The principles of control systems for protection devices

S. Stevanović
Institute of Power Engineering
Warsaw University of Technology
ul. Koszykowa 75, 00-662 Warsaw
POLAND
stevanovic@ien.pw.edu.pl

E. Wilson
Department of Automation
University of Strathclyde
Glasgow UK
e.p.wilson@strath.ac.uk

Abstract: - Paper describes requirements for present and future systems of remote control of microprocessor protection devices with laboratory stand for testing solution based on mentioned requirements. Described subjects allow seeing the most possible way of remote control of power system substation devices development. Descriptions of common system features and telecommunication network configuration were also included.

Key-Words: - remote control systems, power system protection, telecommunication standard, telecommunication link, SMS, SCS.

1 Introduction

For many years protective relays have been fully autonomous devices the only objective of which was to protect an electrical system against fault consequences. Latter introduction of the microprocessor to protective relays has increased their functionality and provided not only digital representation of settings but also added communication facilities enabling both remote monitoring of protective devices by direct extraction of settings and remote control of primary devices connected to the relays.

The need of fast and reliable access to the protection devices is caused by the fact that devices are installed in station located outside the city and user computers are located in the grid operator office or offices in cities. Distances between supervision centers and substation items may be very big, then without remote control facilities equipment maintenance become cumbersome, especially in conditions where access to power system components is not easy because of the lack of adequate infrastructure. The introduction of the microprocessor to protective relays has increased their functionality, among others efficient remote control. During many years, this was done using dedicated dial-up links to each substation from a grid control center.

Right now in times of widely used network technology, it is possible to conduct high speed and error free data exchange on long distances so remote control in times of telephone/modem networks are declining. Use of new high speed technology goes along with a worldwide tendency to entrust a external telecommunication company for conducting data exchange instead of using dedicated channels in internal network as it was previously. Taking it into account, one has to consider the possibility, in which remote devices can be reachable for people not employed by grid operator and when data exchanged with those devices can be overhear or intentionally changed.

The above-mentioned circumstances has led to a certain evolution in the formulation of requirements related to remote control systems used for ensuring a proper operation of power system protection devices compared to the demands existing several years ago.

Several years ago, the most important problems engineers had to deal with were the following:

- errors appearing in data exchange during telephone/modem connections,
- the use of vendor specific protocols and lack of common program allowing to change the settings of devices manufactured by other protection producers,

- lack of good communication programs for performing and sustaining data exchange data between protection devices of different vendors, especially in case of errors which could occur during telephone/modem connection,
- different sets of settings necessary to properly set up a defined protection function implemented in different manufacturer devices,
- different communication ports and standards, necessary to provide correct data exchange with protection devices from different manufacturers.

The most important problems which are expected in the next future are as follows:

- data exchange through third party/unsecure telecommunication network,
- high possibility of unauthorized access to telecommunication channel and access to remote protection devices,
- big number of protection set up programs versions, which are dedicated to or correctly cooperates, with selected versions of protection devices,
- high level of internal programmable logic use of protection device and lack of common program or standards allowing to set up internal programmable logic implemented in devices manufactured by different manufacturers.
- still no common program and standard allowing to setup all needed protection functionalities (IEC61850 standard allows for the implementation of fundamental parameters only).

Such situation force operators to develop clear requirements that should be applied in order to solve the subsequent problems by searching for new or modifying known remote control solutions of protection devices.

In this paper such requirements are presented together with proposed solution based on state-of-the art technology. Additionally the laboratory stand, which allows correct testing of proposed remote control system for protection devices is presented.

2 Requirements that must be met by devices used in system of remote control of protections

The first requirement is to have installed properly specialized vendor programs dedicated to data exchange/setup with specific protection devices on a dedicated computer. This device is very often called concentrator and acts as an agent installed in station, allowing local data exchange between a defined protection device and a dedicated vendor software using available communication standards of communication between the substation concentrator and office computer.

The concentrator should be a really universal device that can act as common platform allowing merging as one consistent system : modern and older microprocessor protection devices, their dedicated software and the communication system. The following additional requirements mentioned in [1] should also be met:

- the concentrator should enable data exchange with all types of power substation devices, which handle remote control,
- the concentrator must allow performing communication through a variety of serial ports that use different transmission standards,
- the concentrator must allow to carry out a proper work of programs which are necessary to set up all needed telecommunication links for different devices. Additionally it should supervise the state of both telecommunication links and communication channel.
- the concentrator must provide remote control of devices installed in substation using WAN links or a set of dedicated phone line and modem. In older solutions where there was no WAN connection a telephone line and analog modem is used and the concentrator had to handle such a communication type. Presently and in the future, LAN/WAN port connection is used as primary channel for remote control and access used, and the present and future concentrators should handle this type of connection which is commonly is carried out by means of Ethernet/IP port. Modem connection using telephone network (wired or GSM) is still present as a back-up communication link which is activated in case of LAN/WAN link failure.
- the concentrator must allow the installation and correct work of dedicated programs developed by specific manufacturers, programs necessary to set up all parameters needed by substation protection and other devices connected to concentrator. (the above-mentioned programs operates mostly under Windows platform but there are a few older devices the management software works under DOS system required),
- concentrator supervising programs should allow the transmission of all data to the protection device, even in case of loss-of-connection with the remote office supervising program. Those programs should also

automatically change state of concentrator in such case to the state when it is waiting for the next connection:

- concentrator supervising programs should grant access to the concentrator resources (telecommunication links, vendor programs etc.) only to authorized people. The type of granted access should be clearly defined and should depend on the specific functionality to be given to a defined user,
- the concentrator should withstand any type of cyber attack carried out from different network ports,
- the concentrator should be able to secure telecommunication link or use technology which allows to secure telecommunication link provided by unsecure telecommunication provider.

3 Concept of system that meets the objectives set

In the 90's the most popular type of telecommunication port installed in protection devices was RS232, RS485 was also used but more rarely.

Before, optical or electro-optical converters and switches were used for interconnecting channels with desired devices through concentrator, RS ports and protection devices.

In older solutions, between concentrator asynchronous RS ports and protection devices, couples of optical or electro-optical converts and switches have been used to obtain possibility of crossing channels to desired device.

Nowadays, the Ethernet LAN used as a component of substation infrastructure can be used as a medium for data exchange between the concentrator and protection devices. Almost all modern protective relays are equipped with Ethernet/IP optical or electrical ports. They are connected with Ethernet switch through electrical or optical wires. Device Identification and communication is IP-based. Data exchange with SCADA servers is performed by means of IEC61850 standard.

Even now, sometimes there are still situations when there is a need for data exchange with older device type, equipped with asynchronous port. Such asynchronous channels may be done using LAN infrastructure. Data exchange is performed by means of tunneling method and dedicated devices called Asynchronous Port Servers (APS – one example of device is: NportServer). Such devices, depending on configuration, can have from one to few (e.g. eight) asynchronous serial ports of configurable standard (RS232/RS485/RS422). Each APS device is connected to the substation LAN and has an unique IP address. During the concentrator configuration process, each APS and its asynchronous ports is given an unique com port identifier and all programs running on concentrator can use such ports during normal work.

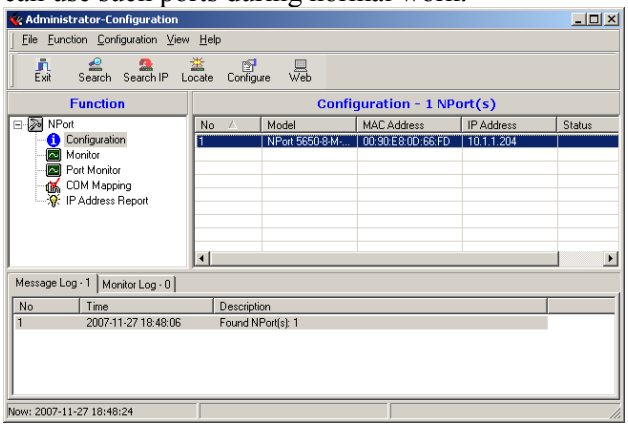

Fig. 1. Configuration of asynchronous port server

Fig. 1 and Fig. 2. depict an example of configuration of asynchronous ports, together with connection map of its ports to different concentrator COM ports.

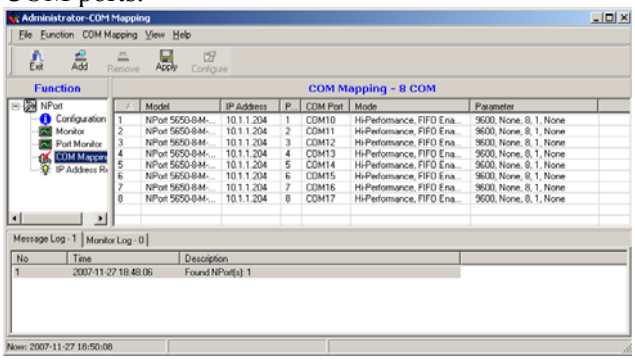

Fig. 2. Configuration of particular asynchronous port and its mapping into concentrator COM ports

The structure of telecommunication infrastructure, used by concentrator for data exchange with protection devices, has been simplified by using Ethernet/LAN together with APS device. In such structure two main working arrangements (star and ring) can be used. The star arrangement is presented on Fig. 3 while the ring one presented on Fig. 4.

In star arrangement (Fig. 3) APS devices are connected with Ethernet switch through optical fibers. The use of this type of devices depends on network switch construction and/or configuration. Using optical fibers to form local telecommunication network in substation makes possible the elimination of electromagnetic interference and makes error free connections

between concentrator and protection devices. What is more, such connections maintains galvanic isolation between any device installed in this system of remote control.

Star type configuration can be used in small substations where the overall number of protection devices is not very large (from a few up to several elements).

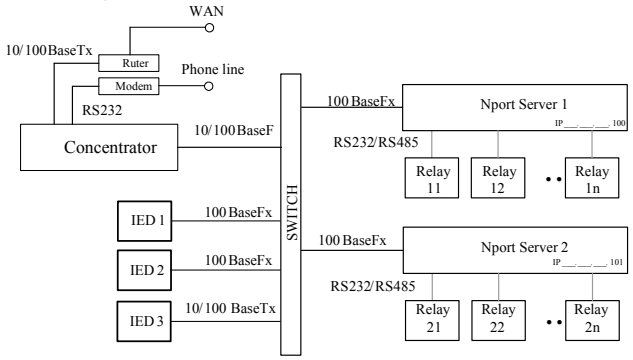

Fig. 3. Telecommunication infrastructure of remote control system using star connections and asynchronous ports server devices

In more expanded systems it is more convenient to use an arrangement based on circular connection, presented in Fig. 4. In this arrangement the network is more resistant to a possible damage thanks to closed loop links between Ethernet switches and the use of Spanning Tree Protocol by those switches. In normal operation one of these links is not active and is only activated in case of lack of connection between switches.

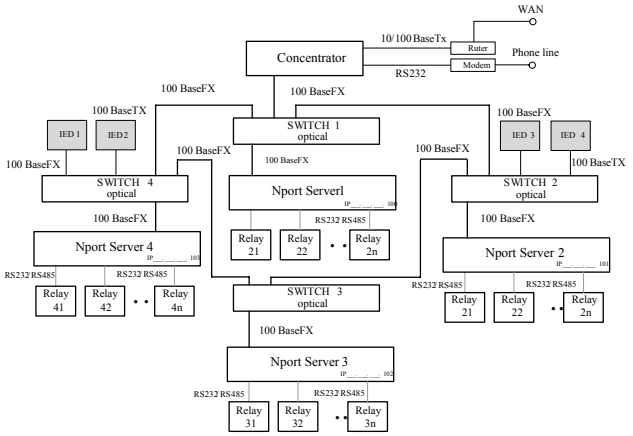

Fig. 4. Remote control system telecommunication infrastructure using ring configuration and optical switches

It is worth to notice, that communication between protection devices and Ethernet switch have always galvanic isolation but in case electrical connections (10/100BaseTX) presented on Fig. 3 and Fig. 4 this isolation is week (approx. 500V), performed by small transformers installed on each port inside switch. On Fig. 3 and Fig. 4connection supporting best galvanic isolation made on the base of fiber optic are presented (100Base FX).

4 Program allowing remote control of concentrator over large distances

Remote control of concentrator over long distances can be achieved through the well-known and widely used remote desktop software. This technology provides data exchange between two computers running defined similar or different operating systems, allowing remote control of distant computer. The software on the controlling computer transmits its own keyboard and mouse activity to the controlled computer, where the remote control software implements these actions.

There are many programs supporting remote desktop technology and some of them are even parts of the installed in a computer operating system. The controlling computer (referred to in this context as the client installed in the office) displays a copy of the image received from the controlled computer's (in this context the server, which is the concentrator) display screen. The concentrator has a host program which runs in the background, waiting for the connection coming on chosen communication ports like serial modem port or Ethernet/IP network port. In case of need of setting up protection in a defined substation, one should use local computer with remote program to set up the connection. This can be done by choosing a remote program, usually from a selection list of connections identified by names, IP numbers or telephone numbers. After establishing a connection with the distant host, a dialogue window containing fields with user and password request appears. If the user identification has been successful usually a list of protection devices grouped according to the configuration of substation, bus voltages, feeders and protection type, is shown.

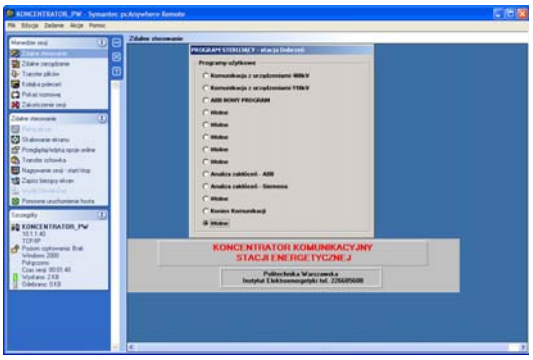

Fig. 5. Screen seen by the user after successful login to concentrator host computer – list of voltage levels are shown

In order to facilitate the access of the user to a particular application, to set up of particular protection installed in particular switchyard, very often some kind of control application is running on concentrator. The interface of this control application has the form of selection list allowing to verify or change the settings of a defined protection installed in a switchyard.

An example of selection list with a set of bus levels is shown in Fig. 5. After selecting the voltage level and the feeder, the protective relays installed at this level is displayed (Fig. 6.).

The selection list gives access not only to protections setup programs, but also to other applications dedicated to fault recorders control, fault locator management, teleprotection devices control etc.

Using the choice list, the users access is restricted to the applications shown on the list. After selecting one list item a defined telecommunication port is automatically chosen, and there is no possibility that a protection has been chosen by mistake (for example the same type but installed in different feeder).

The choice list of controlling program may contain various items. Its content depends on the connections to be monitored and the installed protections in a defined station, namely the number of feeders, the number of protections and other devices.

As it has been previously mentioned, a defined telecommunication port and type of connection are selected, the proper program is executed after choosing a defined protection type from the list.

Fig. 7. and Fig. 8. depict two examples of concentrator captured screens presenting programs used for data exchange with ABB protections.

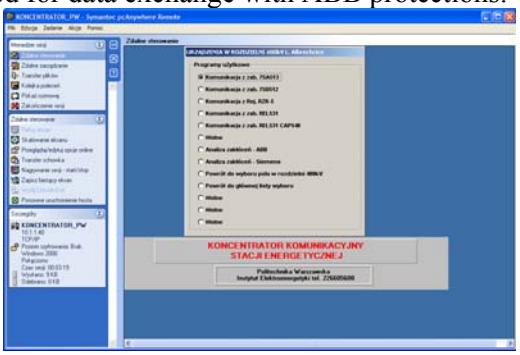

Fig. 6. Concentrator users screen with the choice of protections installed in particular feeder

There are many programs (according to certain IT journals more that 90) that can be used for remote control depending on the operating system installed. One the most popular type of programs, widely used for several years in Windows system environment is PcAnywhere. Also such applications like VNC, TeamViewer, UltraVNCare are very popular.

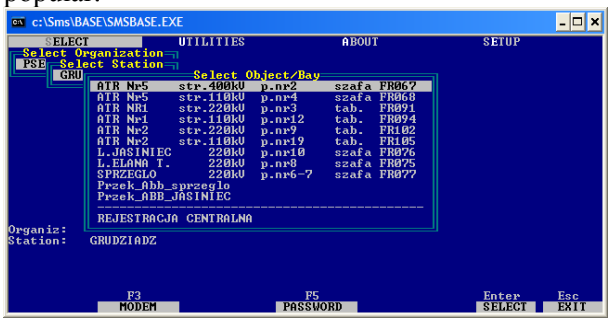

Fig. 7. Concentrator user screen with application SMS-BASE used for older ABB protections

One of the older versions of programs used for setting of protections, operating under the DOS operating system is presented on Fig. 7. A newer version is depicted in Fig. 8. The older version works in a text-based user interface while the newer uses graphic user interface. Both versions can be run on concentrator operating system and used for protections management.

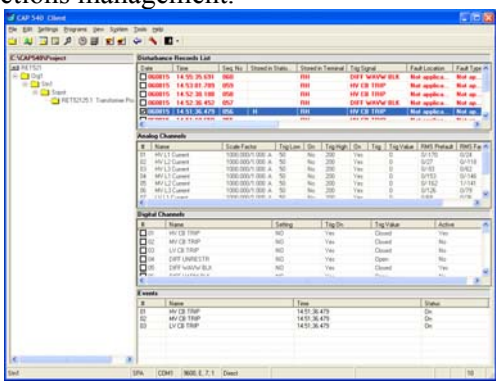

Fig. 8. Concentrator users screen with application CAP540, used for modern ABB relays

5 Laboratory stand used for concentrator testing

In order to test a new concentrator concept and its telecommunication connections an appropriate laboratory stand has been developed. Due to the extensive use of Ethernet/IP network components in concentrator telecommunication connections, a special emphasis was put on the verification of their operation.

The laboratory stand makes also possible the conduction of the following operations:

- verification of the interoperability of protections equipped with Ethernet/IP ports [2],
- control of the cooperation of older protections equipped with asynchronous ports (RS232, RS485),
- verification of additional concentrator features like access to other devices i.e. digital fault

recorder, transformer cooling controller, access to concentrator via www and others.

Before installation on site, the remote control of a defined device, including the use of substation LAN system for telecommunication links, is checked by running appropriate tests on the laboratory stand. All devices used in laboratory stand are standard devices usually used in substation protection system. Its design allows:

- easy modification of the configuration of telecommunication connections linking together its various elements,
- checking typical telecommunication applications,
- validating the information exchange with the devices using asynchronous serial ports (standard RS232, RS485 and optical connections using a wavelength of 850 or 1300 nm) by using a tunneling mechanism in IP packets,
- exchanging data with devices over an Ethernet network using Ethernet/IP at 10 and 100Mb/s via electrical or optical links,
- exchanging data over WAN network using routers , channels of nx64kb and 100Mb/s configured in SDH nodes [3], [4].

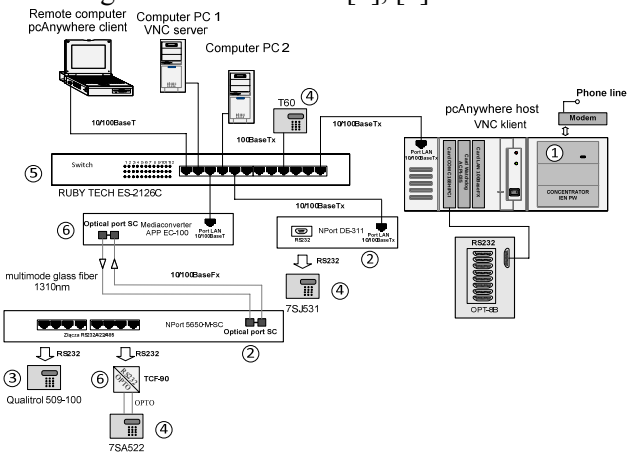

Fig. 9. Block diagram of laboratory stand and its main components (1- concentrator, 2 and 6- asynchronous ports servers, 3- transformer cooling controller, 4- T60 protection device, 5- Ruby Tech ES ES-2126C switch, 6-mediaconverters, connectors etc.)

The laboratory stand has been equipped with several PC computers and other necessary devices, allowing the design of various configurations and simulation of real network load presented in Fig. 9.

The following devices can be enumerated:

- concentrator (no. 1),
- asynchronous ports servers (RS232/485/422) NportServer 5650, DA663 DA-311 and DA-302 (no. 2),
- transformer cooling controller Qualitrol 509-100 (no. 3),
- GE transformer protection T60, distance protection 7S522, overcurrent protection 7SJ531(no. 4),
- Ethernet switch Ruby Tech ES-2126C (no. 5),
- RS232/OPTO converters, Ethernet media converters and other connectors, (no. 6).

Because of limited space, more detailed information concerning additional elements of laboratory stand like PC computers and various protection devices have been omitted.

4 Conclusion

As can be seen in presented paper, Ethernet networking technology imposes change in requirements for the equipment of power substation protection devices remote control system.

Those requirements force the use in such systems particular telecommunication devices, connections and configuration programs. To check effectively the behavior of various devices in mentioned remote control system adequate laboratory stand has been made and set of tests has been performed, which has been performed, proving the correct work of main system components.

References:

[1]J. Savković-Stevanović, Fuzzy logic control system modelling, *International Journal of Mathematical Models and Methods in Applied Sciences,* **3** (Issue 4):327-334,2009.

[2] J. Savković-Stevanović,J.Djurovic, An inverse model of the fuzzy logic controller of the distillation plant, *Comput. Ecol. Eng., Vol.4* (Issue 1):23-31, 2008.

[3] J.Savkovic-Stevanovic, Knowledge base information processing, *WM-SCI2009-The 13th World Multiconference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA*,10-13 July, 2009.

[4] T.Mošorinac, A fuzzy controller, *Comput. Ecol. Eng.*,Vol 4 (Issue 1): 1-7, 2008, ISSN1452-0729.

[5] M. Ivanović-Knežević, S. Krstić, A reactor fuzzy control system, *Comut.Ecol.Eng.*,Vol.4 (Issue 1) 16-22, 2008, ISSN1452-0729.

[6] H. Jiang, J. Yu, C. Zhou, Consensus of multi-agent linear dynamic systems via impulsive control protocols. *International journal of Systems Science,, Vol.42* :967-976, 2011.

[7] Y. Shang, Multi-agent coordination in directed moving neighborhood random networks. *Chinese Physics B*, *Vol. 19*:070201, 2010.

[8] G. Gregoire, H. Chate, Onset of collective and cohesive motion. *Physics Review Letters, Vol. 92*, 2004.