FORUM TELECONTROLLO RETI DI PUBBLICA UTILITÀ 2013

ANIE AUTOMAZIONE

ANIE FEDERAZIONE

CONFINDUSTRIA

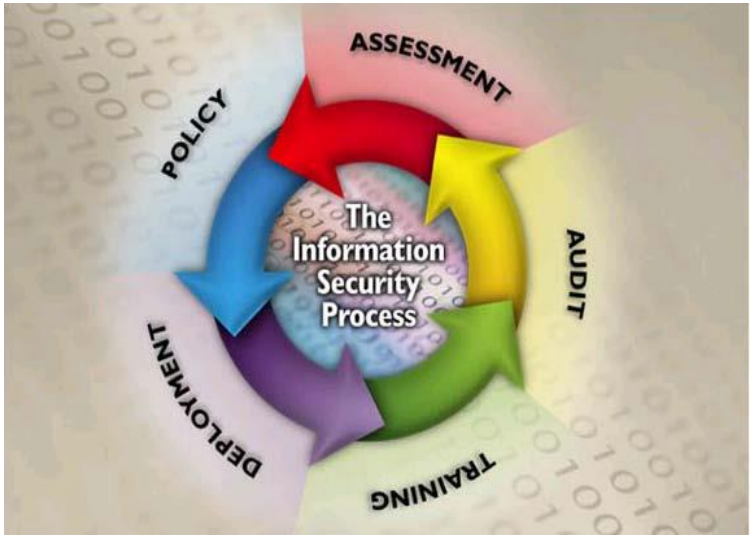
IEC 62351 nei sistemi di controllo per la Generazione del Gruppo Enel

Enel Produzione
Federico Bellio

Enel Servizi
Gian Luigi Pugni

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**)

Introduzione

I **protocolli di comunicazione** sono una delle parti più **critiche** per il funzionamento del Sistema Elettrico poiché sono responsabili per il recupero di informazioni da apparecchiature di campo e, viceversa, per l'invio di comandi di controllo.

I 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 **non è più un concetto accettabile** (se mai lo è stato), per l'adozione di protocolli aperti e standard (a partire dallo stack TCP/IP)

Le **reti di telecomunicazioni** e telecontrollo di ciascun operatore del mercato sono **fortemente interconnesse** con quelle degli altri operatori.

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**.

Introduzione

L'obiettivo della sicurezza logica dei protocolli nel contesto della gestione dei sistemi elettrici ha come fine primario la **disponibilità** del sistema di supervisione e telecontrollo rispetto a possibili minacce di natura sia dolosa che involontaria, garantendo perciò la **disponibilità** del sistema elettrico. Esiste cioè una correlazione diretta tra la disponibilità del sistema elettrico e quella del sistema ICT che consente di governarlo.

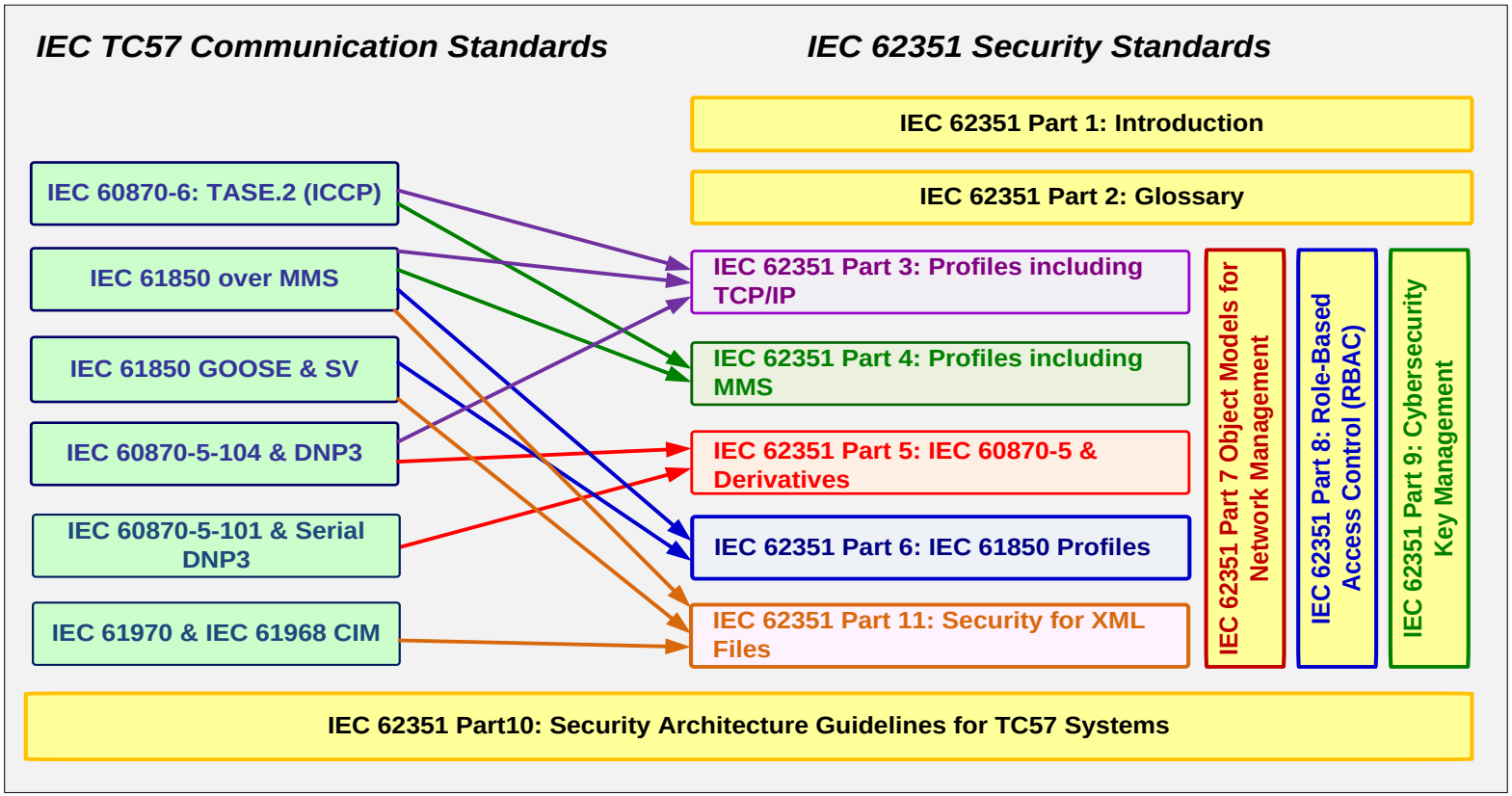
Per far ciò è necessario garantire anche l'**integrità**, la **riservatezza** delle informazioni insieme ad una ulteriore caratteristica di "**non ripudiabilità**" dell'informazione

La norma IEC 62351, curata dal IEC TC 57 WG15, definisce la "*data and communications security for power systems management and associated information Exchange*".

L'obiettivo è la realizzazione della **sicurezza end-to-end** tra tutti i sistemi che partecipano all'infrastruttura di telecontrollo mediante mutua autenticazione delle parti e cifratura e firma dei messaggi.

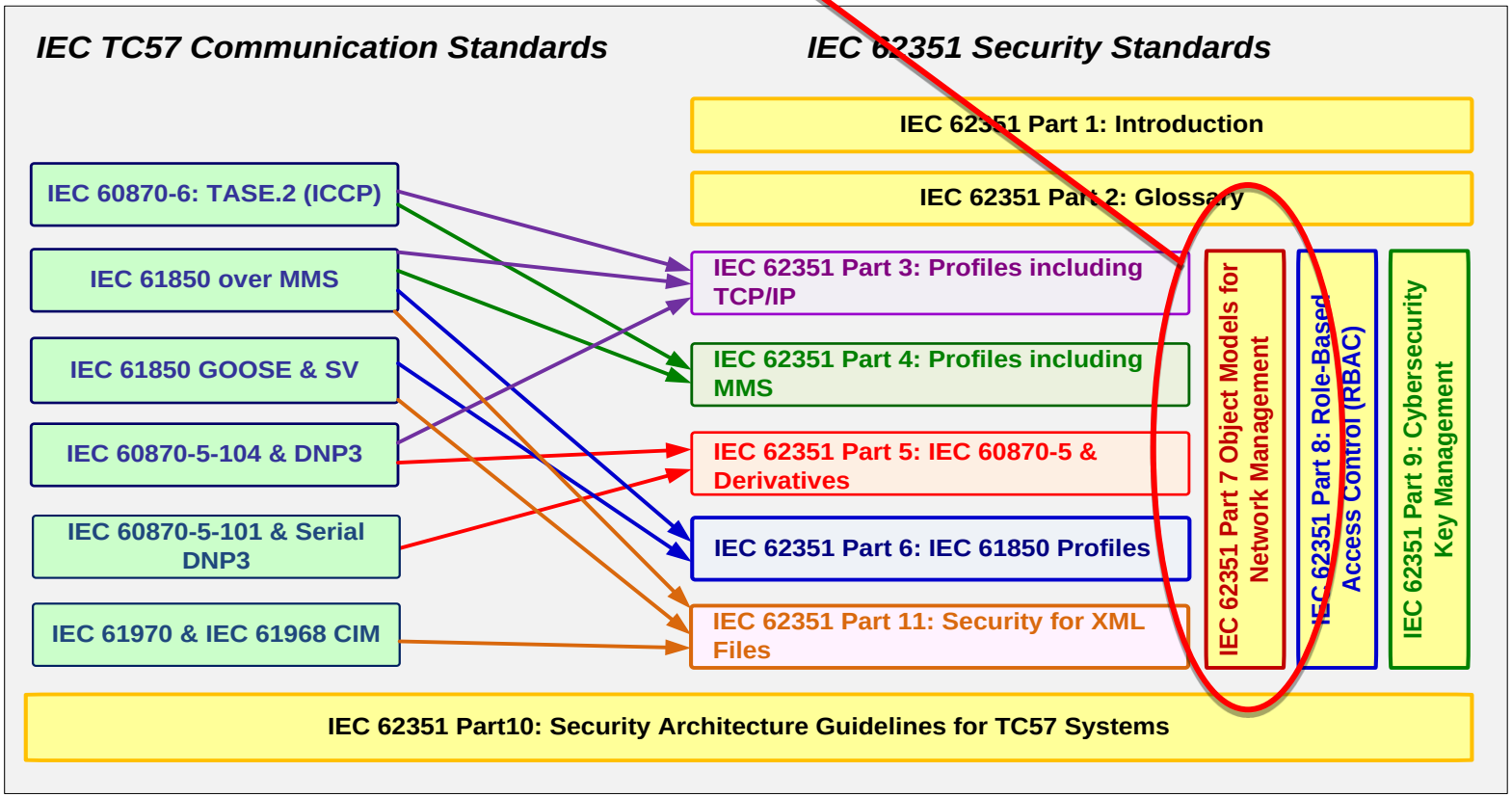
La Norma IEC 62351

Le parti dalla **3-6 e 11** si riferiscono alla messa in sicurezza dei protocolli **IEC 61850 e IEC 60870**.
Le parte **7 , 8 e 9** definiscono invece metodologie comuni di sicurezza (**Network and System Management, Role Based Access Control e Key Management**) , essenziali per abilitare l'infrastruttura di sicurezza.



La Norma IEC 62351 Part 7

Network and System Management



Part 7: Network and System Management

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

- Reti geografiche e locali di telecomunicazioni
- Remote Terminal Units (RTU) e Intelligent Electronic Devices (IED)
- Sistemi SCADA di impianto e SCADA Centrali

Ciascuno di questi oggetti contribuisce al telecontrollo delle infrastrutture vere e proprie del sistema elettrico. La crescente potenza e capacità di interazione dei sistemi di telecontrollo nuova generazione li espone ad una serie di rischi:

- Errori software
- Problemi nella comunicazione
- Anomalie hardware (ad esempio alimentatori, batterie)
- Malware

Spesso l'anomalia o l'evento è riconoscibile solo attraverso la correlazione di informazioni di monitoraggio provenienti da più di elementi ed è vitale per avviare il ciclo di prevenzione e reazione

E' essenziale monitorare lo stato di salute dei sistemi e essere informati tempestivamente di eventi anomali

Le premesse e le esperienze

Il monitoraggio integrato dei sistemi attraverso una infrastruttura di 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.

E' possibile ed opportuno valorizzare 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 inoltre 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.

Monitoraggio integrato dei sistemi attraverso una infrastruttura di Network and System Management (NSM)

Obiettivi dell'NSM

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

- **Deterrenza e il ritardo**: cercando di evitare gli attacchi, o almeno ritardarli
- **Rilevamento di attacchi**: la rilevazione è fondamentale per tutte le altre misure di sicurezza. Le funzionalità IDS possono svolgere un ruolo importante.
- **Valutazione di attacchi**: per determinare la natura e la gravità dell'attacco.
- **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**

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

- il **monitoraggio dello stato delle applicazioni software, dispositivi hardware, e comunicazioni**.
- il **monitoraggio delle prestazioni dei sistemi e delle comunicazioni**.
- il **rilevamento delle intrusioni.** Questo rilevamento intrusioni utilizza naturalmente le informazioni ottenute mediante il monitoraggio di stato ed il monitoraggio delle prestazioni
- **Gestione della configurazione,** 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.

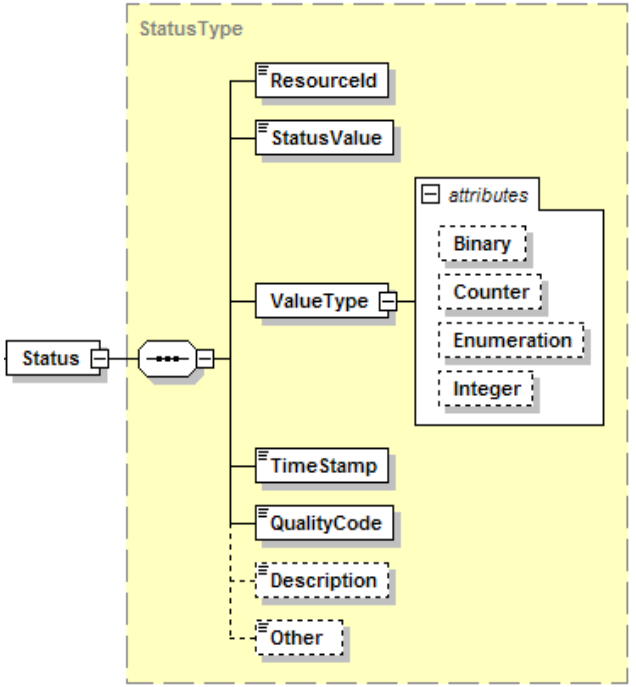
Data Object Model

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:

- L"ID" della risorsa da monitorare
- Il "nome dell'oggetto", che rappresenta l'identità del "data object"
- Indicatore di qualità del data value
- Il timestamp di cambiamento.

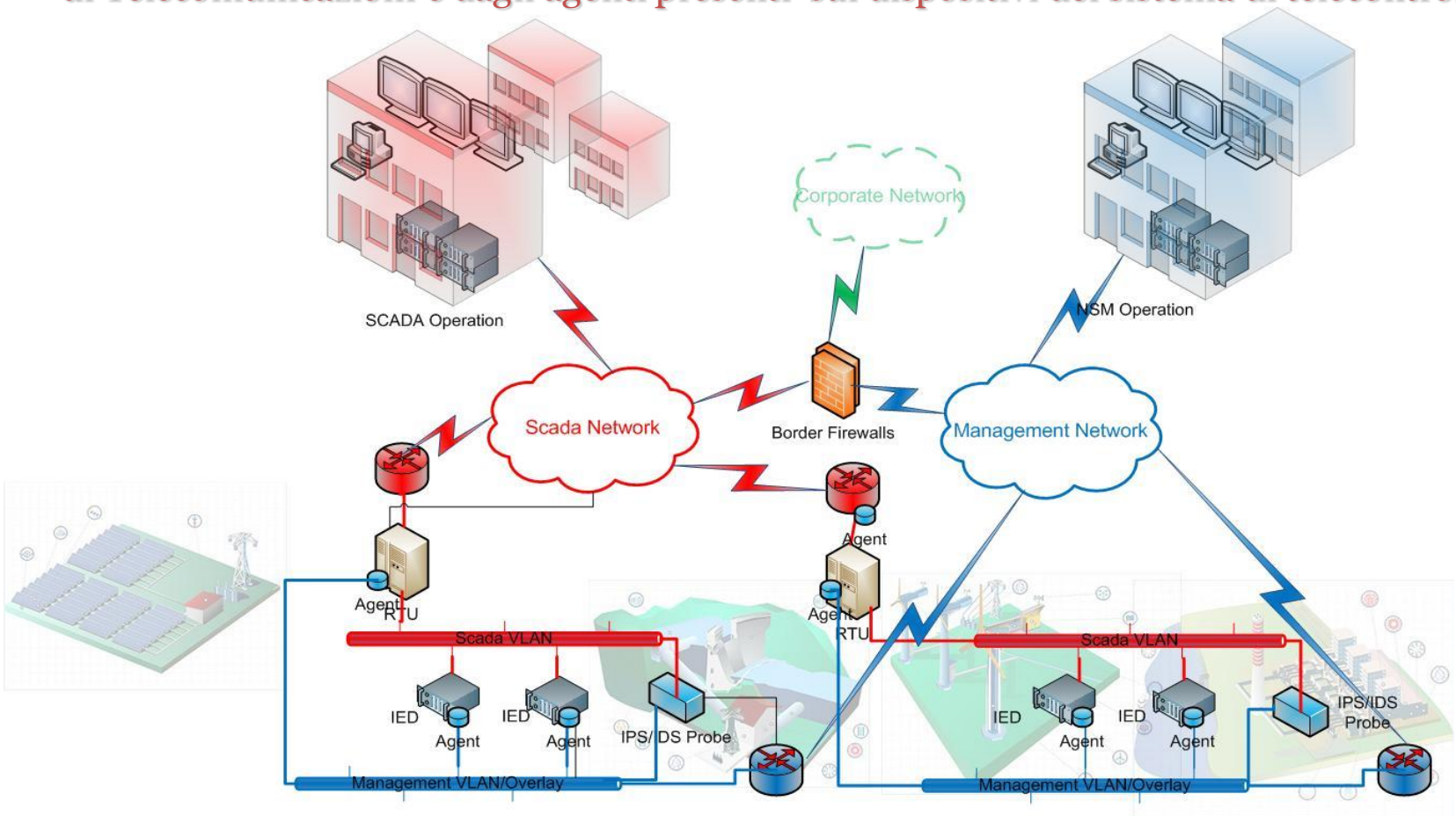
Gli oggetti possono essere in sola lettura o anche scrivibili.
La norma introduce alcune categorie di oggetti organizzati in tre livelli principali:

- "Networks and Protocols"
- "End Systems"
- "Intrusion Detection"



Architettura

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 dagli agenti presenti sui dispositivi del sistema di telecontrollo.



Protocolli per il monitoraggio

In 62351-7 è impiegato il concetto di "agente" (derivato dal gergo SNMP). 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 può ospitare più agenti

L'agente costituisce il punto di traduzione tra gli oggetti logici (NSM data objects) descritti nella norma negli elementi specifici previsti dai protocolli veri e propri tra cui:

•IEC 61850 è concepito per monitorare e controllare oggetti delle infrastrutture elettriche, diventerà abbastanza naturale quando la sua diffusione sarà adeguata, anche a livello di sistemi SCADA . Non include tuttavia il monitoraggio e la correlazione dell'ambiente di Telecomunicazioni.

•SNMP è adottato universalmente in ambito Telco/ICT e a livello di ogni Utility esiste una infrastruttura NSM per il monitoraggio ed il controllo della rete basata su questo protocollo. SNMP permette di ereditare anche gli oggetti di telecomunicazione

In termini molto pragmatici l'approccio che si è deciso di sviluppare per breve e medio termine si basa sull'impiego del protocollo SNMP, mentre l'adozione di IEC 61850 come protocollo NSM costituisce una prospettiva più largo respiro

Considerazioni sul protocollo SNMP

Occorre considerare anche alcuni limiti e potenziali criticità che l'impiego di SMNP in ambiente di Telecontrollo:

•Sicurezza del protocollo: solo l'ultima versione (SNMPv3) del protocollo prevede un meccanismo di cifratura e autenticazione e pertanto l'adozione di questa versione è obbligatoria. E' opportuno inoltre pertanto di prevedere ulteriori meccanismi di protezione a supporto.

•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.

Nell'ambito delle reti di telecomunicazioni è spesso adottata una tecnica di trasporto di più reti logiche all'interno della stessa infrastruttura fisica di telecomunicazioni mediante la segregazione in differenti VLAN e mediante l'impiego di reti geografiche 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 assegnazione priorità del traffico per evitare conflitti con il traffico di Telecontrollo.

Monitoraggio Integrato

Il 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.

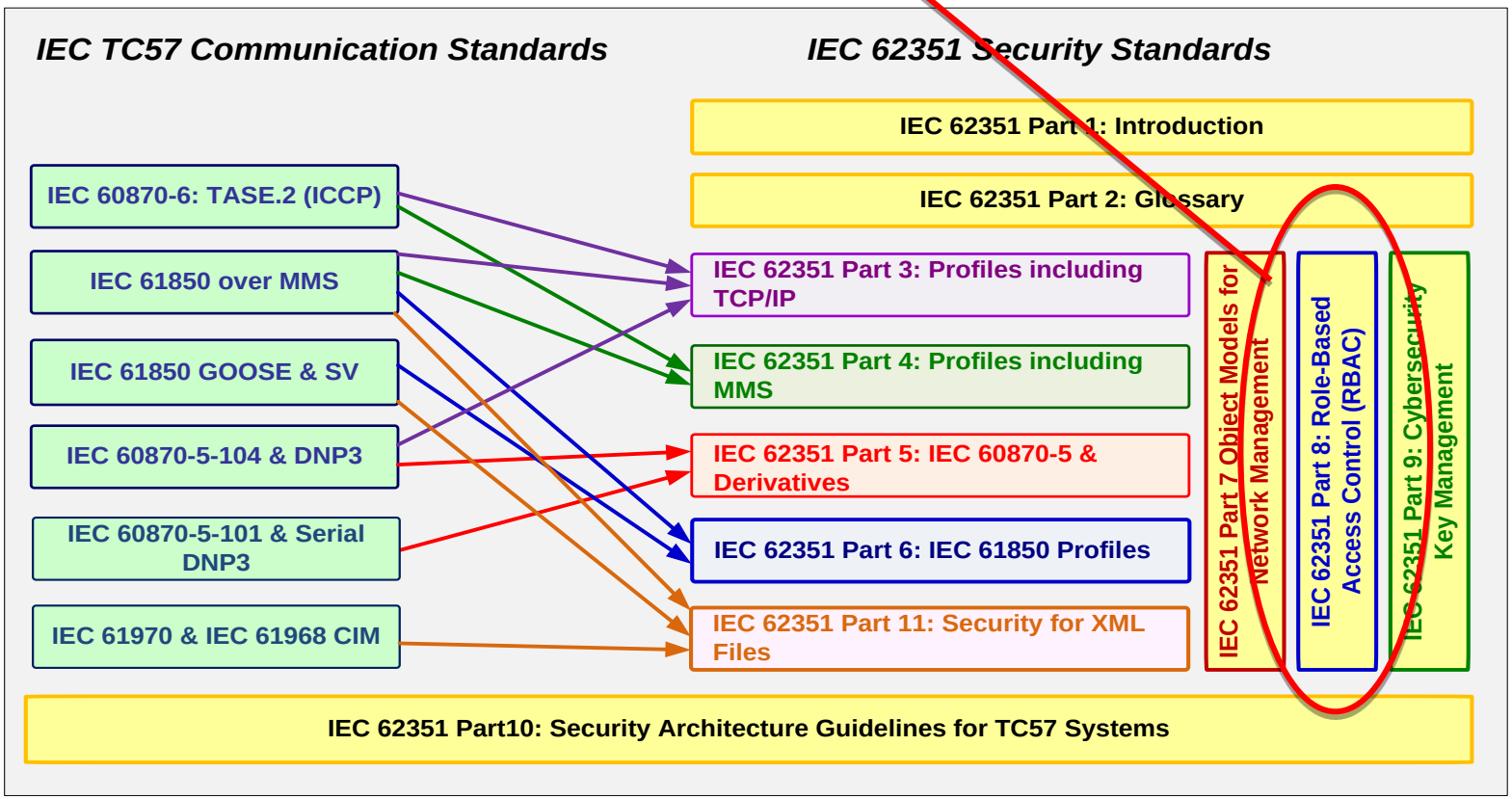
Di fatto è possibile ottenere una quasi automatica integrazione dei nuovi oggetti all'interno del sistema dei sinottici di gestione della rete e convogliare gli eventi di sicurezza e gli allarmi ai sistemi di correlazione esistenti.

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.

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 Enterprise. Adottando protocolli standard si garantisce inoltre la corretta interoperabilità e di condivisione degli eventi di sicurezza non solo a livello Enterprise ma anche a livello di unità di gestione del rischio federate.

La Norma IEC 62351 Part 8

Role Based Access Control



Role Based Access Control (RBAC)

Introduzione

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) al fine di 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).

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).

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.

RBAC Process Model

Separazione: Soggetti, Oggetti, Diritti e Ruoli

Role Based Access Control (RBAC): controllo d'accesso dei soggetti alle risorse basato sui ruoli.

Chi sono i **soggetti** (subjects del RBAC): persone fisiche e agenti d'automazione (automated agents: moduli software, programmi, servizi indipendenti che devono accedere alle risorse).

Quali sono le risorse (o **oggetti**, objects del RBAC): 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.

Quali sono i **ruoli** (roles del RBAC): sono un insieme di **diritti** elementari sulle risorse (ad esempio al ruolo *supervisore* può corrispondere l'insieme di diritti di elencare e leggere lo stato di elementi di uno SCADA);

Cos'è un **diritto**: è la facoltà di esercitare una certa operazione (elementare) su un oggetto (ad esempio elencare, creare o eliminare un oggetto, leggere o modificare lo stato di un oggetto, ecc.).

RBAC Process Model
Definizione dei Ruoli

La tecnica RBAC (rif. ANSI INCITS 359-2004) consente di semplificare la complessità che deriva nel mappare direttamente i soggetti sui possibili diritti dei singoli oggetti, definendo il ruolo come entità intermedia di svincolo.

Come posso arrangiare i **soggetti** in **gruppi**, spesso in stretta relazione con le strutture organizzative a cui appartengono, posso anche 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).

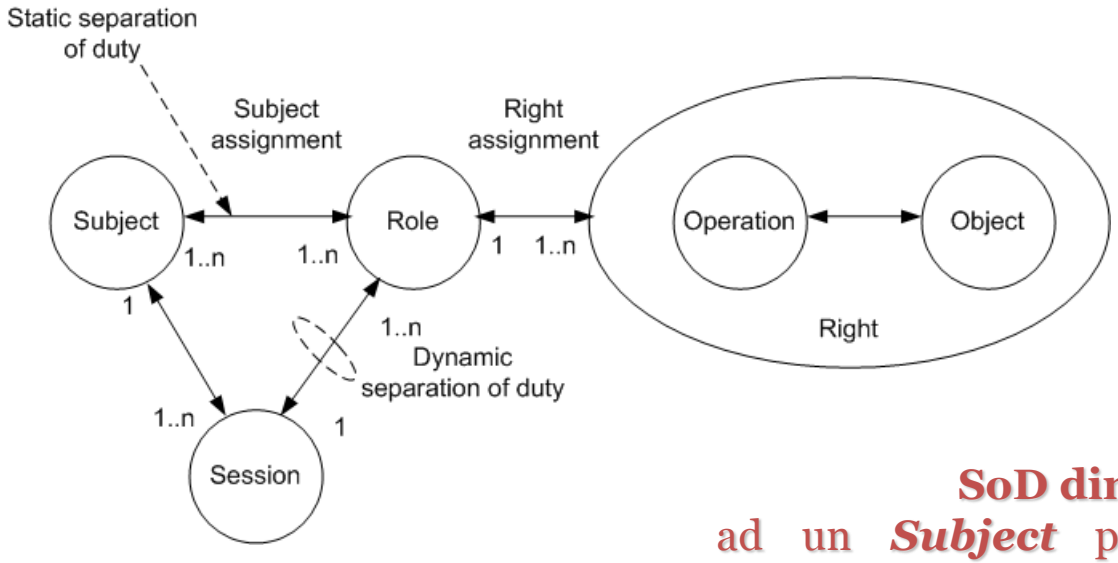
RBAC mette in pratica il principio normalmente accettato secondo il quale un individuo in una organizzazione aziendale cambia ruolo e responsabilità più spesso di quanto cambino i diritti contenuti nel ruolo stesso (esempio: è più facile che il ruolo di DB Administrator passi da Tizio a Caio piuttosto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

RBAC Process Model

Diagramma RBAC

SoD statica

ad un ***Subject*** posso associare più ***Role***, un ***Role*** si può assegnare a più ***Subject,*** ad ogni ***Role*** sono assegnati più ***Right*** (facoltà di esercitare un ***Operation*** su un ***Object***)



SoD dinamica

ad un ***Subject*** posso associare più ***Session***, ad ogni ***Session*** posso associare più ***Role,*** ad ogni ***Role*** sono assegnati più ***Right***

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

Value	Role \ Right	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.										

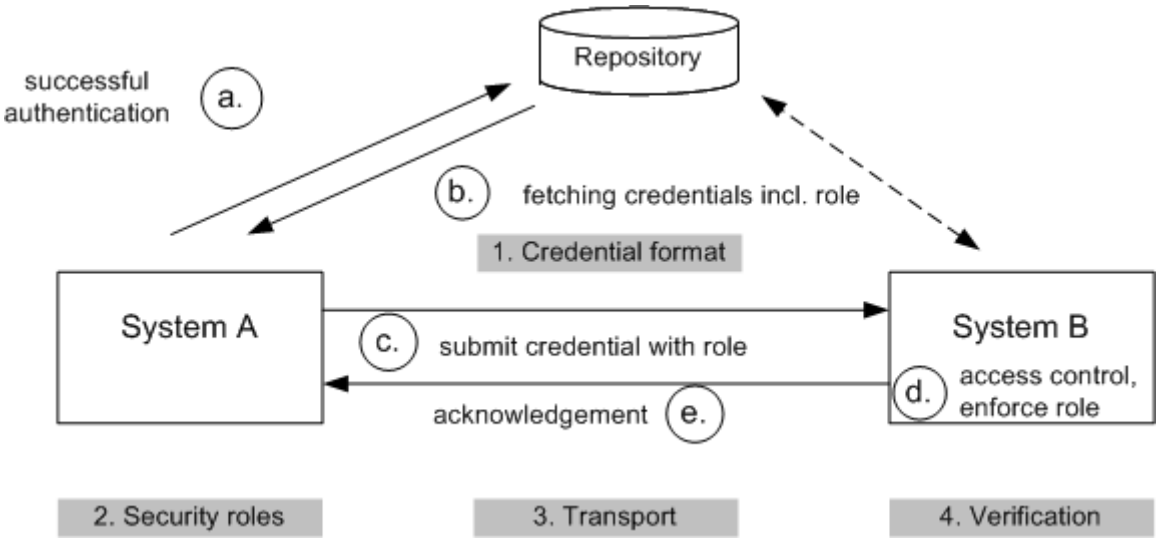
In modo analogo la norma definisce alcune assegnazioni di diritti (permessi) su operazioni predefinite in ambito della modellistica IEC 61850 (es.: diritto ALLOW e DENY sulle operazioni d'accesso Associate, Release e Abort)

Due modelli d'accesso alle risorse: push e pull

PUSH Model

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

a. il soggetto A si autentica e richiede il suo *access token;*
b. A ottiene il suo *access token;*
c. A *push* il suo *access token;*
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.



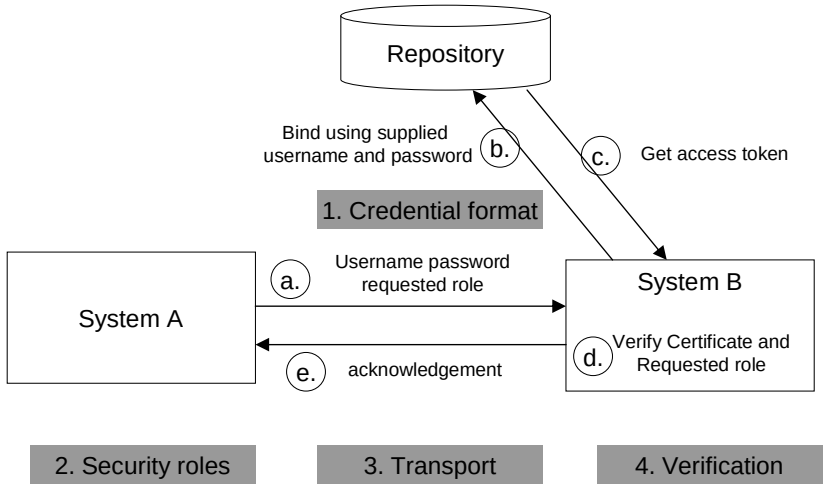
IEC 62351-8 norma gli aspetti numerati nelle caselle ombreggiate

Due modelli d'accesso alle risorse: push e pull

PULL Model

Il secondo modello è detto PULL: 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 l'*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. (es. A è un utente domino 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)

a. il soggetto A fornisce le sue credenziali di autenticazione a B;
b. B richiede l'*access token* di A sulla base delle sue credenziali;
c. B *pull* l'*access token* di A;
d. B verifica l'*access token* del soggetto A e concede l'accesso richiesto in base al ruolo inserito nell'*access token*
e. B invia la sua risposta ad A.



IEC 62351-8 norma gli aspetti numerati nelle caselle ombreggiate

RBAC Access Token

Profili degli access token

L'*access token* è un contenitore con tempo di vita finito (che ha validità in un intervallo temporale definito) rilasciato e amministrato da un'entità di gestione dell'identità dei soggetti. L'accesso a questa entità avviene attraverso un servizio LDAP sicuro (v3 su SSL/TLS).

L'*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 dell'*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*:

•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 l'*access token* definito per IEC 62351-8, nome e ruolo del soggetto, entità emittente, istante di emissione e *Area of Responsability (AoR)* che consente di restringere la validità di un ruolo di un soggetto ad un insieme di oggetti (tipica è la necessità di restringere un ruolo a oggetti di un area geografica o funzionale).

Applicazione RBAC in ENEL

SCADA geografici per gli impianti di Generazione

Nel 2010 è stato progettato un dominio Active Directory per realizzare un sistema di autenticazione dedicato ai sistemi telecontrollo (Sistemi Centrali per la Teleconduzione, SCT).

Il sistema consente di autenticare qualche centinaio di 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 utenti 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 per il rilascio degli *access token* previsti dalla parte 8 secondo il *key management* della parte 9.

Conclusioni

In questa presentazione abbiamo analizzato sinteticamente due 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 e 61850) che non sempre vengono messi in evidenza.

Conclusioni

Sistemi elettrici di potenza interconnessi e interoperabili

Infrastrutture di automazione e telecontrollo interconnesse e interoperabili

Protocolli, NSM *e* RABC
Standard
Famiglie IEC
60870 – 61850 – 61968 - 61970
62351

Sistema elettrico di potenza sicuro

- ✓**Protocolli messi in sicurezza (IEC 62351 parti 3, 4, 5, 6)**
- ✓**Infrastruttura ICT monitorata (IEC 62351 parte 7 - NSM)**
- ✓**Accessi all'infrastruttura controllati (IEC 62351 parte 8 – RBAC).**

Federico Bellio
Enel Produzione
Via Torino 14
30172 Venezia-Mestre (VE)
tel . +390418215592
mail federico.bellio@enel.com
Membro: CT 57-CEI, TC 57-CENELEC, WG15 TC 57-IEC, CIGRE

Gian Luigi Pugni
Enel Servizi
Viale Italia, 26
20099 Sesto San Giovanni (MI)
tel: +390223207827
mail: gianluigi.pugni@enel.com
Membro: CT 57-CEI, TC 57-CENELEC, WG15 TC 57-IEC, SG-CG/SGIS, AHG8 (IPv6)