FAST AND SECURE AUTOMATIC RETRIEVAL OF DATA FROM MULTI-VENDOR DEVICES - THE PORTUGUESE EXPERIENCE

Miguel LOURO
EDP Distribuição – Portugal
miguel.louro@edp.pt

Jaime GUISADO
EDP Distribuição – Portugal
jaime.guisado@edp.pt

Carlos FORTUNATO
EDP Distribuição – Portugal
carlos.fortunato@edp.pt

Carlos CURA
EDP Distribuição – Portugal
carlos.cura@edp.pt

Bruno ANTUNES
EDP Distribuição – Portugal
bruno.antunes@edp.pt

Miguel AREIAS
EDP Distribuição – Portugal
miguel.areias@edp.pt

Miguel GROSSINHO
EDP Distribuição – Portugal
miguel.grossinho@edp.pt

Luís Pinto PEREIRA
QEnergia – Portugal
luis.pereira@qenergia.pt

Fernando PIMENTA
QEnergia – Portugal
fernando.pimenta@qenergia.pt

ABSTRACT

Nowadays protection systems generate large amounts of useful data. The most important of which are the oscillographic records, because they allow: fault location estimation; validation of relay settings; validation of coordination among protections.

This important information traditionally resided in the protection units and could only be retrieved through vendor proprietary software. Retrieving this information could be conducted in two ways: a specialized technician had to physically go to the substation (expensive solution); by use of a slow analog modem with a tendency to breakdown (especially in remote areas exposed to lightning strikes) and a high probability to stop working due to communication errors.

Recently EDP has begun to equip all the substations with an IP network through optical fiber. This fast and reliable network, which is also intended for other application other than remote access, eliminates the communication constraints.

Due to technological differences the substations were, for this purpose, separated in two groups: Substations with a modern protection system complying with IEC 61850; Substations with older protection units for which a pilot-project was conducted using the communications gateway Kalkitech SYNC2000. This device communicates with protection units from several vendors, using standardized (ex.: IEC61850) or proprietary protocols (ex.: ABB SPA-BUS), and has mechanisms for retrieving oscillographic records.

The usage of standard tools such as FTP and file sync programs proved to be cost effective and reliable to get the information to a central location.

INTRODUCTION

Disturbance records from protection units are becoming increasingly important in power system operation and maintenance because they can be used for applications such as: determining incorrect relay settings; relay coordination checks; fault location; asset condition monitoring; analysis of complex events. However, retrieving these records has been complex up until now because of proprietary software to access the information and lack of a fast and reliable telecommunications structure to transmit it to a central location.

Recently these obstacles have been removed by the appearance of IEC 61850, which standardizes the access to disturbance records, the appearance of vendors that offer a backwards compatibility solution with older protection units and the establishment of a fast and reliable IP network in EDP's substations.

The aim of this paper is to present the solutions being used, and tested, by EDP to achieve a cost effective disturbance data automatic retrieval.

EDP'S IP NETWORK (FLEXNET)

EDP owns a fiber optic network with more than 6500Km, a PDH network with 500 nodes, a SDH network with 100 nodes and 84 microwave links.

To deliver new generation services in substations, EDP decided to implement an IP network.

In phase one, 33 nodes were implemented without any backbone using the existing networks.

In phase two, 40 nodes were implemented over optical fiber, using a IP/MPLs backbone from an external Telecom Operator, and interconnected both networks:

- Each ring has about 10 substations.
- Each application uses a different physical port in the terminal equipment, and each application uses a different VLAN (IEEE 802.1q).

The network must have 99.99% availability for SCADA application, with the higher priority. The Packet loss must be under 1% and the reconfiguration of layer 2 area must be below 50ms. For security purposes a NAC (Network Access Control) and two firewall, one internal, and another external, were implemented.

Implementation of the First phase of the project occurred in 2007.

The implementation of second Phase began in the last quarter of 2011. During 2013 EDP will evaluate the government model, and will decide the rollout of the Third

Phase of 450 nodes.

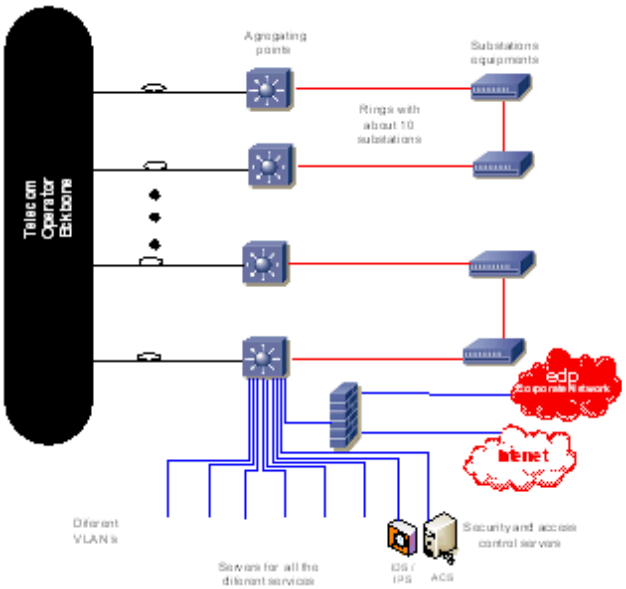

Figure 1 – IP network structure.

Application	Expected Bandwidth
SCADA	100 Kbps
Telemetering	9,6 Kbps
Telemanagement of Telecontrol and Protection equipments	1Mbps
Supervision of power DC systems	64 kbps
Supervision of telecommunications systems	64 kbps
Power Quality	512 kbps
Video surveillance	1 Mbps
Voice	64Kbps
Access to corporate applications	2 Mps

Table 1 – Flexnet bandwidth requirements by service

AUTOMATIC RETRIEVAL OF DISTURBANCE RECORDS

Modern Protection systems

The most modern protection systems acquired by EDP are IEC 61850 native. Vendors such as ABB and Siemens offer solutions that allow for an automatic retrieval of disturbance data to a local PC.

ABB systems may be configured to retrieve disturbance records in two ways: "on event", which causes the immediate record retrieval from the IED where the event occurred (the events are typically trips or protection function starts); scheduled retrieval (typically performed in the early hours of the morning), that retrieves all new records. For the REF5xx series, IED's records are cleared after the retrieval and the information is accessible only at the substation PC which has a high storage capacity.

Siemens systems only perform schedule retrievals. The time set for the scheduled retrieval is user defined but is typically between 5 to 10 minutes in Portugal. This system is located in the substation's local SCADA (PAS) and maintains the information in the IED avoiding record duplication by comparing lists of retrieved records. However, the data stays in the PAS system. Another software, RECPro Collector, is used to copy the disturbance records to the local PC.

Nowadays, about 15% of EDP's substations are equipped with automatic disturbance record retrieval.

Older Protection systems

Retrieval of Oscillographic Fault Records from Protection Relays has been, traditionally, a task exclusively performed by OEM's own Configuration / Parameterization Software, and this is especially true for legacy devices that implement proprietary communication protocols like SPA Bus (ABB), Courier (Alstom / Areva), Modbus (GE), and many more.

The challenge of having a system capable of retrieving Oscillographic Fault Records from Protection Relays, independently of the Manufacturer, required the adoption of a flexible platform, both in terms of Hardware and Software.

The chosen device was Kalkitech's Communication Gateway SYNC2000. This choice was based on SYNC's flexibility in terms of communication interfaces (six Serial / one Ethernet) and the large quantity of implemented communication protocols, both proprietary and standard.

- IEC 60870-5-101, Master and Slave
- IEC 60870-5-104, Master and Slave
- IEC 60870-5-103, Slave
- IEC 61850, Client and Server
- SPA Bus, Master
- Courier, Master
- MODBUS RTU / TCP, Master and Slave
- FTP, Client and Server
- SNTP, Client and Server

Additionally, Kalkitech's availability to customize the device on a project basis proved to be critical in the final choice.

Figure 2 – Kalkitech's SYNC2000 Gateway

Requested development concerned the implementation of Oscillographic Fault Record retrieval for ABB's REx 500 Series of Protection Relays, including conversion to COMTRADE format, all performed by SYNC2000.

A test environment was created in Portugal and included a REL511 *2.5 Protection Relay from ABB. Software development was carried out in India and took advantage of a permanent VPN link to Portugal. Validation tests were performed together by QEnergia and EDP Distribuição.

Figure 3 – ABB's REL 511 *2.5

In order to field test the developed solution, a Substation was chosen based on the following criteria:

- Monitoring and Control based on an RTU System
- Availability of IP Data connection to EDP's WAN
- Availability of ABB's REx 500 Protection Relays
- Availability of IEC 61850 Protection Relays
- Availability of a permanent Substation PC

Caeira Substation, close to the city of Évora, was the chosen one as all the above criteria's were met. The following devices were installed at the Substation:

- Kalkitech SYNC2000
- eWON 3G Router with integrated Ethernet Switch
- SAIA PLC with Analog Output Modules

Figure 4 – Equipment installed for the demonstration project

Communication with ABB Protection Relays (3x REL511 and 3 x SPAJ140C) was performed via SPA Bus Protocol and used a serial port of SYNC2000 (SPA Bus Master) for this purpose. Following features were successfully implemented / tested:

- Time Synchronization of all SPA Slaves (*)
- Retrieval of Distance to Fault from REL511 units
- Output of Distance to Fault to Substation RTU (mA)
- Fault Record – FR retrieval from REL511 units (**)
- Automatic conversion of FR's to COMTRADE
- Transfer of COMTRADE FR's to FTP Server (PC)
- Access via CAP540 (PC) to Protection Relays (***)

(*) SYNC2000 Time Synchronization was insured via SNTP protocol, using Substation LAN and existing GPS Receiver.
(**) Fault Record retrieval made on a scheduler basis
(***) Use of SYNC2000's Transparent Channel feature, which makes it possible to prioritize serial communications, thus giving priority to CAP540 access over SYNC's Master.

Oscillographic Fault Record retrieval from IEC 61850 Protection Relays was very fast (less than 5 seconds for a new record), mainly due to the fact that all devices made available RDRE1 Logical Node (event based retrieval) and enabled File Browsing to be performed by an IEC 61850 Client (SYNC2000). Records were natively available in COMTRADE format.
During the demonstration project at Caeira substation the following IED were connected to SYNC2000 via an IEC 61850 connection:

- 4 x Siemens 7SA612
- 10 x Siemens 7SJ622
- 2 x Siemens 7UT613
- 1 x Siemens 7SS522

About 35% of EDP MV feeders have protection unit's with oscillographic recording and no automatic retrieval.

Getting the information to a centralized location

Both automatic disturbance records retrieval solutions, for modern and older protection systems, concentrate the information at the substations level. However, its analysis is performed at a centralized level and therefore the information must be made accessible at that point.
There are two solutions for this problem which rely on a fast IP network, such as the EDP's Flexnet. The first solution is used for the modern systems. In this case the disturbance records are stored in a shared Windows file system at the substation's PC. The centralized file system can be synchronized with the remote one by using a file sync program readily available from the Internet, most of which are freeware. EDP experience is that scheduled file sync over the Flexnet is cheap and highly reliable.
The second solution is targeted for SYNC2000 based systems and relies both on SYNC's internal flash storage (200 MB) to temporarily store disturbance records and on its internal FTP client. The later can be configured to send the disturbance records based on a pre-defined schedule (every five minutes, for instance). So, at the central location a simple FTP server is all that is required to store the data coming from SYNC2000.
Both solutions are cheap and readily available in freeware programs.

CYBERSECURITY

SCADA systems evolved from hardware and software in the 1970s to current systems that include standard PCs and operating systems, TCP/IP communications, and Internet access. This evolution brings the possibility to integrate with business systems promoting external connections and information sharing. Even considering SCADA systems less vulnerable as the traditional Information Technology (IT) systems, because it was built based on a specific and proprietary software only known by a few people (security through obscurity), the connections between these two systems promote a growing concern about security.
Aware of this problem, EDP designed and implemented a security architecture in order to protect the SCADA system. Therefore, using a common strategy for addressing security, a single security perimeter was established including in it all vulnerable critical cyber assets. All external access to the

SCADA system has been protected by a strong access control scheme. In fact, all connections from outside, establish either from other corporate networks or from internet, were made based on strong authentication procedures and encrypted protocols, and accesses filtered by firewalls.
At this moment EDP, as well as the SCADA community, are recognizing the importance of protecting their systems and stopped believing that they are invulnerable or, at least, realized that hackers might be interested in their applications, probably know more than expected about their SCADA systems, and may be willing to invest enough to attack, including getting some form of internal access. The security perimeter strategy, in spite of ensuring a good level of security from outside, provides little or no security against someone inside the physical perimeter. The vulnerabilities and threats inside the security perimeter need to be addressed in order to improve security for SCADA control systems. An attack from inside represents a greater threat because it might be performed by someone who has got deeper knowledge of the system architecture and, on the other hand, has the cover of being already inside the security firewall perimeter.
EDP is now addressing these problems, through several initiatives that aims at identifying current risks under a holistic attack model (inside as well as outside) and develop new schemes and techniques to bring its systems to the next (and higher) level of security and dependability. One of the first steps is related to the segregation of networks, creating different security levels and promoting effective control communication between them.
Security measures include the separation the IEC 61850 networks from each other and from the SCADA network thus preventing a denial of service (DoS) attack that would impact on the critical IED to IED communication at the substation level. The separation has traditionally been achieved by using two network boards in the RTU and the local PC. When the retrieval device has only one Ethernet board it is possible to use the "port forwarding" feature of the router to insure the IED's critical communication remains unaffected by a DoS attack. However, the disturbance record retrieval device will be affected.

COSTS AND BENEFITS

Retrieving disturbance records from a substation with no remote access means that a person must physically go to site. On average, at least half a day is need to complete the procedure, which is performed by a highly skilled technician (due to knowledge necessary to deal with a variety of IED from multiple vendors each, with its specific software). In extreme cases, the disturbance record retrieval may take an entire day.
If the substation has remote access through an analog modem link, it takes a minimum of 2 hours to retrieve the first record. The connection is extremely slow, it has frequent failures (some of which actually disable the connection at the remote end), and the retrieval process is extremely time consuming. Sometimes it is quicker to just send a technician to the substation than to use the analog modem link.
So, the manual retrieval of the disturbance records is costly and somewhat demotivating because most of the time is spent driving. Traditional remote accesses are also time consuming.
Automated disturbance record retrieval has several direct benefits such as:

- cost reduction due to elimination of the need to drive to the substation;
- cost effective increase of the number of substation with fault location (from about10% at the MV level to about 50%);
- Lower delay times between event occurrence and data analysis availability.

CONCLUSIONS

Oscillographic disturbance records are becoming increasingly important to the network's operation and maintenance.
Due to the standardization of access to IED's recordings (defined in IEC 61850) and the appearance of vendors that offer compatible solutions for older relays, it is now possible to automatically retrieve large amounts of data from protection relays. SYNC2000 Gateway from Kalkitech was successfully tested for this purpose.
Additionally, this data must be accessible from a central location through a fast and reliable IP network such as EDP's Flexnet so that its full potential for fault location, incorrect protection settings detection and protection coordination validation can be unleashed. Readily available tools in the Internet can be used with high reliability.