Testing della Sicurezza nelle Comunicazioni Standard delle Smart Grid

Giovanna Dondossola, Roberta Terruggia, Paolo Wylach

Telecontrollo Made in Italy: a step forward for a better life, Milano 29-30 settembre 2015

Agenda

- Smart Grid – comunicazioni e sicurezza
- Testbed RSE e metodologia sperimentale
- Caso d'uso esaminato
- Risultati sperimentali
- Lesson learned

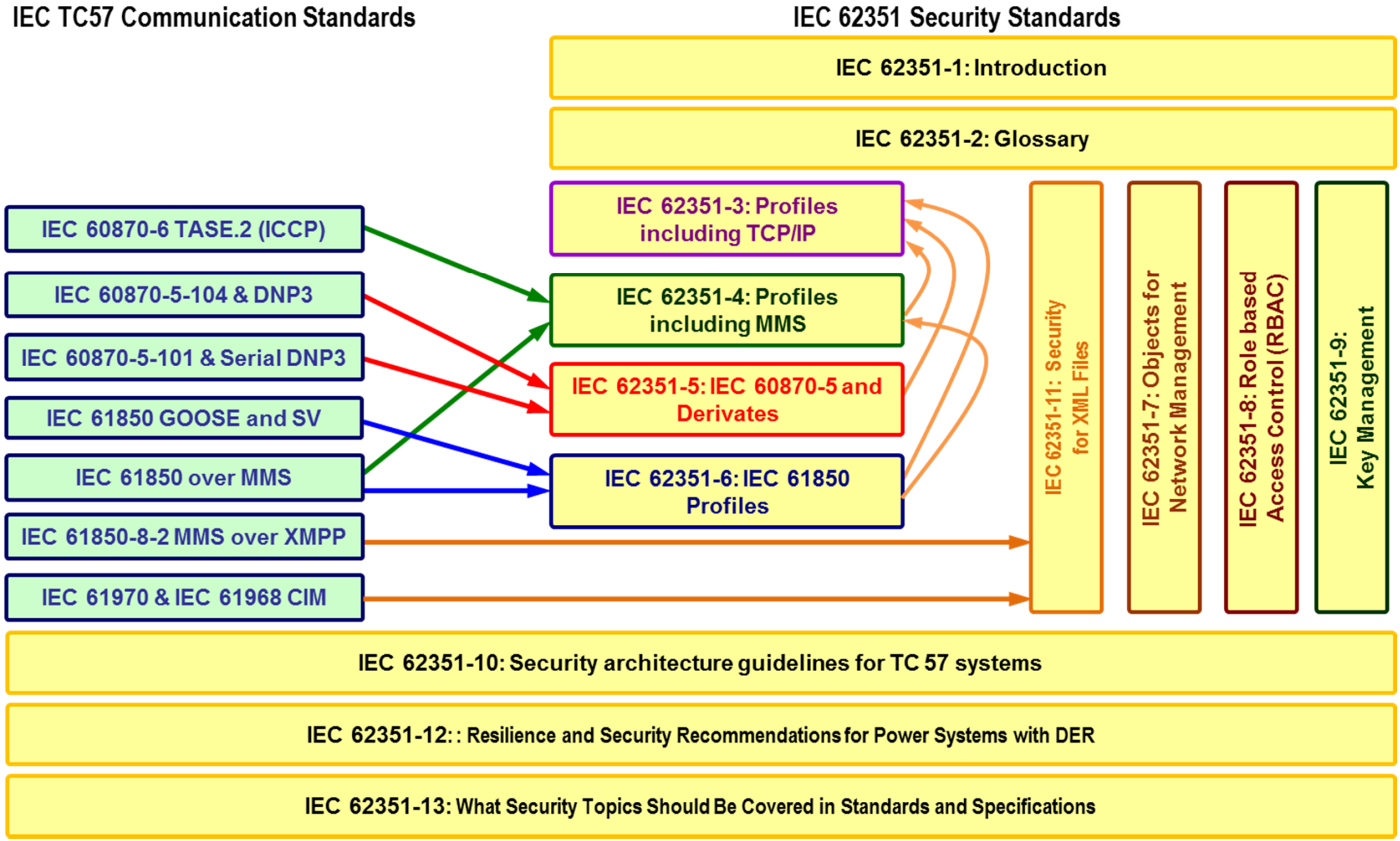
Smart Grid – comunicazioni e sicurezza

- **Le smart grid hanno un'architettura di rete molto complessa**
  - **Eterogeneità di *operatori*, *dispositivi*, *protocolli*, *tecnologie*** ***Interoperabilità?***
  - **Reti di controllo non isolate, comunicazioni tra domini diversi** ***Sicurezza?***

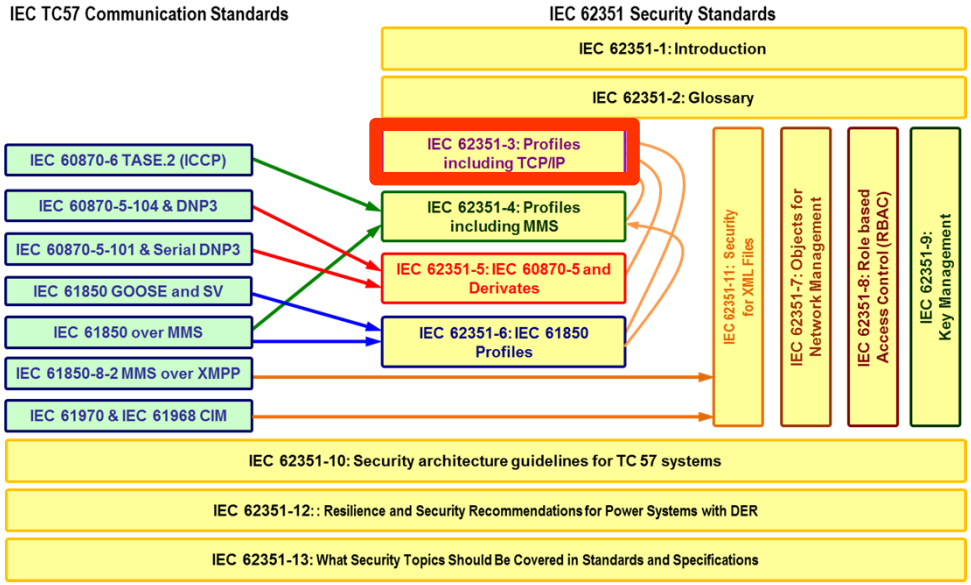
- **Necessità di impiego di standard ICT**
  - **Protocolli e tecnologie di comunicazione**
  - **Sicurezza delle comunicazioni**

Proposta di una metodologia sperimentale per la valutazione degli standard di sicurezza

Mapping of TC57 Communication Standards to IEC 62351 Security Standards



End-to-end security → IEC 62351-3 (TLS)



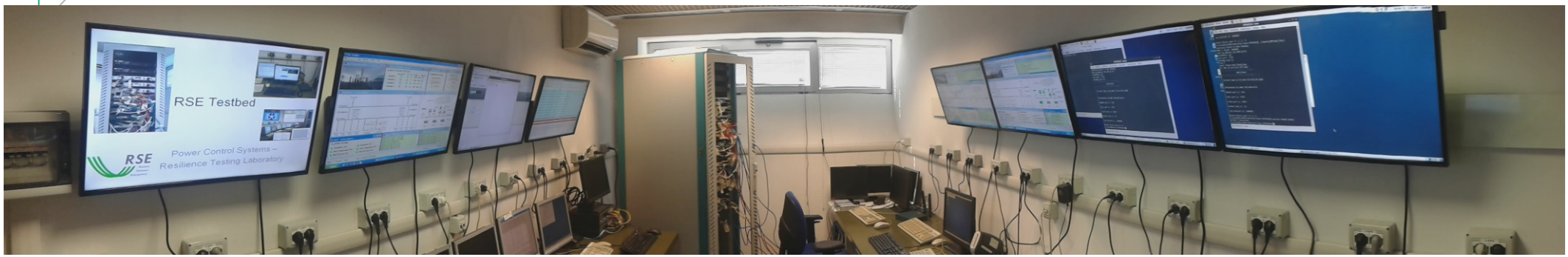
Vincoli alle specifiche TLS

- Versione → TLS v1.2 (retrocompatibilità v1.0 e v1.1 , indicazione IS 2014)
- Scambio bidirezionale e verifica dei certificati (mandatory)
- MAC (Message Authentication Code)
- Public key exchange (dimensione delle chiavi, algoritmi etc.)
- Session renegotiation, session resumption

IEC 62351 Part 3: Communication network and system security – Profile including TCP/IP

- Specifica come fornire la sicurezza ai protocolli SCADA e di telecontrollo che utlizzano TCP/IP come layer di trasporto
- Contrasta gli attacchi più critici dei sistemi di telecontrollo (*MITM, Replay, Eavesdropping)*
- È un riferimento per tutti gli standard IEC che necessitano di sicurezza per i protocolli basati su TCP/IP

RSE PCS-ResTest Lab



Grid and ICT Control Centres

NTP, PTP

Syslog, SNMP

IEC 60870-5-104

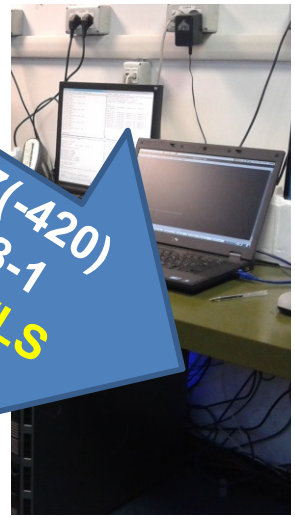
Substation Control

IEC 61850-7(-420)

IEC 61850-8-1

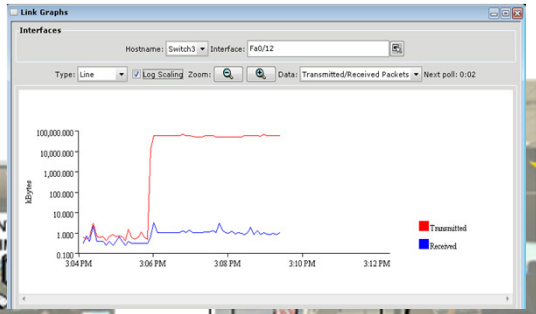
IEC 62351-3, TLS

DER Control



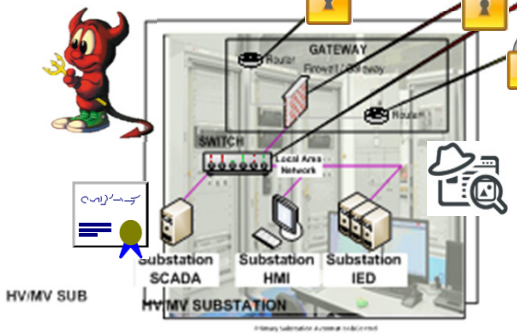
Testbed RSE – Tecnologie e strumenti

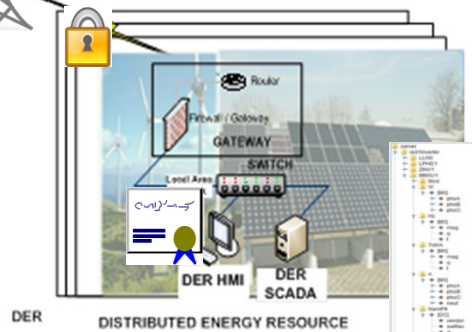
Control Center HMI



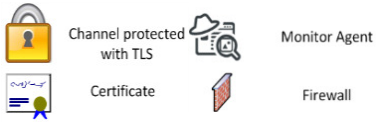
ICT Monitoring

LTE M2M





DER IEC 61850 Profile



- Monitoring
- Security
- 4G/3G M2M
- Attacks
- Fault Manag.
- Visualisers
- Trace Analysers
- ICT network simulators

Caratterizzazione test

PARAMETRI TEST

- Durata test
- Numero run
- Numero messaggi applicativi inviati
- Frequenza invio messaggi applicativi

TECNOLOGIE DI RETE

- Tipo di rete: fissa, mobile
- Tecnologia di comunicazione
- Protocolli di comunicazione
- Parametri caratteristici dei protocolli di comunicazione

MISURE DI SICUREZZA

- Protocolli di sicurezza
- Parametri caratteristici del protocollo (algoritmi di cifratura e firma, lunghezza chiavi, ecc.)

ATTACCHI

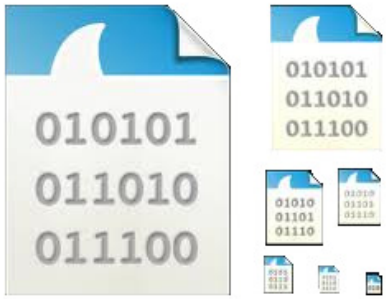
- Tipo di attacco
- Parametri caratteristici dell'attacco (frequenza, dimensione pacchetti ecc.)

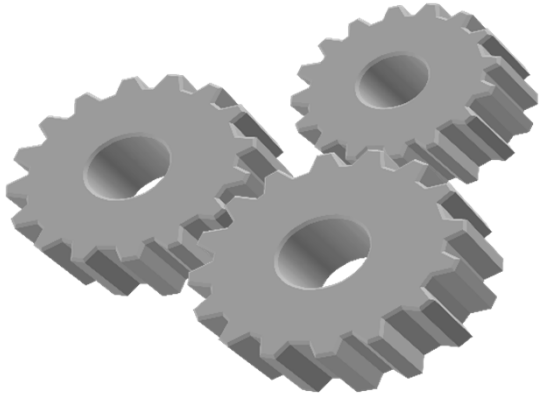
NUMERO DI SERVER

POSIZIONE GEOSPAZIALE DEI SERVER

ORARIO E GIORNO DI SVOLGIMENTO DEL TEST

Analisi delle tracce

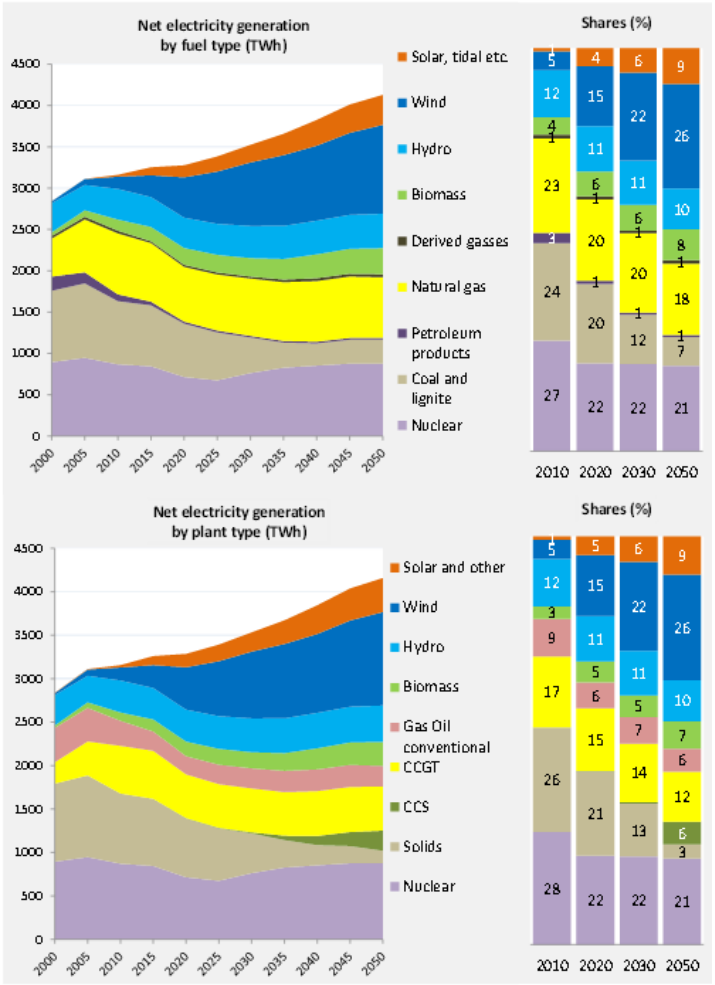


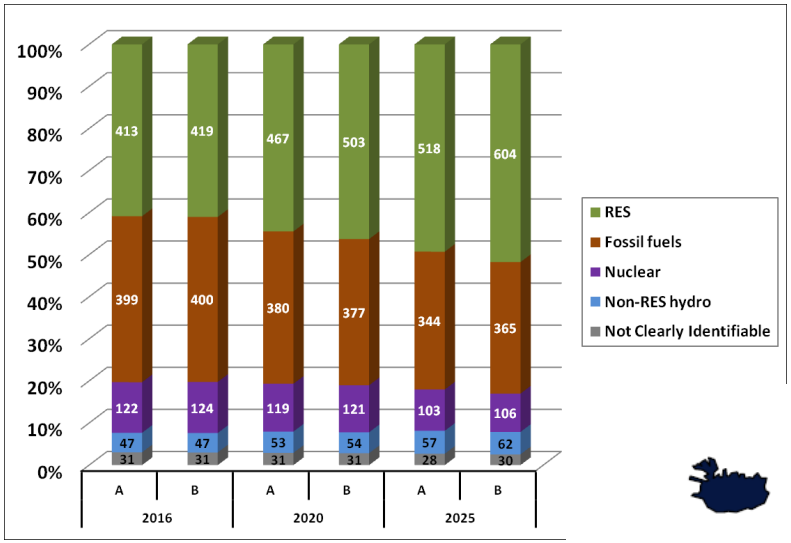


Tracce + **Tool di analisi** = **Misure**

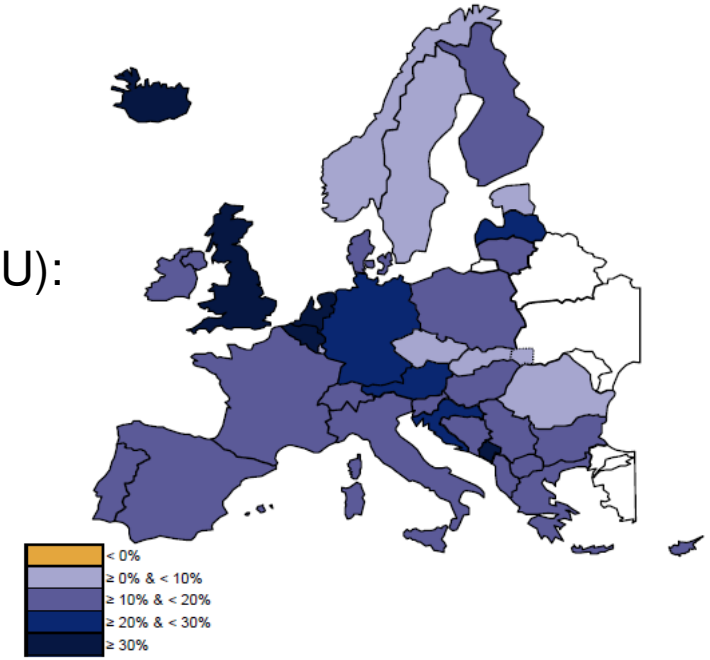
Controllo DER nelle reti MT – motivazioni

Percentuale di RES in aumento





Capacità RES installata (EU): proiezione 2016/2025

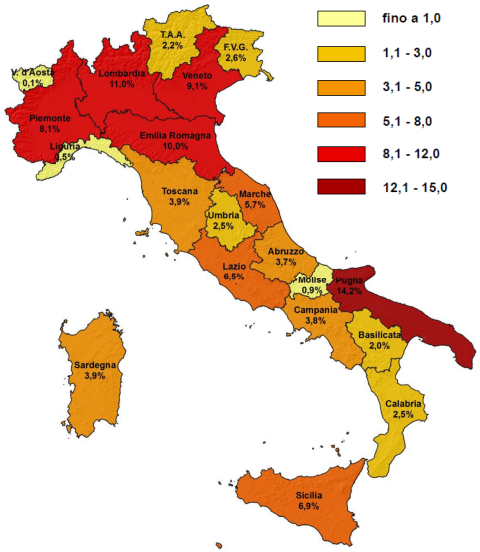


EU ENERGY, TRANSPORT AND GHG EMISSIONS TRENDS TO 2050 (EC)

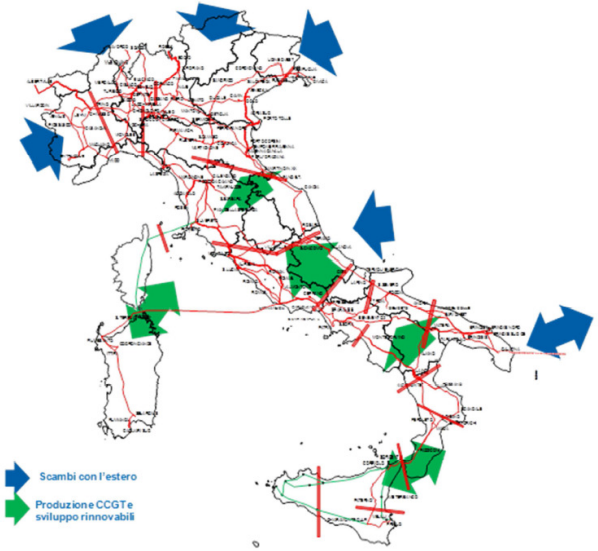
Fonte: ENTSO-E Scenario Outlook & Adequacy Forecast 2015

Controllo DER nelle reti MT – motivazioni

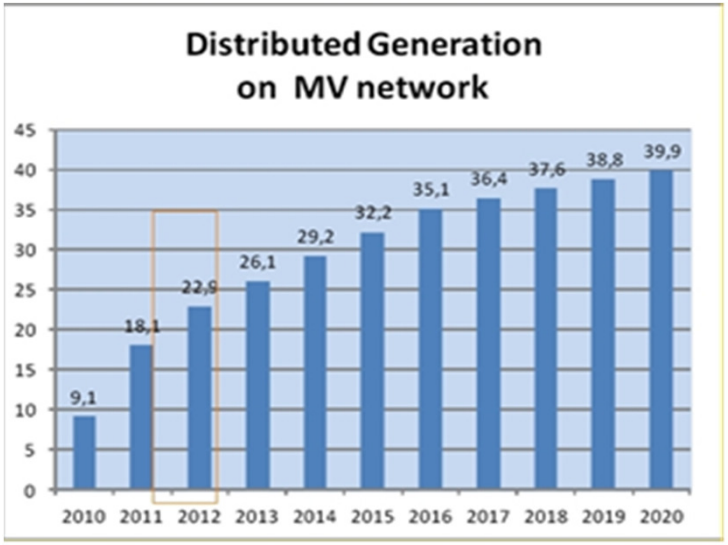
Range di tensione fissati dallo standard EN 50160



Distribuzione regionale potenza fotovoltaica
GSE Rapporto statistico Fonti Rinnovabili 2013



Limiti di trasporto e rischi di congestione
TERNA Piano di Sviluppo 2015



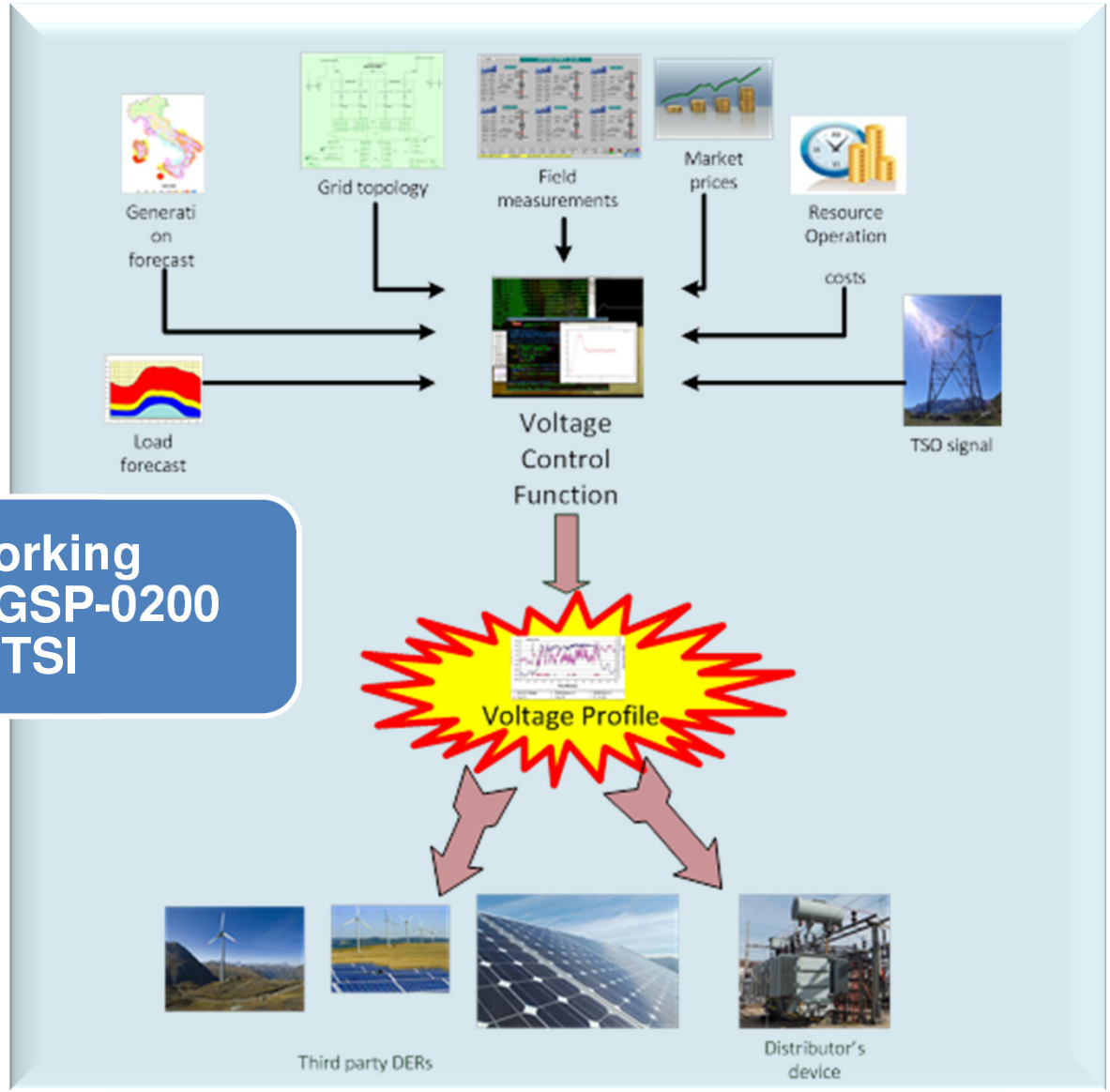
- Circa 40 GW da fonti rinnovabili installate (PV/eolico) connesse alla rete MT entro il 2020
- Regole di connessione (**Norma CEI 0-16**)

  Vincoli obbligatori potenza RES MT

  200 kW < P_n < 6 MW
- Topologia di rete estesa

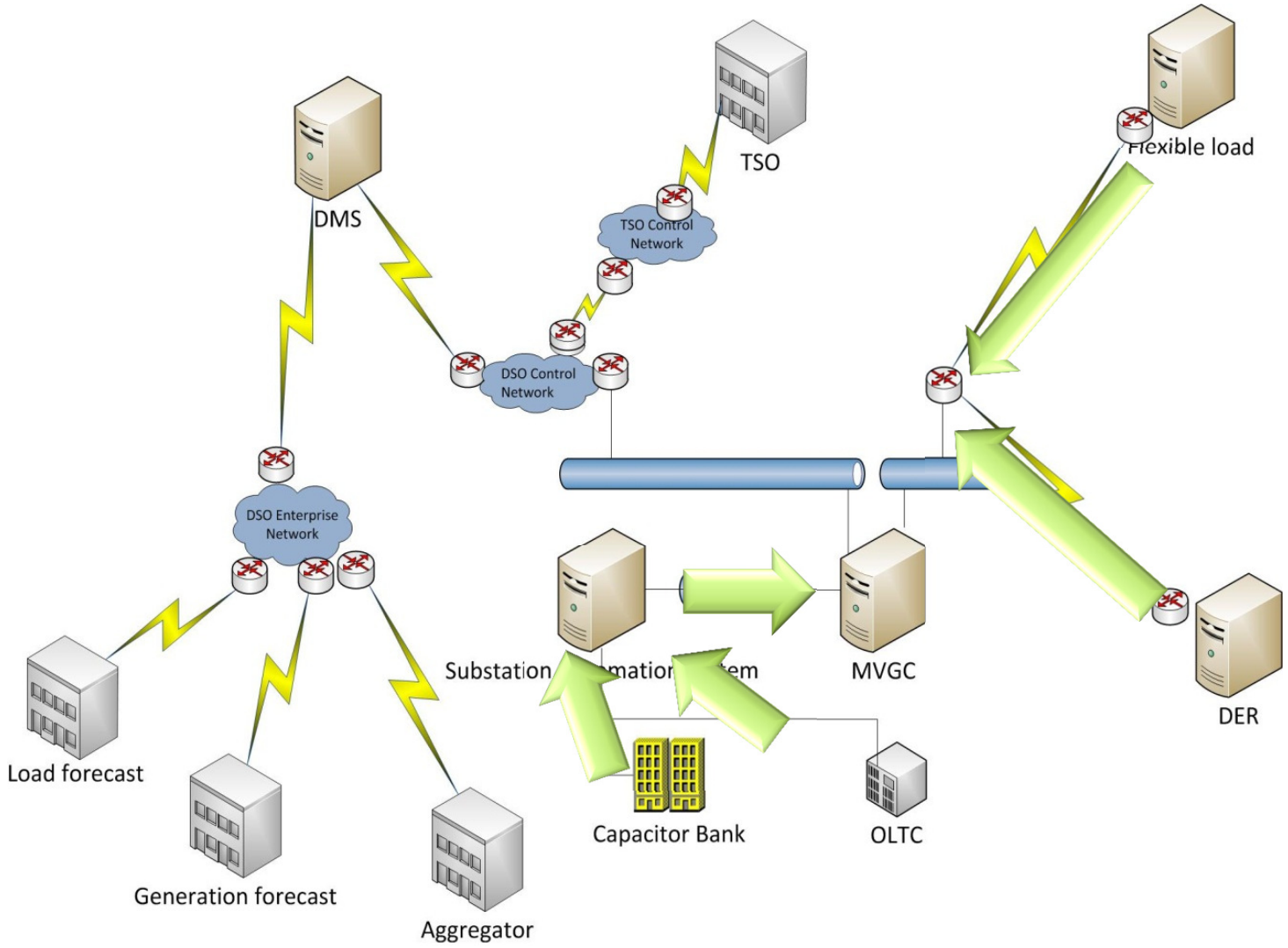
Enel Distribuzione S.p.A. Piano di Sviluppo annuale e pluriennale delle Infrastrutture 2013 – 2015
Enel CIRED 2012

DER Control Use Case – Function

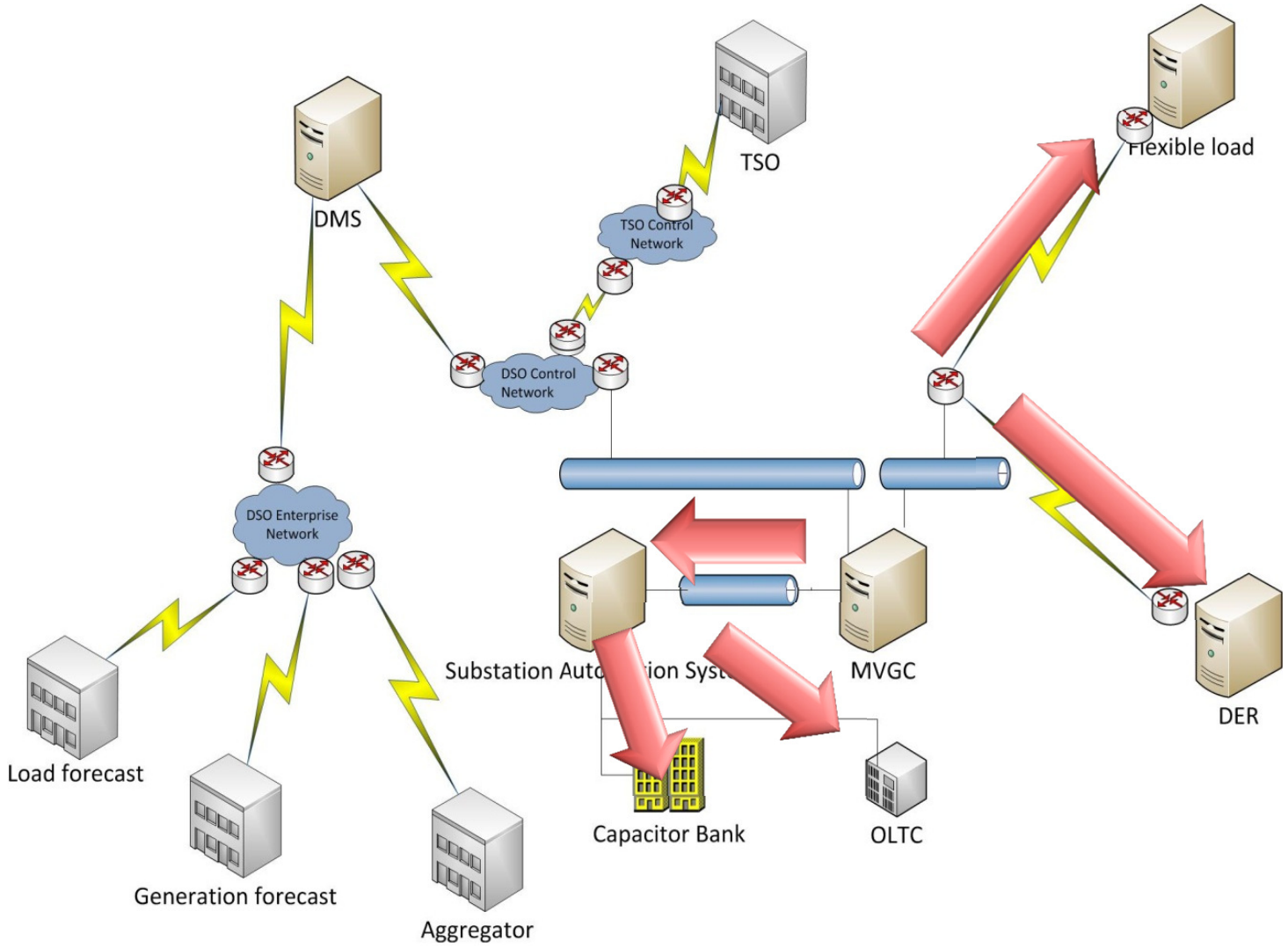


Basato su SGSP Working Group Use Case WGSP-0200 CEN / CENELEC / ETSI

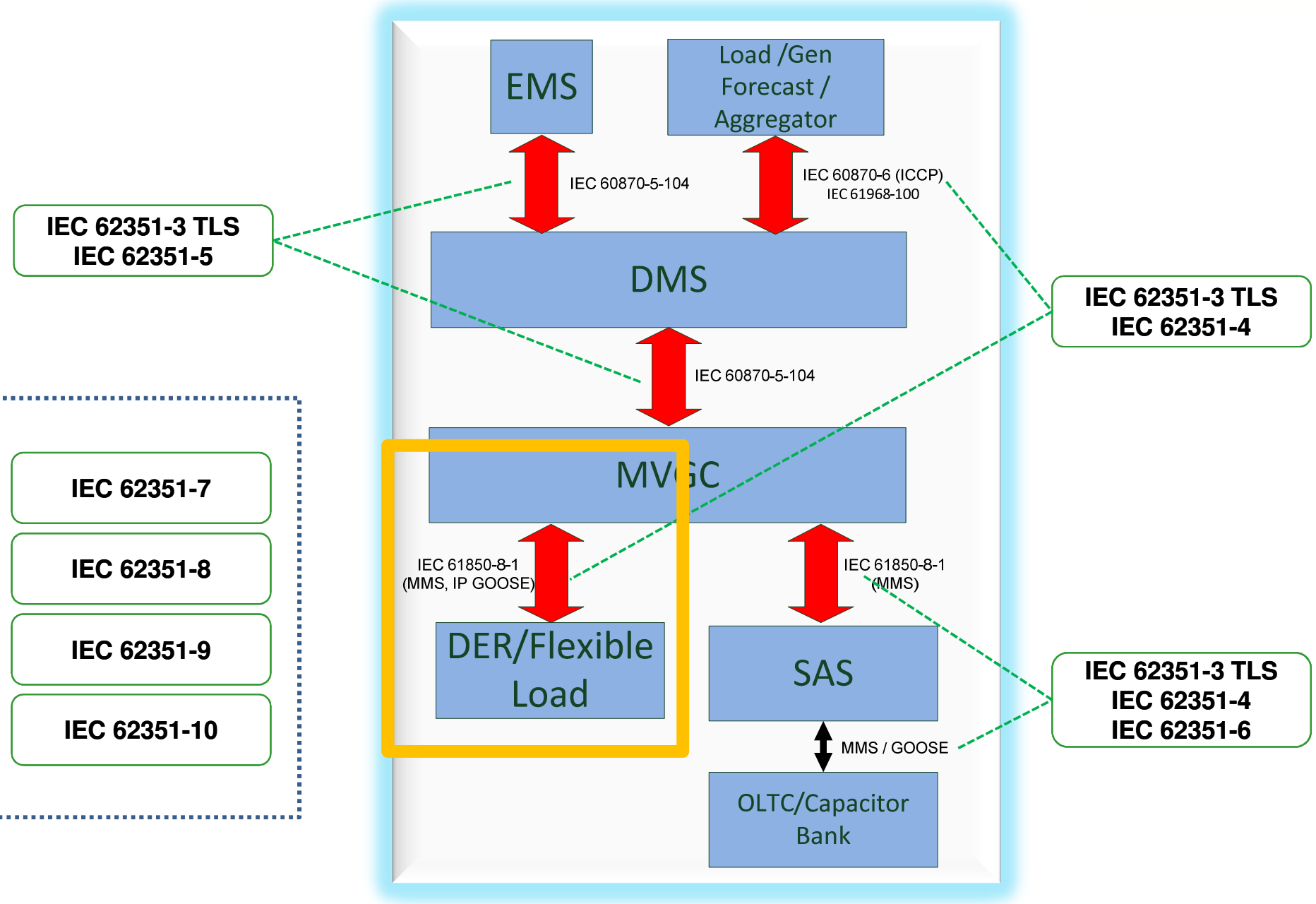
Flussi informativi e misure RES



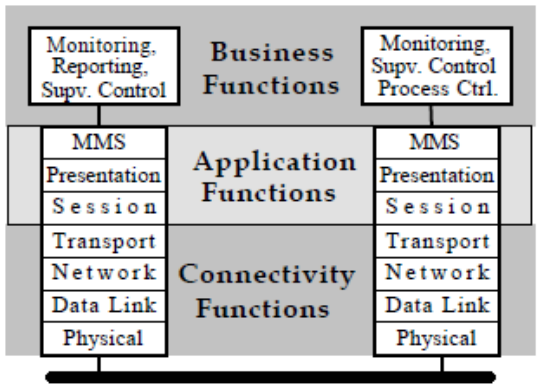
Flussi informativi e misure RES



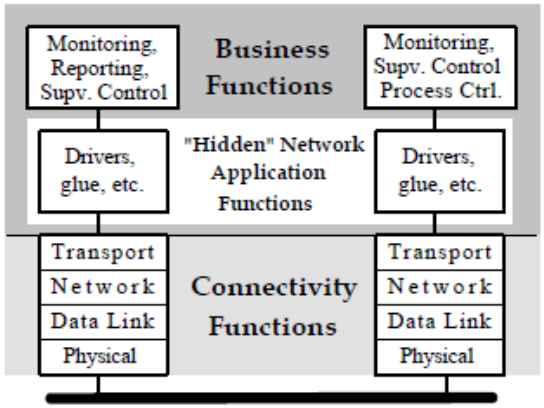
Protocolli di comunicazione – Introduzione sicurezza



Comunicazioni Sottostazione/DER – IEC 61850 (MMS)



The MMS View of Network Applications



The Common View of Network Applications

IEC 61850-8: Specific communication service mapping (SCSM)

IEC 61850-8-1: Mappings to MMS

Manufacturing Message Specification ISO 9506

Application layer protocol

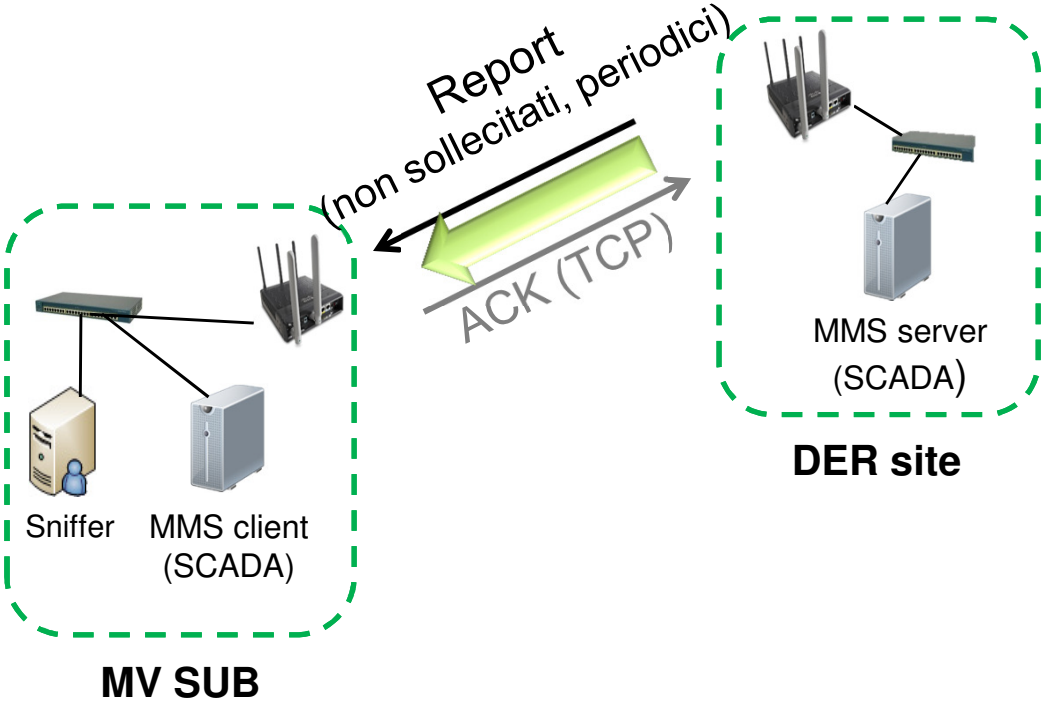
Internationally standardized messaging system for the exchange of real-time data and supervisory control information

Indipendente da:

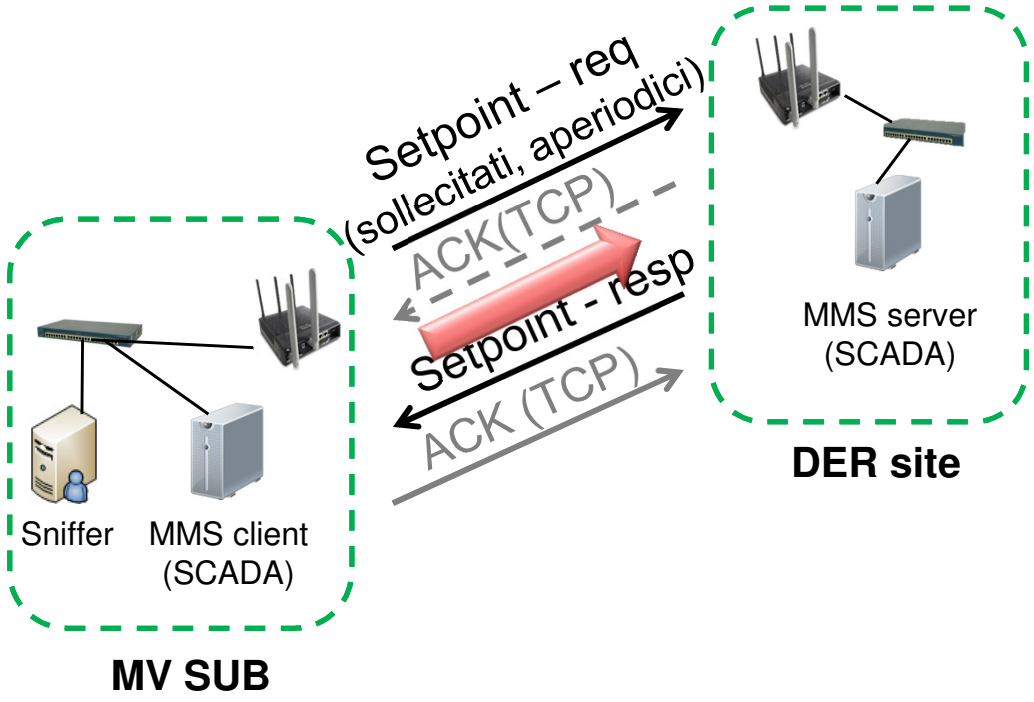
- Funzione applicativa svolta
- Vendor del dispositivo impiegato

Comunicazioni Substation/DER – Messaggi

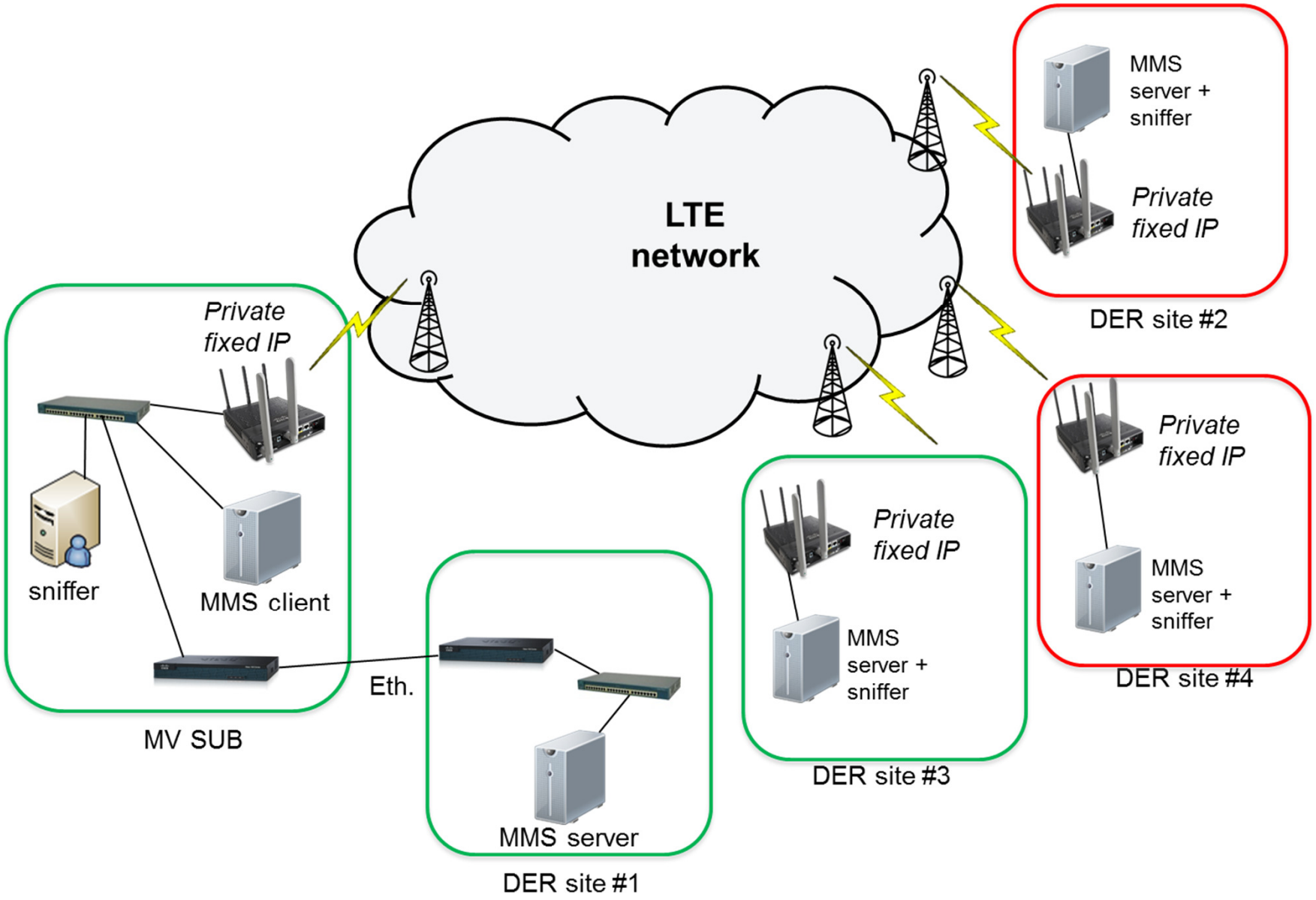
MMS Reports



MMS Setpoints



Test Bed RSE – Rete di comunicazione DER



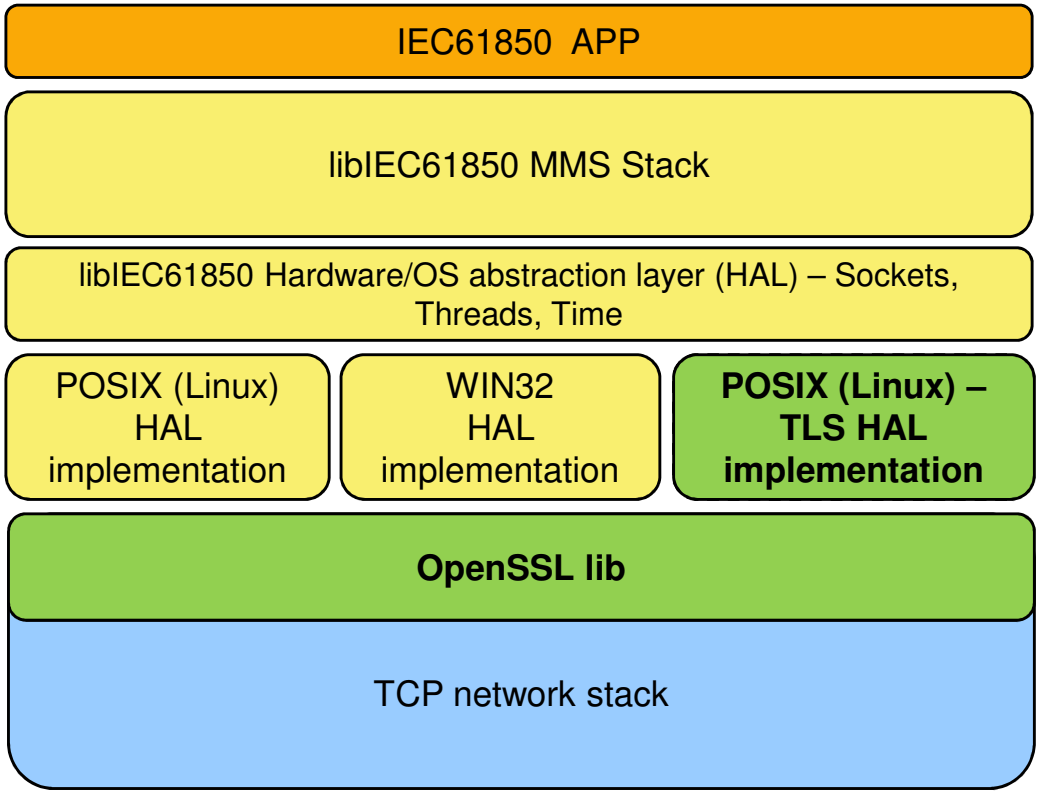
Test Bed RSE – implementazione IEC 62351-3 nelle comunicazioni DER

Modulo di comunicazione client/server MMS

- Implementato con libIEC61850
- Trasmissione MMS report, MMS setpoint

TLS HAL

- TLS v. 1.2
- Funzioni di autenticazione e cifratura con libreria OpenSSL
- Scambio bidirezionale di certificati client-server
- TLS session renegotiation e resumption
- Integrazione nella libIEC61850



Misure di QoS

TCP/TLS Handshake Time	• Durata handshake TCP/TLS
MMS HandshakeTime	• Tempo richiesto per la creazione della sessione MMS
MMS Profile Exchange Time	• Durata dello scambio profilo MMS tra client e server
TLS renegotiation/resumption Time	• Tempo richiesto per le operazioni di renegotiation e resumption TLS
RTT (Round Trip Time)-Report	• Tempo che intercorre tra l'inivio di un report e la ricezione del corrispondente ack TCP lato server MMS
RTT-Setpoint	• Tempo che intercorre tra l'inivio di una setpoint request e la ricezione del corrispondente ack TCP lato client MMS
Inter-Report Time and Inter-Setpoint Time	• Tempo che intercorre tra l'invio di due report/sepoint consecutivi
Retransmissions	• Numero di ritrasmissioni TCP • Numero di report/setpoint ritrasmessi
# of TCP/MMS/TLS sessions	• Numero di sessioni TCP, TLS e MMS stabilite con successo • Numero di tentativi falliti per stabilire sessioni TCP, TLS e MMS
Session Overhead Rate	•Tempo impiegato per il setup e la ripresa della sessione. Tempo non disponibile, sulla base del tempo totale, per le attività di controllo della griglia
Losses	• Numero di report/setpoint persi

Parametri dei test effettuati

Test A
- 10 run di 500 report inviati da ogni server MMS

Test B
- 1 run della durata di 2 ore che prevede l'invio sia di report da parte del server MMS, sia di setpoint da parte del client MMS

Test C
- 1 run della durata di 24 ore circa con l'invio periodico di report da parte del server MMS.

- Frequenza invio report: 2 s
- Frequenza invio setpoint: 30 s

TECNOLOGIE DI RETE
- Wired Ethernet, 4G LTE
- Protocollo IEC 61850-8-1 MMS
- Profilo MMS: 211 variabili (test ETH), 214 variabili (test LTE)

MISURE DI SICUREZZA
- **Test Plain security**: ACL
- **Test Standard security**: ACL + IEC 62351-3 (TLS)
  - RSA key exchange
  - Firma dei certificati RSA 1024 bit
  - Cipher suite AES256-GCM-SHA384
  - Tempo di rinegoziazione 500 s

NUMERO DI SERVER DER
- 1 wired VLAN Ethernet
- 3 4G LTE

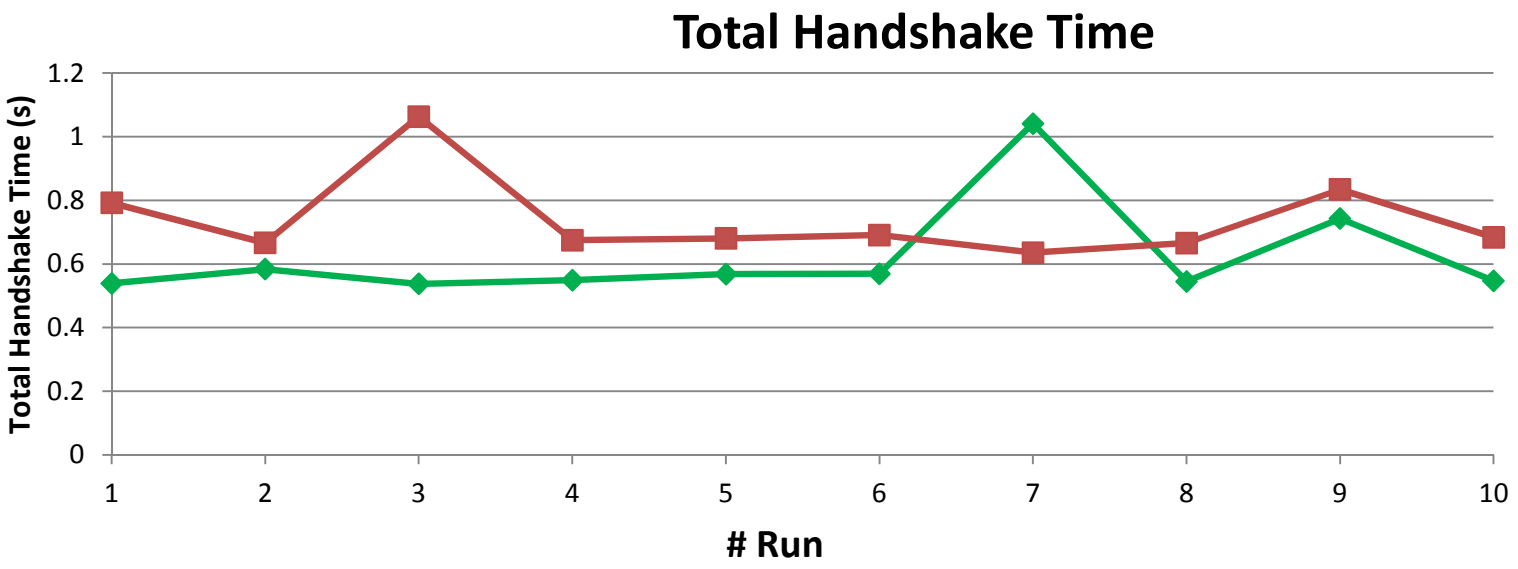
POSIZIONE GEOSPAZIALE DEI SERVER DER
- Server wired in lab RSE
- Server LTE posizionati in celle distinte, distanza max MV SUB-DER 10 km

Risultati sperimentali – impatto della sicurezza sulle prestazioni delle comunicazioni

Test Case	Network	Metrics (time in seconds)							
		TCP Handshake Time (Test A)	*TLS Handshake Time (Test A)*	*MMS Session Time (Test A)*	*MMS Profile Exchange Time (Test A)*	*Inter-Report Time (Test C)*	*RTT-Report (Test C)*	*Inter-Setpoint Time (Test B)*	*RTT-Setpoint (Test B)*
Normal	**ETH**	0.001533	-	0.0104	0.1294	2.0105	0.0000981	30.0637	0.00111
Security (TLS)	**ETH**	0.001534	0.03137	0.0117	0.1321	2.0105	0.0000992	31.0588	0.00117

Test Case	Network	Metrics (time in seconds)							
		TCP Handshake Time (Test A)	*TLS Handshake Time (Test A)*	*TLS Renegotiation Time (Test a)*	*MMS Session Time (Test A)*	*MMS Profile Exchange Time (Test A)*	*Total Handshake TIME (Test A)*	*RTT-Report (Test B)*	*RTT-Setpoint (Test B)*
Normal	**LTE (media)**	**0,083604**	**-**	**-**	**0,108277**	**0,430621**	**0,622501**	**0,120362**	**0,127264**
	LTE DER 1	0,151685	-	-	0,115203	0,39076	0,657648	0,070623	0,150611
	LTE DER 2	0,048699	-	-	0,091818	0,449561	0,590078	0,079802	0,084774
	LTE DER 3	0,050427	-	-	0,117811	0,451541	0,619779	0,210662	0,146406
Security (TLS)	**LTE (media)**	**0,068582**	**0,169039**	**0,166031**	**0,077534**	**0,423705**	**0,73886**	**0,119339**	**0,117928**
	LTE DER 1	0,072463	0,122148	0,164631	0,0700804	0,4012721	0,665964	0,140235	0,069777
	LTE DER 2	0,082715	0,236397	0,155755	0,0755988	0,4317688	0,826479	0,125581	0,074769
	LTE DER 3	0,050567	0,148572	0,177707	0,0869221	0,4380745	0,724136	0,148863	0,213471

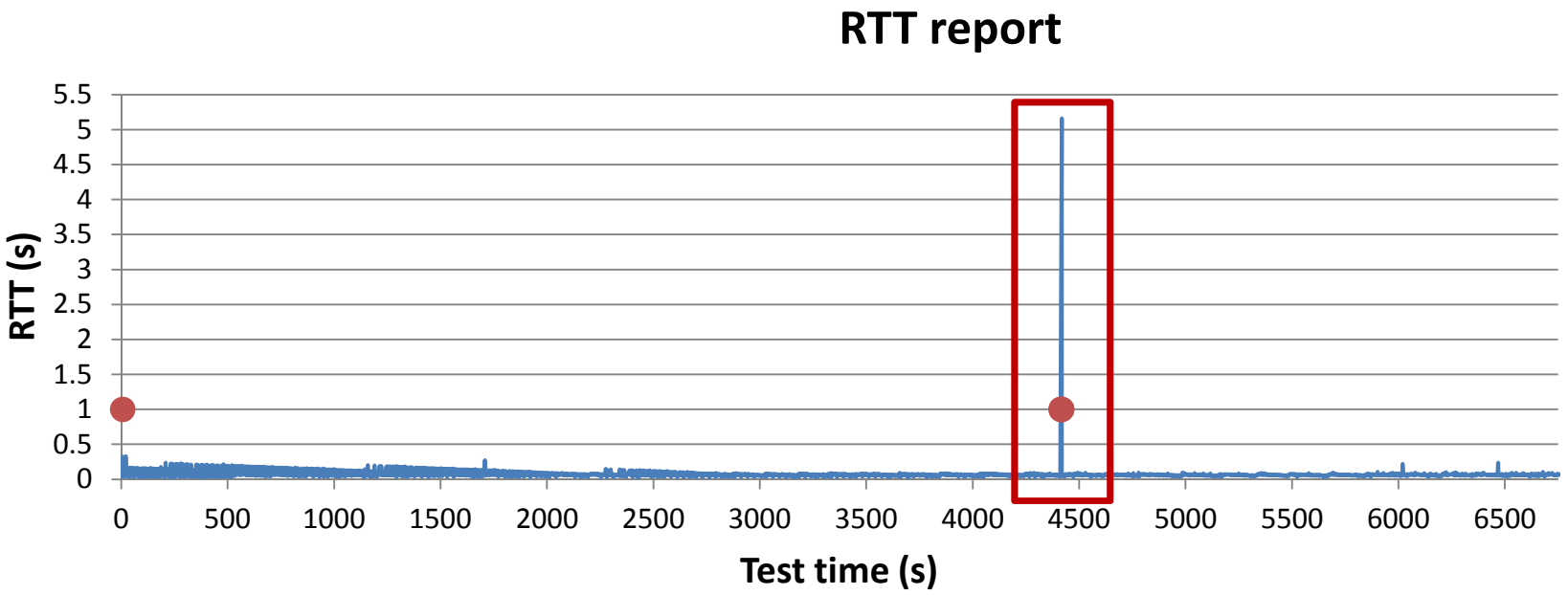
Risultati sperimentali



4G LTE

Plain Security

Standard Security

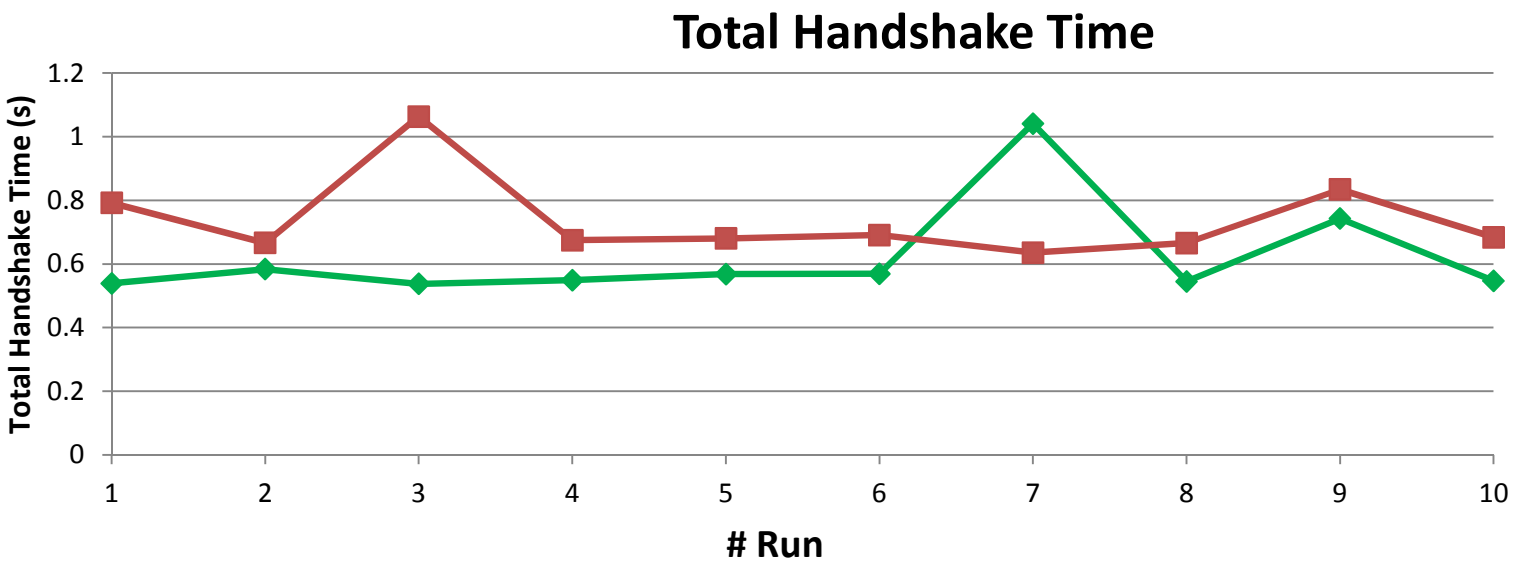


4G LTE

RTT report

Report retran

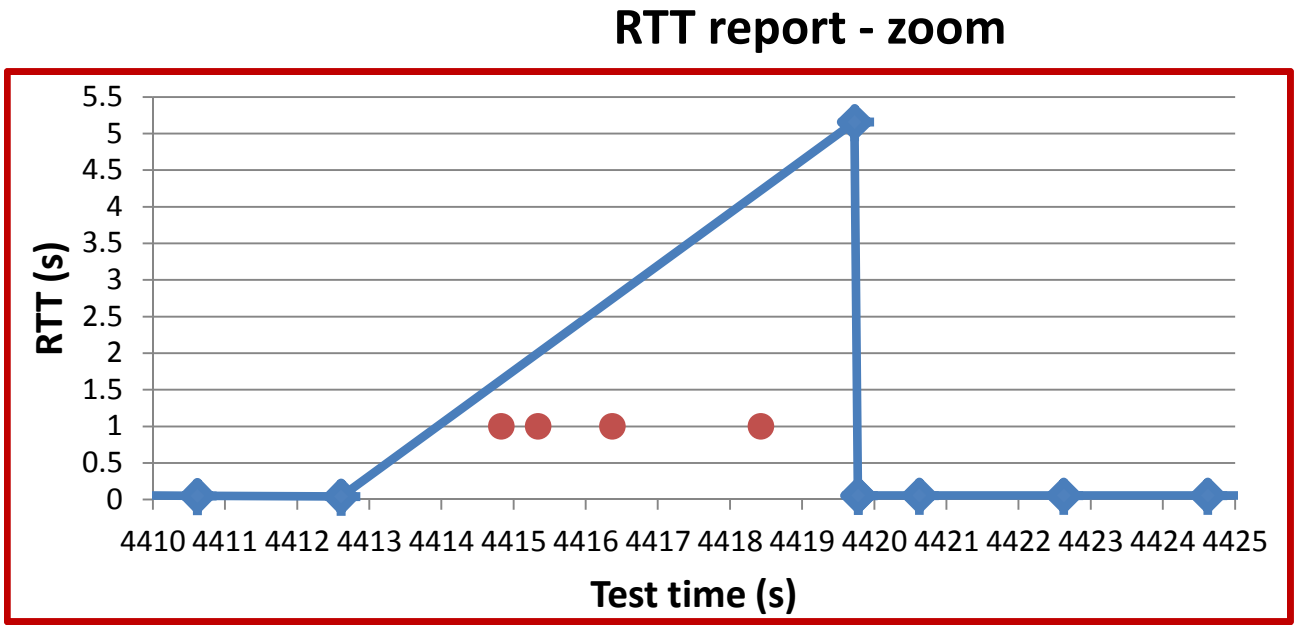
Risultati sperimentali



4G LTE

Plain Security

Standard Security



4G LTE

RTT report

Report retran

Risultati sperimentali – considerazioni

LAYER SICUREZZA TLS

- Overhead temporale non significativo nello scambio messaggi MMS
- Aggiunta di un'ulteriore fase di handshake: incremento del Total Handshake Time
- Dimensione certificati: possibili ritrasmissioni TCP durante handshake TLS

Rispettando i vincoli dello standard IEC 62351-3, ricercare la configurazione del protocollo TLS più adatta ai requisiti dell'applicazione di comunicazione in esame

CONSIDERAZIONI RETE

- Prestazioni su rete wired ethernet stabili, utilizzate come riferimento
- Prestazioni su rete wireless dipendenti dalle condizioni di traffico della cella 4G agganciata e quindi dalla posizione geospaziale dei server

Lesson learned

Punto di partenza:

Necessità di sicurezza nelle comunicazioni ICT delle Smartgrid

Metodologia di test

- Importanza di un ambiente di test basato sull'uso di protocolli e procedure standard
- Elaborazione di un piano di test e individuazione di indicatori di performance adatti allo scopo
- Necessità di una soluzione valida per *deep packet inspection* di traffico cifrato

Risultati

- L'aggiunta del layer TLS ha impatto limitato sulle performance delle comunicazioni
- Gli effetti dell'introduzione della sicurezza (aumento Total Handshake Time, ritrasmissioni TCP, rinegoziazione) vanno soppesati in merito al caso d'uso / applicazione considerata

Ringraziamenti

- **Vodafone – piattaforma test M2M LTE**
  - Stefano Marzorati
  - Mario La Rosa

- **Progetto Europeo SmartC2Net**
  - www.smartc2net.eu
  - D6.2 Integrated test beds – Description

GRAZIE PER L'ATTENZIONE

Paolo Wylach
RSE S.p.A.
Viale Raffaele Rubattino 54
20134 Milano
mail: paolo.wylach@rse-web.it