Testing della Sicurezza

nelle comunicazioni standard delle Smart Grid

Giovanna Dondossola, Roberta Terruggia, Paolo Wylach

Ricerca sul Sistema Energetico – RSE Spa

Via Rubattino 54 I-20134 Milan – Italy

giovanna.dondossola@rse-web.it

roberta.terruggia@rse-web.it

paolo.wylach@rse-web.it

La trasformazione delle reti elettriche di distribuzione da reti passive a reti attive cui stiamo assistendo negli ultimi anni comporta l'introduzione di nuove funzionalità ICT (Information and Communication Technology) e l'allineamento dei sistemi ICT in esercizio. In questo contesto è indispensabile che entità appartenenti a domini diversi siano in grado di comunicare in maniera standardizzata e sicura. Ad esempio, il DSO (Distribution System Operator) dovrà essere in grado di interagire con i DER (Distributed Energy Resource), le risorse energetiche distribuite, e con tutti gli altri attori coinvolti nella gestione e nel controllo del sistema elettrico. L'utilizzo di protocolli di comunicazione standard risulta quindi indispensabile per facilitare l'interazione tra le diverse entità.

Un elemento chiave nello sviluppo delle reti ICT è rappresentato sempre più dalla sicurezza delle comunicazioni. Con l'avvento delle Smart Grid le reti di controllo non risultano più isolate e quindi relativamente protette da attacchi informatici. Dovendo comunicare con soggetti esterni, gli operatori hanno dovuto "aprire" le loro reti per permetterne l'accesso da parte di entità appartenenti ad altri domini. Per ragioni di convenienza economica le connessioni delle Smart Grid possono utilizzare reti di comunicazione di terze parti, potenzialmente soggette ad attacchi informatici che possono comportare problemi di comunicazione tra i vari componenti ICT delle Smart Grid. Questo può causare instabilità nella rete elettrica o addirittura il danneggiamento dei dispositivi.

Questo lavoro propone una metodologia sperimentale per la valutazione degli standard di sicurezza applicabili alle comunicazioni per il controllo delle Smart Grid.

Elementi caratterizzanti della metodologia realizzata nel Lab PCS-ResTest presso RSE sono l'implementazione dei flussi di controllo standard, l'integrazione delle funzionalità di sicurezza delle comunicazioni e la valutazione dell'impatto di queste sulle prestazioni delle comunicazioni end-to-end attraverso sessioni di test e l'elaborazione di indicatori di QoS (Quality of Service).

Per illustrare i passi essenziali della metodologia si sono analizzate le comunicazioni tra una stazione primaria e le risorse di energia distribuita (DER) per la funzionalità di controllo di tensione sulla rete di media tensione. Per queste comunicazioni si è valutato lo standard IEC 61850 focalizzandosi in particolare sul profilo MMS (Manufacturing Message Specification) definito all'interno dell'IEC 61850-8-1. I moduli di comunicazione sviluppati scambiano report MMS standard, applicando l'intero stack di protocolli presente

nelle applicazioni reali. Per rendere più completa l'analisi, si sono valutate tecnologie di comunicazione eterogenee, sia wired sia wireless.

Per quanto riguarda gli aspetti di sicurezza è stata analizzata la serie di standard IEC 62351 (Power systems management and associated information exchange - Data and communications security), che fornisce specifiche indicazioni al fine di rendere sicure le comunicazioni implementate secondo i protocolli tipicamente adottati nel dominio delle reti elettriche.

In particolare la parte 3 dell'IEC 62351 (Profiles Including TCP/IP) è relativa alla sicurezza end-to-end delle comunicazioni e richiede l'implementazione di un layer di sicurezza TLS (Transport Layer Security), definito nel RFC 2246 dell'IETF. L'obiettivo di questa parte dello standard è garantire, nelle comunicazioni basate sui protocolli TCP/IP, la protezione dei messaggi di telecontrollo, evitando potenziali accessi non autorizzati alle comunicazioni, la modifica o il furto dei messaggi stessi. È quindi possibile considerare questo una contromisura valida per gli attacchi di tipo man in the middle e replay. Lo standard definisce l'insieme di procedure necessarie ad instaurare un canale di comunicazione cifrato utilizzando il TLS, a seguito di un processo di autenticazione degli end-node che intendono instaurare la comunicazione sicura: per questo scopo essi sono dotati di certificati digitali emessi da una certification authority valida. L'IEC 62351-3 pone dei vincoli per le funzionalità di session resumption e per la rinegoziazione della sessione, richiedendo inoltre una serie di controlli per verificare la validità dei certificati sottomessi.

Grazie all'implementazione degli aspetti principali richiesti dall'IEC 62351-3 all'interno dei moduli di comunicazione presenti nel componente di stazione primaria e nel componente del DER, è stato possibile eseguire diverse sessioni di test al fine di valutare differenti scenari riguardanti le funzionalità di controllo di tensione nelle reti attive. I test si sono focalizzati sulla valutazione delle comunicazioni con reti eterogenee senza e con l'introduzione delle misure di sicurezza. Per poterne analizzare l'impatto sono stati identificati e calcolati diversi indicatori che permettono di ottenere misure specifiche rispetto ai protocolli utilizzati, così da valutarne in maniera precisa l'overhead richiesto e le criticità in relazione ai requisiti prestazionali dell'applicazione di controllo.

Il paper presenterà i risultati ottenuti dall'applicazione della metodologia spiegando la loro ricaduta sullo sviluppo degli standard di sicurezza, sulla loro integrazione nei dispositivi in vista dei necessari adeguamenti richiesti dall'evoluzione della rete elettrica e il loro impatto sull'esercizio della Smart Grid.