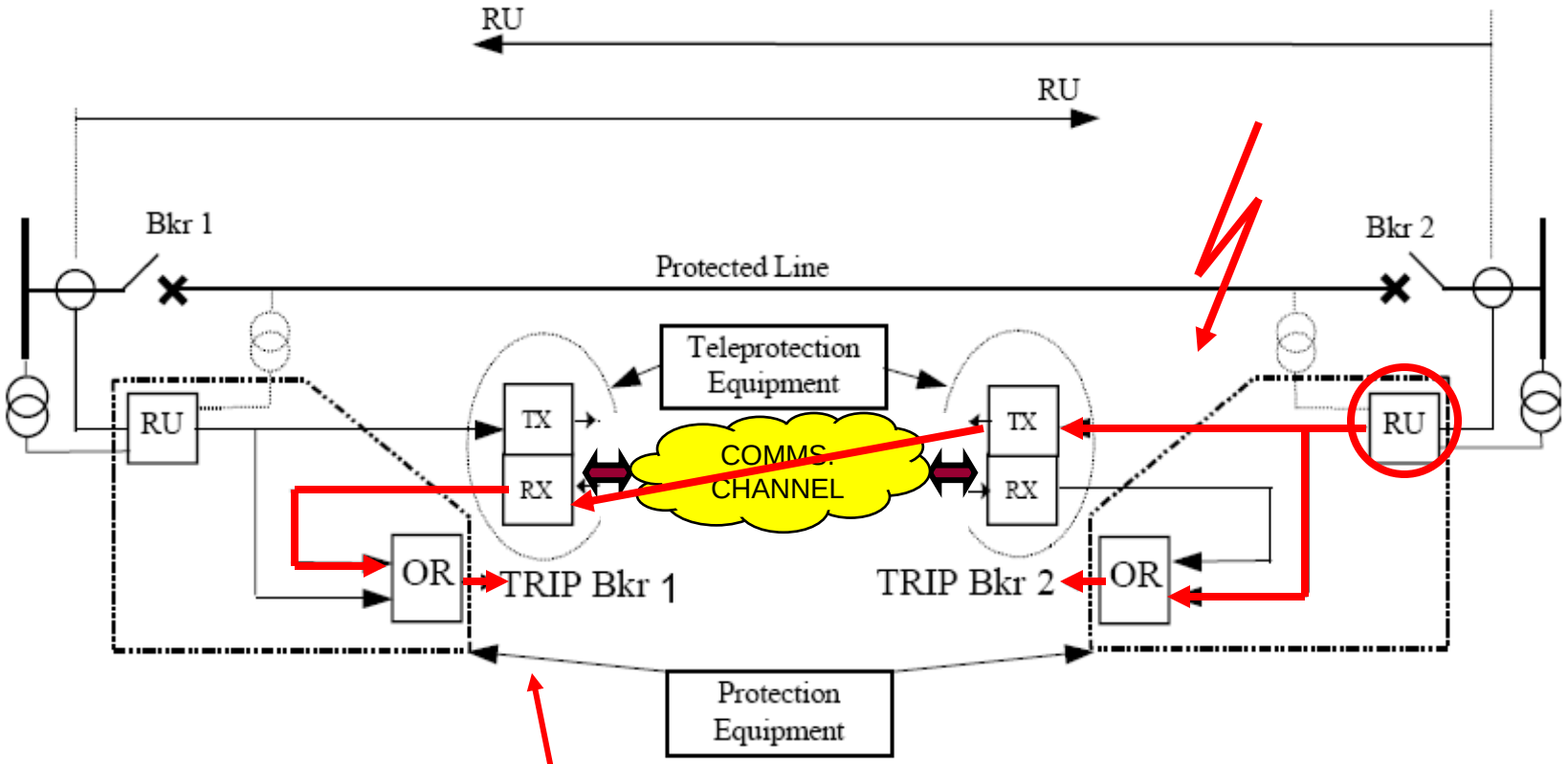
A NEW TELEPROTECTION SYSTEM OVER IP NETWORKS

D2-01_10

Fernando Castro
Fernando.castro@cgglobal.com

Lima, October 15th-16th, 2015

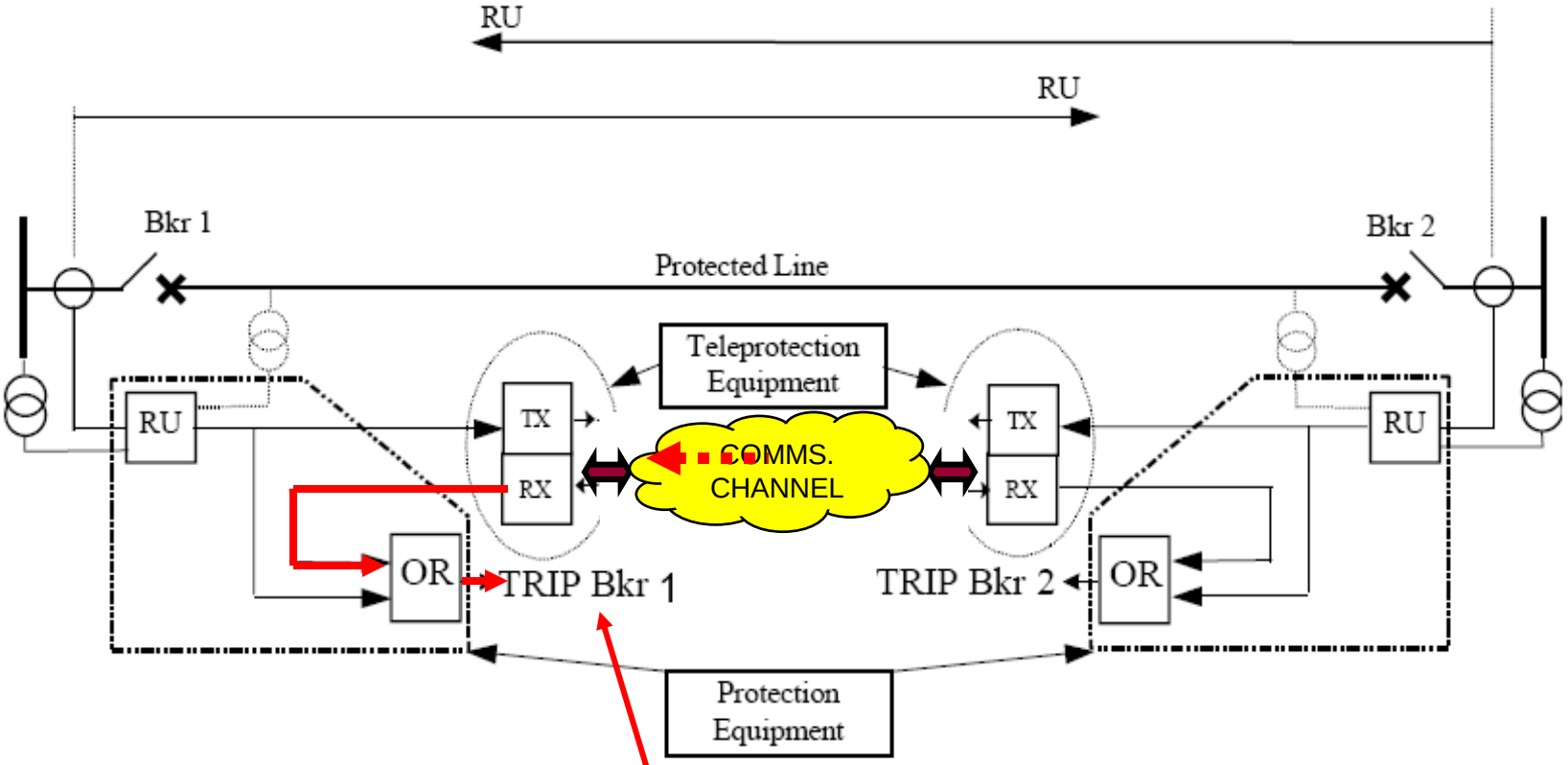
PERFORMANCE PARAMETERS OF TELEPROTECTION SYSTEMS



RU - underreaching trip function, must be set to reach short of remote terminal and must overlap in reach with RU at remote terminal

BREAKER 1 IS TRIPPED UPON RECEPTION OF THE TELEPROTECTION COMMAND

Ref. "Protection using Telecommunications" CIGRÉ JWG 34/35.11 Technical Brochure, 2001



RU - underreaching trip function, must be set to reach short of remote terminal and must overlap in reach with RU at remote terminal

BREAKER 1 IS ERRONEOUSLY TRIPPED

Ref. "Protection using Telecommunications" CIGRÉ JWG 34/35.11 Technical Brochure, 2001

KEY PARAMETERS OF A TELEPROTECTION TERMINAL

- **Dependability:**
  - The ability to detect a teleprotecton command at the receive side in spite of the presence of channel impairments
  - Usually measured in terms of Probability of Missing Command (Pmc)
- **Security:**
  - The ability of the receiver to reject a a false command that has been simulated by the channel impairments
  - Usually measured in terms of Probability of Unwanted Command (Puc)
- **Maximum Actual Transmission Time (Tac):**
  - A real command may be detected by the receiver in spite of the channel impairments, but it may be detected at a later time than expected (the channel impairments delay the proper detection of the transmitted command)
  - If this delay is too long the received command is no longer useful (physical damage to the line has already happened)
  - To be regarded as a useful command, real commands have to be detected at the receiver before a maximum actual transmission time (Tac)

PERFORMANCE OF A TELEPROTECTION SYSTEM

Protection scheme	Maximum actual transmission time T_{ac} ms		Channel quality		Noise duration T_B ms	Security P_{ac}		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).

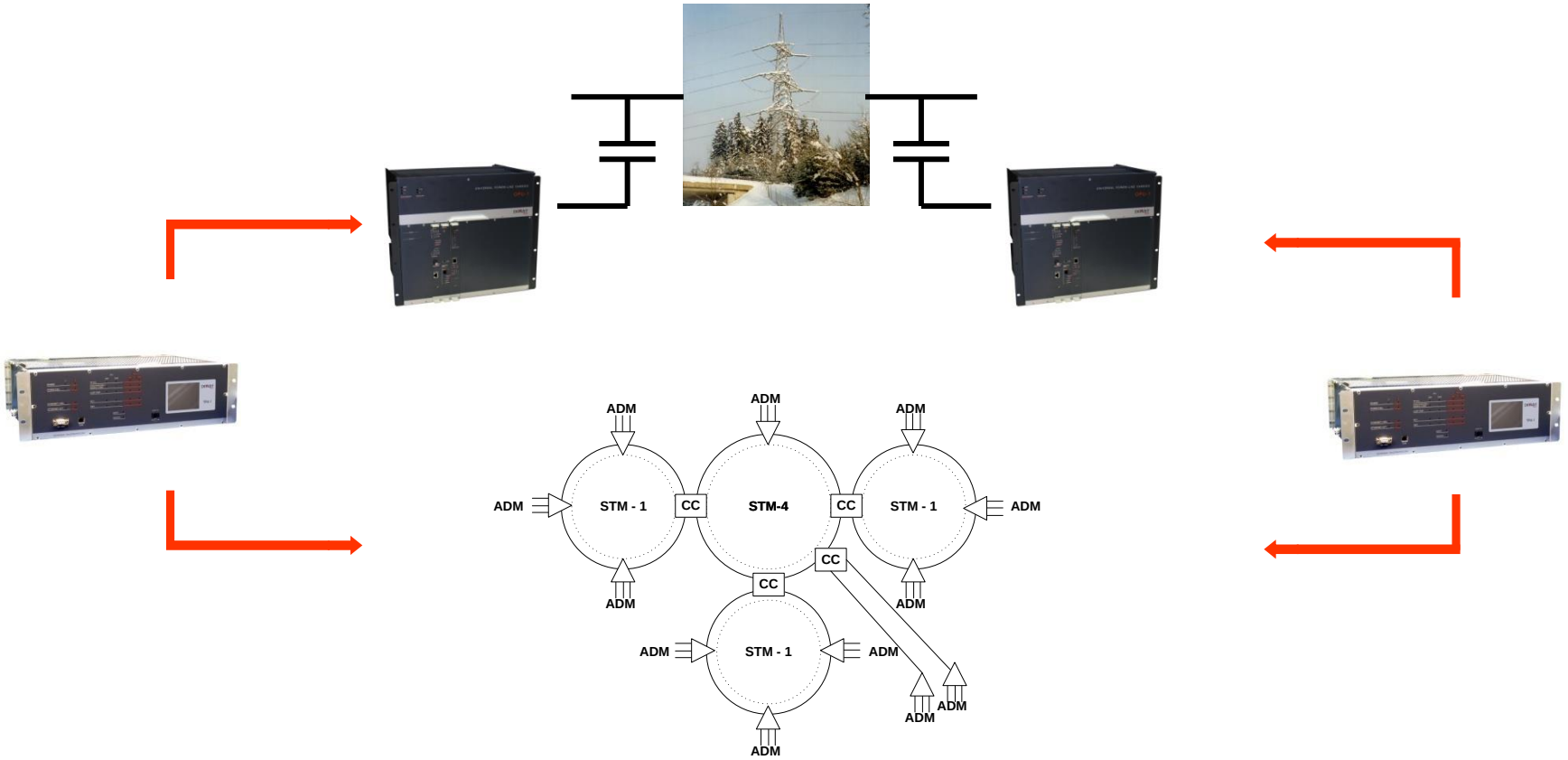
N/A: Not applicable.

(from IEC 60834-1)

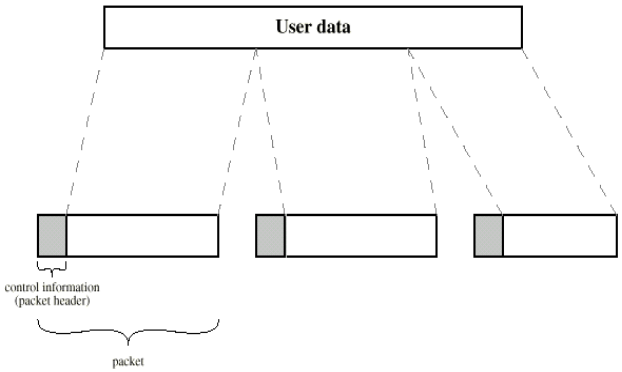
TRANSMISSION OF TELEPROTECTION SIGNALS OVER DEDICATED CIRCUITS

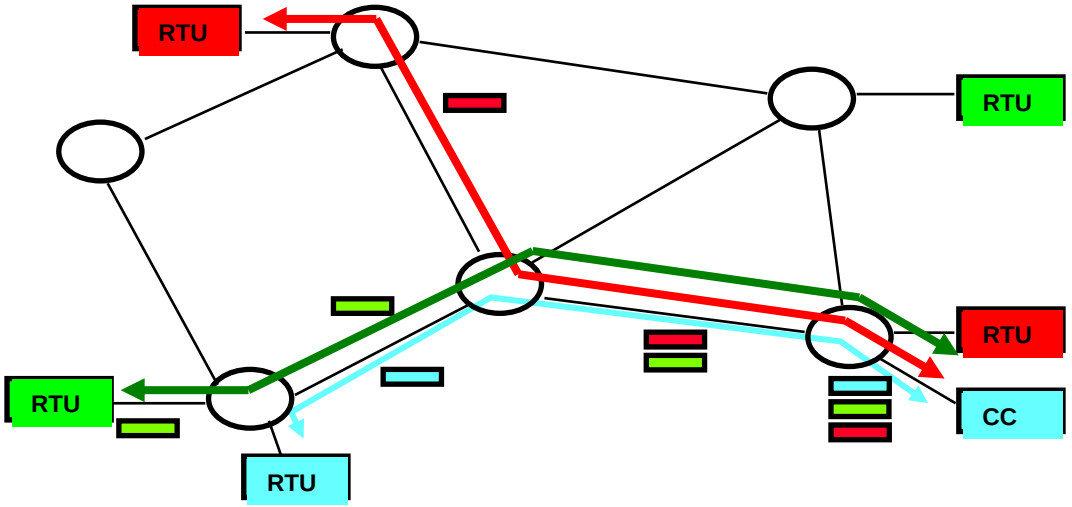
SMART GRID Solutions by

Smart solutions. Strong relationships.



PACKET SWITCHING NETWORKS





- The user information is split into packets

- All packets are statistically multiplex and share the communications network
- The network is more efficient
- The design of the network becomes CRITICAL

TELEPROTECTION OVER IP/MPLS NETWORKS

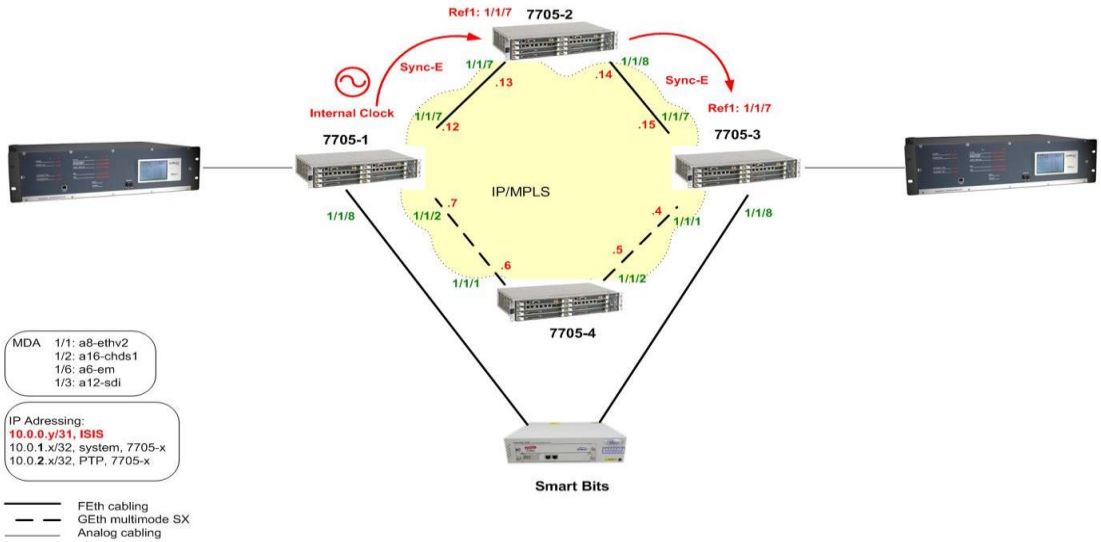
SMART GRID Solutions by

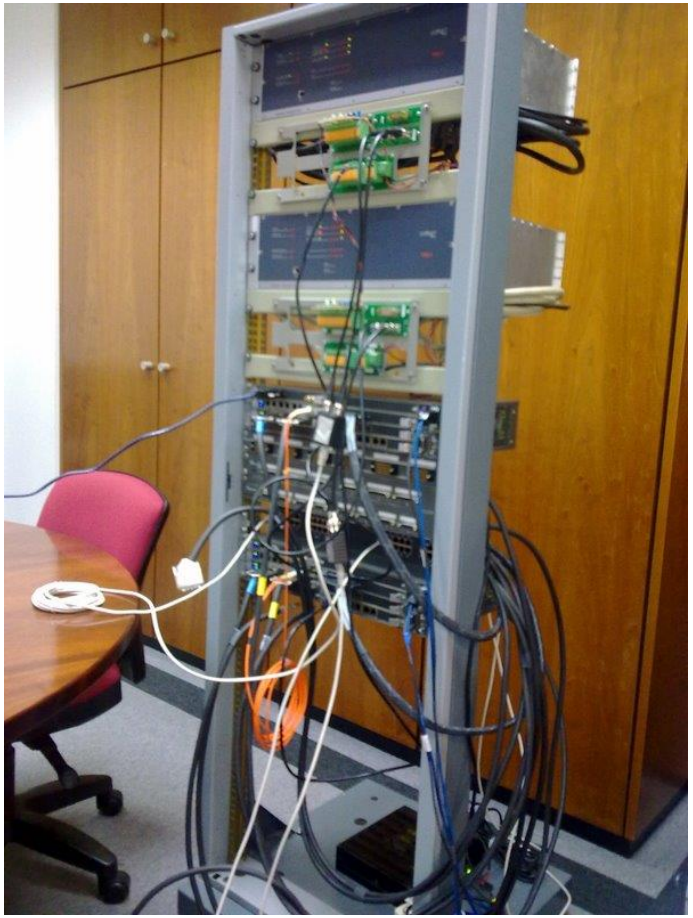
Smart solutions. Strong relationships.

DIMAT

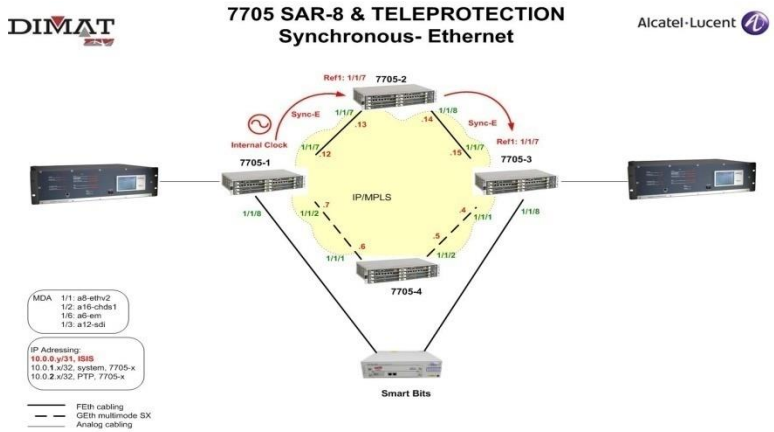
Alcatel·Lucent

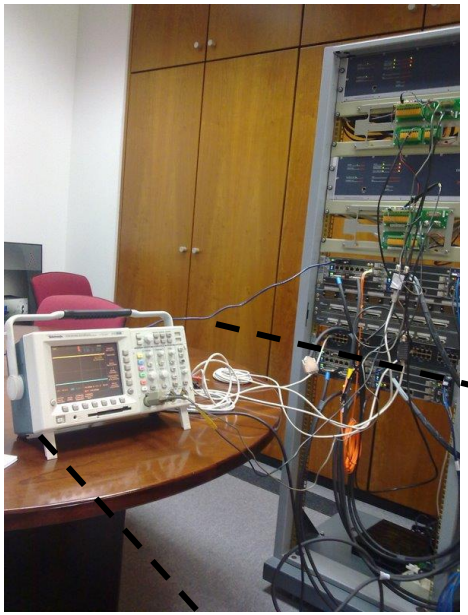
7705 SAR-8 & TELEPROTECTION
Synchronous- Ethernet

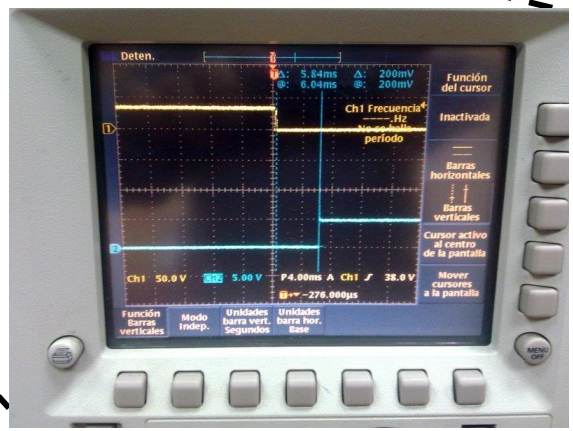




TELEPROTECTION OVER IP/MPLS NETWORKS



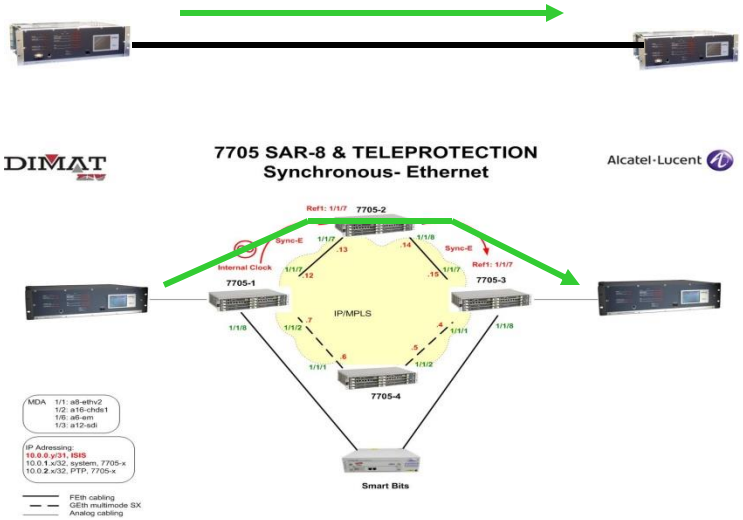


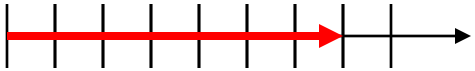


Impact on nominal transmission time, security and dependability of:

- **Jitter buffer size**
- **Network congestion**
- **Path rerouting**

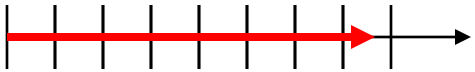
EFFECT OF IP/MPLS NETWORK ON NOMINAL TRANSMISSION TIME (m / n = 1 / 1):





2,48 ... 3,29 msec

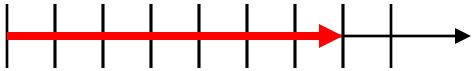
(m / n = 1 / 1 common configuration for blocking applications) (Jitter buffer = 5 msec) (Packetization buffer = 256 bytes)



4,64 ... 5,92 msec

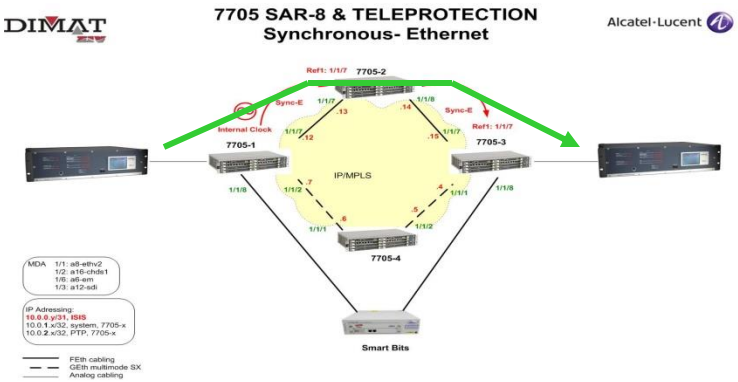
(m / n = 1 / 1 common configuration for blocking applications) (Jitter buffer = 5 msec) (Packetization buffer = 256 bytes)

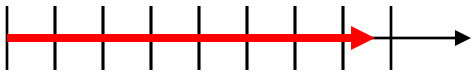
EFFECT OF IP/MPLS NETWORK ON NOMINAL TRANSMISSION TIME (m / n = 15 / 15):



13,4 ... 14,2 msec

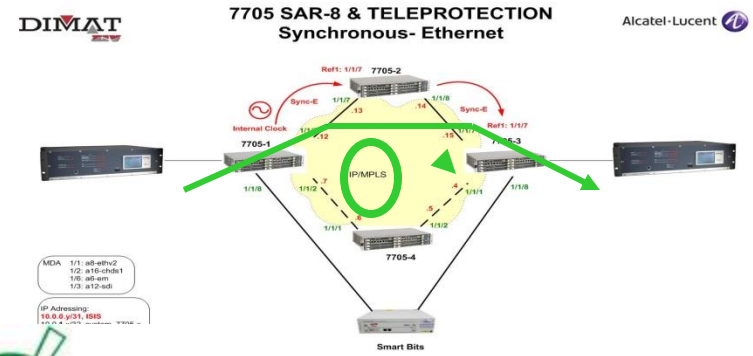
(m / n = 15 / 15, direct trip)

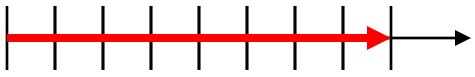




15,2 ... 16,8 msec

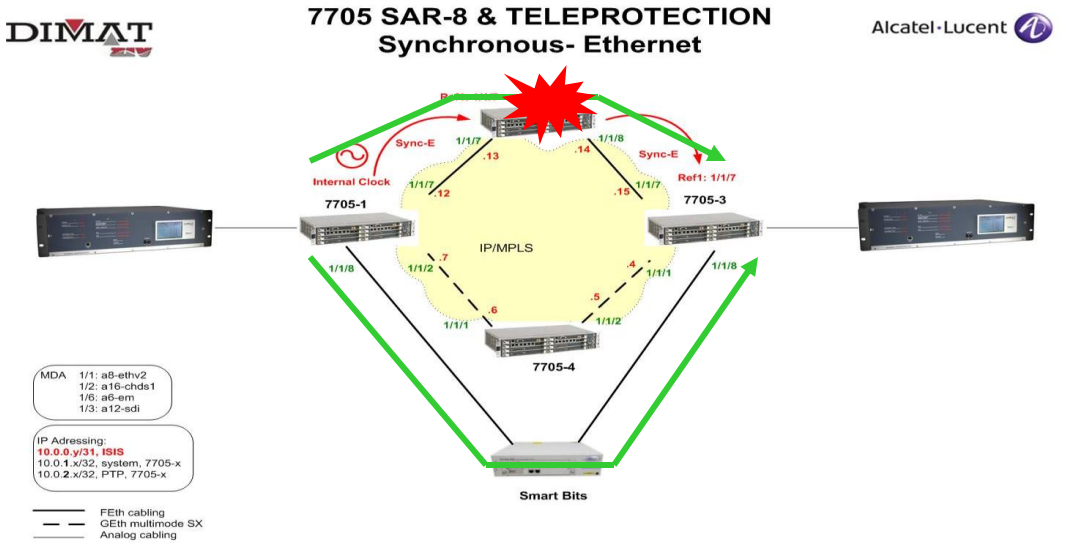
(m / n = 15 / 15, direct trip)
(NO OTHER TRAFFIC)
or
(CONGESTION WITH ADDITIONAL TRAFFIC AT 1 Gb/S, 500 BYTE SIZE)
(Jitter buffer = 5 msec)
(Packetization buffer = 256 bytes)





15,2 ... 16,8 msec
(m / n = 15 / 15, direct trip)
(CONGESTION WITH ADDITIONAL TRAFFIC AT 1 Gb/S, 1500 BYTE SIZE)
(Jitter buffer = 5 msec)
(Packetization buffer = 256 bytes)

EFFECT OF IP/MPLS NETWORK PATH REROUTING ON DEPENDABILITY AND SECURITY:



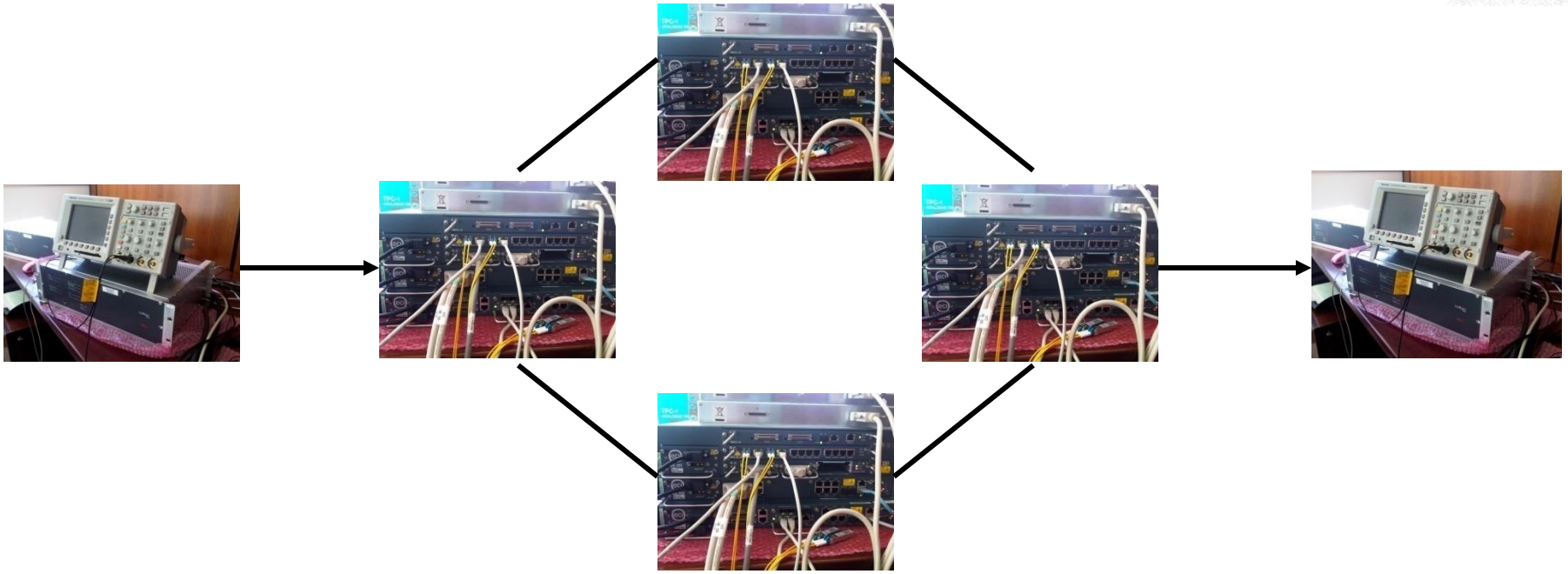
- No alarms during switching to alternative path

- No losses of guard message during switching

- No interruptions of command state during switching

- Very good performance even for low values of jitter buffer (2 msec)

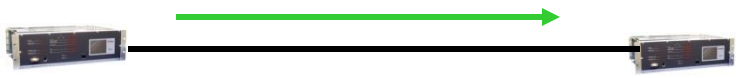
- No false commands were observed

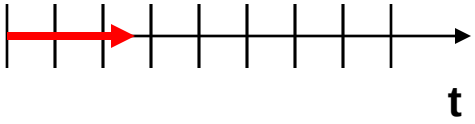


Impact on nominal transmission time, security and dependability of:

- **Jitter buffer size**
- **Network congestion**
- **Path rerouting**

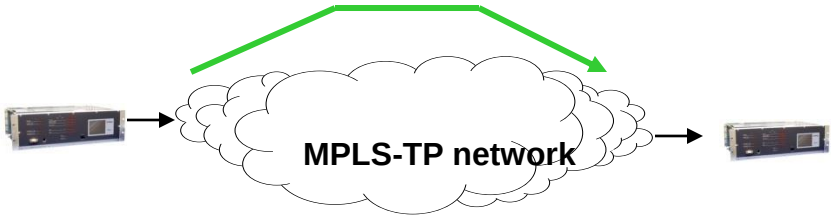
EFFECT OF MPLS-TP NETWORK ON NOMINAL TRANSMISSION TIME (m / n = 1 / 1):

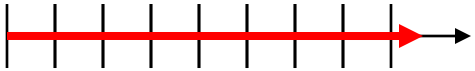




2,48 ... 3,29 msec

(m / n = 1 / 1 blocking applications)

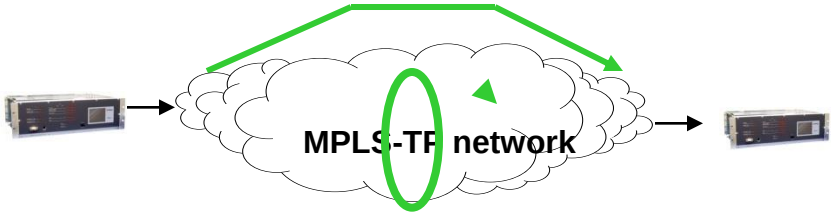




7,44 ... 8,44 msec

(m / n = 1 / 1 blocking applications)

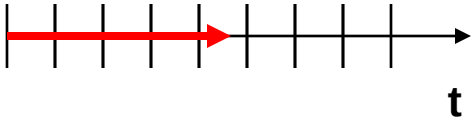
(Jitter buffer = 5 msec)
(Packetization buffer = 256 bytes)



7,92 ... 8,72 msec

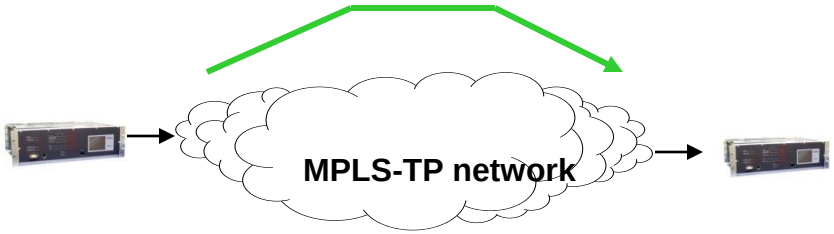
(m / n = 1 / 1 blocking applications)
(Jitter buffer = 5 msec)
(Packetization buffer = 256 bytes)
(Network congested)

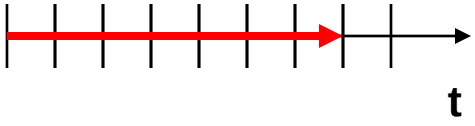
EFFECT OF MPLS-TP NETWORK ON NOMINAL TRANSMISSION TIME (m / n = 15 / 15):



13,4 ... 14,2 msec

(m / n = 15 / 15, direct trip)

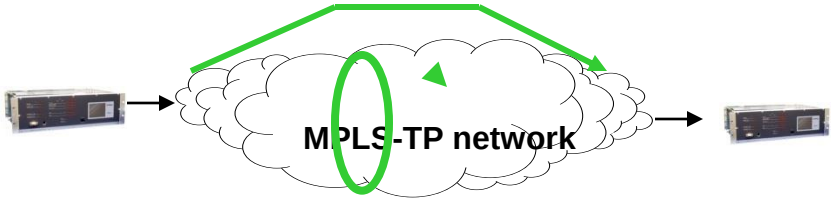


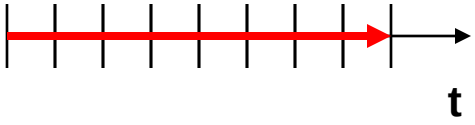


20 ... 20,6 msec

(m / n = 15 / 15, direct trip)

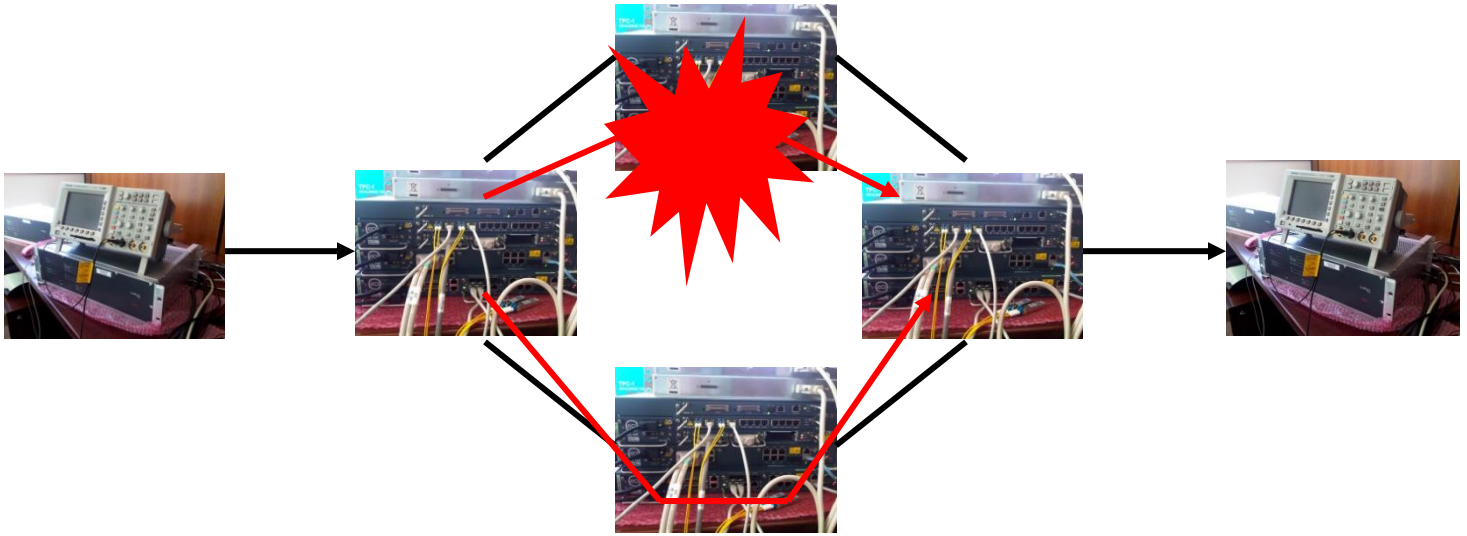
(Jitter buffer = 5 msec)
(Packetization buffer = 256 bytes)





20,8 ... 21,2 msec
(m / n = 15 / 15, direct trip)
(Jitter buffer = 5 msec)
(Packetization buffer = 256 bytes)
(Network congested)

EFFECT OF MPLS-TP NETWORK PATH REROUTING ON DEPENDABILITY AND SECURITY:



- No alarms during switching to alternative path.

- No losses of guard message during switching

- No interruptions of command state during switching

- No false commands were observed

- **The transmission of teleprotection signals over IP/MPLS or MPLS-TP with circuit emulation is feasible**

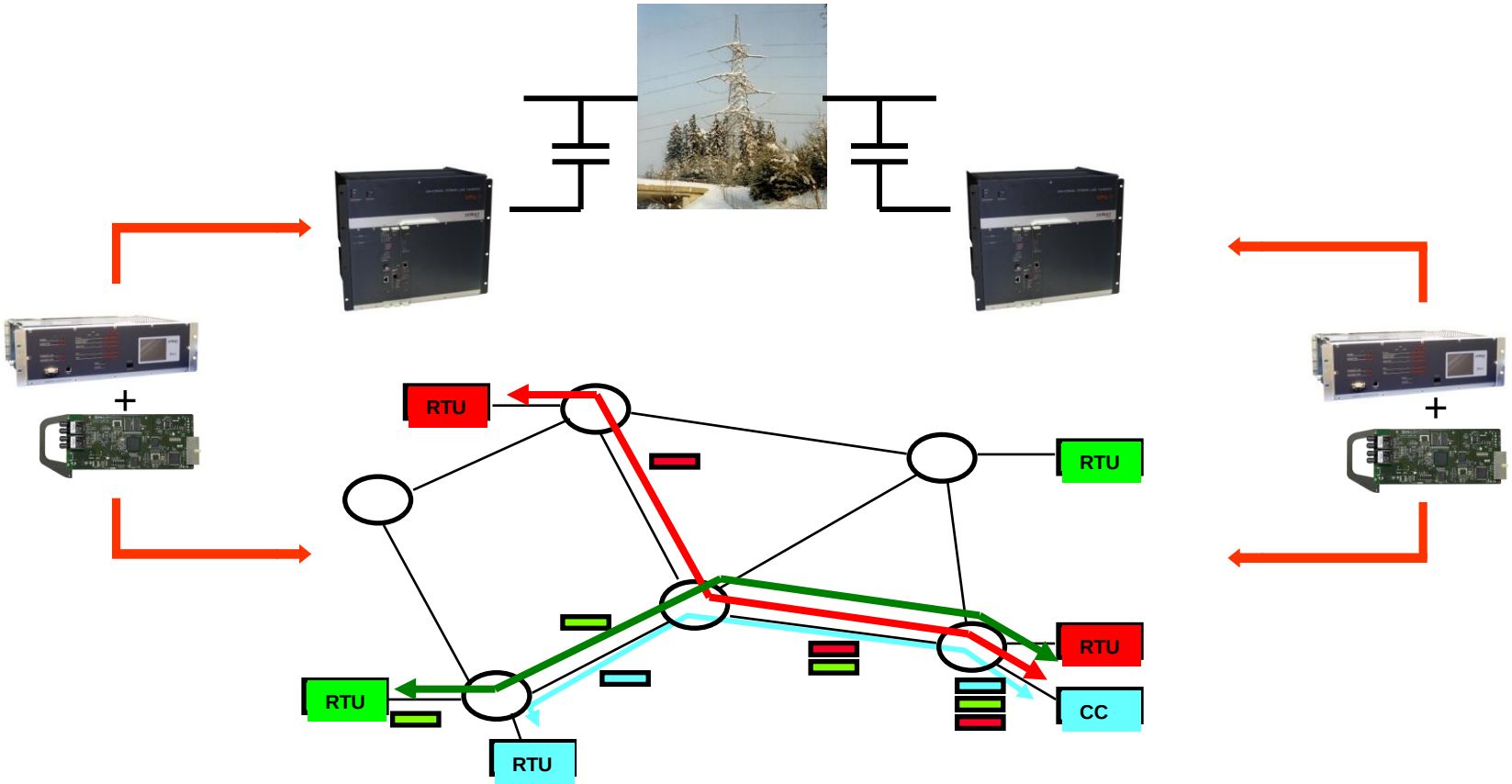
- **Jitter buffer has an impact on transmission time**

- **Useful concept for legacy teleprotection systems**

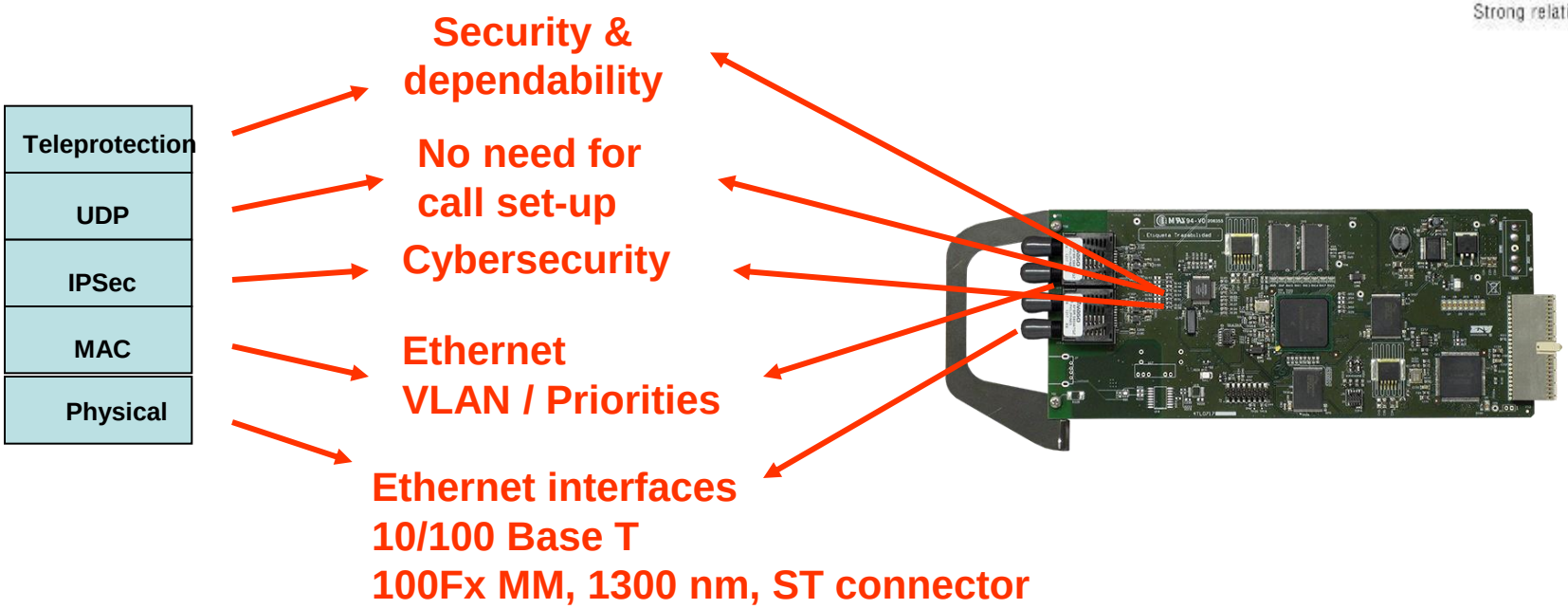
IPIT : NEW TELEPROTECTION INTERFACE FOR PACKET SWITCHING NETWORKS

SMART GRID Solutions by

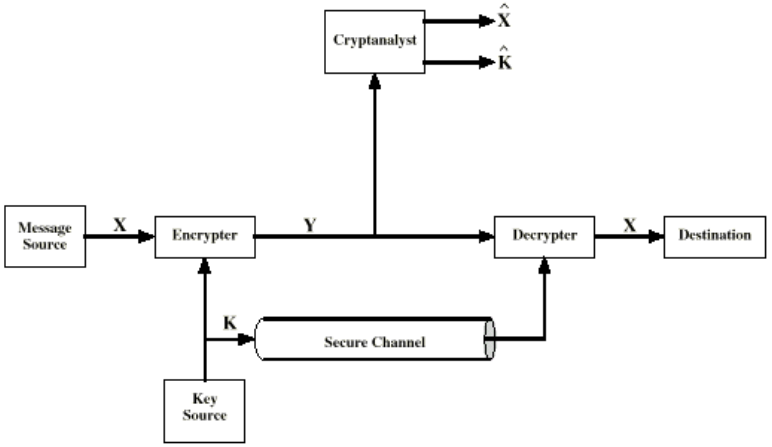
Smart solutions. Strong relationships.



NATIVE IP INTERFACES FOR TELEPROTECTION SYSTEMS



Packet Networks	⇒	The teleprotection information is already packet in nature
Burstiness	⇒	Guard and command have different rates
Statistical multiplexing	⇒	VLANS and priorities
IP Network	⇒	Packet numbering and redundant communications
Cybersecurity	⇒	Cryptography

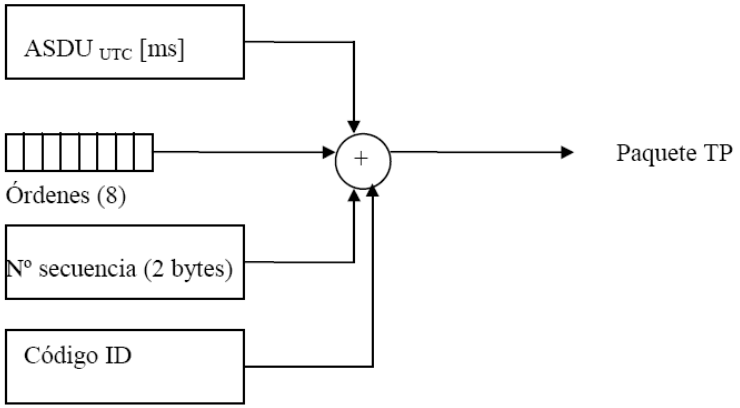


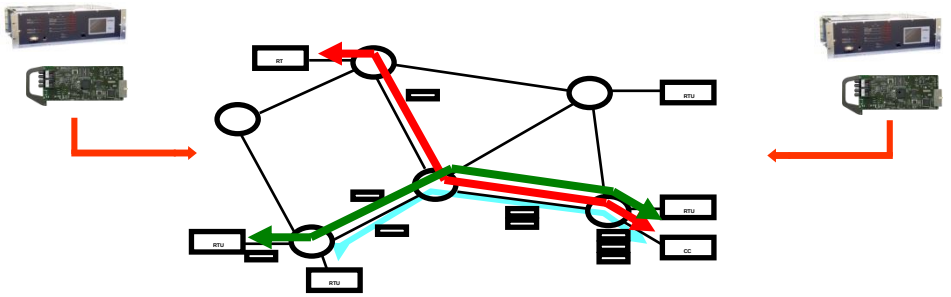
- **Symmetrical key**
- **Asymmetrical key**

- Cybersecurity: Standard IEEE 1686 Ed. September -> Access control to the terminals

-Criptography on IP interface: Symetrical encryption AES-256, key exchange, dynamic update of encryption keys

PACKET NUMBERING





Transmitted packets : 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 – 10 – 11 –12 – 13 – 14 – 15

Received packets : 1 – 2 – 3 – 4 – 9 – 5 – 6 – 7 – 8 – 10 – 11 – 12 – 13 – 14 – 15

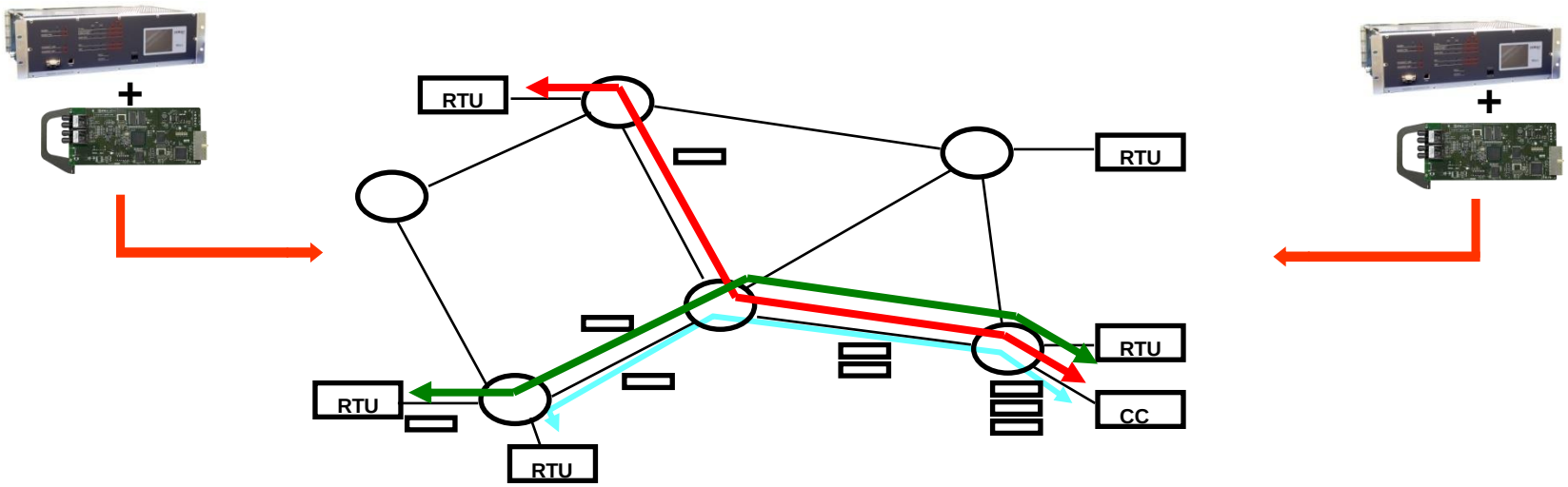
Valid packets

Invalid packets

Valid packet

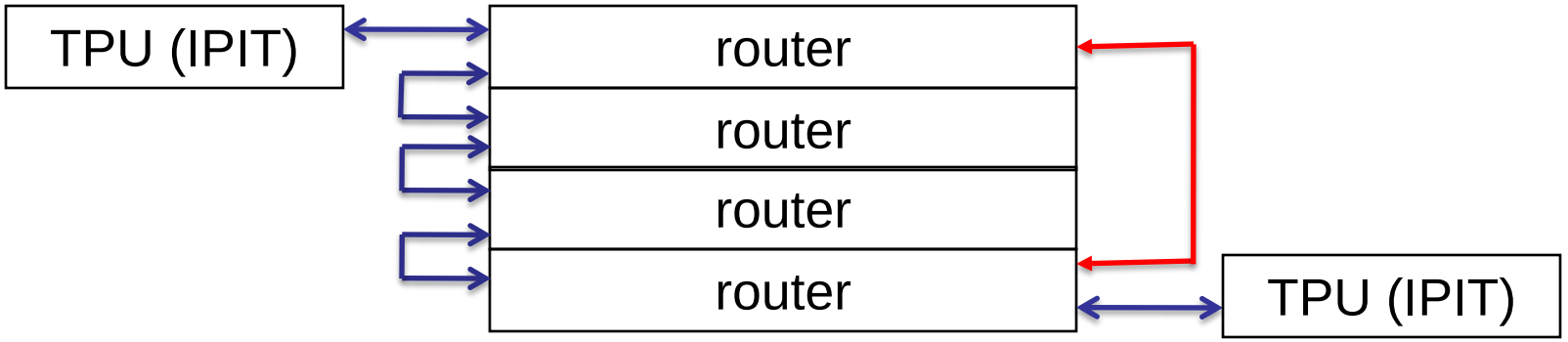
MEASURING THE TRANSMISSION TIME

- Synchronism with PTP (IEEE1588)
- Time stamps in teleprotection packets
- Transmission time is measured for every packet
- MTD and CDV are measured. Alarm is raised if too high
- CLR is measured. Alarm is raised if too high



- **Teleprotection terminals with IP interface delivered to Spain & Argentina**

- **Validation tests :**



- **Commands correctly sent and received**
- **Extremelly low transmission times (around 0.2ms)**
- **Few difference between both paths (0.2us; 225us vs 245us)**
- **Red path disconnection results in a short alarm of loss of signal**

Q1-17: Based on your experience, what are the future expectations of this technology? What is your advice to EPUs?

- IP networks are here to stay…

- Many Power Utilities are still using dedicated circuits (PLC, SDH,…)

- For redundancy purposes, a combination of dedicated circuits and IP networks is suggested

Q1-18: What is the impact on reliability and costs compared to existing teleprotection?

- Teleprotection over IP networks can perfectly work in terms of security, dependability and transmission time

- Network congestion and/or reconfiguration does not have any impact on teleprotection performance

- No impact on costs if IP network is deployed, but good network engineering is important

Thank you