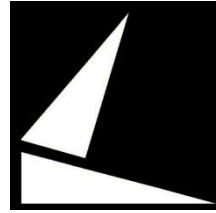


8-10 March 2011
Manchester



EES-UETP Protection of Future Networks with Distributed Generation

ICT Implementation Aspects for Smart Grid Protection

Fabrizio Garrone



Ricerca sul Sistema Energetico - RSE S.p.A.

ICT Implementation Aspects for Smart Grid Protection

Outline

- **Smart Grid Scenarios and ICT**
- **Smart Grid Implementation**
- **Cyber-Risk Scenarios**
- **RSE Experiences**
- **Conclusions**



ICT Implementation Aspects for Smart Grid Protection

Smart Grid Scenarios and ICT

- New view of Electric Power System due to introduction of Smart Grid concepts
 - Supervision (WAMS, Meter)
 - Control (voltage, FACTS)
 - Protection (Infrastructure, Service)



- Impact of Smart Grid on Power Grid management :
 - Operation aspects
 - Control Algorithm (involving DER)
 - Protection aspects
 - Undesired trip , Unintentional islanding



ICT Implementation Aspects for Smart Grid Protection

Smart Grid Scenarios and ICT

- DSO additional communication requirements due to DER
 - Collect information from remote DERs
 - Control DERs that are not in DSO ownership
 - Bi-directional data exchange with DERs



ICT Implementation Aspects for Smart Grid Protection

Smart Grid Implementation

- Communication networks challenges
 - Public networks
 - Different TELCO providers
 - Plug-in devices
 - Lowest cost
 - Could be shared with more applications/services
 - Security



ICT Implementation Aspects for Smart Grid Protection

Smart Grid Implementation

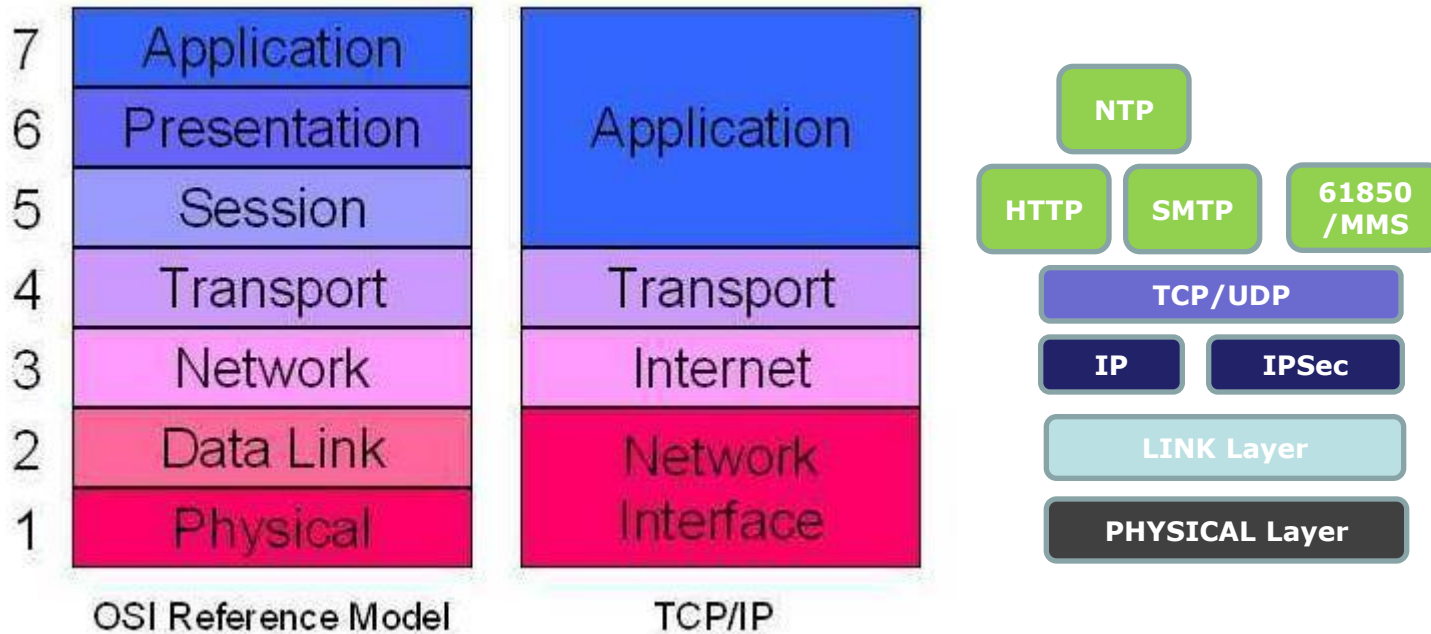
- Solutions (communications)
 - IP technology for all applications
 - Different Communication technologies (Wired, optical fiber, PLC, wireless)
- Solutions (security)
 - Authentication
 - Access rules
 - Encryption



ICT Implementation Aspects for Smart Grid Protection

Smart Grid Implementation

- Communication stacks



ICT Implementation Aspects for Smart Grid Protection

Cyber-Risk Scenarios

- Cyber-Risk definitions
 - Threat
 - Threat (Deliberate, Accidental) (Active, Passive)
 - Attacker / Threat Agent
 - Hackers, Organized Crime, Insider, Terrorists, Software defects, Natural Disaster...
 - Consequences
 - Loss of Control
 - Loss of Communication
 - Attack techniques
 - Brute Force, Bypass, DoS, Malware, Man-In-The-Middle,...
 - Vulnerability
 - Integrity
 - Reliability
 - Availability



ICT Implementation Aspects for Smart Grid Protection

Cyber-Risk Scenarios

- Overall NERC recommendations
 - New planning and analysis techniques to integrate Smart Grid devices and systems
 - Review the characteristics of Distribution
 - Coordinate development of standards
 - New risks metrics to evaluate physical and cyber vulnerabilities due to integration



- Some IEC TC57 WG15 Conclusions:
 - Security considered also in design
 - Security not only “encryption”

ICT Implementation Aspects for Smart Grid Protection

RSE Experiences

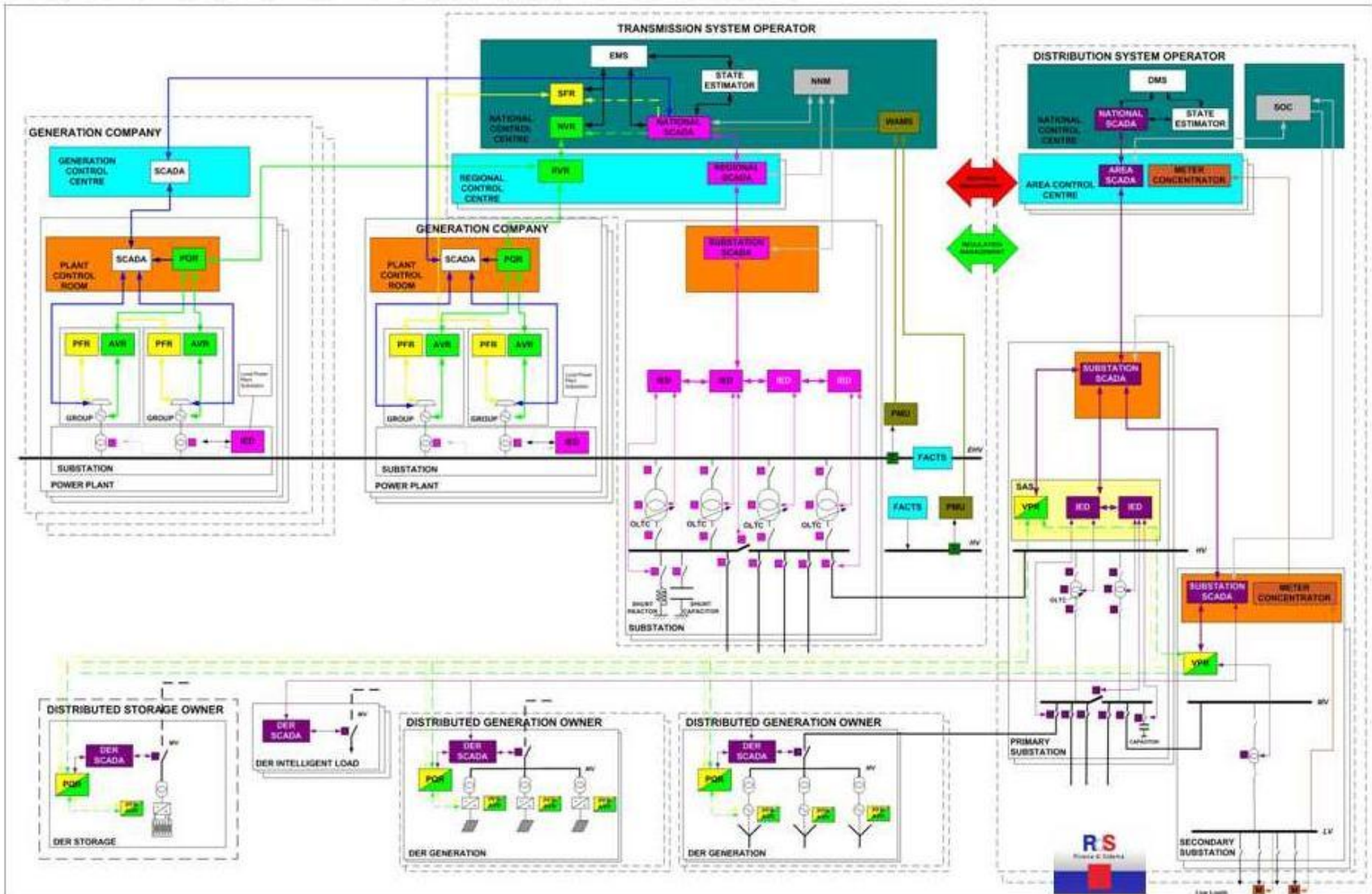
- RSE more significant experiences:
 - Research Fund for the Italian Electrical System
 - European Projects



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Overview

Electric Power System Infrastructure



- Performances requirements by application classes
 - Supervision: no particular time constraints, large amount of data transfer
 - Control: delay in secondary (seconds) and in tertiary (minutes) voltage control algorithms
 - Protections: strict time requirements, short messages



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Overview

- Identify performance requirements
 - Define levels of performances for each application/service
 - Main performance communication indexes:
 - Channel rate
 - Reliability
 - Latency



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Overview

Time Requirements

	Transfer rate	Latency	Priority	Reliability	Availability
Peak shaving (generation curtailment)	✓	✓✓	✓	✓	✓
Anti-islanding	✗	✓✓	✓✓	✓✓	✓✓
Voltage and reactive power regulation	✓	✓	✓✓	✓	✓

✓✓ High, ✓ Medium, ✗ Low

High: 10^2 msec

Medium: sec

Low: minutes



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Protection

- Activities focused on DER Protection
 - Motivations
 - Experimental evaluation of new solutions for protection of DG sources (anti-islanding)
 - Objectives
 - Verify different communication channels and protocols
 - Develop a test methodology
 - Results
 - Tests using real and emulated communication networks
 - Identify metrics



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Protection

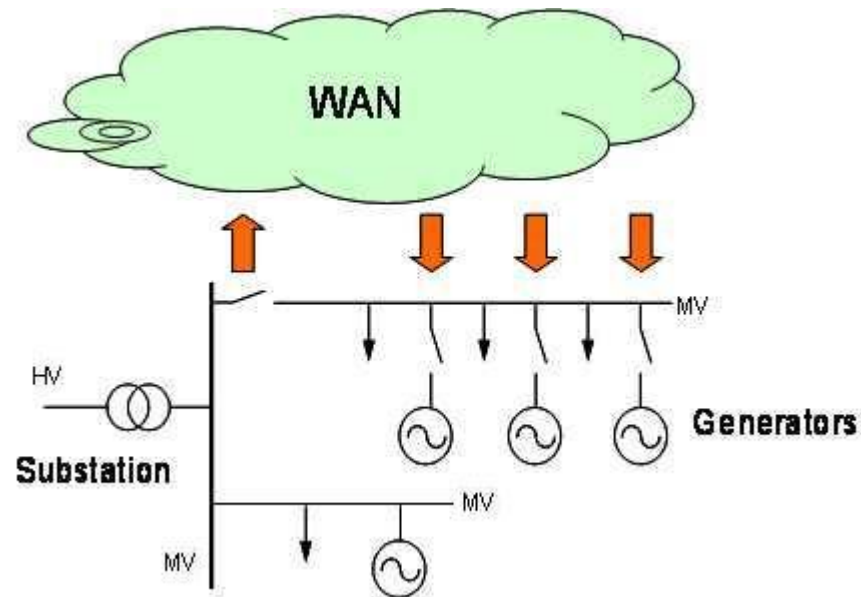
Requirements:

- **undesired trips:** when the communication link between the PS and DG is present and a “normal condition” signal is sent periodically, protections could use larger detection ranges
- **unintentional islanding:** anti-islanding messages from PS should reach generators within the typical detection time of generator protection (~100 msec).



Communication over public IT network involves:

- cyber-security
- standard protocols



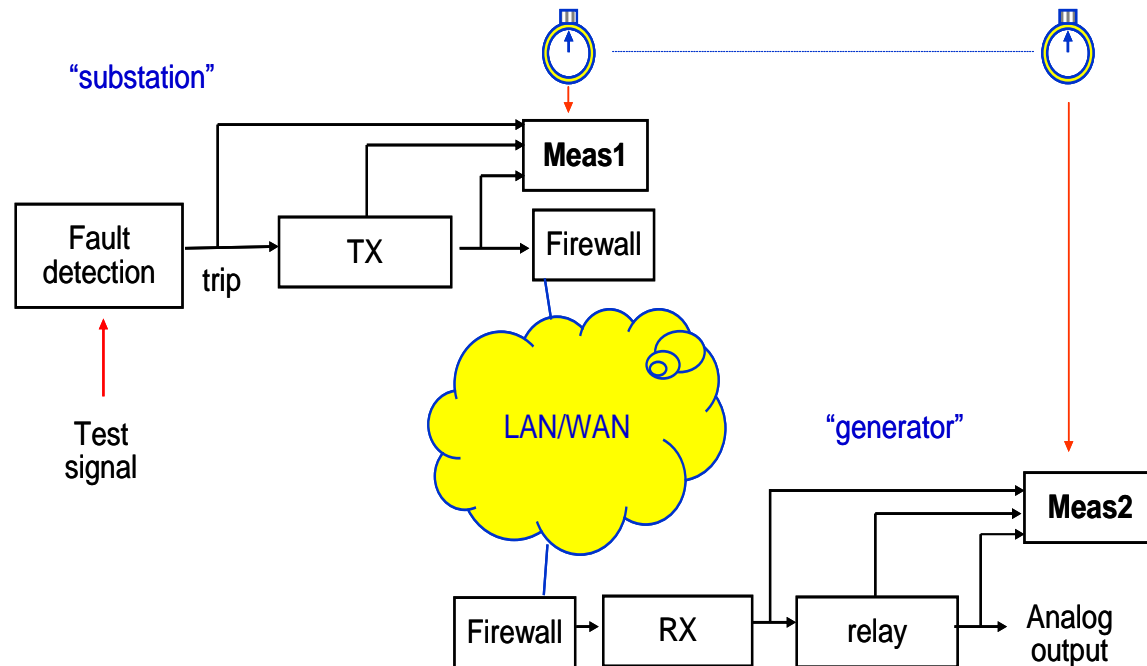
- Testing Setup
 - Scenario with Substation and Protections
 - Time synchronisation
 - Communications on Public Networks
 - Wi-Fi
 - WiMAX
 - Optical fiber
 - Standard Protocols



ICT Implementation Aspects for Smart Grid Protection

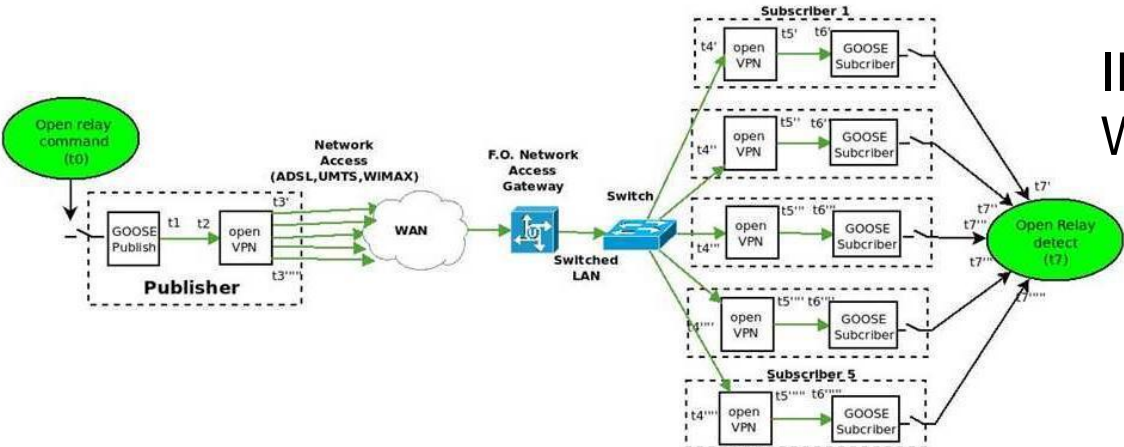
RSE Experiences - Protection

- **Experimental activity:**
 - to identify each single contribution to the overall transmission time
- **Three different configurations evaluated:**
 - protection units
 - PCs
 - IEC 61850 GOOSE embedded devices



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Protection

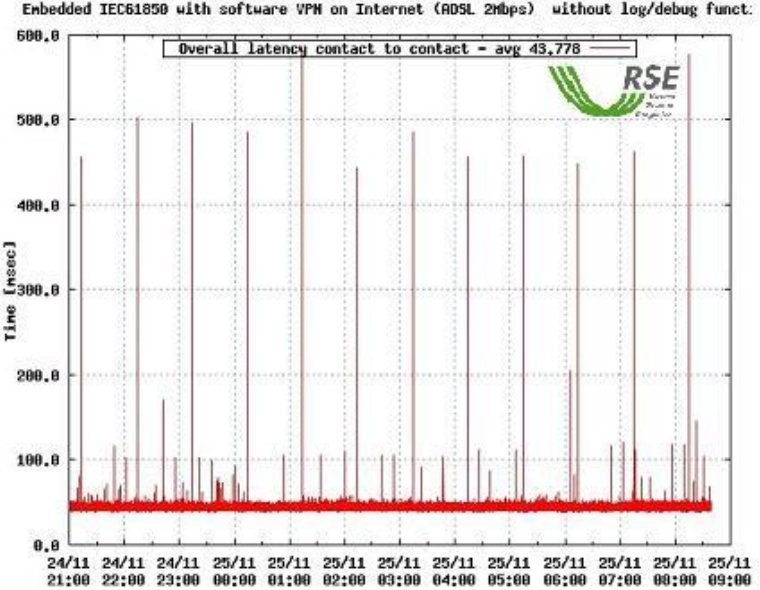


IEC 61850 GOOSE over WAN, encrypted (VPN)

→ level 2 multicast
(publisher > subscribers)

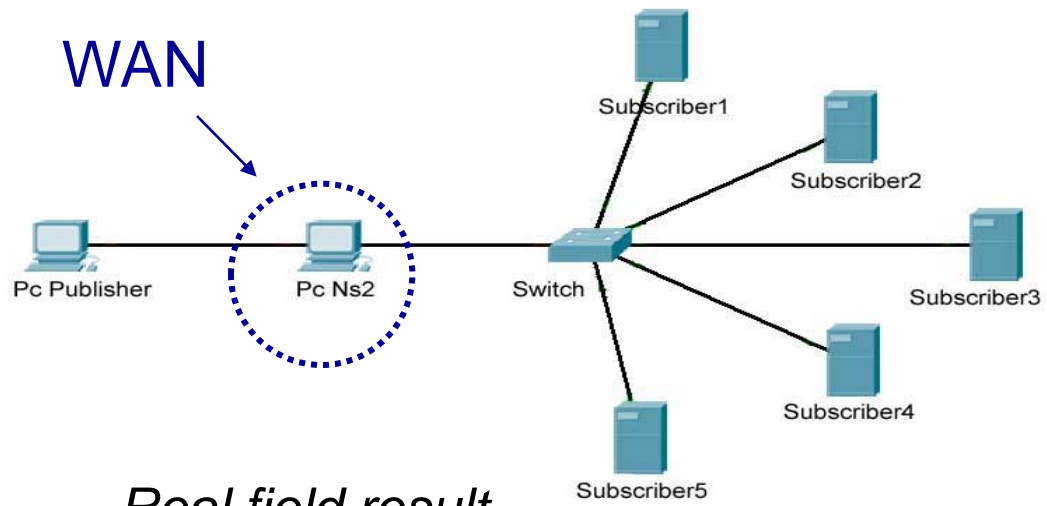


**WAN contribution around 20 msec,
average I/O latency below 50 msec.**
(peaks are related to the key exchange in the VPN)



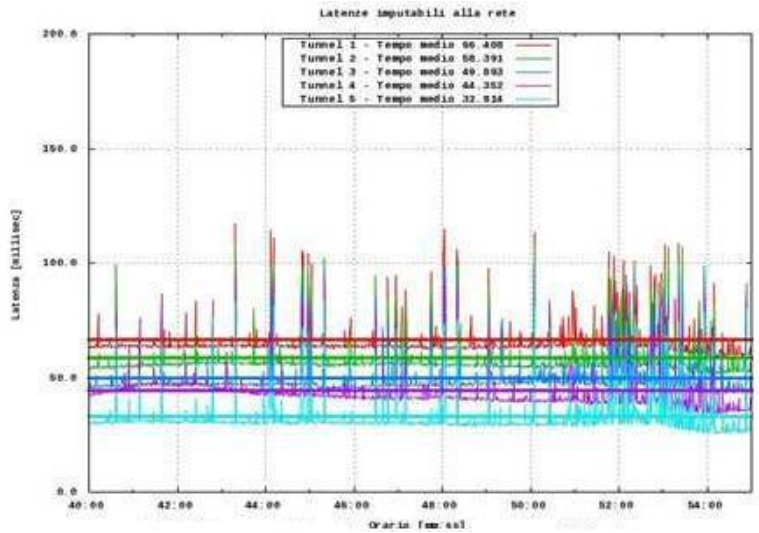
ICT Implementation Aspects for Smart Grid Protection

RSE Experiences - Protection



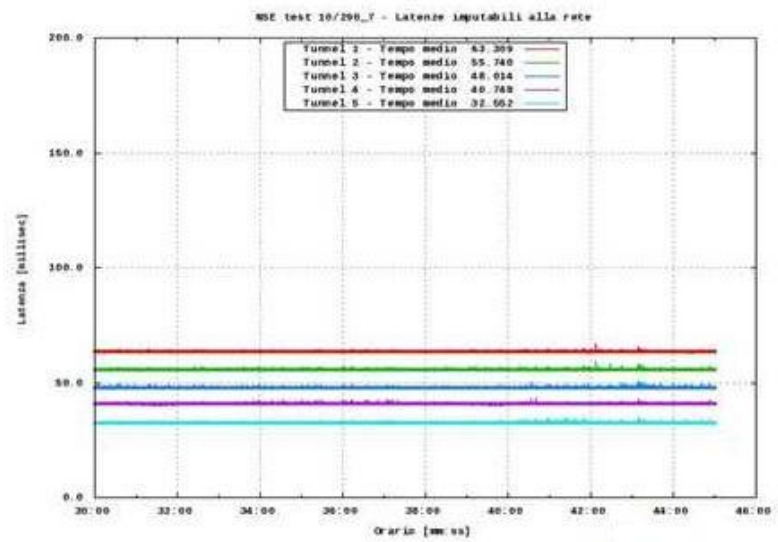
- End-to-end transmission time
- GOOSE 61850, VPN
- 5 subscribers

Real field result



WAN contribution to the overall latency (VPN tunnels with embedded HW)

Emulation result



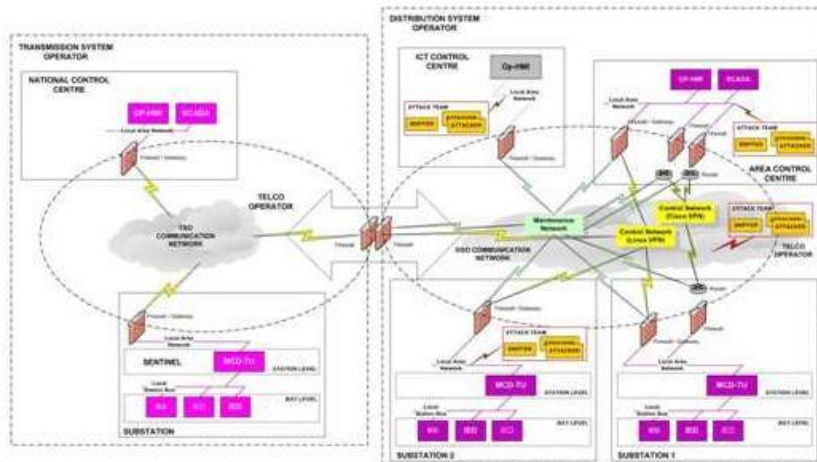
- Activities focused on ICT Security
 - Motivations
 - Experimental evaluation of cyber-risk
 - Objectives
 - Verify impact of cyber-attacks to operation in normal and emergency conditions
 - Develop a cyber-risk-assessment methodology
 - Results
 - Tests setup, attack tools
 - Identify metrics



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences – ICT Security

- Experimental setup
 - Scenarios with TSO and DSO operation functions in normal and emergency conditions
 - Protocols (IEC 60870 family)
 - Communication (Use of IP and IPsec)
 - Attack tools (DoS and Intrusion)
 - Metrics (evaluate delay)



- **Experiments configuration**

- The experiments cover different types of DoS attacks
- The experiments cover attacks to IEC 60870-5-104 communication through Substation/Centre gateways implementing IPsec VPN tunnels

Characteristics	Values
Attack Type	DoS, Intrusion, Viral Infection, Malware
Attack Technique	Packet replying, Packet flooding
Attack Tool	UDP flooding, Syn flooding, TCP replay, Ping
Attack Target	<IP Address – Port Number>
Attack Source / Number of Attackers	<n> / <n>
Attack Sequence Number	<n>
Architectural Pattern / Security Level	IP forward, firewall, VPN, Redundancy
WAN Implementation	Hub Ethernet network 10Mbps, Switched Ethernet 10/100 Mbps
Communication Protocol	TCP/IP, IEC 60870-5-104



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences – ICT Security

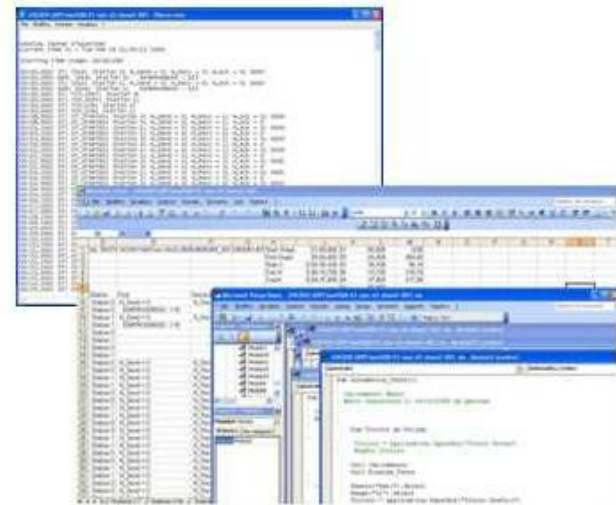
- Denial of the DSO supervision and control functions
 - Preclusion of manual Operator's intervention
 - DSO Extraordinary maintenance
 - Pre-emergency defense actions (load shedding)
 - Failure of automatic actions in emergency conditions
 - Automatic load shedding



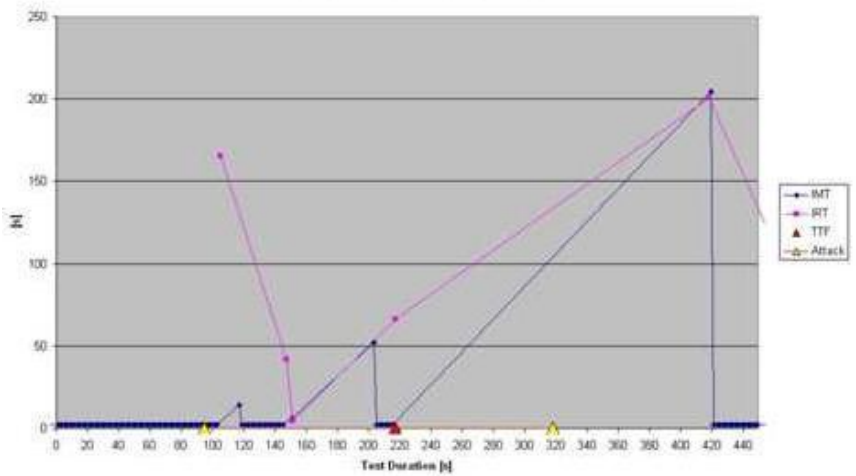
ICT Implementation Aspects for Smart Grid Protection

RSE Experiences – ICT Security

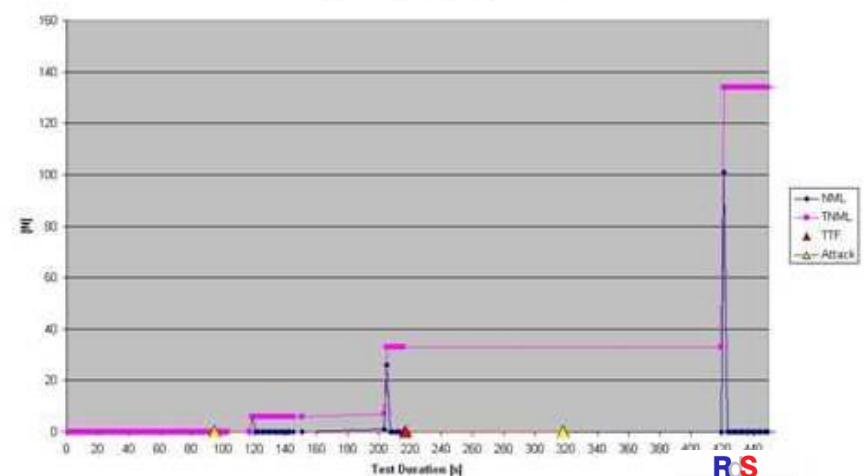
- Testbed applications extended with communication logs
- Excel based application for elaboration of communication measures and their graphical representation
- Measures
 - Inter Message Time (IMT)
 - Inter Reconnection Time (IRT)
 - Time To Failure (TTF)
 - Number of Lost Messages (NLM)
 - Total Number of Loss Messages (TNLM)



104_w_UDPFlooding500_S1_VPH_2d-acc Station 1



104_w_UDPFlooding500_S1_VPH_2d-acc Station 1



ICT Implementation Aspects for Smart Grid Protection

RSE Experiences – ICT Security

- Lessons
 - The increasing bandwidth consumption up to the saturation of the network stack resources of the VPN gateways causes communication crashes
 - The effectiveness of the DoS processes on permanent TCP/IP connections depends on the overloading of the communication resources
 - The effectiveness of the DoS process on Electrical Infrastructure depends on its actual state



ICT Implementation Aspects for Smart Grid Protection

Conclusions

- RSE lessons learned till now:
 - Design
 - Security as add on value
 - Authentication aspects (more users - key exchange)
 - Testing
 - Scenarios (definition of experiment setup standardization CIM – IEC 61850)
 - Communication channels (evaluation of different technology, market devices)
 - Protocol analysis (evaluation of vulnerability of single protocol used for one specific function)
 - Community
 - Experience exchange (DERlab, DERri, EERA, SEESGEN ICT)



ICT Implementation Aspects for Smart Grid Protection

Acronyms

CIM – Common Information Model

DER – Distributed Energy Resource

DG – Distributed Generation

DoS – Denial of Service

DSO – Distribution System Operator

FACTS - Flexible Alternating Current Transmission Systems

GOOSE – Generic Object Oriented Substation Events

ICT - Information and Communication Technology

MMS – Manufacturing Message Specification

NERC – North American Electric Reliability Corporation

NTP – Network Timing Protocol

PLC - Power Line Carrier

TCP – Transmission Control Protocol

TSO – Transmission System Operator

UDP – User Datagram Protocol

VPN – Virtual Private Network



Bibliography (recent):

- IEC Smart Grid Standardization Roadmap - June 2010 – Edition 1.0
- IEC TC 57 Standards (IEC 61850, IEC 60870, IEC62351 ...)
- NIST IR 7628 Guidelines for Smart Grid Cyber Security – August 2010 - 3 voll
- NERC Reliability Considerations from the Integration of Smart Grid – December 2010
- GAO Electricity Grid Modernization – Progress being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed – January 2011
- Cigrè SC D2 Information Systems and Telecommunication



ICT Implementation Aspects for Smart Grid Protection

Links

UE Projects:

- DERlab <http://www.DER-lab.net>
- SEESGEN ICT <http://seesgen-ict.rse-web.it/>
- CRUTIAL <http://crutial.rse-web.it/>
- OPEN Meter <http://www.openmeter.com/>
- ADDRESS <http://www.addressfp7.org/>
- DERri <http://www.DER-ri.net>

Italian Projects:

- RSE <http://www.rse-web.it/english/default.asp>
- Ricerca di Sistema <http://www.ricercadisistema.it/>
- Politecnico di Milano
<http://www.fondazionepolitecnico.it/pagine/SmartDGLab.aspx>
- TERNA <http://www.terna.it/>
- GSE <http://www.gse.it/>



Thank you for your attention

Contact:

Fabrizio Garrone

Power System Development Department

RSE S.p.A.

tel. +39 0239927232

Email fabrizio.garrone@rse-web.it

