Federico Bellio
Enel Produzione
Via Torino 14
30172 Venezia-Mestre (VE)
tel . +390418215592
mail federico.bellio@enel.com

Gian Luigi Pugni
Enel Servizi
Viale Italia, 26
20099 Sesto San Giovanni (MI)
tel: +390223207827
mail: gianluigi.pugni@enel.com

IEC TS 62351 nei sistemi di controllo per la Generazione del Gruppo Enel

Abstract

La norma TS 62351 "Power systems management and associated information exchange – Data and communications security" è stata sviluppata in ambito IEC dal TC-57 ad iniziare dai primi anni 2000, le prime parti sono state pubblicate nel 2007. La norma vuole rispondere all'esigenza di sicurezza che deriva dall'aver adottato per il controllo dei sistemi dedicati alla Generazione, Trasporto e Distribuzione dell'Energia Elettrica, infrastrutture sempre più evolute e complesse da un punto di vista informatico. Il problema della sicurezza è affrontato a tutto tondo nel modo classico per un ambito informatico: rendere lo scambio dati tra sistemi adeguato in termini di confidenzialità, integrità, disponibilità e non ripudio. In un tipico approccio top - down la norma è divisa in parti che rappresentano tasselli o strati delle misure da adottare per rendere lo scambio dati sicuro. Due tasselli o strati, a torto talvolta considerati secondari, riguardano due sotto-sistemi invece fondamentali per raggiungere i requisiti di sicurezza auspicabili in una infrastruttura critica qual'è il sistema elettrico di un Paese o di un gruppo di Paesi le cui reti elettriche sono interconnesse: la parte 7 "Network and System Management" che riguarda la gestione dell'infrastruttura per il controllo e la supervisione della rete, dei sistemi informatici e di telecomunicazioni a governo di un sistema elettrico e la parte 8 "Role Based Access Control" che riguarda l'infrastruttura per consentire l'accesso al contempo aperto e sicuro alle informazioni di una risorsa preziosa qual'è l'energia.

In questa memoria saranno illustrati i criteri progettuali che guidano l'implementazione di questi due tasselli fondamentali nei sistemi di automazione e telecontrollo per il governo della Generazione del Gruppo Enel in Italia.

IEC TS 62351 for Enel Group, Generation Area

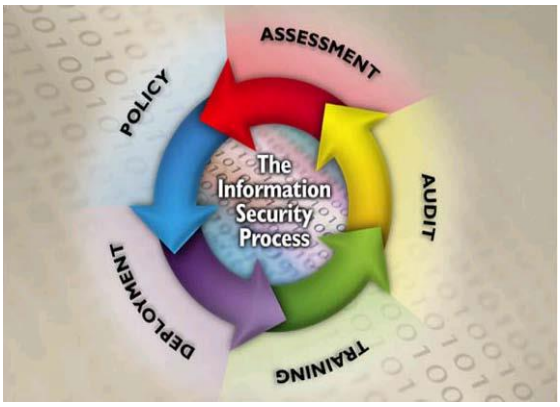
Abstract

The standard TS 62351 "Power systems management and associated information exchange - Data and communications security" has been developed within the IEC TC-57 since the early 2000s, the first parts were published in 2007. The aim of this standard is to respond to the security needing that comes from the growing complexity of control systems dedicated to Power systems. The security issue is addressed in the traditional way for a computer science: making data exchange and management protected in terms of integrity, availability, confidentiality and non-repudiation. The standard is divided into parts that actually define the layers of countermeasures to be taken in order to secure data exchange, infrastructure administration and system control. Two of this security layers, sometimes considered secondary, are in fact essential to cover the security requirements of an Power system serving group of countries whose electricity grids are also interconnected (a complex critical infrastructure). The first layer is described in part 7 - "Network and system Management", and concerns the infrastructure management for the control and supervision of the network, computer systems and telecommunications environment that are part of the electrical telecontrol system. The second layer is described in part 8 - "Role Based Access control", which concerns the infrastructure and the mechanism to control and grant the access to resources and devices inside such a valuable environment.

This report will describe the design criteria that guided us in the implementation of these two fundamental pieces in the automation and remote control inside Hydro Generation Area of the Enel Group in Italy.

Indice

1 Premessa



La sicurezza informatica nasce da un ciclo di miglioramento continuo, con il pieno coinvolgimento delle Business lines e delle altre funzioni aziendali per l'identificazione, la qualificazione dei Rischi e progettazione e attuazione delle contromisure.

Il modello proposto intende perseguire il miglioramento continuo attraverso il contributo attivo delle diverse funzioni aziendali, ciò comprende attività per:

- La costante misura (**Audit**) della completezza e dello stato di attuazione dei controlli di sicurezza
- L'identificazione e la qualificazione e la gestione dei Rischi (**Assessment**)
- La definizione delle nuove politiche per l'attuazione della sicurezza, da cui derivano l'aggiornamento dei controlli (**Policy**)
- L'attuazione (**Deployment**) dei nuovi controlli
- La formazione in modo da rendere realmente efficace l'attuazione consapevole dei controlli di sicurezza (**Training**)

I protocolli di comunicazione sono una delle parti più critiche per il funzionamento del Sistema Elettrico poiché sono responsabili del recupero di informazioni da apparecchiature di campo e, viceversa, per l'invio di comandi di controllo. Nonostante la loro funzione fondamentale, ad oggi, nei protocolli di comunicazione sono raramente incorporate le misure di sicurezza, compresa la sicurezza contro gli errori involontari e di malfunzionamenti nei sistemi di alimentazione, guasti alle apparecchiature di comunicazione, o di sabotaggio intenzionale.

Dal momento che questi protocolli sono stati per lungo tempo molto specializzati e proprietari, la "Security by Obscurity" è stato l'approccio adottato in prevalenza per molti anni. Oggi la "Security by Obscurity" non è più un concetto accettabile (se mai lo è stato), perché l'utilizzo intensivo di soluzioni standard ed aperte, a partire dallo stack TCP/IP, rende i protocolli di telecontrollo vulnerabili a famiglie di attacchi molto estese.

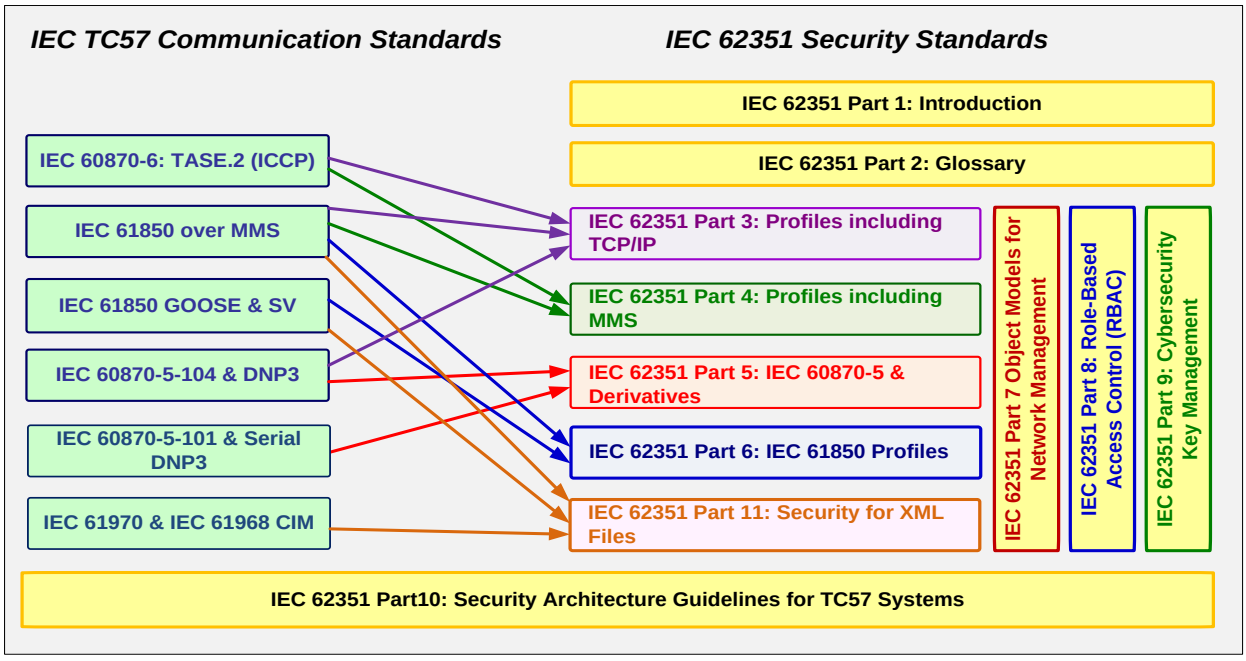
L'Industria Elettrica si basa sempre più sull'impiego dell'informazione per gestire il sistema elettrico e si trova a dover gestire parallelamente una seconda infrastruttura di telecomunicazione e controllo, basata su sistemi e concetti di natura prettamente informatica. Queste infrastrutture sono tra loro fortemente interconnesse e interdipendenti.

Le reti di telecomunicazioni e telecontrollo di ciascun operatore del mercato sono peraltro fortemente interconnesse con quelle degli altri operatori, con un preciso parallelismo rispetto alle esistenti

interconnessioni presenti nel sistema elettrico. Ciò comporta che gli effetti di eventuali minacce non possano essere considerati locali o regionali ma che gli impatti debbano essere considerati in relazione ad un perimetro di rischio potenzialmente molto ampio.

L'obiettivo della sicurezza logica dei protocolli nel contesto della gestione dei sistemi elettrici ha come fine primario la **disponibilità** (spesso indicata come resilienza) del sistema rispetto a possibili minacce di natura sia dolosa che involontaria, garantendo perciò la disponibilità costante di energia. Per far ciò è necessario garantire anche l'**integrità**, la **riservatezza** delle informazioni insieme ad una ulteriore caratteristica di "**non ripudiabilità**" dell'informazione[1].

La norma IEC 62351, curata da IEC TC 57 WG15, definisce la "data and communications security for power systems management and associated information Exchange". La norma è strutturata in un insieme di specifiche parti, ciascuna delle quali sviluppa e definisce un tema specifico. In particolare le parti dalla 3 alla 6 si riferiscono alla messa in sicurezza dei protocolli IEC 61850 e IEC 60870. L'obiettivo è la realizzazione della sicurezza end-to-end tra tutti i sistemi che partecipano all'infrastruttura di telecontrollo e automazione mediante mutua autenticazione delle parti, cifratura e firma dei messaggi.



Nella presente nota viene trattata la tematica di sicurezza che si riferisce alla parte 7 (definizione dei requisiti di monitoraggio dei sistemi e delle reti)[2] e alla parte 8 (RBAC – Role-Based Access Control) della norma IEC 62351[3].

Questi due aspetti della sicurezza, a volte sottovalutati, costituiscono un elemento abilitante e necessario per il completamento di una infrastruttura di sicurezza logica vera.

La gestione delle abilitazioni di accesso alle risorse di sistema e di rete (IEC 62351-8), pensata in modo da associare i privilegi di accesso in base all'appartenenza ad una classe di soggetti (ruolo), invece che allo specifico soggetto, è infatti un presupposto indispensabile per permettere una corretta attuazione delle tecniche di protezione indicate in tutte le norme della famiglia IEC 62351, che presuppongono la corretta reciproca identificazione delle parti prima di consentire l'accesso a qualsivoglia risorsa.

Il monitoraggio degli eventi e dello stato dei sistemi è (IEC 62351-7) è finalizzato al riconoscimento in tempi opportuni di un potenziale stato di rischio, che può avere natura dolosa, di errato intervento oppure di malfunzionamento di uno o più componenti di sistema. E' inutile aver previsto una adeguata ridondanza di componenti all'interno di un sistema se non si viene informati di un guasto o della presenza di una minaccia: la conseguenza sarebbe che anche se in modo ritardato il disservizio si presenterebbe, magari al momento del secondo guasto o del tradursi della minaccia in un caso di rischio reale.

2 Network and System Management (IEC 62351-7)

I sistemi di telecontrollo dei sistemi di generazione e trasporto dell'energia si basano sull'impiego di una serie di strumenti:

- Reti geografiche di telecomunicazioni
- Reti locali di impianto
- Intelligent Electronic Devices (IED)
- Sistemi SCADA di impianto
- Sistemi SCADA centrali.

Ciascuno di questi oggetti contribuisce al telecontrollo delle infrastrutture vere e proprie del sistema elettrico. I sistemi SCADA sono in grado tramite questo sistema di strumenti di controllare in modo affidabile il sistema, *a patto che ciascuno di questi strumenti si comporti secondo quanto previsto, e che non sia a sua volta in uno stato anomalo.*

Può sembrare un controsenso il preoccuparsi dello "stato di salute" di dispositivi nati proprio per il monitoraggio e il controllo ma dobbiamo ricordare che proprio la crescente potenza e capacità di interazione dei sistemi di telecontrollo di nuova generazione li espone ad una serie di rischi, ad esempio:

- errori software, che possono manifestarsi in modo spontaneo sotto forma di malfunzionamenti o essere fonte di vulnerabilità;
- problemi nella comunicazione (packet loss, ritardi, disconnessioni periodiche), che possono essere mascherati dalla ridondanza dei protocolli o delle connessioni, fino ad un certo limite che poi provoca la perdita dell'apparato;
- anomalie hardware (ad esempio alimentatori, batterie) che diventano evidenti solo al momento del guasto;
- malware, che possono provocare un anomalo utilizzo di risorse del dispositivo.

In alcuni casi l'anomalia o l'evento sono relativi ad un singolo oggetto, ma in molti casi il riconoscimento di un evento o di una situazione di potenziale rischio è possibile solo attraverso la correlazione di informazioni di monitoraggio provenienti da più di elementi, soprattutto in presenza di tentativi di intrusione, che si manifestano spesso in modo progressivo prima nei confronti degli apparati di rete e poi nei confronti degli end-point.

Per questo motivo è opportuno, anzi, necessario che gli eventi e lo stato dei sistemi vengano raccolti e correlati da una infrastruttura unificata, in grado di raccogliere, classificare e correlare gli eventi e lo stato di funzionamento di ciascun dispositivo, sia esso appartenente al dominio dei sistemi di telecontrollo (IED, SCADA, ecc.) o al dominio delle infrastrutture di comunicazione e supporto (firewall, IDS/IPS, router, switch ecc.).

Il monitoraggio integrato dei sistemi attraverso una infrastruttura di Network and System Management (nel seguito NSM) costituisce da molto tempo un caposaldo per gli operatori di telecomunicazioni e per i provider ICT, che si sono pertanto attrezzati con strumenti e protocolli di monitoraggio adeguati e possiedono anche processi organizzativi finalizzati a questo scopo.

Questo fatto suggerisce l'opportunità di utilizzare questa esperienza, e in molti casi anche le soluzioni tecnologiche, per integrare il monitoraggio degli eventi e degli stati dei sistemi a livello Enterprise, in una infrastruttura NSM di alto profilo, magari in quella già esistente per la gestione della rete e dei sistemi informatici. L'adozione di sistemi NSM integrati a livello Enterprise offre perciò l'opportunità di ottenere la correlazione di eventi di sicurezza provenienti non soltanto dall'ambiente di processo, ma anche dall'ambiente gestionale, con il quale peraltro i sistemi di processo devono ormai molto spesso interagire per rispondere alle esigenze di business di un mercato aperto.

2.1 La norma 62351-7

La sicurezza end-to-end coinvolge molto di più che la crittografia o l'autenticazione, che costituiscono i principali metodi di sicurezza. L'intera infrastruttura di telecontrollo deve essere protetta e affidabile al fine di garantire la sicurezza e l'affidabilità delle operazioni sui sistemi Elettrici. Ciò comporta anche l'attuazione delle azioni di monitoraggio necessarie a riconoscere i sintomi delle anomalie e associarli a possibili minacce, adottando per quanto possibile le contromisure opportune.

Dal punto di vista operativo la sicurezza può essere attuata secondo più livelli di intervento:

- **La deterrenza e il ritardo**, cercando di evitare gli attacchi, o almeno ritardarli abbastanza a lungo in modo da predisporre adeguate contromisure.
- **Rilevamento di attacchi:** la rilevazione è fondamentale per tutte le altre misure di sicurezza in quanto in caso di attacco non riconosciuto, poco si può fare per impedirlo. Le funzionalità IDS possono svolgere un ruolo importante.
- **Valutazione di attacchi**, per determinare la natura e la gravità dell'attacco. Per esempio è necessario valutare se l'attacco ha violato la riservatezza dei dati privati, o se l'attacco è poco più di un fastidio.
- **La comunicazione e la notifica**, in modo che le persone responsabili e i sistemi possano essere messi a conoscenza dell'attacco in modo tempestivo.
- **Risposta agli attacchi**, che comprende le azioni da parte dei responsabili per mitigare l'effetto dell'attacco in modo tempestivo. Questa risposta poi può impedire o ritardare un attacco successivo.

In questo contesto l'infrastruttura NSM ha un ruolo importante attuando :

- il **monitoraggio dello stato** delle applicazioni software, dispositivi hardware e comunicazioni. Questa azione di monitoraggio è in grado di fornire notifica delle modifiche di stato, come ad esempio guasti alle attrezzature, modifiche di configurazione anomale, errori software o guasti, interruzioni temporanee della comunicazione e fallimenti di comunicazione permanenti.
- il **monitoraggio delle prestazioni** dei sistemi e delle comunicazioni. Questa raccolta e correlazione di informazioni è in grado di registrare le condizioni del traffico di dati, le variazioni

di prestazioni delle applicazioni software, cambiamenti del flusso dei dati (in volume e tipologia), risultati di performance nelle comunicazioni, ecc

- il **rilevamento delle intrusioni**. Oltre a evidenti intrusioni, tale rilevamento deve essere sensibile alle condizioni "normali", al fine di tentare di rilevare anche quelle minime variazioni di contesto che potrebbero essere sintomo di un'intrusione. Questo rilevamento intrusioni utilizza naturalmente le informazioni ottenute mediante il monitoraggio di stato ed il monitoraggio delle prestazioni
- **Gestione della configurazione**. La configurazione delle reti di comunicazione e dei sistemi può essere gestita, sia attraverso la definizione di modifiche automatiche basate su eventi (ad esempio attivando nuove regole sui firewall in caso di attacco riconosciuto da parte di un virus), oppure selezionando manualmente una nuova configurazione, fino all'intervento di attivazione di componenti di riserva.

Le infrastrutture NSM sono già costantemente utilizzate per il monitoraggio e il controllo delle infrastrutture di telecomunicazioni, anche di quelle a supporto delle reti di processo, ma le informazioni raccolte sono purtroppo circoscritte all'ambito, seppur significativo, dei sistemi di rete (router firewall e IDS). Il monitoraggio viene svolto quindi primariamente dagli operatori che gestiscono il sistema di telecomunicazioni e spesso questo monitoraggio non comprende gli apparati di rete appartenenti alla LAN di impianto, che non contribuisce pertanto alla raccolta di informazioni.

La parte 7 della norma IEC 62351 intende colmare questa mancanza introducendo innanzitutto il concetto di monitoraggio della rete di telecontrollo, includendo anche la parte relativa all'impianto di automazione e poi assegnando anche un ruolo attivo ai componenti di telecontrollo e automazione, in qualità di fonte di informazioni per il monitoraggio. Ai sensi della parte 7 i componenti dei sistemi di telecontrollo (SCADA, RTU, IED …) devono predisporre la gestione di propri oggetti di monitoraggio e controllo, nei quali sono memorizzati valori che potranno essere interrogati o valorizzati dall'infrastruttura NSM. Inoltre è prevista la generazione spontanea di eventi che, analogamente a quanto già predisposto per gli apparati di rete, possono allertare l'infrastruttura NSM di particolari situazione critiche in atto.

La norma introduce innanzitutto i concetti relativi alla definizione degli oggetti specifici destinati al monitoraggio dei sistemi di telecontrollo ed automazione, introducendo classi specifiche di grandezze da tenere sotto osservazione oppure valori suscettibili di controllo da parte del sistema NSM. Questa definizione avviene secondo un criterio di astrazione, senza dare per scontato l'uso di uno specifico protocollo di monitoraggio, in modo da lasciare aperta la realizzazione di soluzioni di monitoraggio basate su protocolli ad oggetti diversi.

La norma si ispira comunque al modello dei sistemi di monitoraggio basati sul protocollo SNMP (Simple Network Management Protocol), che rappresenta lo strumento classicamente utilizzato per il monitoraggio delle reti informatiche, lasciando tuttavia aperta la strada alla mappatura degli oggetti di monitoraggio in oggetti classicamente appartenenti all'ambito di processo per esempio basati sulla norma IEC 61850.

L'edizione 1 della norma IEC 62351-7 non si spinge tuttavia alla mappatura dei "generic objects" negli oggetti dei diversi protocolli, attività che viene rimandata ad una successiva revisione. La norma è stata

peraltro oggetto di una attività di valutazione/sperimentazione di EPRI che ha pubblicato uno studio nel quale suggerisce numerosi interventi di raffinamento della norma[4].

Il nostro interesse si è focalizzato sulla possibilità di procedere verso una traduzione della norma nei protocolli di monitoraggio, a partire dall'SNMP e IEC 61850. SNMP ha l'indubbio vantaggio di consentire una veloce integrazione dei nuovi oggetti all'interno dell'infrastruttura NSM già esistente, che è responsabile del monitoraggio della nostra rete e dei sistemi ICT. Lo scopo è quello di attuare una dimostrazione sul campo della soluzione di monitoraggio integrato dei sistemi di telecontrollo e dei sistemi di rete, ottenendo una più esaustiva correlazione degli eventi e un più completo stato del sistema, valorizzando al contempo gli investimenti già effettuati nei sistemi NSM esistenti.

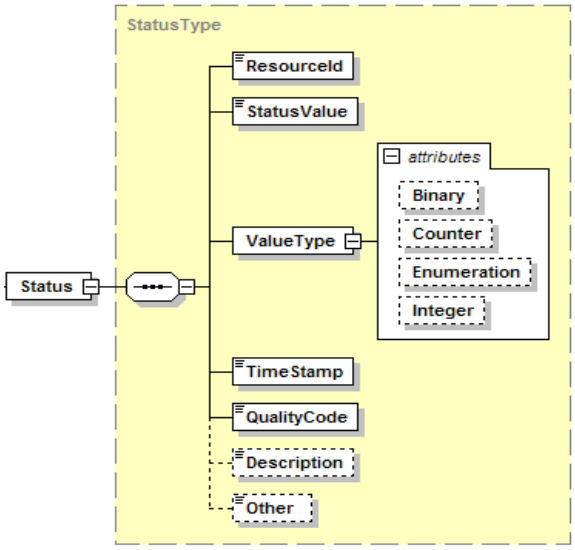
2.2 Data Objects Model

Per ottenere il monitoraggio integrato delle entità coinvolte nell'ambito dei sistemi di telecontrollo la norma 62351-7 utilizza un modello ad oggetti di tipo astratto, che possono essere di tipo semplice, cioè associati ad esempio ad un valore booleano o numerico, e più frequentemente oggetti strutturati che sono costituiti in modo ricorsivo da oggetti semplici o da ulteriori strutture.

La norma prevede che ciascun oggetto, oltre ai valori ad esso associati, comprenda alcuni campi essenziali tra i quali:

- L"ID" della risorsa da monitorare, che rappresenti l'identificatore univoco dell'elemento oggetto del monitoraggio (IED, Canale di comunicazione o altro);
- Il "nome dell'oggetto", che rappresenta l'identità del "data object";
- Indicatore di qualità del data value, essenziale per valutare l'attendibilità dell'oggetto stesso;
- Il time stamp di cambiamento.

Gli oggetti possono essere in sola lettura o anche scrivibili.



La norma introduce alcune categorie di oggetti organizzati in tre livelli principali. Il primo livello comprende il monitoraggio dei "Networks and Protocols" ed è finalizzata pertanto a mantenere sotto osservazione il comportamento del layer di comunicazione con attenzione ai seguenti aspetti:

- Network Configuration Monitoring and Control, che riguarda il monitoraggio e la gestione della rete intesa come intera infrastruttura e come singoli componenti, inclusi gli endpoint, router, switch ecc.;
- Network Backup Monitoring, intendendo che lo stato di salute delle infrastrutture di riserva deve essere mantenuto sotto osservazione costante;

- Network Communications Failures and Degradation Monitoring. Questa classe di oggetti è finalizzata a evidenziare variazioni nelle prestazioni e nella affidabilità dei componenti di rete anche quando questi comportamenti anomali non si configurano come un guasto conclamato. Lo scopo è riconoscere in modo preventivo uno stato di potenziale degrado in modo da intervenire tempestivamente con le appropriate contromisure;
- Communication Protocol Monitoring, intendendo con "protocol" il vero e proprio protocollo applicativo, con l'obiettivo di riconoscere situazioni anomale che possono derivare da messaggi malformati o manomessi, tentativi di Denial Of Service (magari con l'intenzione di provocare buffer overflow). In termini concreti lo scopo è quello di raccogliere lo "stato di salute" della comunicazione applicativa, per avere da un lato le statistiche sulla comunicazione e dall'altro le informazioni sulle situazioni anomale che possono essere sorprendentemente numerose.

Il secondo livello riguarda il monitoraggio degli "End Systems", per avere un quadro dello stato di funzionamento degli endpoint, che possono essere gli IED o gli SCADA:

- Monitoring End Systems. Per ciascuna di queste entità è definita nella norma una serie di oggetti che permette di valutare mediante valori semplici o strutturati la coerenza dello stato effettivo del dispositivo rispetto ai valori attesi.
- Security Control and Management of End Systems. Particolare evidenza nella norma è data agli oggetti di sicurezza dell'endpoint, che come gli altri sono soggetti a raccolta e a controllo di coerenza.

Il terzo livello riguarda le funzionalità di "Intrusion Detection"

- Segnalazione degli "Unauthorized Access", il riconoscimento di tentativi di accesso non autorizzati ad una risorsa
- Riconoscimento di un Esaurimento risorse a causa di un attacco Denial of Service (DoS)
- Riconoscimento e segnalazione dei Buffer Overflow a seguito di attacchi DoS
- Riconoscimento e conteggio di PDUs alterate o comunque malformate
- Segnalazione dei tentativi di accesso fisico, includendo le manomissioni di alimentazione
- Segnalazione degli accessi da Network Addresses non ammessi.

Questa serie di informazioni, opportunamente raccolta da parte degli endpoint e dei sistemi di rete che costituiscono l'infrastruttura di Telecontrollo, costituisce una vera e propria miniera di informazioni che può e deve essere utilizzata in modo proficuo per riconoscere lo stato di salute dell'intero sistema oltre che dei singoli componenti.

Quindi ogni elemento dell'infrastruttura, ai sensi della IEC 62351-7, possiede una sorta di immagine interna del proprio stato e delle proprie prestazioni, rispetto ad un certo numero variabile di oggetti di monitoraggio e controllo che ne descrivono lo stato, le prestazioni e che possono essere utilizzati (quando scrivibili) per modificarne alcuni comportamenti.

2.3 L’architettura del sistema di monitoraggio

Ogni elemento del sistema porta con sé una potenziale notevole complessità, che diventa difficile da governare quando si intende considerare l’intero sistema. La quantità di informazioni disponibili possono essere così tante da superare facilmente, come ordine di grandezza, la quantità di informazioni classicamente scambiate per l’esercizio delle funzioni dei sistemi di telecontrollo.

Per questa ragione è opportuno prestare attenzione alla tecnica di interrogazione di questi oggetti ed alla architettura del sistema di monitoraggio adottata dal sistema di monitoraggio centrale.

Gli oggetti descritti nel capitolo 2.2 possono essere ricevuti con differenti tempi e modalità:

- in modo non sollecitato, mediante invio spontaneo da parte dell’oggetto dei dati verso il sistema centrale di monitoraggio, al superamento di soglie prestabilite di specifiche variabili;
- mediante interrogazione da parte del sistema centrale, con periodicità lunga (giornaliera). Per molti oggetti non è necessaria una raccolta costante di valori, soprattutto se si è adottata una soluzione complementare di invio non sollecitato in caso di allarme;
- mediante interrogazione frequente da parte del sistema centrale, per ottenere un trend dettagliato nel tempo di alcuni valori associati a specifici oggetti. Questa modalità presuppone un traffico di rete più intenso (e un maggior impegno di risorse sull’endpoint) e perciò si deve intendere come una tecnica di approfondimento di informazioni raccolte con gli altri metodi.

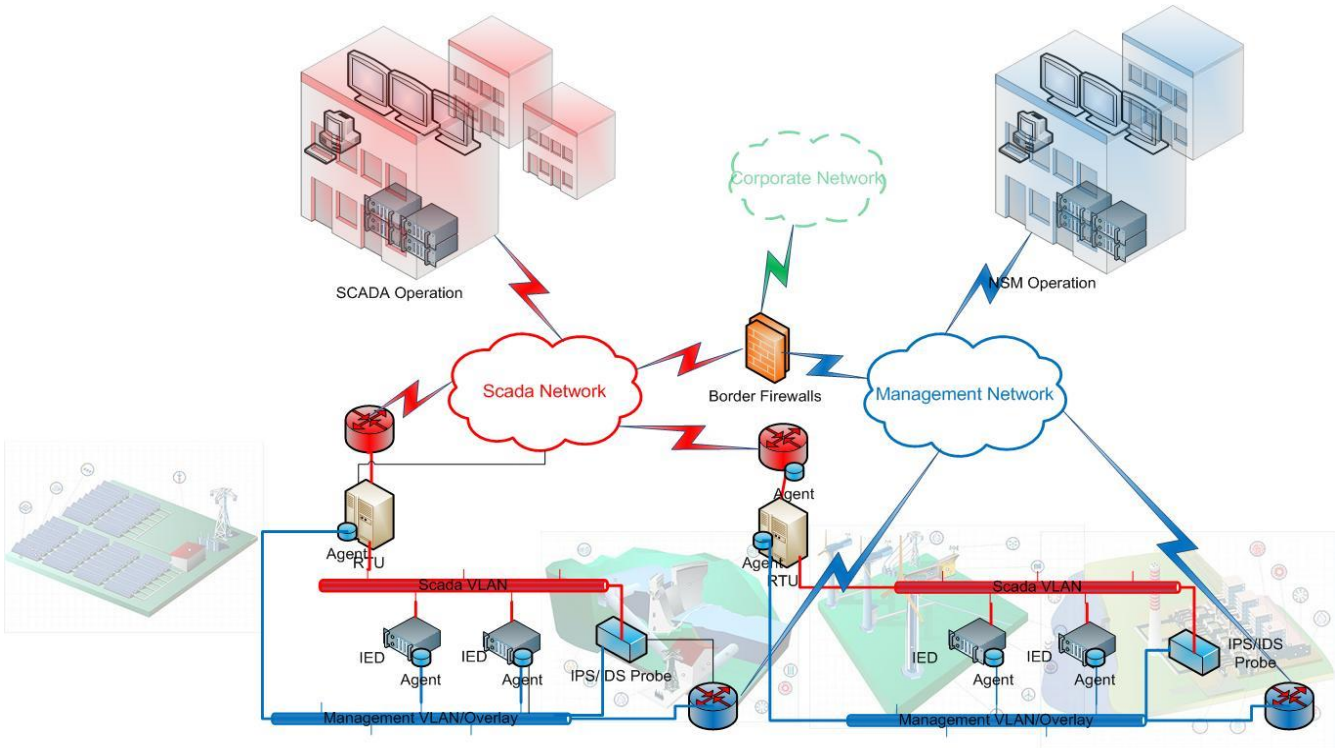


Figura 1 - Architettura del sistema di monitoraggio

In Figura 1 è rappresentata la gerarchia di raccolta degli eventi e delle variabili provenienti dai diversi elementi del sistema di Telecontrollo.

Il livello gerarchico superiore è rappresentato dal sistema centrale NSM che ha il compito di raccogliere le informazioni provenienti dai differenti componenti della rete di Telecomunicazioni e dai dispositivi afferenti al sistema di telecontrollo.
Come detto in precedenza la scelta dei protocolli utilizzati per la comunicazione è, secondo la norma 62351-7, aperta con l'intenzione di effettuare la mappatura degli oggetti utilizzando differenti protocolli. Per questo motivo il sistema centrale NSM può assumere la fisionomia di oggetti tecnologicamente provenienti sia dal mondo delle telecomunicazioni e dei sistemi ICT che dal mondo dello SCADA.
L'infrastruttura di telecomunicazioni deputata al NSM è rappresentata in modo logicamente separato dalla rete di supporto al Telecontrollo per sottolineare la differente vocazione dei due servizi. In effetti, anche per motivazioni relative alla *Separation of Duties* e per aumentare la resilienza, il monitoraggio e controllo dello stato di salute dell'infrastruttura dovrebbe essere delegato a responsabili (e potenzialmente a centri di controllo) diversi da quelli che sono responsabili dell'esercizio del Telecontrollo (anche questo aspetto è evidenziato nello schema).
All'interno della rete di Telecomunicazioni sono rappresentati, oltre agli oggetti di telecontrollo, anche numerosi elementi appartenenti alla rete stessa (router, switch) oltre ad dispositivi cui è demandata la gestione della sicurezza (firewall, IDS/IPS).

2.4 Protocolli per il monitoraggio

La corrente edizione della norma 62351-7 consente di introdurre a questo punto il concetto generico (seppure derivato dal gergo SNMP) di "agente".
L'"agente" è quell'entità software/hardware a cui è delegata la gestione, a livello di singolo endpoint, di oggetti di monitoraggio tra loro affini (per esempio perché appartenenti tutti alla classe delle interfacce di rete). Ogni endpoint (o altro elemento di rete) può ospitare diversi tipi di agente deputati alla gestione di classi di oggetti afferenti ai diversi livelli logici (dal livello di comunicazione di rete al livello applicativo). L'agente costituisce il punto di traduzione tra gli oggetti logici (NSM data objects) descritti nella norma negli elementi specifici previsti dal protocollo di management. L'attuale edizione della norma non include ancora le appendici di mapping verso gli specifici protocolli ma menziona in particolare SNMP e IEC 61850.

I protocolli SNMP e IEC 61850 sono strutturati secondo un paradigma ad oggetti che si sposa in modo naturale con la logica della norma IEC 62351-7 e rappresentano una altrettanto naturale esposizione della funzionalità di monitoraggio centrale verso due i due mondi NSM: quello classico Telco/ICT e quello SCADA. Entrambi i protocolli offrono vantaggi e punti di attenzione.

Il protocollo IEC 61850 è concepito per monitorare oggetti delle infrastrutture elettriche raccogliendo in modo rapido ed efficiente le informazioni da un numero anche elevato di dispositivi distribuiti e permette

l'esecuzione tempestiva di comandi. La sua adozione come protocollo di monitoraggio diventerà abbastanza naturale quando la sua diffusione sarà adeguata a livello di sistemi SCADA centrali, mantenendo però separato il ruolo di sistema centrale NSM.

SNMP[5] è adottato universalmente in ambito Telco/ICT e normalmente le Utility utilizzano una infrastruttura NSM per il monitoraggio ed il controllo attraverso questo protocollo. La mappatura degli NSM data objects della norma 62351-7 può essere effettuata pertanto su SNMP MIBs in modo relativamente agevole. Peraltro, oltre alla possibilità di ereditare il monitoraggio degli apparati di rete e sicurezza esistenti, SNMP permette di ereditare anche gli oggetti logici relativi alle componenti di rete che sono già ben descritte nei relativi MIB, permettendo di focalizzare l'attenzione sulla definizione dei MIB necessari a definire gli oggetti specifici della IEC 62351-7.

In termini molto pragmatici l'approccio che si è deciso di sviluppare prevede l'impiego in prima battuta del protocollo SNMP.
Abbiamo tuttavia considerato anche alcuni limiti e potenziali criticità che l'impiego di SMNP in ambiente di telecontrollo può comportare:

- Sicurezza del protocollo: solo l'ultima versione (SNMPv3[6]) del protocollo prevede un meccanismo di cifratura e autenticazione e pertanto l'adozione di questa versione è obbligatoria.
- Impegno di risorse e scalabilità. Sia per le risorse impiegate a livello di endpoint che per il potenziale traffico di rete generato occorre effettuare un corretto dimensionamento dell'architettura e dei processi di monitoraggio.

Sulla base delle esigenze espresse, la norma IEC 62351-7 dovrà essere oggetto di revisione per includere la mappatura verso i protocolli di monitoraggio citati e con l'occasione verranno raffinati anche l'insieme degli oggetti di monitoraggio.

2.5 Coesistenza tra monitoraggio e controllo

Sulla base delle considerazioni espresse nel capitolo precedente, in merito alla possibile invasività del monitoraggio, è opportuno prevedere alcune precauzioni, per evitare che il traffico di telecontrollo possa essere penalizzato da quello del monitoraggio dei sistemi.
Il problema della segregazione dei protocolli NSM rispetto ai protocolli applicativi (che nel nostro caso sono quelli specifici di Telecontrollo) non è tuttavia una novità.
Nell'ambito delle reti di telecomunicazioni è infatti spesso adottata una tecnica di trasporto di più reti logiche all'interno della stessa infrastruttura fisica di telecomunicazioni. A livello di rete locale ciò può essere realizzato mediante la segregazione in differenti VLAN, mentre a livello geografico è possibile adottare una analoga segregazione mediante l'impiego di reti MPLS. In alternativa è possibile adottare soluzioni di connessioni di rete cifrate in overlay rispetto alla rete fisica.

Oltre alla segregazione è inoltre necessario considerare in modo completo gli aspetti di priorità del traffico che devono essere impostati per evitare che il traffico di monitoraggio, che può generare anche volumi significativi, possa penalizzare il traffico di telecontrollo. Anche in questo caso esistono adeguati strumenti di rete che si possono adottare per garantire un corretto equilibrio delle prestazioni.

2.6 Integrazione del monitoraggio dei sistemi di telecontrollo e monitoraggio della rete

L'attivazione del monitoraggio mediante SNMP permette di effettuare una integrazione abbastanza diretta dei componenti delle infrastrutture di telecontrollo all'interno del sistema di monitoraggio già utilizzato per le infrastrutture di rete e ICT.

Di fatto è possibile ottenere una quasi automatica integrazione dei nuovi oggetti all'interno dei sinottici di gestione della rete e la raccolta degli eventi di sicurezza e degli allarmi nei sistemi di correlazione esistenti.

Si tratta di una forma di integrazione che non riguarda solamente gli aspetti di natura tecnologica, anche se certamente significativi, ma che permette anche di impiegare in modo proficuo e valorizzare i processi organizzativi che sono già ben rodati per la gestione dell'NSM centrale. L'adozione e l'avvio di una l'infrastruttura NSM comporta infatti, oltre agli aspetti tecnici, la predisposizione di una struttura organizzativa e dei relativi processi (includendo i processi di risk e crisis management).

Poiché questa organizzazione e questi processi sono già in essere a livello degli esistenti sistemi NSM di rete e ICT, la convergenza verso questo contesto può rappresentare da un lato un modo per accelerare l'avvio del monitoraggio dei sistemi di telecontrollo, dall'altro lato l'opportunità di offrire una visione integrata dei rischi a livello aziendale. Per esempio si può pensare di realizzare cruscotti integrati destinati ai diversi livelli aziendali, da quello tecnico a quello manageriale, offrendo una visione integrata e omogenea del rischio per tutti quei sistemi che in ultima analisi sono di fatto sistemi di rete e ICT.

Ciò non è in contrasto anzi rappresenta il duale della possibilità di utilizzare per le funzioni di monitoraggio, con una prospettiva di più lungo periodo, anche i protocolli SCADA (ad esempio IEC 61850), che in questo caso possono permettere di aggiungere alla visione "di impianto", una più dettagliata serie di informazioni riguardanti i sistemi di telecontrollo.

3 Role-Based Access Control (IEC 62351-8)

3.1 La norma 62351-8

La parte 8 della norma IEC 62351 nasce per definire formalmente come regolamentare l'accesso alle risorse di un sistema di automazione e telecontrollo.

Viene affrontato e risolto in modo efficace quello che è, prima di tutto, un problema organizzativo. In ogni azienda ci sono strutture organizzative a cui sono demandati compiti e delegati *diritti aziendali* che, quella specifica struttura organizzativa, esercita nell'interesse dell'Azienda.

In 62351-8 viene formalizzato un principio ampiamente riconosciuto in ogni organizzazione umana: la separazione delle competenze (*Separation of Duties*, SoD). In ogni azienda, solo per fare alcuni esempi, la funzione Amministrazione è separata dalla funzione Acquisti, come la funzione Audit, o controllo interno, è separata da quella di Security, o sicurezza interna.

Il motivo di questa separazione funzionale è semplice: si vuole evitare il conflitto di interessi di per se contrapposti, nell'esercitare i *diritti* conferiti dall'Azienda ai vari gruppi in cui è suddivisa (*unità organizzative*). Le funzioni aziendali, come in una moderna democrazia, agiscono le une nei confronti delle altre con un sistema di pesi e contrappesi che consentono l'equilibrio dei vari poteri o, per dirla con il linguaggio di prima, dei vari *diritti aziendali*.

3.2 Controllo d'accesso alle risorse basato sul ruolo

Questo concetto SoD si traduce nel nostro specifico contesto, sistemi di automazione e telecontrollo per il mondo elettrico, nel regolamentare l'accesso alle varie risorse (dai dispositivi di campo ai DB di configurazione di SCADA).

Consideriamo, per esempio, i dati in un archivio, per esso occorre definire: chi può solo consultarli, chi può modificarli, chi può crearne di nuovi o rimuovere quelli esistenti; oppure, per fare un altro esempio, occorre definire il *perimetro di visibilità* sui dati dell'archivio, cioè, chi può accedere a tutti i dati e chi solo ad una certa parte all'interno di un perimetro prestabilito. Altri esempi di risorsa di cui regolamentare il diritto d'accesso sono: spazio disco, spazio RAM, tempo di CPU, file systems, categorie di comandi, ecc..

La tecnica d'implementazione della SoD nella norma IEC 62351-8 prende il nome di *Role-Based Access Control (RBAC)*, che potremmo tradurre come: *controllo d'accesso alle risorse basato sul ruolo*.

I soggetti (*subjects* del RBAC) a cui si applicano i diritti di accesso non sono solamente persone fisiche, raggruppate in strutture organizzative, ma possono essere anche *agenti d'automazione (automated agents)*, cioè programmi o applicazioni a cui vengono assegnati dei diritti d'accesso in maniera analoga a quanto avviene per degli utenti. Un soggetto è, ad esempio, un modulo d'automazione pensato come un qualcosa che deve accedere a dati di processo per poi agire su attuatori al fine di modificare (automatizzare) il processo stesso.

Le risorse sono l'oggetto della tecnica RBAC (o oggetti appunto, *objects* del RBAC) e sono costituiti da qualsiasi risorsa di sistema (un file, un dispositivo, un database, un record, ecc.) di cui i soggetti hanno necessità guadagnare l'accesso o, detto in altre parole, ottenere un diritto di una qualche forma d'accesso.
I ruoli (*roles* del RBAC) sono un insieme di diritti elementari sulle risorse (elencare, creare o eliminare un oggetto, leggere o modificare lo stato di un oggetto, ecc.; ad esempio al ruolo supervisore può corrispondere l'insieme di diritti di elencare e leggere lo stato di elementi di uno SCADA).

In una sola frase diremo che RBAC è una tecnologia per regolamentare l'accesso dei soggetti alle risorse del sistema mediante la definizione di *ruoli*, dove un ruolo è il permesso di esercitare un insieme di diritti di accesso ad alcune risorse, ed un *diritto* è la facoltà di esercitare una certa operazione (elementare) su un oggetto.

La tecnica RBAC[7] consente di semplificare la complessità che deriva dal *mappare* direttamente i soggetti sui possibili diritti dei singoli oggetti, definendo il ruolo come entità intermedia di svincolo.

Mentre da un lato posso arrangiare i soggetti in gruppi, spesso in stretta relazione con le strutture organizzative a cui appartengono, dall'altro lato posso arrangiare i vari diritti d'accesso alle risorse in ruoli. I ruoli non coprono tutte le possibili combinazioni dell'insieme di diritti contenuti nel ruolo, ma solo giusto quelle necessarie a realizzare una corretta separazione di competenze (SoD).

RBAC mette in pratica il principio normalmente accettato secondo il quale un individuo in una organizzazione aziendale cambia ruolo e responsabilità più spesso di quanto cambino i diritti contenuti nel ruolo stesso (esempio: è più facile che il ruolo di DB Administrator passi da Tizio a Caio piuttosto che cambino i diritti (le operazioni consentite sul DB) all'interno del ruolo di DB Administrator).

3.3 RBAC il modello generale (Process model)

Il modello classico RBAC è riportato in figura 2. Esistono due modi di accesso alle risorse da parte dei soggetti che danno luogo ad una separazione delle competenze statica o dinamica.

Nel primo modo d'accesso (SoD statica) il soggetto appartiene staticamente ad un ruolo e guadagna l'accesso alle risorse definite dal quel specifico ruolo.
Esempio di SoD statica è l'accesso al nostro computer con un utente appartenete ad un OU di dominio a cui i diritti d'accesso alle risorse del PC è stata stabilita dall'amministratore del dominio a cui siamo stati assegnati; i diritti assegnati al ruolo sono fissi, statici, sempre gli stessi fintantoché apparteniamo alla OU citata.

Nel secondo modo d'accesso (SoD dinamica) il soggetto può aprire più sessioni, anche contemporaneamente, ad ogni sessione corrisponde un diverso ruolo.
Un esempio di SoD dinamica, proseguendo l'esempio di prima dell'accesso al PC, l'abbiamo quando, inseriti in un OU d'amministrazione, possiamo accedere in certi momenti alle risorse del PC "come amministratori", il ruolo di amministratore del nostro PC ci viene assegnato temporaneamente, per una singola operazione.

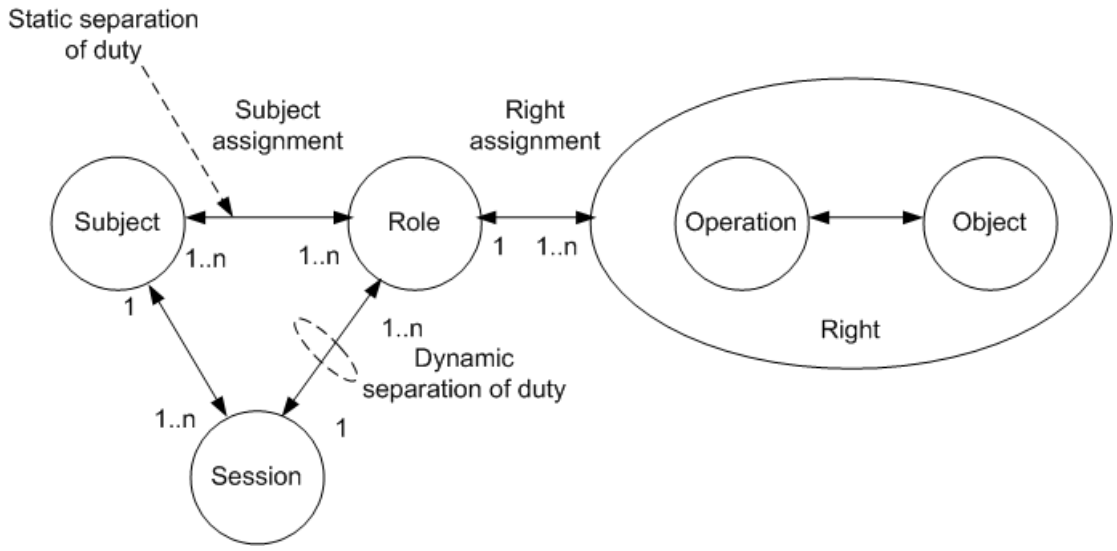


Figura 2 – RBAC: Diagramma con separazione di competenze statica e dinamica

Nella SoD statica: ad un soggetto (*Subject*) posso associare più ruoli (*Role*), un ruolo si può assegnare a più soggetti, ad ogni ruolo sono assegnati più diritti (*Right*), cioè la facoltà di esercitare un operazione (*Operation*) su un oggetto (*Object*).

Nella SoD dinamica: ad un soggetto (*Subject*) posso associare più sessioni (*Session*), ad ogni sessione posso associare più ruoli (*Role*), ad ogni ruolo sono assegnati più diritti (*Right*).

3.4 Assegnazione dei Diritti nei Ruoli predefiniti in IEC 62351-8

La norma prevede un set minimo di ruoli che deve essere garantito per l'interoperabilità fra sistemi standard; sono comunque previsti dei ruoli *Private* che avranno validità solo locale sul singolo sistema (azienda) per il quale vengono definiti.
Nei set di ruoli minimi possiamo riconoscere quelli classici di un sistema di automazione e telecontrollo (vedi figura 3): solo lettura (*VIEWER*), operatore (*OPERATOR*), addetto alla configurazione o operatore della stazione di ingegneria (*ENGINEER*) e installatore (*INSTALLER*); accanto a quelli specifici per la gestione degli accessi e della sicurezza dei sistemi: amministratore della sicurezza (*SECADM*), addetto al controllo - audit della sicurezza (*SECAUD*) e addetto alla gestione RBAC (*RBACMNT*). Come si vede in tabella ciascun ruolo standard ha un identificatore numerico.
IEC si riserva un gamma di identificatori di ruolo (da 7 a 32767) per usi futuri.

Mentre possono essere definiti degli identificatori, e quindi dei ruoli, di validità locale (*Private*) da attribuire in uno specifico contesto. Potrebbero essere definiti ruoli propri di un'azienda, al di fuori di quelli standard, tanto quanto ruoli definiti all'interno di un specifico ambiente applicativo.

Value	Right / Role	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7...32767>	Reserved	For future use of IEC defined roles.										
<-32768 .. -1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

Figura 3 – RBAC: ruoli predefiniti standard e ruoli privati

La tabella stabilisce l'associazione tra ruolo e diritti specifici per l'ambiente del controllo di processo e specificatamente alla modellazione degli IED (Intelligent Electronic Device) come prevista dalla norma IEC 61850[8].

Non è nell'intenzione di questa memoria entrare nei dettagli dei compiti di ciascun ruolo, ci basti elencare, come già fatto per i ruoli, i diritti legati alla gestione degli IED, che altro non sono quelli classici degli ambienti di telecontrollo e automazione.

Importante dire che i diritti elencati sono obbligatori, cioè devono trovare applicazione negli specifici IED delle nostre realizzazioni standard IEC 62351.

- VIEW: è il diritto di elencare, scoprirne l'esistenza (discovery), di un oggetto;
- READ: è il diritto di leggere tutte o in parte le caratteristiche/proprietà di un oggetto;
- DATASET: è il diritto che consente la gestione completa dei data-set permanenti e non permanenti come definiti in IEC 61850;
- REPORTING: è il diritto di accedere a report/log degli IED, istantanei o memorizzati (buffered);
- FILEREAD: è il diritto a leggere oggetti di tipo file;

- FILEWRITE: è il diritto di scrivere/leggere gli oggetti di tipo file, questo diritto contiene il precedente;
- FILEMNGT è il diritto che consente di trasferire e cancellare file verso i dispositivi logici (Logical-Device);
- CONTROL: è il diritto che consente di operare azioni di controllo, cioè operare comandi verso il campo;
- CONFIG: è il diritto che consente, localmente o remotamente, di configurare le caratteristiche di un servizio o dispositivo;
- SETTINGGROUP: è il diritto che consente le operazioni da remoto di "Settings Groups";
- SECURITY: è il diritto che consente operazioni legate alla sicurezza su servizi o dispositivi.

In modo analogo la norma definisce alcune assegnazioni di diritti (permessi) su operazioni predefinite in ambito della modellistica IEC 61850 (es.: diritto ALLOW e DENY sulle operazioni d'accesso Associate, Release e Abort).

3.5 I modelli d'accesso alle risorse RBAC: PUSH e PULL

L'accesso sicuro alle risorse si ottiene mediante l'autenticazione del soggetto seguita dalla verifica del livello d'accesso alla risorsa consentita dal ruolo assegnato al soggetto.

Per ottenere queste funzionalità è necessario avere a disposizione un DB centralizzato (centralized repository) dove sono memorizzati gli utenti con diritto d'accesso e il loro ruolo. Ogni applicazione interroga questo DB per ottenere quale diritto d'accesso ha un soggetto alle risorse manipolate dall'applicazione stessa.

Il ruolo di un soggetto è trasportato in un contenitore denominato "*access token*" (gettone d'accesso).

Nell'implementare le tecniche RBAC possiamo avere due approcci detti PUSH e PULL.

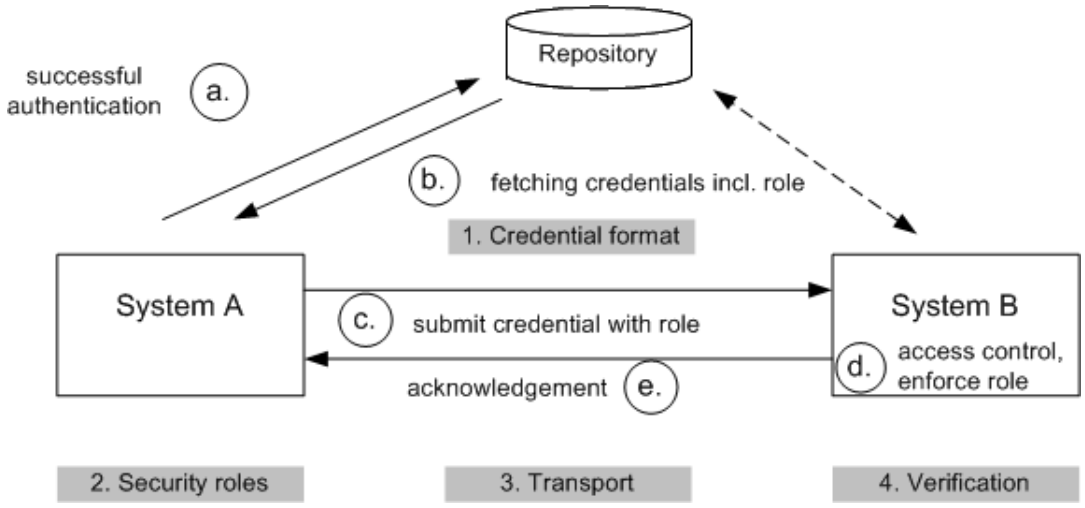


Figura 4 – RBAC: modello d'accesso PUSH

In figura 4 è riportato il modello PUSH: la richiesta d'accesso ad un oggetto viene spinta (*push*) da A (richiedente) a B (concedente); la richiesta d'accesso di A all'oggetto (*access token* contenente l'identità dell'utente e il suo ruolo) viene inviata a B, nella risposta B accorda o nega l'accesso in base alle operazioni consentite sull'oggetto al ruolo contenuto nel *access token* di A.

I passi che portano un soggetto ad ottenere i diritti sulle risorse dovuti al suo ruolo sono:

a) il soggetto A si autentica e richiede il suo *access token*;
b) A ottiene il suo *access token*;
c) A *push* (manda verso) il suo *access token* verso l'applicazione B;
d) B verifica il *access token* del soggetto A e concede l'accesso richiesto in base al ruolo inserito nel *access token*
e) B invia la sua risposta ad A.

Un esempio di questa modalità d'accesso è quello di client attivato in una sessione utente verso un server in ambiente con dominio d'accesso. Il server concede all'utente i diritti consentiti dal suo ruolo, ruolo corrispondente alla OU del dominio.

Il secondo modello è detto PULL (figura 5): la richiesta d'accesso ad un oggetto viene prelevata (*pull*) da B (concedente) sulla base dell'identità di A (richiedente); il soggetto A richiede l'accesso all'oggetto di B fornendogli le sue credenziali di autenticazione, B preleva lo *access token* di A ottenendo il suo ruolo, B accorda o nega l'accesso in base alle operazioni consentite sull'oggetto al ruolo di A.

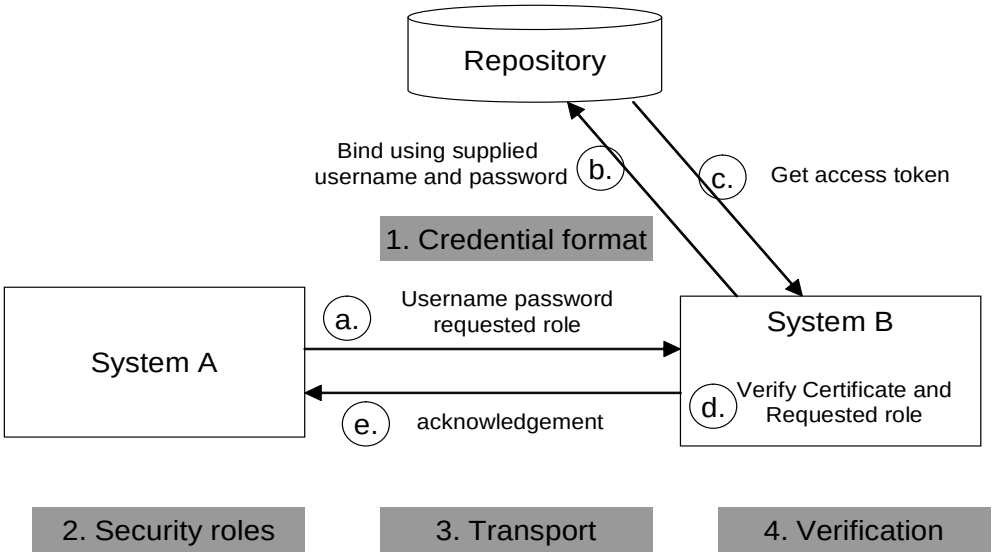


Figura 5 – RBAC: modello d'accesso PULL

I passi che portano un soggetto ad ottenere i diritti sulle risorse dovuti al suo ruolo sono:

a) il soggetto A fornisce le sue credenziali di autenticazione a B*;*
b) B richiede lo *access token* di A sulla base delle credenziali inviate*;*
c) B preleva (*pull*) lo *access token* di A*;*

d) B verifica lo *access token* del soggetto A e concede l'accesso richiesto in base al ruolo inserito nello *access token*
e) B invia la sua risposta ad A.

Un esempio di questa modalità d'accesso : A è un utente di dominio AD che chiede accesso al Terminal Server di B, B verifica le credenziali di dominio di A ottenendo la OU (ruolo) di appartenenza, B apre la sessione TS se la OU a cui appartiene A ha diritto d'accesso al server B.

In entrambe le figure le caselle ombreggiate rappresentano gli aspetti normati in IEC 62351-8.

3.6 I profili degli *access token* RBAC

Lo *access token* è un contenitore con tempo di vita finito, cioè ha validità in un intervallo temporale definito, rilasciato e amministrato da un'entità di gestione dell'identità dei soggetti (il *Repository* delle figure 4 e 5).

L'accesso a questa entità avviene attraverso un servizio LDAP sicuro (v3 su SSL/TLS)[9].

Lo *access token* può essere impiegato:

- all'interno di una sessione, è il caso di quando esiste un dialogo racchiuso in un canale di comunicazione *end-to-end* fra due entità,
- oppure la validità dello *access token* può essere limitata ad un singolo messaggio.

La norma IEC 62351-8 prevede tre profili che impiegano oggetti standard quali *ID certificates*, *attribute certificates* e *software tokens* definiti nello standard X.509v3[10]:

- Profilo A – *X.509 ID certificate con estensione*
- Profilo B – *X.509 Attribute certificate*
- Profilo C – *Software token*

Per tutti i profili ci sono dei campi obbligatori, tra i quali: OID che identifica lo *access token* con codifica specifica che indica l'impiego per IEC 62351-8, nome e ruolo del soggetto, entità emittente, istante di emissione e Area of Responsibility (AoR) che consente di restringere la validità di un ruolo di un soggetto ad un insieme di oggetti.

AoR risponde alla tipica necessità nel campo del telecontrollo di restringere un ruolo a oggetti di un area geografica o funzionale. Si evita così di creare ruoli analoghi per aree geografiche o funzionali differenti, cioè ruoli funzionalmente identici ma da applicare a insiemi d'oggetti differenti. Impiegando AoR nel ruolo si crea un ruolo da applicare ad una specifica area (geografica o funzionale) di competenza di una specifica classe di soggetti.

3.7 Applicazione RBAC nei sistemi per la Generazione in ENEL

In Enel è stato progettato e attivato, a partire dal 2010, un dominio Active Directory per realizzare un sistema di autenticazione dedicato ai sistemi telecontrollo (Sistemi Centrali per la Teleconduzione, SCT) e i sistemi di automazione degli impianti di generazione da fonti rinnovabili più evoluti.

Il sistema consente di autenticare qualche centinaio di *users* (utenti, dipendenti Enel e dipendenti di alcune ditte fornitrici con ruolo di manutentori), oltre a un centinaio di *computers*, inseriti nel dominio specifico di telecontrollo. I ruoli sono attribuiti alle *Organization Unit* (OU) di dominio, che raggruppano *users* e *computers*.

I concetti RBAC sono sufficientemente e fedelmente implementati per i servizi del Sistema Operativo impiegato, anche i servizi SCADA accettano connessione utente a cui vengono concessi i diritti sulla base della loro appartenenza alle varie OU.

Nei prossimi tre anni prevediamo una prima implementazione rigorosa della norma IEC 62351 applicata agli SCT e alla sua rete di RTU connesse su intranet dedicata via protocollo IEC 60870-5-104.

Dovranno essere implementate varie parti della norma IEC 62351: le parti 3 e 5 per la messa in sicurezza *end-to-end* delle connessioni 60870-5-104 che di conseguenza richiederà creare l'infrastruttura di chiave pubblica (Public Key Infrastructure PKI) per il rilascio degli *access token* previsti dalla parte 8 secondo il key management della parte 9.

4 Conclusioni

In questa memoria abbiamo analizzato sinteticamente le parti 7 e 8 della norma IEC 62351 “data and communications security for power systems management and associated information Exchange”.

Le due parti riguardano il monitoraggio dell’infrastruttura di telecontrollo e automazione (NSM) del sistema elettrico e l’attribuzione dei ruoli (RBAC) ai soggetti che operano su questa infrastruttura.

NSM e RBAC sono due aspetti della sicurezza dei sistemi di automazione e telecontrollo che completano quelli più classici che riguardano la messa in sicurezza dei protocolli di comunicazione tipici (famiglie IEC 60870, 61850, 61968 e 61970) che non sempre vengono messi in evidenza.
In realtà questi due strumenti costituiscono un’eredità, ormai consolidata, proveniente dal mondo ICT che nel corso degli anni si è dovuto dotare di strumenti tecnici e organizzativi per far fronte alla complessità e alle minacce che l’impiego di protocolli e sistemi di pubblico dominio ha imposto.

E’ opportuno sottolineare l’aspetto di coordinamento indispensabile fra la parte tecnica e quella organizzativa delle misure di sicurezza che permette di attuare il ciclo virtuoso posto in premessa.
Il primo aspetto di coordinamento riguarda proprio la definizione e l’assegnazione dei ruoli (*policy*) che poi devono essere attuati con gli opportuni strumenti tecnologici (*deployment*) oggetto di questa memoria.
Non va trascurata, a questo punto, la formazione delle persone (*training*) che ha lo scopo di rendere tutti consapevoli dei rischi, delle contromisure e del ruolo di ciascuno.
Il ciclo si chiude attraverso l’attuazione del monitoraggio operativo (attraverso NSM), ma anche complessivo a chiusura del ciclo di sicurezza (*audit*).
I sistemi elettrici di potenza, oggetto primario di questa memoria, sono per natura interconnessi e interoperabili a livello continentale.
Questa caratteristica richiede sistemi di controllo e supervisione anch’essi interconnessi e interoperabili.
Le norme emesse dal TC57 IEC hanno lo specifico scopo di ottenere questa interoperabilità dei protocolli di telecontrollo e automazione per i sistemi elettrici di potenza. Norme raggruppate per famiglie, ciascuna per uno specifico ambito applicativo (60870 telecontrollo, 61850 automazione, 61968 DMS, 61970 EMS).
Un sistema elettrico di potenza risulterà gestito in sicurezza se si adotteranno le misure di messa in sicurezza descritte nella norma IEC 62351.
In particolare i singoli protocolli applicativi vengono messi in sicurezza secondo le tecniche descritte nelle parti 3, 4, 5 e 6.
Inoltre, come abbiamo voluto sottolineare in questa memoria, è necessario attuare un corretto ed efficace monitoraggio dell’infrastruttura ICT, in accordo con 62351-7, insieme alla regolamentazione dell’accesso all’infrastruttura ICT secondo quanto descritto in 62351-8.

Ringraziamenti

Ringraziamo tutti i colleghi che in Enel hanno consentito la stesura di questa memoria leggendo pazientemente queste pagine e dandoci consigli e ritorni utili ad una più esatta e completa descrizione dei temi trattati.

Bibliografia

[1] **IEC 62351-1 TS Ed.1**: Power systems management and associated information exchange – Data and communication security – Part 1: Communication network and system security – Introduction to security issues;

vedi anche **White Paper on Security Standards with Cybersecurity**

http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf

[2] **IEC 62351-7 TS Ed.1**: Power systems management and associated information exchange – Data and communication security – Part 7: Network and system management (NSM) data object models

[3] **IEC 62351-8 TS Ed.1**: Power systems management and associated information exchange – Data and communication security – Part 8: Role-Based Access Control

[4] **Network Security Management for Transmission Systems**, EPRI, 31-Dec-2012,

http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001024421

[5] **IETF SNMPv2**: RFC 1441, RFC 1452: Simple Network Management Protocol, version 2

[6] **IETF SNMPv3**: RFC 3411, RFC 3418: Simple Network Management Protocol, version 3

[7] **ANSI INCITS 359-2012**: Information Technology - Role Based Access Control

[8] **IEC 61850**: Power Utility Automation

[9] **IETF RFC 4511**: Lightweight Directory Access Protocol (LDAP)

[10] **IETF X.509v3**: standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI), vedi anche I documenti specifici RFC 5280 e RFC 4158.