Testing della Sicurezza nelle comunicazioni standard delle Smart Grid

Paolo Wylach
RSE S.p.A
paolo.wylach@rse-web.it

Giovanna Dondossola
RSE S.p.A
giovanna.dondossola@rse-web.it

Roberta Terruggia
RSE S.p.A
roberta.terruggia@rse-web.it

INDICE

Lista degli acronimi

Acronimo	Definizione
ACL	Access Control List
CEI	Comitato Elettrotecnico Italiano
CEN/CENELEC/ETSI	European Committee for Standardization/European Committee for Electrotechnical Standardization/European Telecommunications Standards Institute
DER	Distributed Energy Resources
DMS	Distribution Management System
DPI	Deep Packet Inspection
DSO	Distribution System Operator
EMS	Energy Management System
GPS	Global Positioning System
GSM	Groupe Special Mobile
HAL	Hardware Abstraction Layer
HV-AT	High Voltage - Alta Tensione
ICCP	Inter-Control Center Communications Protocol
ICT	Information Communication Technology
IETF	Internet Engineering Task Force
IEC	International Electrotechnical Commission
IP	Internet Protocol
LAN	Local Area Network
LTE	Long Term Evolution
M2M	Machine to Machine
MMS	Manufacturing Message Specification
MVGC	Medium Voltage Grid Controller
MV-MT	Medium Voltage - Media Tensione
NS	Network Simulator
NTP	Network Time Protocol
OLTC	On-Load Tap Changer
PCS-ResTest	Power Control System – Resilience Testing Laboratory
PKI	Public Key Infrastructure
PTP	Precision Time Protocol
QoS	Quality of Service
RES	Renewable Energy Source
RFC	Request For Comments
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SG-CG	Smart Grid Coordination Group
SNMP	Simple Network Management Protocol

Acronimo	Definizione
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
UDP	User Datagram Protocol
VLAN	Virtual local Area Network
WAN	Wide Area Network

1. Premessa

La necessità di una gestione ottimizzata degli dispositivi connessi alla rete elettrica ha portato all'introduzione di funzionalità ICT (Information and Communication Technology) nelle reti di telecontrollo e all'interno dei dispositivi di rete stessi. La natura di queste reti, le cosiddette Smart Grid, è molto eterogenea: vengono impiegati dispositivi di vendor diversi e sono necessarie interconnessioni tra le reti di operatori differenti. Dal punto di vista informatico, nelle comunicazioni occorre impiegare un linguaggio comune definito da uno standard condiviso, mentre un altro aspetto molto importante è la sicurezza delle comunicazioni stesse.

Come ogni rete di comunicazione informatica, le Smart Grid non sono esenti dalle minacce di natura ICT, che si concretizzano in attacchi di vario genere, con molteplici meccanismi di azione e obiettivi diversi. Nel contesto specifico, la necessità di misure di difesa è più che mai critica data la natura dei flussi informativi in esame: occorre mettere in campo delle soluzioni che possano fornire un livello di protezione adeguato a questi sistemi.

Questa relazione si pone l'obiettivo di fornire una metodologia sperimentale, fondata sull'esperienza del laboratorio PCS-ResTest di RSE, per la valutazione degli standard di sicurezza ICT destinati alle comunicazioni per il controllo delle Smart Grid.

2. Smart Grid e sicurezza informatica

Come introdotto brevemente nella premessa, negli ultimi anni si sta assistendo ad una forte evoluzione delle reti elettriche di distribuzione, caratterizzata dal progressivo abbandono del modello di rete passiva grazie all'introduzione di nuove funzionalità ICT, in cui tutti i nodi della rete possono contribuire al bilancio energetico del sistema elettrico globale.

Queste funzionalità sono necessarie per conseguire una gestione della rete "intelligente", che integri e ottimizzi il funzionamento di tutti gli elementi ed essa connessi, che siano generatori, consumatori o utenti finali in grado di effettuare entrambe le operazioni. La gestione dei flussi multidirezionali di energia che transitano sulla rete (atta a garantire l'equilibrio tra la domanda e l'offerta di energia) e le operazioni di telecontrollo ICT, consentono di integrare la gestione distribuita e cambiare il ruolo dell'utente finale, non più solo consumatore ma anche produttore che immette energia nella rete (utente attivo).

L'architettura di queste reti, le Smart Grid, risulta quindi essere molto complessa. Basti pensare all'eterogeneità dei dispositivi e delle tecnologie impiegate dai diversi operatori, che potrebbero implementare protocolli di comunicazione differenti, anche non standard. Connettendo le reti di più operatori si rafforza la necessità di garantire l'interoperabilità tra i vari sistemi coinvolti, in modo che porzioni di rete non rimangano isolate.

Un esempio pratico è l'interazione tra il DSO (Distributed System Operator) e i DER (Distributed Energy Resource), le risorse energetiche distribuite, e tutti gli altri soggetti coinvolti nella gestione e nel controllo del sistema elettrico. I protocolli di comunicazione impiegati dovranno essere standard, e ciò rappresenta un requisito fondamentale della gestione della rete "smart".

Nell'architettura sin qui descritta, ai fini dell'interoperabilità tra i sistemi, gli operatori devono consentire l'accesso alle proprie reti a soggetti esterni. Il relativo isolamento di cui precedentemente godevano questi sistemi forniva una protezione dagli attacchi di tipo informatico che provenivano dall'esterno della rete. Lo scenario è stato cambiato dall'apertura delle reti: esse sono vulnerabili a questi tipi di attacchi, realizzati con intenti che possono variare, ad esempio sottrarre dati sensibili, manomettere comandi di telecontrollo in transito sulla linea o bloccare le trasmissioni. Se a questo fattore si aggiunge che per convenienza economica le Smart Grid possono affidarsi a reti di comunicazione pubbliche o di terze parti, potenzialmente vulnerabili data l'eterogeneità del traffico dati, la situazione esige una seria considerazione delle misure di protezione contro gli attacchi ICT.

3. Standard di sicurezza ICT

Dal punto di vista normativo, il WG15 del TC 57 IEC sta curando l'elaborazione della norma IEC 62351 che definisce la "Power systems management and associated information exchange - Data and communications security". Lo standard è strutturato secondo un insieme di parti, ciascuna delle quali riguardante un specifico aspetto del tema sviluppato della norma: la parte 1 e la parte 2 definiscono rispettivamente gli obiettivi dello standard (i concetti generali) e il glossario. Le restanti parti specificano i dettagli tecnici: le parti da 3 a 6 e la 11 indirizzano protocolli o componenti particolari, mentre le parti da 7 a 10, la 12 e la 13 sono di livello sistema in supporto alle altre parti per comunicazioni specifiche.

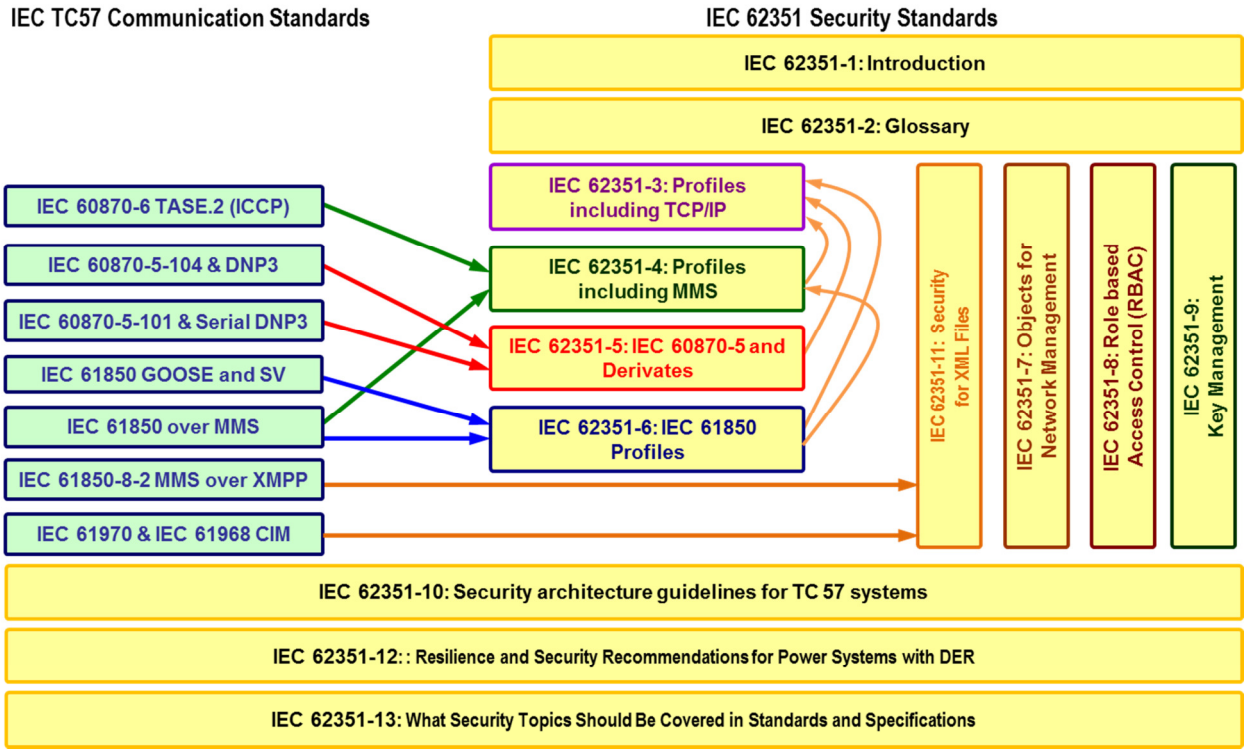

Figura 3-1 Mapping dei protocolli di comunicazione TC57 con i corrispondenti standard di sicurezza IEC 62351

Nella Figura 3-1 è possibile osservare quali parti dello standard interessano i diversi protocolli di comunicazione sviluppati dal TC57. L'obiettivo della norma è garantire la sicurezza end-to-end tra tutti i sistemi coinvolti nelle comunicazioni di telecontrollo. Il focus di questo lavoro è rivolto alla parte 4 dello standard IEC 62351, relativa alla sicurezza delle comunicazioni IEC 61850 basate su protocollo MMS. In

particolare l'attività sperimentale descritta si riferisce all'implementazione della sicurezza del layer di trasporto specificata nella parte 3 dello standard IEC 62351, quella riguardante la sicurezza end-to-end di tutti i profili che utilizzino TCP/IP, che quindi interessa anche quelli indirizzati nella parte 4.

3.1 IEC 62351-3 Sicurezza per i profili che includono TCP/IP

La parte 3 dello standard (IS – International Standard 2014) [1], indirizza la sicurezza dei flussi informativi che impiegano i layer TCP/IP, fornendo una protezione end-to-end attraverso l'introduzione del TLS (Transport Layer Security) definito dallo standard IETF RFC 2246 (v 1.0) [2]. L'obiettivo è di garantire la protezione dei messaggi di telecontrollo al fine di evitare accessi non autorizzati alle comunicazioni e modifica o furto dei messaggi. Risulta quindi una misura adatta a contrastare gli attacchi più critici dei sistemi di telecontrollo, quelli di tipo man in the middle e replay. Lo standard definisce le specifiche per creare un canale cifrato con il TLS dopo un processo di autenticazione di entrambe le parti, conseguito mediante uno scambio bidirezionale e la verifica di certificati PKI (Public Key Infrastructure). Questo standard definisce inoltre dei vincoli per la resumption, e la rinegoziazione della sessione, e per la validazione dei certificati impiegati dai peer. Per la gestione delle chiavi si fa riferimento alla parte 9 dello standard IEC 62351.

È importante sottolineare che questo standard si presenta come riferimento per *tutti* gli altri standard IEC che necessitano di sicurezza dei protocolli basati su TCP/IP.

4. Testbed RSE e metodologia sperimentale

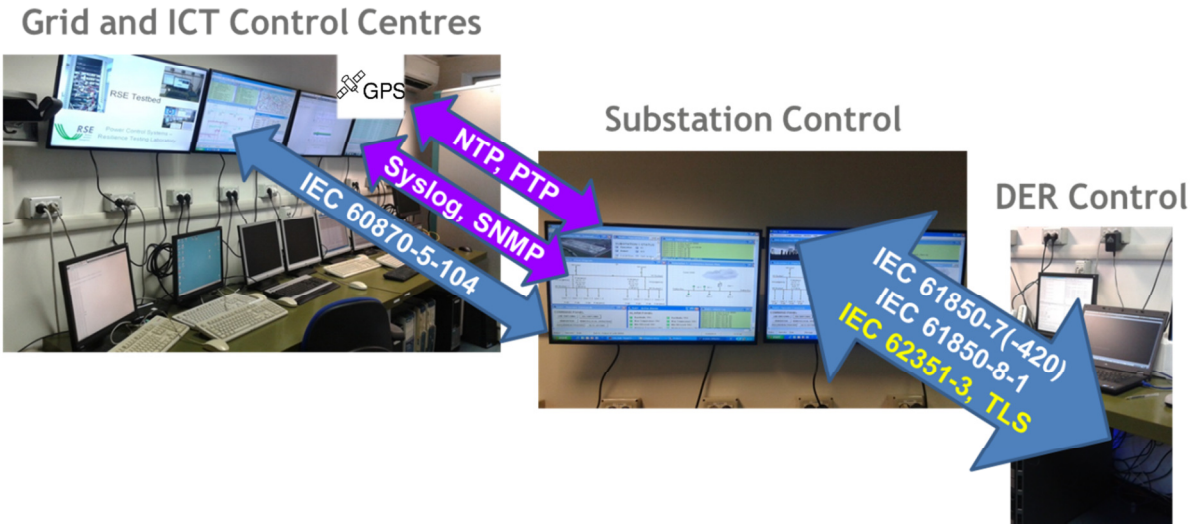

Figura 4-1 Protocolli di comunicazione, sicurezza e monitoring implementati nel laboratorio PCS-ResTest di RSE

Presso il Laboratorio PCS-ResTest di RSE è stato realizzato un testbed in cui sono state implementate le applicazioni necessarie per la gestione dei flussi informativi utilizzati per la regolazione di tensione da parte dei sistemi di controllo e automazione di una stazione attiva AT/MT, utilizzando protocolli di comunicazione standard, IEC 60870-5-104 e IEC 61850 MMS (frecce blu, scritte bianche in Figura 4-1). Per quanto riguarda la sicurezza, le comunicazioni stazione-DER sono messe in sicurezza implementando le funzioni previste dallo standard IEC 62351-3 (freccia blu, scritta gialla in Figura 4-1). Come tecnologie di comunicazione il

testbed utilizza canali Ethernet e connettività wireless fornita da una piattaforma di test M2M 4G LTE, come rete di accesso per le comunicazioni stazione/DER.

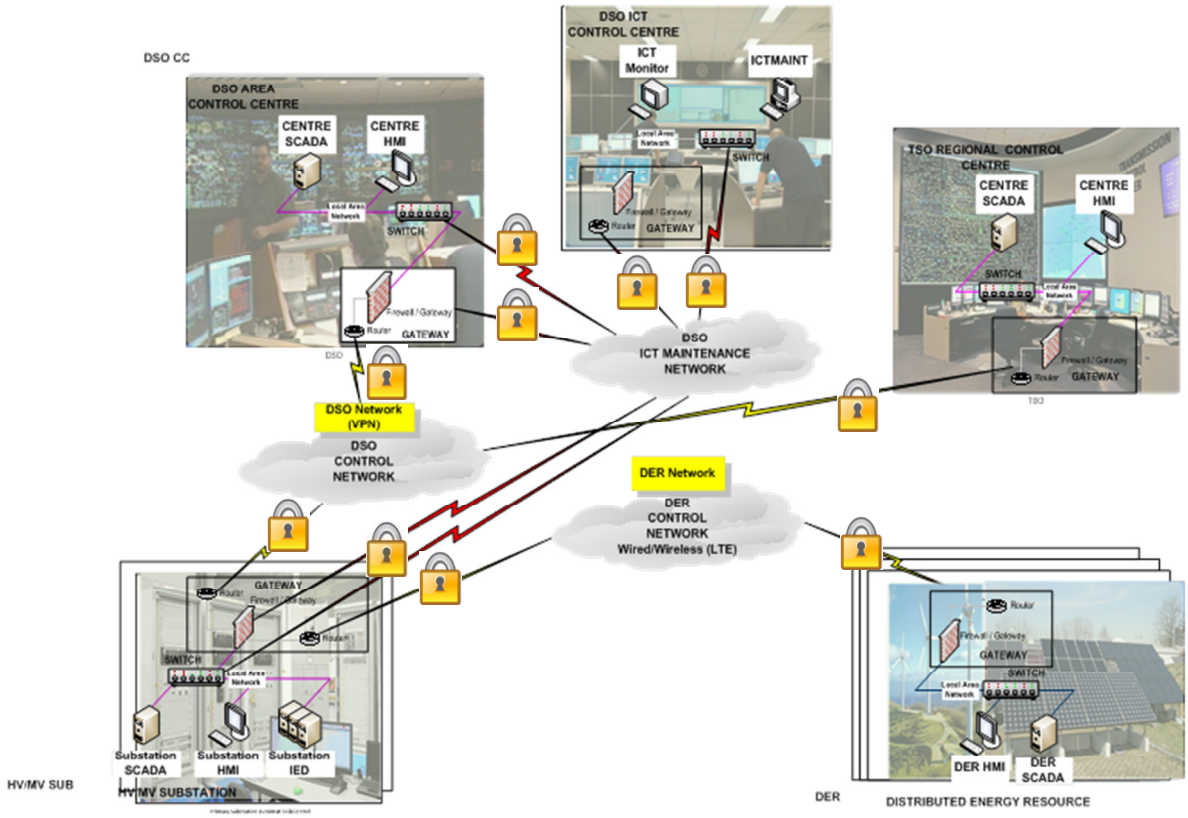

Figura 4-2 Layout dell'architettura del testbed RSE

Nel layout in Figura 4-2, è possibile individuare diverse aree principali, connesse tra di loro:

- **Centro di controllo DSO** controlla in remoto un gruppo di sottostazioni di distribuzione. Per realizzare la funzionalità di controllo, il centro è connesso a *n* sottostazioni AT/MT attraverso una rete di comunicazione ICT . Nel caso specifico il centro controlla due stazioni primarie.
- **Stazioni Primarie (AT/MT)** ognuna di esse include funzioni di automazione, comunicazione, SCADA e HMI per gli operatori in locale. Esse possono controllare generatori distribuiti connessi alla media tensione. In particolare nel testbed sono collocate due stazioni primarie di cui una controllante 4 DER.
- **DER** *m* siti connessi alle reti MT. Nel testbed sono presenti quattro DER, uno connesso attraverso connessione wired e tre distribuiti geograficamente connessi attraverso connessione mobile M2M LTE.
- **Centro di controllo ICT** controlla in remoto i componenti ICT delle reti DSO e contiene una serie di strumenti per il monitoraggio delle comunicazioni e degli apparati. Contiene inoltre server dedicati alla sincronizzazione temporale degli apparati mediante segnale GPS (frecce viola in Figura 4-1), basati sui protocolli PTP (Precision Time Protocol) e NTP (Network Time Protocol).

L'architettura del testbed include diverse reti locali e wide area. Ciascuna delle aree prima descritte è composta da diversi sistemi che comunicano attraverso una rete locale wired (LAN, Local Area Network),

mentre le diverse aree comunicano attraverso WAN (Wide Area Network). In particolare sono presenti le seguenti reti wide area:

- **Rete di controllo DSO** connette le sottostazioni AT/MT al centro di controllo DSO.
- **Rete di manutenzione ICT** utilizzata per la gestione e il monitoraggio dei dispositivi di comunicazione impiegati nel centro di controllo DSO e nelle sottostazioni AT/MT.
- **Rete di controllo DER** connette ogni stazione AT/MT con un gruppo di DER dislocati su aree geografiche differenti, attraverso reti di comunicazione che possono essere eterogenee (wired/wireless).

Le prime due reti (controllo DSO e manutenzione ICT) sono implementate attraverso Ethernet wired, mentre per le reti di controllo dei DER sono state implementate attraverso diverse tecnologie (VLAN Ethernet e M2M LTE), in modo da riuscire a misurare il delay introdotto dalla rete mobile nel tempo totale di trasmissione dei messaggi applicativi MMS.

Al fine di valutare l'efficacia delle misure di sicurezza messe in campo, conformi con quanto indicato negli standard di riferimento, il testbed si avvale di tool per iniettare cyber attacchi. Gli effetti dei processi di attacchi sono visualizzabili dagli strumenti di monitoraggio della rete, che impiegano messaggi syslog e il protocollo SNMP (frecce viola in Figura 4-1).

Attraverso l'utilizzo di strumenti di cattura del traffico quali Wireshark e tcpdump, è inoltre possibile ottenere le tracce delle comunicazioni attive, effettuando le cattura dei flussi informativi sia lato stazione (client) che lato DER (server). Per analizzare le tracce catturate in formato pcap (o pcapng), ed estrarre i valori delle metriche desiderate, è stato sviluppato un apposito tool di analisi.

Per poter analizzare l'impatto dell'introduzione delle misure di sicurezza è stato necessario individuare un insieme di indicatori che consentano di ottenere misure specifiche di QoS (Quality of Service) rispetto ai protocolli impiegati. Gli indicatori selezionati per le sessioni di test della sicurezza MMS qui descritte sono i seguenti:

- TCP/TLS Handshake: durata dell'handshake TCP/TLS
- MMS Handshake Time: tempo richiesto per stabilire la sessione MMS
- MMS Profile Exchange Time: tempo speso per lo scambio del profilo tra client MMS e server MMS distinguendo il tipo di scambio del profilo MMS
- TLS Renegotiation/Resumption Time: tempo richiesto per le operazioni di renegotiation e resumption TLS
- RTT (Round Trip Time)-Report: intervallo tra l'invio di un report e la ricezione del relativo ACK TCP a lato server
- RTT-Setpoint: intervallo tra l'invio di un setpoint e la ricezione del relativo ACK TCP a lato client
- Inter-Report Time and Inter-Setpoint Time: tempo che intercorre tra l'invio di due report/setpoint consecutivi
- Retransmissions: numero di ritrasmissioni TCP, numero di report/setpoint ritrasmessi
- TCP/MMS/TLS sessions: numero di sessioni TCP, TLS e MMS stabilite con successo e numero di tentativi falliti per stabilirle
- 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 rete elettrica
- Losses: numero di report/setpoint persi

L'effetto degli attacchi alle comunicazioni per il controllo delle reti attive può essere valutato anche dal punto di vista simulativo, impiegando dei simulatori di rete ICT. Per la creazione dei modelli necessari sono considerati principalmente i tool di simulazione ns2 e ns3 che, grazie a specifiche funzionalità, includono al loro interno degli stessi moduli di comunicazione client/server utilizzati nel testbed.

Dopo questa breve panoramica delle funzionalità e degli strumenti a disposizione nel testbed RSE, l'attenzione si sposta su un passo importante della metodologia sperimentale presentata, la caratterizzazione delle sessioni di test.

4.1 Caratterizzazione dei test

L'elaborazione della metodologia sperimentale oggetto di questo lavoro non può fare a meno di una adeguata caratterizzazione delle sessioni di test: occorre considerare tutti gli elementi che possono influenzare l'implementazione degli standard e delle soluzioni adottate. Lo schema generale proposto è riportato nel seguito.

Figura 4-3 Schema generale di caratterizzazione delle sessioni di test

Al di là dei parametri standard come durata del test, numero di run ecc., ricoprono un ruolo primario le caratteristiche delle tecnologie di telecomunicazione utilizzate, in quanto le prestazioni del canale di comunicazione potrebbero variare significativamente: basti pensare alle differenze di performance tra quelle di un protocollo di radiocomunicazione più evoluto, come l'LTE, contro quelle di uno storico come il GSM.

Inoltre caratterizzare quanti più parametri dell'attacco o degli attacchi informatici iniettati è fondamentale per valutare l'impatto sui sistemi in esercizio e per sviluppare adeguate contromisure che tengano conto di essi. Specularmente occorre specificare la configurazione delle misure di sicurezza messe in opera per contrastare gli attacchi.

Il quadro di test viene completato da altri parametri di grande importanza, come il numero di server collegati e la loro posizione geospaziale, più l'orario e il giorno di svolgimento del test, elementi che possono variare lo stato della rete, e quindi influenzare le prestazioni delle comunicazioni end-to-end stazione-DER.

5. Il Controllo di Tensione nelle reti attive MT

5.1 Motivazioni

Negli ultimi anni si sta assistendo alla sempre maggiore penetrazione nel sistema elettrico delle fonti energetiche RES (Renewable Energy Sources), come mostrato dal grafico in Figura 5-1, con delle percentuali di potenza RES installata che le proiezioni rivelano saranno sempre più incisive nella rete europea negli anni a venire (oltre il 50% del totale nel 2025).

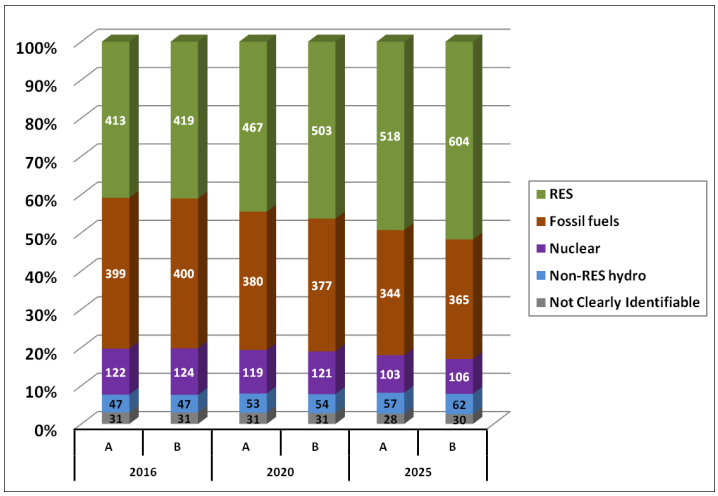

Figura 5-1 Capacità RES installata in Europa, proiezione 2016/2025, Fonte: ENTSO-E Scenario Outlook & Adequacy Forecast 2015

Focalizzandosi sulla rete di distribuzione italiana, è opportuno osservare la proiezione dell'aumento della generazione distribuita connessa alla rete di media tensione: si prevede una potenza totale installata di circa 40 GW nel 2020 (vedi Figura 5-2).

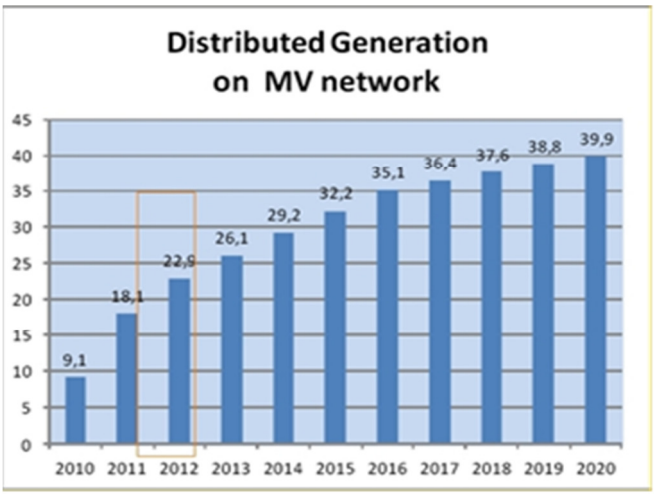

Figura 5-2 Proiezione della potenza da fonti rinnovabili installate collegate alla rete MT – Fonte: Enel CIRED 2012

Questo notevole cambio di panorama del sistema energetico richiede nuove tecniche di controllo e di gestione della rete di distribuzione finalizzate a massimizzare la penetrazione della generazione distribuita, garantendo livelli adeguati di qualità del servizio a tutti gli utenti coinvolti.

Dal punto di vista della regolamentazione, la norma CEI 0-16 [3], "Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica", fornisce una serie di regole per la connessione di RES alla rete MT, in particolare pone dei limiti ai valori indicativi di potenza che è possibile connettere alla rete di media tensione, compresi tra 200kW e 6 MW (trattandosi di impianti di generazione). La norma CEI EN 50160 [4], invece, regola i range di tensione di tutti i dispositivi connessi alla rete, generatori inclusi: essa prescrive che la media del valore efficace della tensione calcolata su 10 min non possa superare il 110 % di U_n.

Altro passaggio rilevante all'interno della norma CEI 0-16 riguarda le comunicazioni Utente-Distributore, in un'ottica di evoluzione verso le Smart Grid: si rende necessario che tutti gli utenti siano dotati di un sistema di comunicazione che permetta lo scambio di segnali con il Distributore, consentendo a quest'ultimo di inviare comandi al fine di implementare logiche di gestione ottimizzate della rete e realizzare azioni necessarie a garantire la sicurezza del complessivo sistema elettrico.

Al fine di realizzare la funzione di controllo di tensione desiderata, con le caratteristiche sin qui descritte, è utile avvalersi nell'analisi di un caso d'uso quanto più aderente al sistema in esame, che consideri quante più variabili, attori e interazioni che lo possono influenzare.

5.2 Descrizione del caso d'uso adottato

Entrando nel dettaglio di quanto detto nella sessione precedente, la connessione di risorse energetiche distribuite alla rete di media tensione può introdurre scostamenti dei valori di tensione rispetto ai termini concordati tra gli operatori della rete di trasmissione e distribuzione, nonché il superamento dei valori accettabili imposti dai vincoli tecnici espressi dalle norme vigenti. Questo porta alla necessità di introdurre in cabina primaria una funzione di controllo di tensione che dal monitoraggio della rete, ottenuto attraverso le misure dal campo, calcoli i setpoint ottimizzati da applicarsi ai DER, ai carichi flessibili e ai componenti di stazione.

Il caso d'uso indirizzato è basato sul SGSP Working Group Use Case WGSP-0200 CEN / CENELEC / ETSI, "Controllo di tensione nelle reti attive MT".

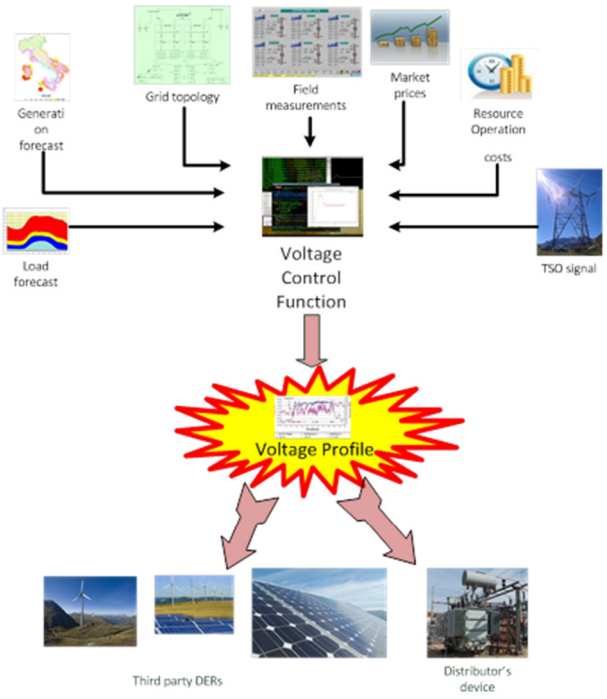

Figura 5-3 Schema del caso d'uso indirizzato

La Figura 5-3 mostra i flussi informativi in ingresso alla funzione di controllo di tensione per le reti MT e i relativi output. Gli input che la funzione richiede devono provenire sia da misure dal campo sia dai sistemi centrali, attraverso diverse reti di comunicazioni.

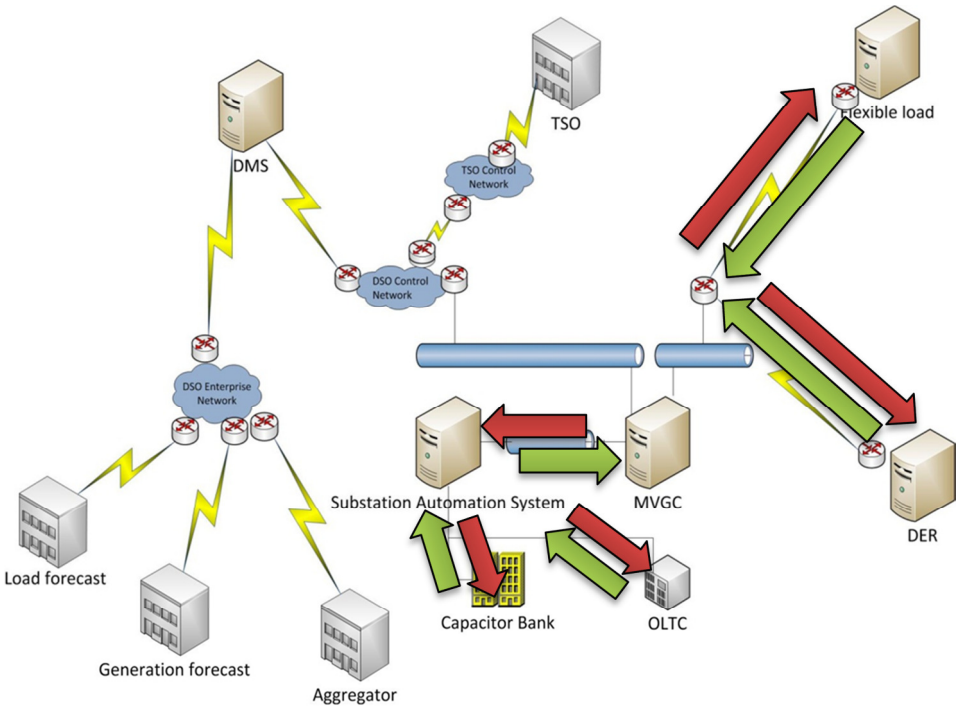

Figura 5-4 Schema dei flussi informativi (rosso) e delle misure RES (verde)

In Figura 5-4 è rappresentato il percorso compiuto dalle misure inviate verso la stazione, come quelle dai DER, dai carichi flessibili e da altri componenti interni alla stazione stessa (frecce in verde), insieme al percorso inverso compiuto dai comandi e i messaggi generati dal MVGC (Medium Voltage Grid Controller) per realizzare la funzione di controllo di tensione (frecce in rosso).

Calandoci nel dettaglio dei protocolli impiegati in questo schema di comunicazione, in Figura 5-5 viene mostrato come le varie parti della norma IEC 62351 siano applicate ai flussi informativi del caso d'uso che ricordiamo essere i seguenti:

- Le comunicazioni tra EMS (Energy Management System) e DMS (Distribution Management System), tra DMS e MVGC avvengono attraverso lo standard IEC 60870-5-104;
- Le comunicazioni tra External Services (Load/Generation Forecast, Aggregator) e DMS utilizzano principalmente l'ICCP e l'IEC 61968-100;
- Le comunicazioni all'interno della stazione, tra MVGC e SAS (Substation Automation System) e tra SAS e OLTC/Capacitor Bank, utilizzano lo standard IEC 61850, protocolli MMS o GOOSE, mentre le comunicazioni tra MVGC e DER/Flexible Load utilizzano MMS o (IP)GOOSE.

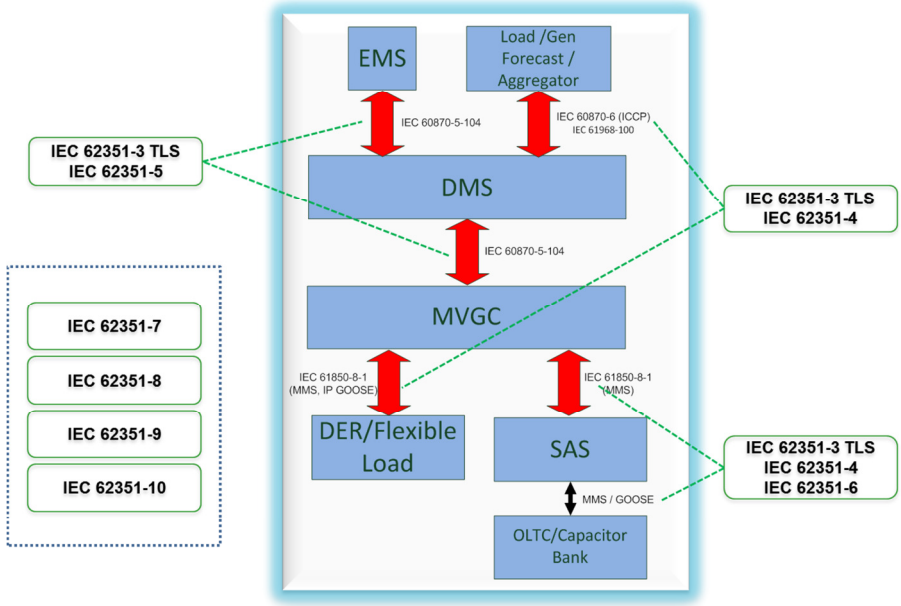

Figura 5-5 Mapping del caso d'uso sullo standard IEC 62351

Il fuoco di questo lavoro copre in particolare le comunicazioni MVGC-DER, che utilizzano lo standard IEC 61850-8-1 MMS, argomento della sezione seguente.

5.3 IEC 61850 (MMS) - Comunicazioni stazione-DER

L' IEC 61850 è uno standard per la progettazione dei sistemi di automazione per le stazioni elettriche, e la parte 8 (SCSM, Specific Communication Service Mapping) [5] si occupa del mapping del modello dati con specifici protocolli. La sottosezione di interesse per questo lavoro, la 8-1, definisce la mappatura con il protocollo MMS (Manifacturing Message Specification).

MMS è un protocollo di livello applicativo, standard internazionale (ISO 9506). Si occupa dello scambio in tempo reale di dati e informazioni di controllo tra dispositivi di rete o software applicativi, scambio che avviene in modo tale da essere indipendente da:

- la funzione applicativa svolta
- il vendor o lo sviluppatore del dispositivo impiegato

Queste due caratteristiche sono fondamentali per la condizione di interoperabilità tra due o più sistemi gestiti da operatori diversi.

All'interno del caso d'uso presentato nella sezione precedente, il principale scambio informativo tra DER e stazione prevede l'invio alla stazione delle misure relative ai DER attraverso report MMS e la trasmissione di setpoint dalla stazione ai DER. Il server MMS situato presso il DER, invia periodicamente i valori delle misure al client MMS installato presso la stazione. In maniera asincrona la stazione può inviare comandi (setpoint) ad uno o più DER a seconda delle necessità di controllo. La sequenza dei messaggi tra stazione e DER è rappresentata in Figura 5-6.

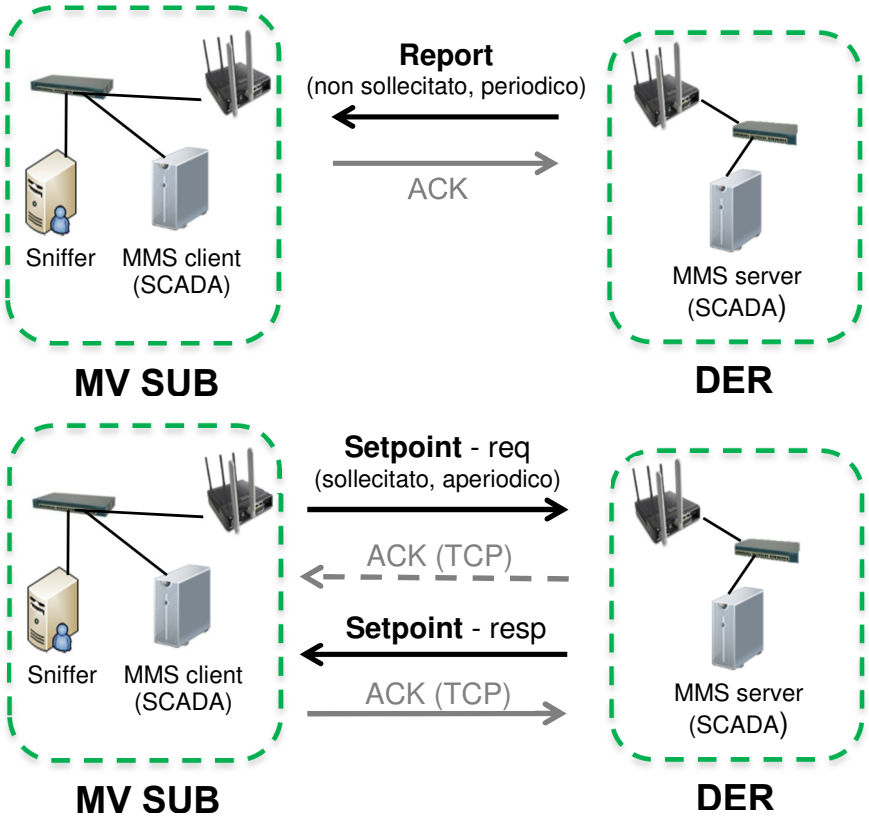

Figura 5-6 Schema trasmissione report e setpoint MMS

6. Piattaforma sperimentale

In questa sezione viene descritto il setup del testbed RSE utilizzato per eseguire le sessioni di test necessarie a valutare i differenti scenari che interessano il controllo di tensione nelle reti attive MT.

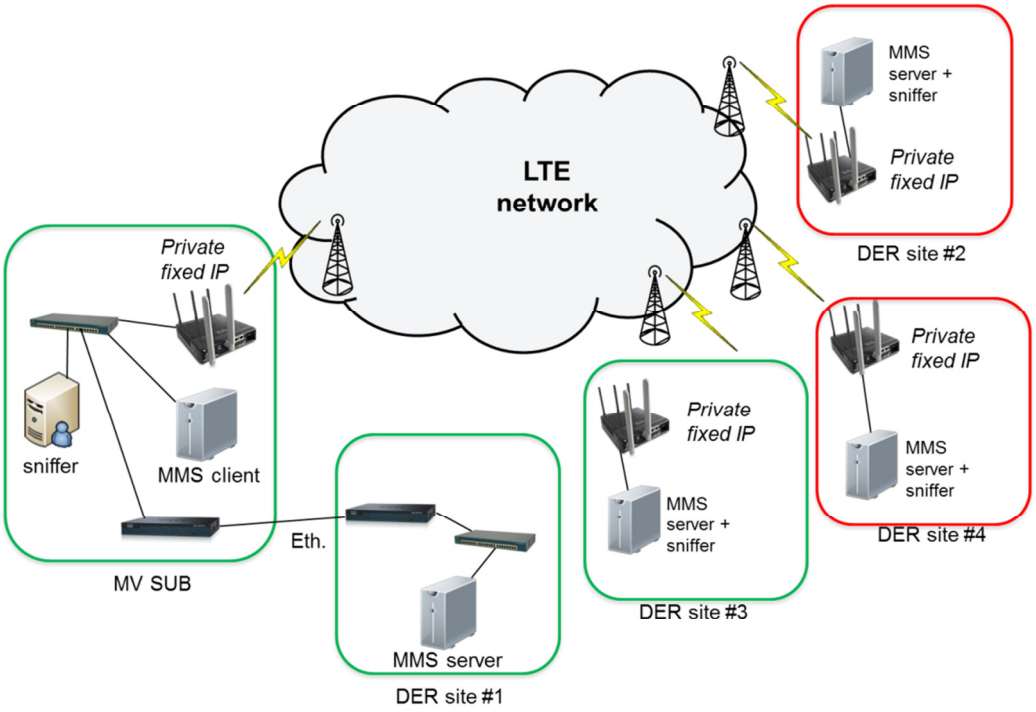

Figura 6-1 Schema della rete di comunicazione DER

La rete di comunicazione dei DER, riportata in Figura 6-1, è di tipo eterogeneo. Un DER e la stazione sono localizzati all'interno del PCS-ResTest Lab di RSE, e sono collegati via VLAN Ethernet, mentre gli altri 3 DER sfruttano la connessione wireless M2M LTE per comunicare con l'MMS client.

Dal punto di vista dei protocolli impiegati, i moduli di comunicazione attivi sulle macchine client e server applicano l'intero stack presente nelle applicazioni reali, in questo caso lo stack IEC 61850 MMS, implementato mediante la libreria libiec61850 [6]. I messaggi scambiati, report e setpoint MMS, saranno quindi conformi a quanto indicato nello standard.

Il supporto alla parte 3 della norma IEC 62351 ha portato l'introduzione di un HAL (Hardware Abstraction Layer) che fornisce la sicurezza desiderata ai moduli di comunicazione MMS. Questo layer implementa il protocollo TLS versione 1.2 (RFC 5246 [7]), grazie alle funzioni di autenticazione e cifratura fornite dalla libreria OpenSSL. Come indicato dallo standard, è previsto lo scambio bidirezionale di certificati tra client e server per instaurare la sessione TLS, e sono disponibili le funzionalità di session renegotiation e resumption.

In Figura 6-2 è riportata l'integrazione del layer TLS nello stack MMS.

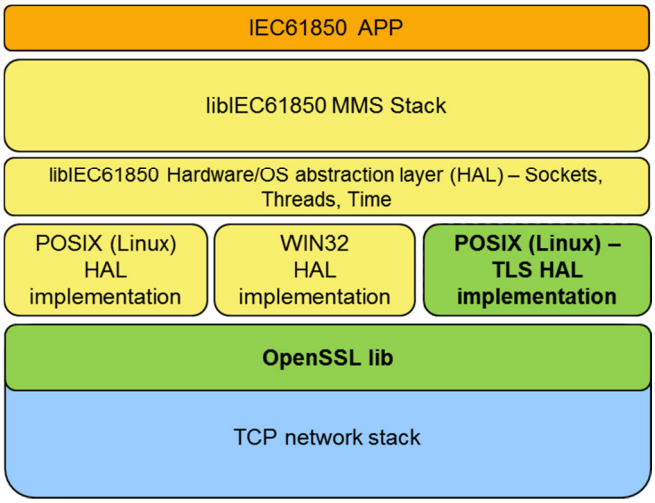

Figura 6-2 Implementazione dello standard IEC 62351-3

Seguendo lo schema di caratterizzazione dei test presentato nella sezione 4.1, nella figura Figura 6-3 sono riassunti i parametri dei diversi test effettuati.

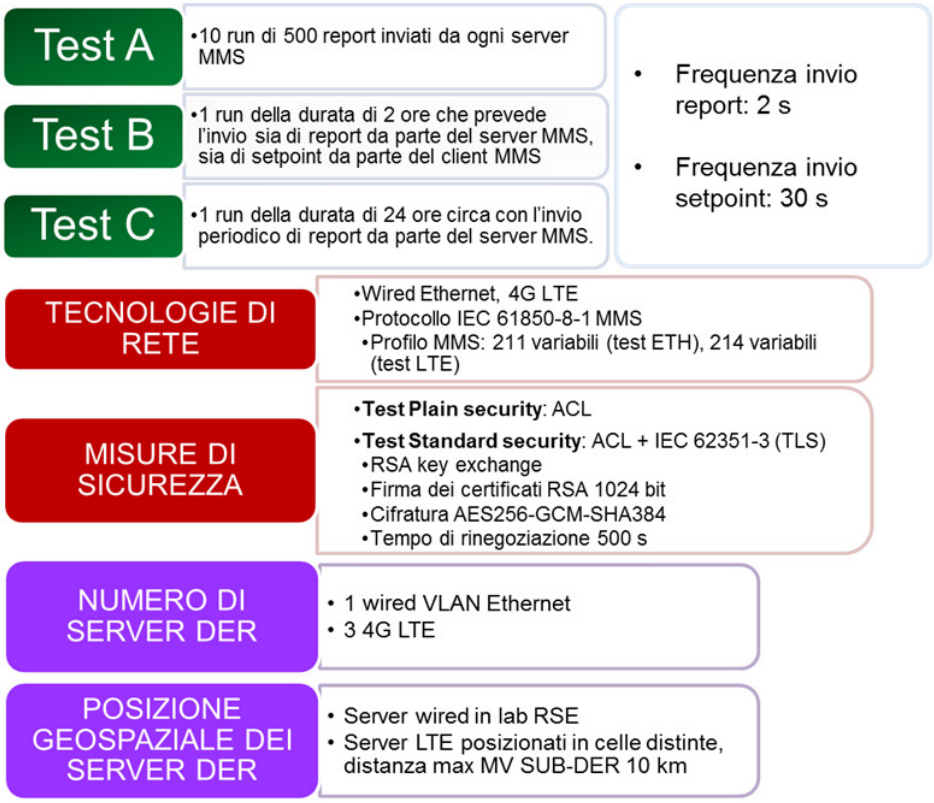

Figura 6-3 Parametri dei test svolti

L'obiettivo è approfondire l'analisi delle comunicazioni tra la stazione DSO e i DER in una situazione di esercizio regolare, senza attacchi. Le misure relative alle comunicazioni VLAN Ethernet sono state utilizzate come riferimento per la misura del ritardo introdotto dalla rete mobile LTE nel tempo totale di trasmissione dei messaggi applicativi MMS.

Dal punto di vista del livello di sicurezza adottato sono distinguibili due casi di test:

- **Plain security** test: alle comunicazioni vengono applicate misure di sicurezza base (controllo accessi) tramite ACL (Access Control List) sui router.

- **Standard security** test: vengono potenziate le misure di sicurezza, applicando lo standard IEC 62351-3 che include il layer TLS.

I risultati dei test, e le relative considerazioni, sono oggetto della successiva sezione.

7. Risultati

In Figura 7-1 è riportata la sequenza di passi che caratterizza il processo di test.

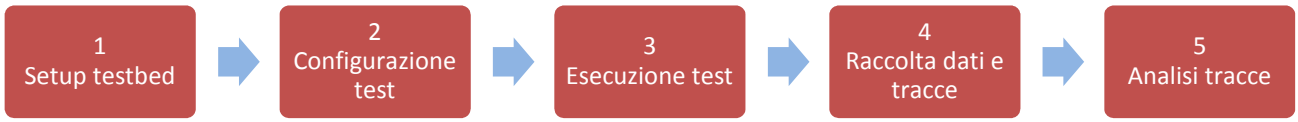

Figura 7-1 Schema del processo di test

Fornendo al tool di analisi le tracce delle catture del traffico di rete ottenute durante l'esecuzione dei test è stato possibile estrarre i valori degli indicatori presentati nella sezione precedente.

In Tabella 1 sono riportati i risultati dei Test A, B e C, realizzati su rete wired Ethernet nei casi di test plain security e standard security, mirati a valutare l'impatto della sicurezza sulle prestazioni delle comunicazioni DER-stazione.

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

Tabella 1: Impatto della sicurezza sulle prestazioni delle comunicazioni, caso end-to-end VLAN Ethernet

Si nota che l'introduzione delle misure di sicurezza, in particolare il layer TLS, non influisce sulle diverse fasi della comunicazione MMS, soprattutto si concretizza in un impatto trascurabile su una metrica di grande importanza come il RTT dei report MMS, i messaggi informativi che il DER invia periodicamente alla stazione. La creazione della sessione TLS è realizzata in una fase di handshake che introduce un esiguo overhead temporale rispetto al caso plain security.

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

Tabella 2: Impatto della sicurezza sulle prestazioni delle comunicazioni, caso end-to-end tecnologia LTE

In Tabella 2 sono esposti i risultati dei test condotti con i 3 DER che impiegano la rete wireless M2M LTE per comunicare con la stazione: si può notare come l'introduzione della sicurezza non sembri comportare effetti incisivi sui valori delle misure. È invece notevole come le performance della rete mobile siano estremamente variabili a causa dell'aleatorietà delle condizioni del canale radio, come si può notare, ad esempio, dalle misure di RTT dei Setpoint. In Figura 7-2 si osserva come il tempo totale di handshake sia superiore con l'introduzione delle misure di sicurezza (Test A). In corrispondenza della run numero 7 l'effetto della prima citata aleatorietà del canale wireless fa si che il tempo totale di handshake nel caso plain security sia quasi il doppio del valore medio per questo caso: addirittura risulta essere maggiore di quello nel caso Standard security.

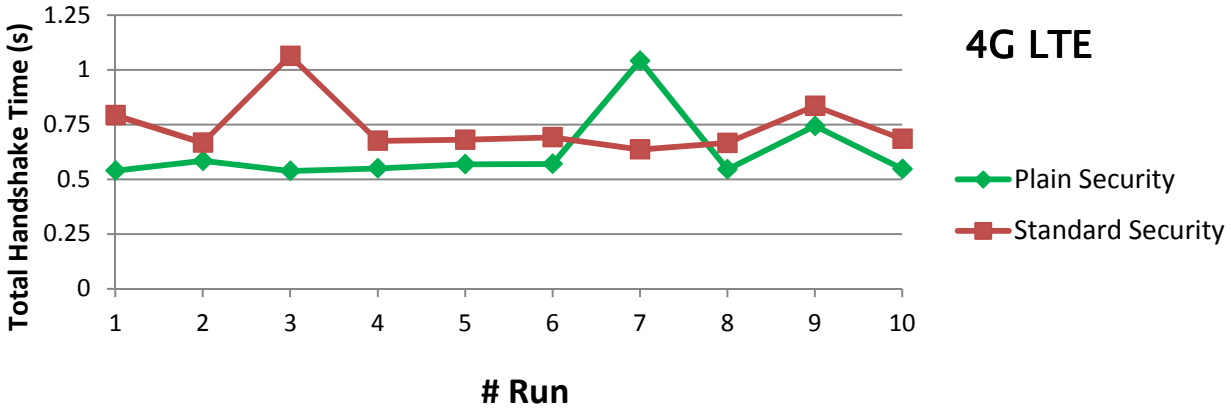

Figura 7-2 Total Handshake Time

È interessante combinare i dati relativi all'andamento temporale del RTT dei report MMS e le ritrasmissioni dei report stessi. L'effetto delle cattive condizione del canale radio possono causare la ritrasmissione dei

report e il conseguente aumento del RTT (come nello zoom in Figura 7-3), che può quindi essere impiegato come indicatore di performance della qualità della linea di comunicazione.

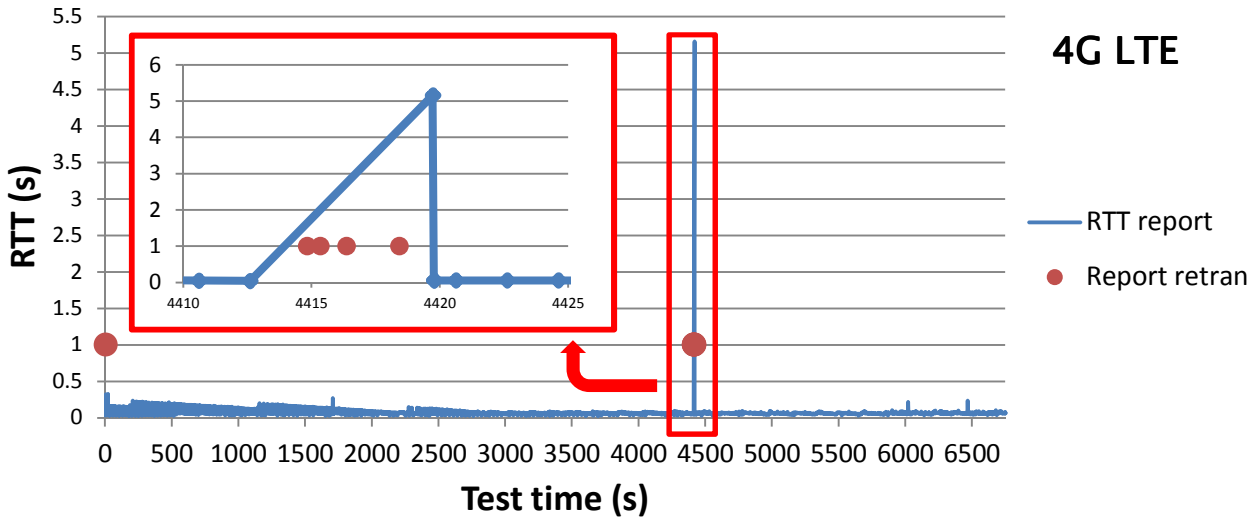

Figura 7-3 Round Trip Time Report MMS

7.1 Considerazioni sui risultati

Un risultato chiaro emerso dai test è la trascurabilità dell'overhead temporale introdotto dal layer TLS nello scambio messaggi applicativi MMS. L'aggiunta di un'ulteriore fase di handshake a quelle TCP e MMS porta a un naturale incremento del Total Handshake Time.

Queste considerazioni sugli effetti dell'introduzione della sicurezza nelle comunicazioni ICT conducono alla seguente riflessione: per una specifica implementazione è opportuno ricercare la configurazione del profilo TLS più adatta ai requisiti dell'applicazione di comunicazione in esame, rispettando i vincoli e le indicazioni dello standard IEC 62351-3.

Vanno altresì fatte alcune considerazioni riguardanti gli aspetti più legati alla rete di comunicazione impiegata. I test hanno mostrato quanto le prestazioni su rete wireless siano dipendenti dalle condizioni di traffico della cella 4G alla quale si è connessi e quindi dalla posizione geospaziale dei DER, elemento certamente non trascurabile nel caso si decida di utilizzare una rete di comunicazione non dedicata preesistente.

Condizioni non favorevoli del canale radio possono causare la ritrasmissione di segmenti TCP e quindi dei report/setpoint MMS, con il conseguente aumento del RTT misurato.

8. Lesson learned e conclusioni

Il punto di partenza di questo lavoro è stato la necessità di fornire adeguate misure di sicurezza nelle comunicazioni ICT delle Smart Grid.

La metodologia di test sviluppata è basata su di un ambiente di prova realizzato impiegando protocolli e procedure standard che possano garantire l'interoperabilità tra dispositivi e sistemi diversi. Nel caso del testbed RSE, la scelta di questi standard di sicurezza è ricaduta sulla norma IEC 62351, parte 4. Nello specifico, per conseguire la sicurezza end-to-end delle comunicazioni essa indirizza la parte 3 dello standard, quella attinente ai profili di sicurezza che includono TCP/IP, che ha raggiunto un buon livello di maturità a fine 2014.

Altro importante step è la scelta di un caso d'uso adatto al sistema che si intende studiare, insieme all'elaborazione di un piano di test e all'individuazione di un insieme di indicatori di performance adatti allo scopo.

L'elaborazione della metodologia ha evidenziato la necessità di studiare una soluzione di deep packet inspection (DPI), necessaria per analizzare il traffico cifrato con il protocollo TLS, valida anche dal punto di vista della realizzabilità in campo, non solo in un ambiente di test. Alcune soluzioni per questo particolare aspetto sono in fase di studio all'interno del WG 15 del TC 57 IEC come estensione della norma IEC 62351.

I risultati sperimentali hanno messo in risalto l'impatto limitato dell'aggiunta del layer TLS sulle performance delle comunicazioni stazione-DER e la necessità di soppesare in modo oculato gli effetti di questa aggiunta, come aumento del tempo totale di handshake o le ritrasmissioni TCP, in merito al particolare caso d'uso indirizzato o all'applicazione considerata.

Gli sviluppi futuri prevedono il consolidamento dei dati mediante un'analisi esaustiva che consideri con precisione giorno e ora di svolgimento dei test, la posizione geospaziale dei server insieme ad altri parametri che possano migliorare la caratterizzazione dei test.

Bibliografia

[1] International Standard IEC 62351-3 Ed.1.0 “Power systems management and associated information exchange - Data and Communication Security – Part 3: Communication network and system security – Profiles including TCP/IP”, Ottobre 2014

[2] IETF RFC 5246 The TLS Protocol, Version 1.0, 1999

[3] Comitato Elettrotecnico Italiano Norma CEI 0-16 “Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company”, 2013

[4] Comitato Elettrotecnico Italiano Norma CEI EN 50160, “Caratteristiche della tensione fornita dalle reti pubbliche di distribuzione dell’energia elettrica", 2011

[5] International Standard IEC 61850-8-1 Ed.2.0. “Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802”, Giugno 2011

[6] libIEC61850 – open source libarary for IEC 61850. [Online] Available: http://libiec61850.com/libiec61850/

[7] IETF RFC 2246 The Transport Layer Security (TLS) Protocol, Version 1.2, 2008

Ringraziamenti

Vodafone – piattaforma test M2M LTE

Stefano Marzorati
Mario La Rosa

Progetto Europeo SmartC2Net

www.smartc2net.eu

D6.2 Integrated test beds – Description