more than 50 ms.

The content of the error counters is also recorded as an oscillogram. All the oscillograms are saved in non-volatile memory of the device and they can be sent to the personal computer as well as viewed by means of a special representation programme.

The results of the practical application of the device "Line Tester"

The device "Line Tester" is used for testing the communication channel of the LDP terminals for 330 kV and 110 kV high-voltage power transmission lines belonging to JSC "Augstsprieguma Tīkls" (*High Voltage Network*). Equal time delays for signal transmission and reception are required for correct operation of the LDP. Below several cases are

described, when the Line Tester helped to explore the LDP unclear operation and indicate the deficiencies or disturbances in the operation of the RPA communication channel.
The LDP equipment installed at the substation No. 60 “Grobiņa” and the substation No. 166 “Venta” on the 110 kV power transmission line LNr.266 several times within a month signalized about periods of disturbed operation, which lasted for not more than 2-3 minutes. The emergency crew that had arrived did not detect any disturbances or faults. The LDP was taken out of operation and the Line Tester was connected to the communication channel. A list of events of the Line Tester is shown in Figure 4.6. With the help of this device, it was stated that within the time period when the LDP communication disturbances were recorded, the total delay time of the communication channel had changed from 2.37 ms to 4.03 ms. In order to prevent unstable operation of the LDP, it was decided to install the GPS equipment, which would ensure the synchronization of measurements at the LDP terminals.
During an external short circuit event, a superfluous actuation of the LDP occurred on the line LNr.247 “Mārupe” – “Zunda”. As a result of the extraordinary testing of the instrument transformers and the protection terminals, an increased unbalance current was stated, the cause of which was not possible to detect initially. It was decided to install the Line Tester, which indicated a communication channel asymmetry of 1.3 ms. After performing the recalculation of the possible differential current in an external short circuit event according to (4.3.), it became evident that the differential current value exceeded the differential protection setting and coincided with the actually stated value. The LDP was taken out of operation until the moment when the communication channel had been adjusted.

Enhancing of the LDP blocking algorithm in the events of communication channel disturbances

The most reliable and efficient solution for the longitudinal differential protection can be synthesized by simultaneously using the optical communication channels and the GPS. Below follows a description of a new LDP operation algorithm, which uses the new opportunities provided by the GPS and, at the same time, takes into account possible failures or disturbances of this system. In this case, it is proposed that a correction of sensitivity should be made instead of effecting complete blocking of the LDP, if necessary. A structural diagram of such an algorithm is provided in Figure 4.2.

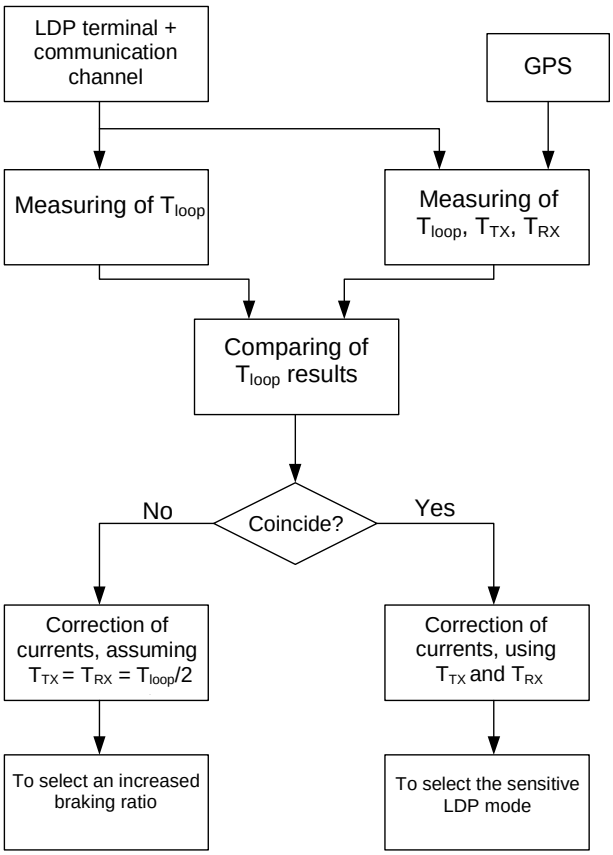

Figure 4.2. A structural diagram for selecting the LDP operation mode

This algorithm is based on the following hypothesis: if within the time interval T_{loop} measurements of two completely different systems coincide, then both systems are considered completely viable. Assuming this hypothesis, the fault of both systems is ignored, which gives erroneous but equal measuring results. Such a possibility theoretically exists, however, the probability of a corresponding event obviously approaches zero. The use of the proposed algorithm makes it possible to maintain the viability of the LDP not only in case of GPS failures, but also in case of a comparatively unstable operation of the optical channel, for example, in case of the changes in the transmission time within a range of 1÷2 ms (for more precise conclusions, additional studies are required).

CONCLUSIONS

1. RPA failures occur due to a number of reasons and diminishing the frequency of their occurrence is still a topical problem worldwide, including Latvia As the functionality of relay protection and automation devices increases, as well as by applying one and the same relay in various power systems, more multifaceted testing of these devices is necessary. The virtual testing method makes it possible to generate testing processes exactly for the processor of the relay protection device. Such a testing complex is cheaper than the classical one, which is made more expensive by the powerful and precise amplifiers. To implement the virtual testing method, it is necessary to install additional memory devices in the testing devices, which should receive the testing cycles and store them in the memory. Also, additional software is needed, which is easy and cheap to implement.

2. The virtual testing method makes it possible to generate testing processes exactly for the processor of the relay protection device. Such a testing complex is cheaper than the classical one, which is made more expensive by the powerful and precise amplifiers;
3. The failures or disturbances of communication channels can case a total relay protection equipment failure. To ensure the quality of used communication channels, the special equipment has been developed and used in the field conditions.
4. In the case of using combined GPS and optical channels gives the opportunity for further increasing of relay protection reliability and efficiency. Given structure, which is capable, to control GPS and optical communication channel at the same time, can assure increased sensitivity of differential protection, if both systems are working properly. In case of GPS failure line differential protection is also available in classical scheme.

Bibliography

1. J. Putniņš. Elektroapgādes sistēmas relejaizsardzības un automātika. (Power Supply System Relay Protection and Automation). State publishing house "Zvaigzne", LV 1013, Riga. 1993. Third revised and enlarged edition.
2. CRIS International Workshop on POWER SYSTEM BLACKOUTS ~ Causes, Analyses and Countermeasures. Lund, Sweden.
3. James S. Thorp, Harles N. Mellowes, Professor in Engineering. The Protection System in Bulk Power Networks. School of Electrical and Computer Engineering. Cornel University. September 8, 2003.
4. Aabø, Y; Goin, R. & Lundqvist, B.: "Risk Analysis: A New Aspect on Protection and Local Control Design", DPSP, Amsterdam, April 2001.
5. M. Igel, P. Schenger. Test Procedures for Protection Devices. AEG ATLAS GmbH and Techniche Universität, Dresden, Germany.
6. IEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems. The Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, NY 10017, U.S.A.
7. Sauhatas A., Loman T., Utan A., Dolgicer A., Leite L. System for Electrical Power Processes Recording. Aktualne Problemy w Electroenergetyce, Gdansk, Jurata, 1997.
8. A. C. Webb. Relay Engineering Services Limites, UK. Computer Generation of Test Quantities for Testing Protection Relays.
9. M. Agrasar, J. R. Hernandez, F. Uriondo, J. Amantegui, J. M. Gallastegui, J.L. Martinez. Optimized Relay Testing Systems.
10. Alexander Dierks. OMICRON electronics GmbH, Austria. New Simulation Models to Dynamically Test Impedance Relays.
11. A Digitally-Controlled, Real-Time, Analog Power-System Simulator for Closed-Loop Protective Relaying Testing. G. Nimmersjo, O. Werner-Erichsen, B. Hillstrom, G. D. Rockefeller. ASEA AB, Vasteras. **Journal Article:** IEEE Transactions on Power Delivery (impact factor: 1.16). 02/1988; DOI:10.1109/61.4239.
12. GPS Synchronized Measurements in Power Systems State Estimation: An Overview R. F. M. Brandao, J. A. Beleza Carvalho, F. M. Barbosa. Inst. Super. de Eng. do Porto, Porto. **Conference Proceeding:** 10/2006; DOI:10.1109/UPEC.2006.367518ISBN: 978-186135-342-9 In proceeding of: Universities Power Engineering Conference, 2006. UPEC '06. Proceedings of the 41st International Conference, Volume: 2.
13. Advanced Synchrophasor Applications. A. P. S. Meliopoulos, G. J. Cokkinides. Sch. of Electr. & Comput. Eng., Georgia Inst. of Technol., Atlanta, GA, USA; **Conference**

Proceeding: 08/2010; DOI:10.1109/PES.2010.5590037 In proceeding of: Power and Energy Society General Meeting, 2010 IEEE.
14. Harmonic Monitoring System via Synchronized Measurements. B. Fardanesh, S. Zelingher, A. P. Sakis Meliopoulos, G. J. Cokkinides. New York Power Authority, New York, NY; **Conference Proceeding:** 11/1998; DOI:10.1109/ICHQP.1998.759956ISBN: 0-7803-5105-3 In proceeding of: Harmonics And Quality of Power, 1998. Proceedings of the 8th International Conference, Volume: 1.
15. Test and Evaluation System for Multi-Protocol Sampled Value Protection Schemes. D. M. E. Ingram, D. A. Campbell, P. Schaub, G. Ledwich. **Conference Proceeding:** 07/2011; DOI:10.1109/PTC.2011.6019243 In proceeding of: PowerTech, 2011 IEEE, Trondheim.
16. Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying. M. G. Kanabar, T. S. Sidhu, Dept. of Electr. & Comput. Eng., Univ. of Western Ontario, London, ON, Canada. **Journal Article:** IEEE Transactions on Power Delivery (impact factor: 1.16). 05/2011; DOI:10.1109/TPWRD.2009.2038702.
17. Comparison of Analog-to-Digital Filter Conversion Methods in a Digital Flickermeter. Soo-Hwan Cho, Gilsoo Jang, Sae-Hyuk Kwon, Jung-Wook Park. **Journal Article:** Electrical Engineering (impact factor: 0.33). 04/2012; 91(3):125-131. DOI:10.1007/s00202-009-0122-1.
18. Comparison of Analog-to-Digital Filter Conversion Methods in a Digital Flickermeter. Soo-Hwan Cho, Gilsoo Jang, Sae-Hyuk Kwon, Jung-Wook Park. **Journal Article:** Electrical Engineering (impact factor: 0.33). 04/2012; 91(3):125-131. DOI:10.1007/s00202-009-0122-1.
19. Z. Wyocki. Silesian. MTZ2 – A Computer Based Relay Test System. Technical University of Gliwice, 44-100 Gliwice, Poland.
20. Marlene Lillian, Stanley I. Thompson. GPS Satellite Synchronized Test System Recreate Fault Conditions to Troubleshoot Protective Relay Schemes.
21. M. E. Agudo WAPA, USA, B. Kasperek, WAPA, USA, S. I. Thompson, AVO International, USA. END-TO-END Relay Testing Using GPS-Synchronized Secondary Injection.
22. Ljubomir A. Kojovic, Timothy R. Day. Cooper Power Systems, Franksville, Wisconsin. Application of Real-Time Power System Simulators for Testing Protective Relay System Operational Characteristics.
23. L. R. Dann, H. J. Vermeulen. Department of Electrical Engineering, University of Stellenbosch. A Transputer Based Waveform Synthesizer for Protection Relay Test and Parameter Estimation Applications.
24. Andrew C. Wevv and Michael Webb. Automated Testing of Power System Protection Relays.
25. Identification and Validation of Dynamic Global Load Model Parameters for Use in Power System Frequency Simulations. J. W. O'Sullivan, M. J. O'Malley, Dept. of Electron. & Electr. Eng., Univ. Coll. Dublin. **Journal Article:** IEEE Transactions on Power Systems (impact factor: 1.94). 06/1996; DOI:10.1109/59.496165.
26. J. Rumbaugh and e. al., *Object-Oriented Modeling and Design*. Englewood Cliffs, NJ: Prentice Hall, 1991.
27. PSS/E-27 Online Documentation, Power Technologies, a division of S&W Consultants Inc., December 2000.
28. Wilson, R. E., Kusters, J.A. International Timekeeping for Power System Users, Developments in Power System Protection. Conference Publication No.434, March 1997, pp. 351-354.
29. Wilson, R. E. Methods and Users of Precise Time in Power Systems, Transaction on Power Delivery, Vol. 7, No 1, January 1992, pp. 126-131.
30. TMS32054x DSP Reference Set. Volume 1: CPU and Peripherals. Literature Number: SPRU131C, Manufacturing Part Number: D425004-9761, Revision A, October 1996.

31. Line Differential Protection with Distance Protection 7SD5. Manual.
32. 110/220 kV Line Protection Terminal LIDA. Manual.
33. Nabae, T. Tanaka, "A New Definition of Instantaneous Active-Reactive Current and Power Based on Instantaneous Space Vectors on Polar Coordinates in Three-Phase Circuits," *IEEE Trans. on Power Delivery*, vol. 11, no. 3, pp. 1238-1243, 1996.
34. E. Emmanuel, "Summary of IEEE Standard 1459: Definitions for Measurement of Electric Power Quantities under Sinusoidal, Nonsinusoidal, Balanced or Unbalanced Conditions", *IEEE Trans. on Industry Applications*, vol.40, no. 3, pp. 869–876, 2004.
35. G. Benmouyal, "The Trajectories of Line Current Differential Faults in the Alpha Plane", Proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 2005.
36. M. G. Adamiak, G. E. Alexander, and W. Premerlani, "Advancements in Adaptive Algorithms for Secure High Speed Distance Protection", *Twenty Third Annual Western Protective Relaying Conference*, October 1996.
37. T. Takagi, Y. Yamakoshi, M. Yamuaura, R. Kondow, T. Matsushima, "Development of a New Type of Fault Locator Using One Terminal Voltage and Current Data", *IEEE Trans*., vol. PAS-101, No. 8, August 1982, pp. 2892-2898.
38. L. Eriksson, M. Saha, S. D. Rockfeller, "An Accurate Fault Location with Compensation for Apparent Reactance in the Fault Resistance Resulting from Remote-End Infeed", *IEEE Trans. on PAS*, PAS-104, No. 2, 1985.
39. A. Sauhats, M. Danilova, "Fault Location Algorithms for Super High Voltage Power Transmission Lines", *in Proc. 2003 IEEE Bologna Power Tech Conf.*