http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2015 Colloquium
October 08 to 09, 2015
Lima – PERU

D2-01_01

A NEW TELEPROTECTION SYSTEM OVER IP NETWORKS

by

FERNANDO CASTRO CERVERA (*)
ZIV Communications
Spain

(34)

SUMMARY

Teleprotection units are a fundamental part of the protection system of the utility. The role of a teleprotection system is to communicate the protection relays at both ends of the line, using a given telecommunications channel. Their performance is measured in terms of robustness against channel impairments; dependability is the ability to receive a command even in the presence of noise, and security is the ability to prevent the noise from causing false commands. Both parameters must meet the requirements expressed in IEC60834-1.

While traditionally teleprotection systems used dedicated channels, like power-line carrier or SDH, the trend today is to move to IP networks. This new channel poses many challenges to the performance of a teleprotection system;

- The delay is no longer a deterministic figure but a random variable that depends on the network traffic, and time stamps have to be used to measure the actual delay from transmitter to receiver to make sure that the Quality of Service requested is not degraded

- The different IP packets transporting the teleprotection information may arrive at the receiver in a different order, so the latest information packet received may not transport the latest information. The teleprotection packets may even be lost

IP networks are exposed to cybersecurity threats and the teleprotection information is a critical system, so cybersecurity countermeasures are needed

KEYWORDS

Teleprotection, protection, relay, IP, cybersecurity

* Antonio Machado, 78-80, 08840-Viladecans (Barcelona), Spain
Fax +34933492258; email: Fernando.castro@cgglobal.com

1. 1. A BRIEF NOTE ON THE TELEPROTECTION CONCEPT

Teleprotection systems are an essential part of the protection system of a high voltage line. The way a teleprotection system supports the operation of the protection system is widely described in [1], from where many examples can be derived. Figure 1 shows the operation of a distance protection system where underreach and overreach systems are used in parallel, together with a teleprotection system. The red arrows show the sequence of operations when a fault occurs, and the conclusion is that the breakers will be tripped when the teleprotection command is received;

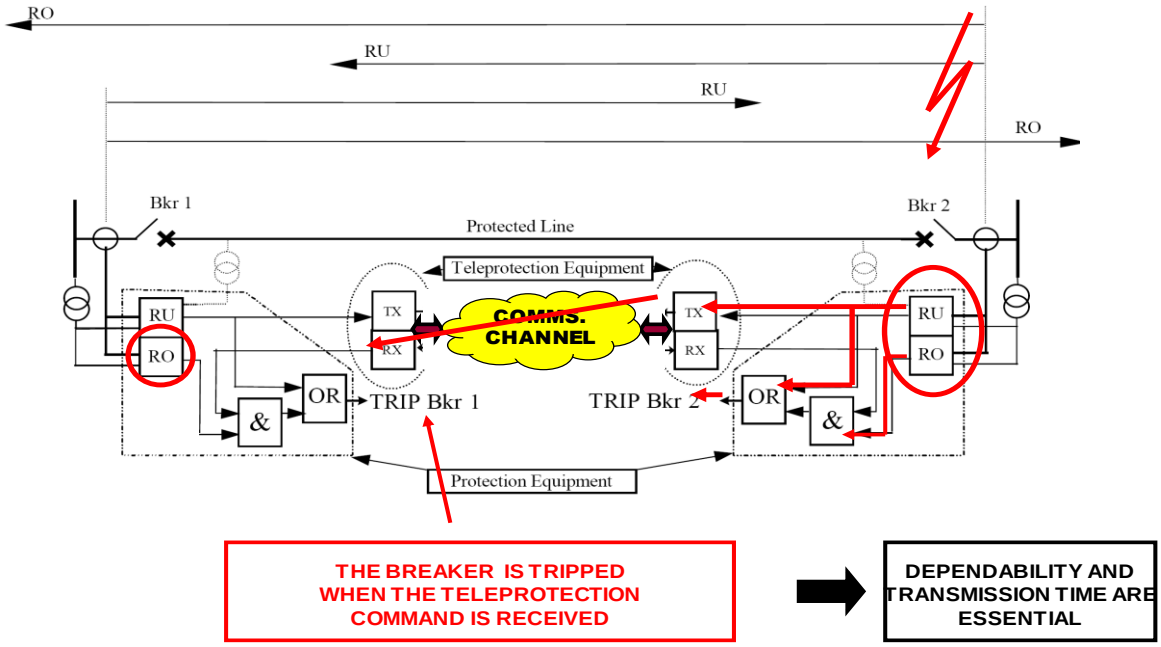

Figure 1: Operation of a distance protection system combining underreach, overreach and teleprotection subsystems

Figure 2 is another interesting example, also from [1], where the operation of a distance underreach system is shown;

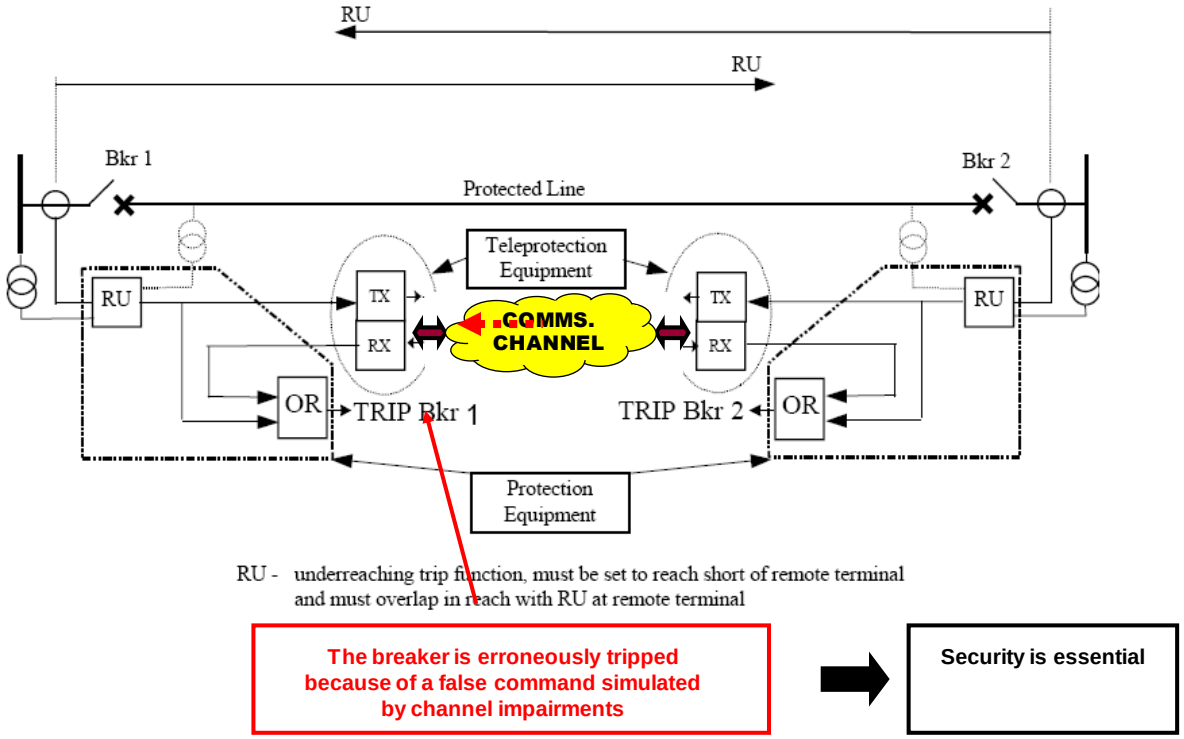

Figure 2: Operation of a distance protection system combining underreach and teleprotection systems

In this second example we can see that the breaker is tripped erroneously because of a false command generated by the communications channel impairments. So, security against channel noise and interferences is an essential performance criteria of teleprotection systems.

The fact that protection systems (very often) require information from both ends of the line, and the subsequent need for a teleprotection system, requires that the performance of a teleprotection system against channel impairments be measured. This is widely covered in IEC 60834-1 Standard [2]. This Standard introduces the fundamental concepts of Dependability, Security and Maximum Actual Transmission Time (Tac):

- Dependability is the ability of the teleprotection receiver to detect an incoming command from the transmitter in spite of the presence of channel impairments, such as channel noise, interferences, frequency deviation, bit error rate (in digital communications systems) or others. It is usually measured in terms of Probability of Missing Command (Pmc), a performance figure that should be as low as possible and in all cases lower than the requirements stated in [2] (see figure 3).

- The mere fact that the command is detected is in itself useless if the command is detected too late. We are protecting physical infrastructure against a fault, and so the command has to be detected before a maximum delay if the system is to protect the HV line against physical damage. This is called Maximum Actual Transmission Time, and it is closely related to Pmc. In fact the computation of Pmc will take into account those commands received within Tac and discard all those commands received after Tac.

- Security is the ability to reject false commands that have been simulated by the channel impairments. This is of particular importance when impulsive noise is present in the line, a common situation in PLC systems, or when bursts of errors take place in digital communication systems, a common situation when an SDH system loses synchronism. Security is measured in terms of Probability of Unwanted Command (Puc). Again IEC 60834-1 gives figures of Puc.

Protection scheme	Maximum actual transmission time T_{ac} ms		Channel quality		Noise duration T_B ms	Security P_{uc}		Dependability P_{mc}
	Analogue	*Digital*	*Analogue S/N dB*	*Digital BER*		*Analogue*	*Digital*	
Blocking	15	10	6	10^{-6}	Continuous	N/A	N/A	$<10^{-3}$
Blocking	15	10	Worst case		200	$<10^{-3}$	$<10^{-4}$	N/A
Permissive underreach	20	10	6	10^{-6}	Continuous or pulsed	N/A	N/A	$<10^{-2}$
Permissive underreach	20	10	Worst case		200	$<10^{-4}$	$<10^{-7}$	N/A
Permissive overreach	20	10	6	$<10^{-6}$	Continuous or pulsed	N/A	N/A	$<10^{-3}$
Permissive overreach	20	10	Worst case		200	$<10^{-3}$	$<10^{-7}$	N/A
Intertripping	40	10	6	$<10^{-6}$	Continuous or pulsed	N/A	N/A	$<10^{-4}$
Intertripping	40	10	Worst case		200	$<10^{-6}$	$<10^{-8}$	N/A

NOTE – The maximum actual transmission times quoted refer to applications for EHV systems.
Longer times may be allowable for lower voltage systems. Longer times may also occur at reduced bandwidths. (See 3.3.1).
N/A: Not applicable.

Figure 3: Figures of Pmc, Tac and Puc required by IEC 60834-1 (see ref. [2])

2. COMMUNICATIONS CHANNELS FOR TELEPROTECTION SYSTEMS

The performance parameters described above (Probability of Missing Command Pmc, Maximum Actual Transmission Time Tac and Probability of unwanted Command Puc) can be generically described as Quality of Service. For many years it has been common practice to use dedicated communications channels for the teleprotection systems, an excellent approach to guarantee the required Quality of Service.

In the analogue domain, for example, Power-Line Carrier has been extensively used thanks to its inherent robustness and controlled delay while providing enough bandwidth for the teleprotection application. In the digital domain several technologies have been used over the last two decades, like PDH with 64 Kb/s as an access rate or SDH with 2 Mb/s as an access rate.

The trend, however, is to migrate to IP networks [3]. Other technologies like MPLS are also being deployed [4]. All packet technologies have common characteristics that have to be taken into account;

- The information to be transmitted is split into packets with an origin and destination address

- The packets from the different information sources are statistically multiplexed. This results in greater overall efficiency in the network, since the periods of silence of a given source are compensated with the periods of activity of other sources

- Packet networks offer inherent redundancy against channel interruptions; if a given communications links is lost the network readjusts its topology and the communications is not interrupted. However this may result in packets arriving at the receiver in the incorrect sequence or being lost during the topology transient

- When two or more information sources are transmitting at the same time the network may not have enough bandwidth for all of them and so some of the packets will be transmitted before others. This results in a random delay, which goes against the fundamental concept of Tac. However we must bear in mind that the teleprotection application is in itself a bursty source of information, since the guard state and the command state have different urgencies

3. TELEPROTECTION SYSTEMS FOR IP CHANNELS

These inherent characteristics of IP channels require that the teleprotection systems be adapted to the new channel conditions. Figure 4 shows a generic protocol stack for a teleprotection system operating over IP channels, and Figure 5 shows a real implementation of such a protocol stack;

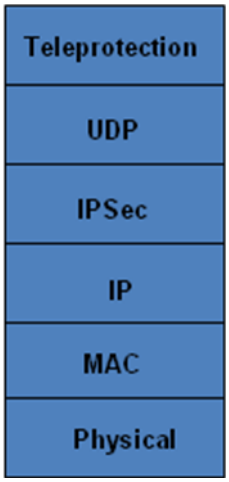

Figure 4: generic protocol stack for a teleprotection system operating over IP channels

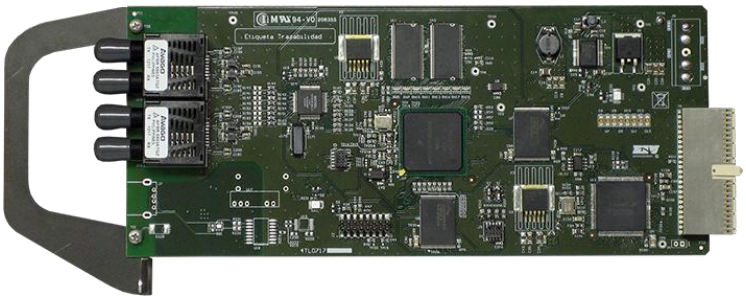

Figure 5: Real implementation of a teleprotection system operating over IP channels

This protocol stack and the implementation shown in figure 5 have the following distinctive aspects;

- The teleprotection application, as it is well know, transmits a guard message under quiescent conditions and a command message under fault conditions. These two messages are of course different and limited in time. This is to say, *the teleprotection is itself packet in nature* even though for many years it has been used over circuit communications channels

- UDP is the preferred transport protocol instead of TCP because of its simplicity. In fact TCP offers sophisticated functionality like flow control and retransmissions, but these are useful when long messages are to be transmitted. The teleprotection application consists of short messages that are continuously retransmitted without the need of a transport protocol. In fact the flow control exercised by TCP may even hinder the transmission time of the teleprotection packets.

- All teleprotection packets must be numbered so that the receiver knows what the latest information is. The basic principle of operation is shown in figure 6; those packets arriving out of sequence will simply be ignored since a more updated packet (packet number 9 in the example), with more updated information, has been received

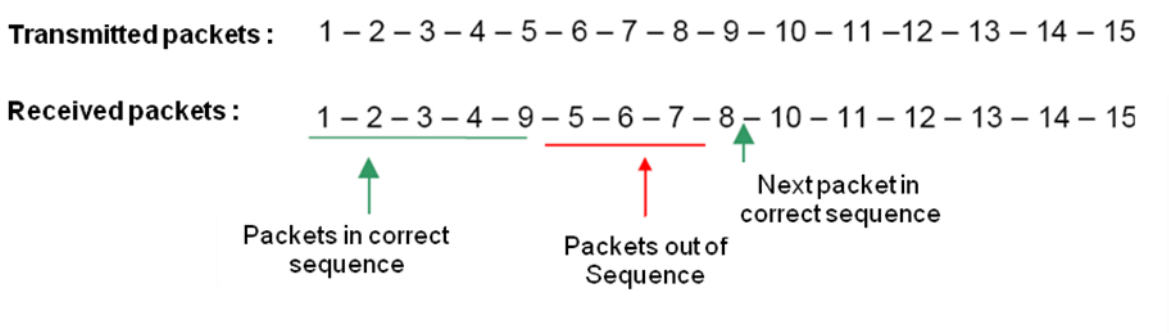

Figure 6: packet numbering and subsequent operation at the receiver

- The IP layer is needed to travel across the network topology. Every teleprotection system must have an IP address, and the teleprotection packets will have to travel from the origin IP address to the destination IP address.

- The IP and MAC layer must implement priorities for the teleprotection packets. In fact teleprotection packets should have the highest priority in the network (except, perhaps, for the network management)

- Even though the teleprotection packets have a high level of priority the delay across the network will still be a random variable. Packets from different teleprotection systems, for example, may collide at network resources. This phenomenon is dealt with at two different levels. First, traffic engineering is so an essential part of a teleprotection system operating over packet channels and has to be taken into account when designing the network. Second, all teleprotection systems must be time synchronised and all

packets must me time stamped. The teleprotection receiver will be able to measure the delay of all individual packets across the network and perform statistics about the quality of service. If the mean delay and/or the delay variation exceed a given threshold an alarm message can be sent, for example, with an SNMP trap message.

Finally the teleprotection information is critical information. A forged packet may result in a breaker being tripped and a loss of supply to customers. The fact that this information is encapsulated in a popular protocol, like IPv4, requires that the information be ciphered. In this respect IEC 62351 [5] gives guidelines on how to protect sensitive and urgent information, like for example GOOSE. Cryptography algorithms like Symmetric Key are particularly useful since they offer very low computation latency, which is important in teleprotection applications.

4. TEST BED

The above mentioned concepts have been implemented and tested in a packet switching network consisting of four MPLS devices. The usual channel impairments, like random latency packet disorder and packet losses, have been induced with additional traffic and communications channel interruptions. The additional traffic has been implemented at different transmission rates, ranging from 1 Mb/s to 1 Gb/s. Different traffic patterns, like ping messages or FTP, have been tested.

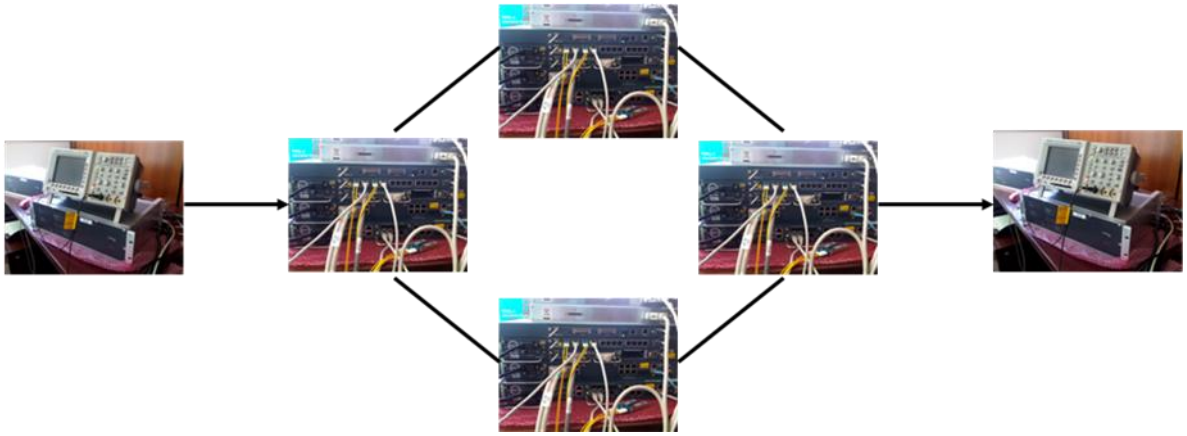

Figure 7: Test bed for the IP teleprotection system

The tests performed show that the transmission time in blocking mode ranges from 7.44 to 8.44 msec, with peaks of 8.72 msec when the network is congested. In direct tripping mode the transmission time ranges from 20 to 20.6 msec, with peaks of 21.2 msec when the network is congested. All these figures are well within those limits specified in [2]. Other test, like the loss of a communications link and subsequent path rerouting, have had negligible impacts on dependability, security, transmission time and even no communications link alarms were generated.

5. CONCLUSIONS

The transmission of teleprotection signals over IP channels is feasible and offers the usual level of performance when dependability, security and transmission time are measured. This requires

a specific design that takes the characteristics of this new communications channel into account, like variable delays. Cybersecurity is also an important aspect to be taken into account.

BIBLIOGRAPHY

[1] “Protection using Telecommunications”, CIGRÉ JWG 34/35.11 Technical Brochure, 2001

[2] “IEC 60834-1, Teleprotection Equipment of Power Systems – Performance and Testing. Part 1: Command Systems”. International Electrotechnical Commission, October 1999

[3] “Line and System Protection using Digital Circuit and Packet Communications”, CIGRÉ JWG D2/B5.30, 2012

[4] “Scalable Communication Transport Solutions over Optical Networks”, CIGRÉ WGD2.35, 2015

[5] IEC 62351 series, “Power System Management-data and Communications Security”, International Electrotechnical Commission