Federico Bellio

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

Luca Cicognani, Stefano Doga

ABB Power System Division
Via L. Lama, 33
20099 Sesto San Giovanni (MI)
tel. +390224142837, +390106073526
mail luca.cicognani@it.abb.com , stefano.doga@it.abb.com

Sicurezza informatica nei sistemi di telecontrollo per impianti di produzione da fonte rinnovabile

Abstract

I moderni sistemi di controllo, ormai da tempo basati su tecnologie hardware e software di mercato, sono sempre più connessi a sistemi esterni e reti aziendali.
E quindi nata l'esigenza della protezione dei sistemi di controllo da potenziali attacchi, del controllo degli accessi e della robustezza delle reti, tematiche tipiche della sicurezza dei sistemi di Information and Communication Technology.

Gli enti normatori hanno regolamentato il settore con la pubblicazione di diversi standard, affrontando recentemente anche nel dettaglio gli aspetti propri della sicurezza e dell'affidabilità dei sistemi di controllo applicati al settore elettrico con la pubblicazione dello standard "Power systems management and associated information exchange - Data and communications security" (IEC 62351).

La memoria presenta i requisiti, i principi e le linee guida tecnologiche utilizzate per adeguare i sistemi di controllo degli impianti di generazione da fonti rinnovabili del gruppo Enel alle direttive stabilite dalla norma IEC 62351.

Abstract

Modern control systems, when based on market solutions, are increasingly linked to external systems and corporate networks. Control systems protection from potential attacks, access control and robustness of networks have become mandatory, these being typical issues of security in the field of Information and Communication Technology.

The regulatory committees have standardized the industry with the publication of several norms, recently addressing in detail the aspects of security and reliability for the control systems applied to the power field with the publication of the Technical Specification "Power systems management and Associated Information Exchange - Data and communications security" (TS/IEC 62351).

The paper presents the requirements, principles and technological guidelines used to make compliant the Enel control system for power generation from renewable resources to the norm IEC 62351.

1. Introduzione

Negli ultimi due decenni del '900 Enel ha sviluppato e messo in campo sistemi SCADA (*Supervisory Control And Data Acquisition*) per telecontrollo dei suoi impianti di generazione basati su apparecchiature (*hardware* hw), ambiente applicativo (*software* sw) e protocolli di scambio dati proprietari. Si approda nei primissimi anni 2000 a tecnologie hw, sw e di comunicazione di largo mercato. Viene realizzata una rete IP (Internet Protocol secondo RFC 1122) su tecnologia standard di mercato con applicazioni basate su Sistemi Operativi (SO) che coprono, per la prima volta ad ampio spettro, da ambienti aziendali (*Enterprise*) fino ad ambienti per sistemi di largo consumo (*Consumer*).

Già alla fine del primo decennio di vita la rete intranet così realizzata, denominata Rete Dati di Telecontrollo (RDT), seppure isolata dall'equivalente rete intranet gestionale nata pochi anni prima per supportare applicazioni quali la posta elettronica, la condivisione di documentazione, ambiente ERP (Enterprise Resource Planning), ecc., evidenzia la necessità di affrontare il problema della sicurezza informatica in maniera sistematica. Infatti, l'estensione della RDT ad alcune centinaia di reti LAN (Local Area Network) di impianto da un lato e dall'altro le vulnerabilità mostrate da SO estremamente diffusi rendono necessario lo sviluppo e l'implementazione di un progetto sistematico di messa in sicurezza.

Parallelamente il Comitato Tecnico 57 del IEC (International Electrotechnical Commission, Technical Committee 57), che ha come missione lo sviluppo di standard per la comunicazione fra sistemi di generazione, trasporto e distribuzione dell'energia elettrica, quali SCADA, EMS (Energy Management System), sistemi di automazione distribuita e teleprotezione, tramite il WG15 (Working Group 15) elabora e pubblica la norma IEC/TS 62351 (prima edizione maggio 2007): *Power systems management and associated information exchange – Data and communications security.* Una normativa che inquadra il problema della sicurezza

informatica e stabilisce un modello standard di messa in sicurezza specificatamente per i sistemi di comunicazione dedicati al telecontrollo dei sistemi di generazione, trasporto e distribuzione dell'energia elettrica basati sui protocolli che nel decennio precedente il TC 57 aveva normato, protocolli che avevano avuto ampia diffusione.

Tramite un percorso complesso e interfunzionale le società di generazione del Gruppo Enel adottano nel 2011 una policy che recepisce il modello di sicurezza indicato nella norma IEC 62351.

Scopo di questa memoria è quello di illustrare le linee e i principi generali che hanno guidato il gruppo di lavoro Enel nella stesura delle linee guida per la l'applicazione della *Policy sulla Sicurezza Informatica dei Sistemi di Processo Informatizzati.*

Sarà anche presentato, per somme linee il progetto, che mira a realizzare per il primo quarto del 2013 un sistema di telecontrollo interamente rispondente alla norma IEC 62351.

2. IEC 62351: La sicurezza informatica nello gestione e nello scambio di informazioni all'interno di sistemi per la generazione, trasporto e distribuzione di energia elettrica

La norma IEC 62351 parte dall'assunto che l'aggiunta di firewall, l'impiego di protocolli criptati, Virtual Private Network (VPN) o altre “scatole di messa sicurezza” inserite nel percorso tra centri di controllo e impianto controllato possa risultare inadeguato in molti casi. La vera sicurezza da capo a capo (*end-to-end*) richiede di assicurare: un accesso autenticato ai dispositivi sensibili del sistema di telecontrollo, un accesso autorizzato ai dati sensibili ai fini del mercato elettrico, disporre di informazioni cronologiche affidabili sul funzionamento e il malfunzionamento degli apparati, eseguire il salvataggio e disporre in ogni momento dei dati per il ripristino degli apparati critici (backup) ed infine una registrazione affidabile di quei dati che consentano di ricostruire in ogni momento gli eventi cruciali.

2.1. Minacce e requisiti di sicurezza

Le minacce alla sicurezza di un sistema informatico possono essere di due tipi involontario o volontario cioè deliberato e intenzionale. Sono del primo tipo le minacce: guasti o malfunzionamenti di apparati, negligenza, disastri naturali; alcune minacce del secondo tipo sono: dipendenti scontenti, spionaggio industriale, vandalismo, pirateria informatica, virus e altre forme auto replicanti di moduli o componenti software, furto, terrorismo.

La norma IEC 62351 individua quattro requisiti di sicurezza fondamentali che persone o applicazioni devono soddisfare:

- **Riservatezza** *(Confidentiality)*: prevenzione all'accesso non autorizzato di informazioni;
- **Integrità** (*Integrity*): prevenzione della modifica e del furto non autorizzato di informazioni;
- **Disponibilità** (*Availability*): prevenzione da provocate indisponibilità di servizi vitali e garantire l'accesso autorizzato di informazioni;
- **Non-ripudiabilità o responsabilità** (*Non-repudiation or accountability*): prevenire il rifiuto di una azione che è avvenuta o la rivendicazione di un'azione che non è avventa.

I quattro requisiti corrispondono a quattro tipi di minaccia:

- Accesso non autorizzato ad informazioni;
- Modifica non autorizzata o furto di informazioni;
- Rifiuto o inibizione di servizio;
- Ripudio o irresponsabilità di servizio fornito o che avrebbe dovuto essere fornito.

Si noti come questi requisiti e minacce siano di fatto a coppie complementari. Si deve impedire l'accesso alle informazioni a persone o applicazioni non autorizzati tanto quanto si deve garantire l'accesso a quelle persone e applicazioni che sono autorizzati. Si deve impedire

la modifica o il furto di informazioni da parte di persone o applicazioni non autorizzate tanto quanto si deve garantire che una azione eseguita o non eseguita da persone o applicazioni autorizzate venga ripudiata o rivendicata.

In relazione ai quattro requisiti di sicurezza una possibile classificazione degli attacchi informatici è la seguente, che prevede sei categorie:

1. **ascolto**: intrusione in una comunicazione, analisi del traffico, intercettazione elettromagnetica o ambientale, indiscrezione da parte di personale, analisi dei supporti di memorizzazione;
2. **modifica**: intercettazione e alterazione, rifiuto o impedimento di una modifica;
3. **interazione**: mascheramento, bypass di controlli, violazione di autorizzazioni, intrusione fisica, inserimento (man-in-the-middle), violazione dell'integrità, furto, ri-esecuzione (*replay)* di azioni;
4. **infezione**, inserimento di codice: *virus/worms*, cavalli di Troia, botole d'accesso (*trapdoor*), emulazione di servizi (*spoofing*);
5. **rifiuto**, **impedimento di servizio**: esaurimento di risorse indotto, fuori servizio di apparati o moduli software;
6. **Post-factum**: rifiuto d'azione eseguita, rivendicazione d'azione non eseguita, alterazione/furto, ripudio.

2.2. Contromisure e scomposizione del problema *sicurezza*

Le contromisure da mettere in campo per garantire i quattro requisiti (riservatezza, integrità, disponibilità e non-ripudiabilità) sono molteplici. Si basano sull'impiego di tecniche, tecnologie o servizi ciascuno utile a soddisfare uno o più requisiti.

L'impiego di sistemi di crittografia, certificati digitali, autenticazione sono utili a mitigare, se non risolvere, i requisiti di riservatezza, integrità e non-ripudiabilità.

La registrazione sicura di tutti gli eventi che riguardano la sicurezza dei sistemi è una caratteristica necessaria a soddisfare tutti quattro i requisiti.

Sistemi di prevenzione o di rilevazione delle intrusioni informatiche (IPS *Intrusion Prevention System*, IDS *Intrusion Detection System*) sono necessari per soddisfare i requisiti di riservatezza, integrità e disponibilità.

Un sistema di firma digitale è necessario per soddisfare il requisito di non-rupudiabilità.

Non solo tecnologie e sistemi, ma una intera gamma di nuovi servizi e ruoli aziendali, sono necessari per garantire i requisiti di sicurezza. Un servizio per il rilascio e la gestione dei certificati digitali è necessario per soddisfare i requisiti di riservatezza, integrità e non-ripudiabilità. Una gestione degli eventi (*incident*) di sicurezza che attivano i sistemi di prevenzione e rilevazione degli agenti di rischio informatico, assistito da un sistema di accertamento e segnalazione automatico delle vulnerabilità di sicurezza note (*Vulnerability Assessment*), sono necessari per soddisfare il requisito di disponibilità. Ancora per soddisfare il requisito di disponibilità è necessario un servizio per il salvataggio ed il ripristino efficacie dei dati vitali ai fini del corretto funzionamento dei sistemi.

Il problema della sicurezza può essere di grande complessità per sistemi che devono garantire la supervisione e il telecontrollo di impianti sparsi su un vasto territorio, estremamente frazionati e per la maggior parte non presidiati. Per affrontare adeguatamente il problema conviene decomporlo in regioni più ristrette di analisi e gestione. Si possono adottare per la scomposizione del problema sicurezza tre approcci:

- **perimetro della sicurezza fisica**, le sei pareti che costituiscono la sala calcolatori, la sala controllo, la sala telecomunicazioni ed ogni altro ambiente che contenga apparecchiature critiche per il corretto funzionamento del sistema; questo è l'ambito in cui vanno adottate le misure per la sicurezza fisica;

- **perimetro della sicurezza elettronica**, il confine logico sulla rete che contiene le infrastrutture critiche al fine di garantire i quattro requisiti di sicurezza; questo è l'ambito in cui vanno adottate le misure di sicurezza informatica (cyber security);
- **il dominio di sicurezza**, definito come l'unità organizzativa in una sezione, dipartimento o società dove i requisiti di sicurezza sono gli stessi o sottoposti al controllo della stessa unità; il concetto di dominio di sicurezza consente di gestire in maniera indipendente i sistemi che ricadono nel dominio stesso fintantoché appartengono o sono in gestione all'unità che costituisce il dominio di sicurezza.

i tre approcci e ambiti possono sembrare indipendenti e l'applicazione integrale della sicurezza ad uno di questi sembra potere escludere la necessità di applicare misure di sicurezza sugli altri, ma non è così perché i tre ambiti sono intersecati e non contenuti l'uno nell'altro. Soddisfare i requisiti di sicurezza significa attivare le contromisure su tutti tre i perimetri.

2.3. Security policy, valutazione del rischio, requisiti di sicurezza di un sistema per la supervisione e il telecontrollo in campo energetico

Un documento sulle politiche aziendali di sicurezza (*Security Policy*, in seguito semplicemente *policy*) ha lo scopo di dettare i criteri per affrontare i problemi di sicurezza globalmente e perciò deve affrontare il problema sotto tutti i tre gli ambiti citati nel paragrafo precedete:

- quello della sicurezza fisica delle infrastrutture critiche ai fini del telecontrollo degli impianti;
- quello della sicurezza logica dei sistemi di telecomunicazioni e informatici;
- del dominio di sicurezza, stabilendone il perimetro e individuando figure professionali a cui demandare i ruoli fondamentali per l'esercizio e la manutenzione

dei sistemi di telecontrollo comprensivi delle loro infrastrutture, fra le quali ci sono quelle che consentono l'esercizio in sicurezza.

Il documento di policy stabilisce i requisiti minimi di sicurezza che vanno garantiti nel sistema a cui è rivolto. La policy stabilisce le modalità e i limiti d'impiego di tecnologie disponibili sul mercato, indica i requisiti di sicurezza su protocolli ed applicazioni, indica alcune caratteristiche dei sistemi di telecomunicazione e le reti che interconnettono le varie parti del sistema di telecontrollo, stabilisce i criteri di assegnazione di utenze, parole chiave e certificati digitali al personale, alle applicazioni e ai dispositivi.

Un documento di policy è anche un documento che deve avere un ruolo divulgativo e, per certi aspetti, un manuale di comportamento. Rendere il personale dell'azienda cosciente dei rischi e le minacce derivanti dall'impiego di tecnologie informatiche è un passo fondamentale verso la gestione sicura di un infrastruttura informatizzata in generale e in particolare per un sistema di telecontrollo degli impianti da fonte rinnovabile.

Il documento di policy deve essere un documento *vivo* che stia al passo con gli aggiornamenti tecnologici mutuabili dall'industria della sicurezza in particolare e del *Information Technology* (IT) più in generale. Il documento di policy dovrebbe avere almeno una revisione annuale.

Una fase importante del processo per la messa in sicurezza di un sistema è quella di valutazione del rischio. Questa è la fase in cui viene deciso cosa va reso sicuro e quale grado di sicurezza è necessario. Lo stesso grado di sicurezza non è necessario e non è sostenibile su ogni parte del sistema.

Per ogni parte del sistema è necessaria una valutazione del rischio. E' necessario valutare il danno derivante da una effrazione al sistema di sicurezza ed analizzare il danno (finanziario, per la sicurezza del personale e sociale) in relazione ai costi che si devono sostenere per realizzare e mantenere il sistema di sicurezza atto ad evitarlo. Per questo la fase di valutazione del rischio deve sempre precedere la fase di sviluppo del sistema di sicurezza. In altre parole

l'analisi del rischio costituisce un requisito del sistema di sicurezza da realizzare nella misura in cui stabilisce per ogni parte del nostro sistema il grado di sicurezza necessario a fronteggiare il danno che potrebbe derivare da una effrazione alle contromisure adottate sulla quella specifica parte del sistema.

La gestione di un sistema di controllo per un sistema elettrico di potenza pone una serie di sfide di sicurezza specifiche e differenti da quelle che s'incontrano in altri ambiti. Per esempio, molte misure di sicurezza sono state sviluppate per fronteggiare i potenziali pirati informatici che viaggiano su internet. La realtà del mondo di internet è però assai lontana dalla realtà del mondo dei sistemi per il controllo di un sistema elettrico di potenza. Per questo nel mondo dell'industria della sicurezza vi sono lacune nella comprensione dei requisiti di sicurezza necessari ad un sistema per il controllo della generazione, il trasporto e la distribuzione dell'energia elettrica; come pure per le conseguenze che questi requisiti comportano sul progetto dei sistemi di telecomunicazione a supporto delle operazioni di controllo.

In particolare i servizi di sicurezza e le relative tecnologie sono stati sviluppati primariamente per industrie che non hanno requisiti stringenti sulle prestazioni e l'affidabilità necessari ad un sistema di controllo per un sistema elettrico di potenza. Per esempio:

- impedire ad un operatore autorizzato di agire su un interruttore di una sotto-stazione elettrica può avere delle conseguenze assai peggiori di quelle derivanti dall'impedire ad un cliente autorizzato di una banca ad accedere al suo conto corrente; perciò, la minaccia di impedimento-di-servizio (*denial-of-service* DOS) è assai più importante rispetto alle classiche transazioni su internet;
- molti canali di comunicazioni impiegati nei sistemi di controllo dell'industria elettrica sono di bassa capacità e gli apparati hanno limitazioni sulla potenza di calcolo e la

capacità di memoria tali da impedire l'impiego di certe misure di sicurezza come la cifratura basate sullo scambio di chiavi digitali;

- molti sistemi sono posti in siti remoti dispersi su un vasto territorio, non sono presidiati, non hanno accessi internet; questo rende la gestione delle chiavi digitali, la revoca dei certificati e altre misure di sicurezza difficili da implementare;
- sebbene comunicazioni senza fili siano largamente impiegate in molte applicazioni, le società elettriche devono essere molto prudenti nell'impiego di queste tecnologie, sia per i disturbi elettromagnetici dei sistemi elettrici di potenza che interagiscono con il segnale radio a bassa potenza tipici delle tecnologie senza fili e sia per il grado di affidabilità richiesto nelle applicazioni di automazione e telecontrollo.

La gestione delle chiavi digitali e della revoca tempestiva dei certificati sulle reti dedicate al telecontrollo degli impianti richiederà di sviluppare nuove metodologie compatibili con i requisiti di affidabilità e disponibilità tipici di questi sistemi.

Le infrastrutture di un sistema di telecontrollo per l'industria elettrica viene spesso visto come una collezione di singole linee di comunicazione, singole base dati, singoli sotto-sistemi con differenti protocolli. Nei sistemi SCADA spesso vengono riportati anche gli stati relativi alla rete di acquisizione dati e degli apparati di telecontrollo. Questo modo d'impostare il problema del monitoraggio della rete di acquisizione dati deriva dai tempi in cui si prevedeva anche del personale, in turno o semi-turno, che presidiava una console dello SCADA dedicata al monitoraggio tempo-reale della rete di comunicazione e degli apparati di telecontrollo. Ora quasi mai questo accade con il risultato che le segnalazioni vengono registrate dai sistemi SCADA ma vengono analizzate a posteriori solo quando un problema di tele-controllabilità viene segnalato dal personale in turno per la tele-conduzione degli impianti del sistema elettrico. In alcuni casi questo approccio può risultare inadeguato e portare a fuori servizi al

sistema elettrico evitabili con un monitoraggio tempo-reale anche degli eventi riguardanti la rete e gli apparati del sistema di telecontrollo.

Ogni società del campo elettrico, in vari modi, ha proprio personale di manutenzione capace di presidiare le singole parti del processo di telecontrollo. I tecnici di telecomunicazione, attraverso i fornitori dei servizi TLC, presidiano le singole connessioni della rete radio, in cavo o fibra ottica; gli esperti di rete possono tracciare lo stato delle connessioni di trasporto dati; gli amministratori delle base dati dei sistemi SCADA possono tracciare la qualità delle singole informazioni; gli esperti delle applicazioni possono analizzare le informazioni relative ai malfunzionamenti applicativi e correggerli, possono rimuovere i motivi per i quali certe applicazioni non danno i risultati attesi; infine tecnici di telecontrollo possono analizzare se un problema segnalato dagli operatori di tele-conduzione dei sistemi elettrici dipende da un problema sulla catena di telecontrollo o da il sistema di automazione dell'impianto tele-condotto.

Nel futuro il problema della gestione delle informazioni scambiate sui sistemi di telecontrollo ed automazione diventerà sempre più complesso. I sistemi SCADA non saranno più sufficienti a monitore anche il sistema di trasporto dati di cui hanno bisogno per funzionare correttamente, vari operatori di telecomunicazioni saranno impiegati per fornire la connettività, le applicazioni di automazione e telecontrollo saranno sempre più integrate, complesse e critiche; una rete di *Dispositivi Elettronici Intelligenti* (IED Intelligent Electronic Devices) capillare dovrà essere monitorata per il buon funzionamento dell'intero sistema. I sistemi SCADA non avranno più tutte le informazioni necessarie a gestire i dispositivi e le reti che consentono la tele-conducibilità degli impianti.

Risulterà sempre più necessario disporre di sistemi atti a monitorare in tempo-reale i sistemi di telecomunicazione, di rete, telecontrollo e automazione disgiunti dai sistemi SCADA e che saranno una evoluzione degli attuali sistemi per la gestione delle reti di telecomunicazione

(*Telecommunication Management Network* o più in generale sistemi di *Network Management*).

2.4. I cinque passi del processo di sicurezza

Proteggere e mettere in sicurezza i sistemi di comunicazione, i dispositivi e le informazioni che sono vitali per un sistema energetico risulterà sempre più importante e quindi sarà una chiave su cui si baserà lo sviluppo delle architetture e dei sistemi per il controllo dei sistemi delle varie fonti di energia.

La sicurezza informatica o cibernetica (cyber security) dovrà fronteggiare le sfide che derivano dalle tendenze del mondo informatico e del mondo industriale più in generale:

- necessità di livelli sempre maggiori d'integrazione con varie entità di *business;*
- incremento dell'impiego di sistemi aperti basati su infrastrutture che comprenderanno nel futuro i sistemi energetici;
- la necessità d'integrare sistemi proprietari esistenti con i nuovi sistemi;
- la crescita di complessità e sofisticazione dei sistemi computerizzati integrati e distribuiti;
- la crescita in sofisticazione e pericolosità di *comunità ostili*.

L'approccio non potrà essere che quello di progettare e pianificare i sistemi con precisi requisiti di sicurezza fin dal principio. La sicurezza va pensata a tutti i livelli in tutti i sotto-sistemi.

Il processo di messa in sicurezza è continuo, circolare e ne statico ne definitivo.

Nel processo di sicurezza si possono individuare cinque passi che sono necessari per lo sviluppo di una robusta strategia di sicurezza. Sebbene il processo sia di natura circolare, analizziamo i cinque passi secondo la sequenza logica di sviluppo di un sistema di sicurezza.

Valutazione del rischio (*assessment*) – il primo passo è quello di analizzare i requisiti funzionali di un sistema e valutarne fino dalla prima fase di progetto gli elementi di rischio e le contromisure da adottare in una logica costi-benefici;

Norme di sicurezza (*policy*) – deve esistere un processo di generazione di norme aziendali che stabiliscono i requisiti per il progetto, lo sviluppo e la gestione dei sistemi critici ai fini del *business* dell'azienda; il documento di policy recepisce le valutazioni uscite dal passo precedente e stabilisce in che modo devono essere progettate, realizzate, gestite e mantenute nel tempo;

Sviluppo dei sistemi di sicurezza (*deployment*) – questa è la fase operativa in cui i sistemi e servizi vengono acquisiti, integrati e verificati; si applicano le politiche di sicurezza stabilite nel documento di *policy;*

Formazione dedicata alla sicurezza (*training*) – una formazione ricorrente sugli aspetti di sicurezza: rischi e minacce da affrontare, tecnologie impiegabili, norme di legge e aziendali sulla sicurezza; la formazione è richiesta a più livelli a seconda del gruppo di personale a cui è rivolta (operatori, manutentori, sistemisti, sviluppatori, ecc.);

Revisione dei sistemi di sicurezza (*audit*) - il processo di revisione è responsabile dell'individuazione di minacce o rischi che il sistema di sicurezza non fronteggia adeguatamente; all'uscita di questo passo s'individuano nuovi requisiti e nuove analisi da portare in ingresso al primo passo, quello di valutazione dei rischi, così da percorrere continuativamente l'intero processo di sicurezza.

Affrontare globalmente in una grossa organizzazione, in una grande azienda, il problema di sicurezza può risultare una missione impossibile. Per ridurre la complessità del problema è senz'altro utile affrontare il problema all'interno di ciascuno Dominio di Sicurezza come definito nei precedenti paragrafi.

3. La sicurezza informatica nei sistemi di telecontrollo per impianti di produzione da fonte rinnovabile

3.1. Generalità

In relazione al processo di sicurezza illustreremo come sono stati tradotti in specifici progetti di sotto-sistemi che realizzano l'infrastruttura su cui operano persone e applicazioni per il telecontrollo di alcune centinaia di impianti di generazione da fonte rinnovabile aventi migliaia di gruppi di generazione di potenza che va da alcune centinaia di kW a quasi 300 MW.

3.2. Politiche di Sicurezza, Sicurezza fisica e Dominio di Sicurezza

Nel gruppo Enel le policy per la sicurezza fisica e logica sono apparse dapprima nel mondo dell'informatica gestionale. Con l'impiego di tecnologie di largo mercato nel progetto e la realizzazione dei sistemi di automazione e telecontrollo ha portato, negli ultimi anni, anche allo sviluppo delle policy anche in questo ambito.

Il processo è stato quello di separare in Domini di Sicurezza. Dopo il dominio gestionale è stato affrontato il dominio di telecontrollo ed automazione; vista la peculiarità di ciascuno, il problema è stato ulteriormente scisso nel Dominio di Sicurezza per i sistemi di Generazione dedicati alle fonti rinnovabili e in quello per la Generazione da fonti fossili.

Alcuni aspetti sono rimasti comuni ai due sotto-domini. La sicurezza fisica è stata affrontata in maniera analoga e sono state individuate soluzioni che hanno portato ad individuare dei progetti comuni per la video-sorveglianza dei siti che, dal processo di analisi del rischio, sono stati considerati critici. Anche alcuni aspetti inerenti la sicurezza logica, che tratteremo nei paragrafi seguenti, sono stati trattati in comune perché in capo alla medesima unità organizzativa. In particolare, come si è detto nel capitolo , si è reso necessario individuare nuove figure organizzative corrispondenti ad altrettante figure professionali. La suddivisione

dei ruoli in tre categorie assolve al giusto grado di separazione di competenze (nota come SOD *Separation Of Duties*):

- un ruolo per la gestione ed il controllo della sicurezza logica, assegnato al classico SOC (*Security Operation Center*) del ICT aziendale;
- un ruolo per la gestione dei sistemi di rete per la RDT, assegnato a chi aveva finora gestito si sistemi SCADA geografici con la loro rete d'acquisizione dati;
- un ruolo per la gestione dei singoli sistemi in ambito locale, assegnato, volta per volta, al gruppo che gestisce il ciclo di vita dei singoli sistemi.

3.3. Sicurezza elettronica o logica

Di seguito analizzeremo per somme linee l'architettura e gli aspetti salienti del sistema di telecontrollo degli impianti di generazione da fonte rinnovabile sotto l'aspetto della sicurezza elettronica o logica come definita nel capitolo

3.3.1. Architettura

Di seguito sono descritte brevemente le principali componenti del sistema di telecontrollo (figura 1). Presso gli impianti di generazione, nella maggior parte dei casi, sono presenti sistemi di controllo locale con server dotati di sistema operativo commerciale che gestiscono e controllano dispositivi distribuiti su una rete locale di processo.

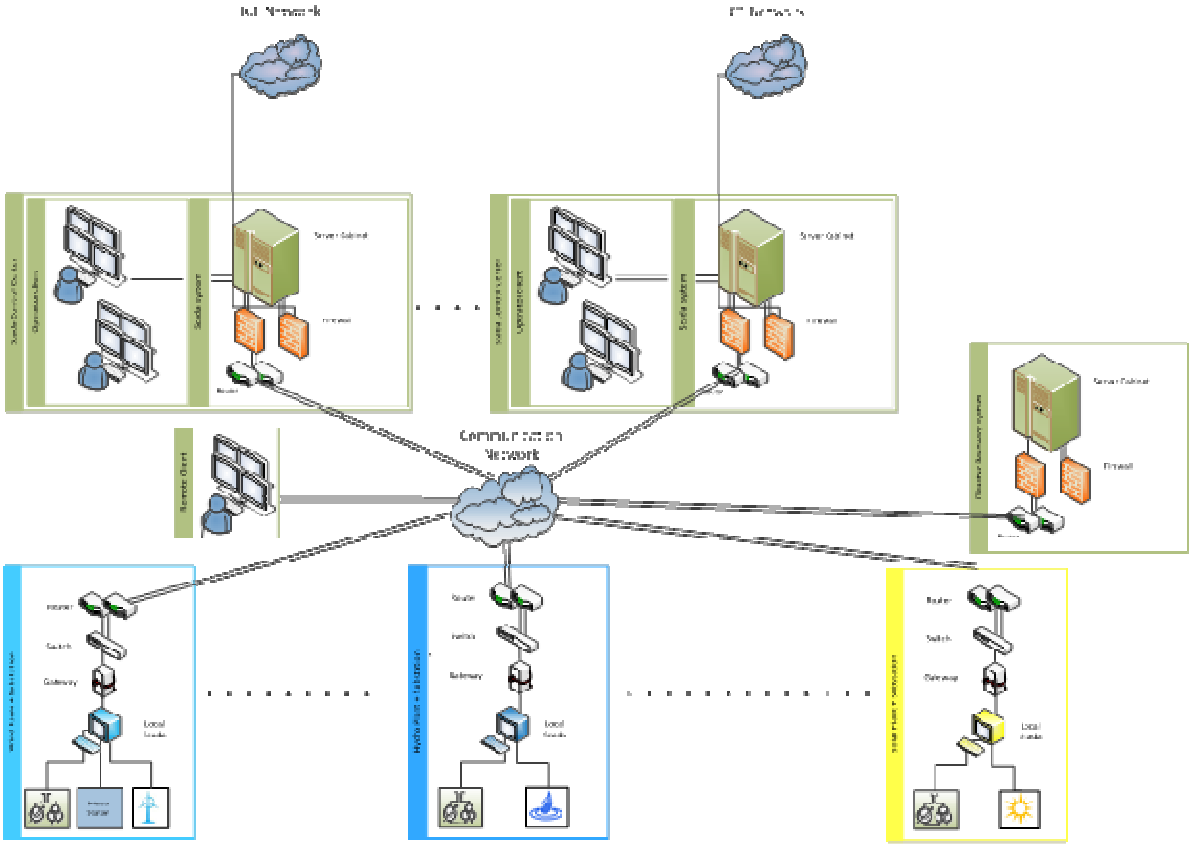

Fig. 1. Architettura del sistema

Tramite un opportuno gateway e attraverso la Rete Dati di Telecontrollo (RDT), ciascun impianto è esercito da remoto da un Centro di Controllo (CC) che svolge funzioni di monitoraggio e controllo da remoto con presidio costante.

Ciascun Centro di Controllo è dotato di una rete locale sulla quale sono collegate un certo numero postazioni operatore. E' inoltre possibile accedere remotamente ai server di telecontrollo, attraverso la RDT, da postazioni operatore remote, distribuite sul territorio.

I dati acquisiti dagli impianti sono pubblicati ad altre funzioni aziendali per supportare le attività di trading e manutenzione degli impianti.

Sul territorio sono presenti più CC tra i quali sono suddivisi gli impianti di produzione su base geografica.

Ogni CC può essere funzionalmente replicato in un centro di recupero del disastro in caso di totale impossibilità di esercire gli impianti.

La complessità del sistema mette in luce notevoli criticità dal punto di vista della sicurezza informatica:

- distribuzione geografica dei punti di accesso alla rete, presenza di diverse reti locali ed elevato numero di sistemi da proteggere e controllare (server telecontrollo, server sistemi locali, postazioni operatore, ecc.);
- necessità di condividere informazioni con altre strutture aziendali e quindi di aprire, in maniera controllata, la rete di telecontrollo verso la rete aziendale;
- requisiti di alta affidabilità e prestazioni per poter supportare in maniera efficace l'esercizio degli impianti;
- gestione sofisticata del backup delle configurazione per ottimizzare la gestione del recupero del disastro.

3.3.2. Infrastruttura di autenticazione

Per fronteggiare una tra le principali minacce cioè l'accesso non autorizzato ad informazioni e la conseguente possibilità di modifica non autorizzata o furto delle informazioni, risulta fondamentale gestire in maniera sicura e centralizzata il controllo degli accessi al sistema. In questo paragrafo sarà illustrata brevemente l'infrastruttura utilizzata per garantire l'accesso ai sistemi della RDT con credenziali univoche e centralizzate, conforme ai requisiti in termini di:

- scadenza e rinnovo delle password e della loro complessità;
- ruoli differenziati alle varie utenze in funzione dei diversi compiti assegnati e della diversa competenza territoriale;
- salvo restando la centralizzazione delle credenziali, possibilità di ciascun CC di funzionare in autonomia dalla rimanente parte della infrastruttura.

Questi requisiti sono stati implementati sfruttando i servizi offerti dai moderni sistemi operativi per server che permettono di centralizzare in unica struttura, in maniera gerarchica,

le informazioni circa le unità organizzative, gli utenti, l'hardware, le applicazioni e i criteri di autorizzazione e autenticazione. Si tratta dei concetti "foresta", "albero di dominio" e "dominio", riassunti nelle figure 2, 3, 4

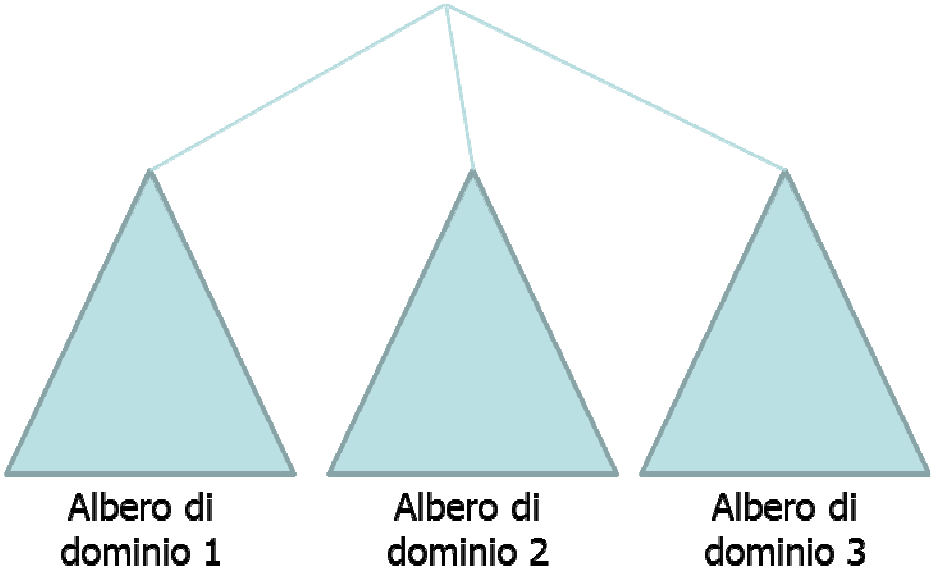

Fig. 2. Foresta alberi di domini

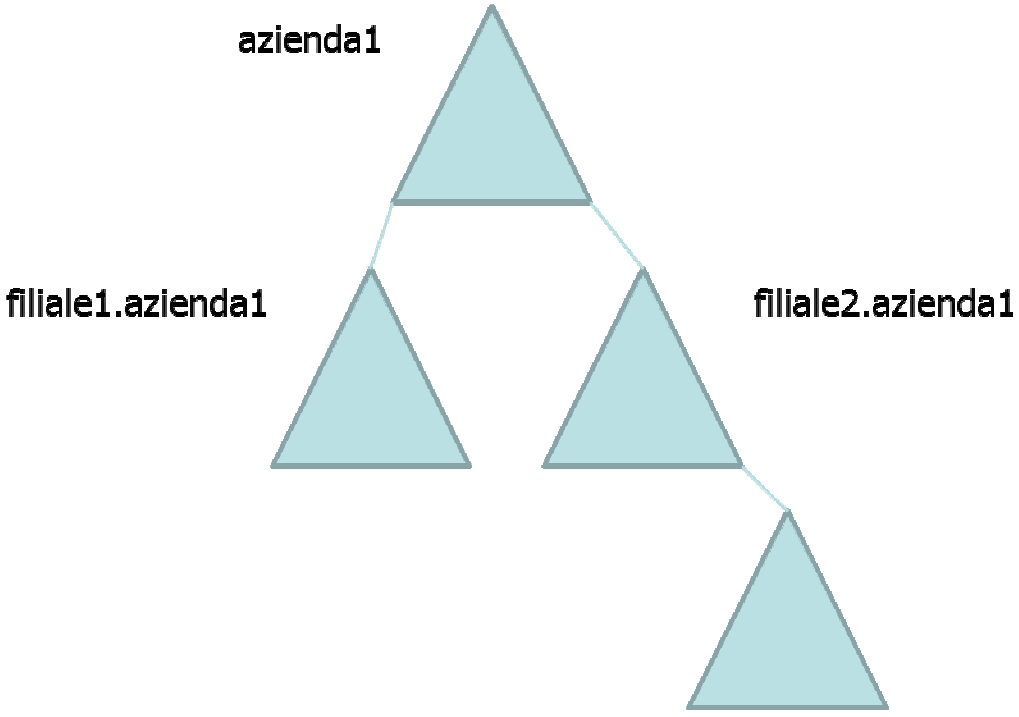

Fig. 3. Albero di domini

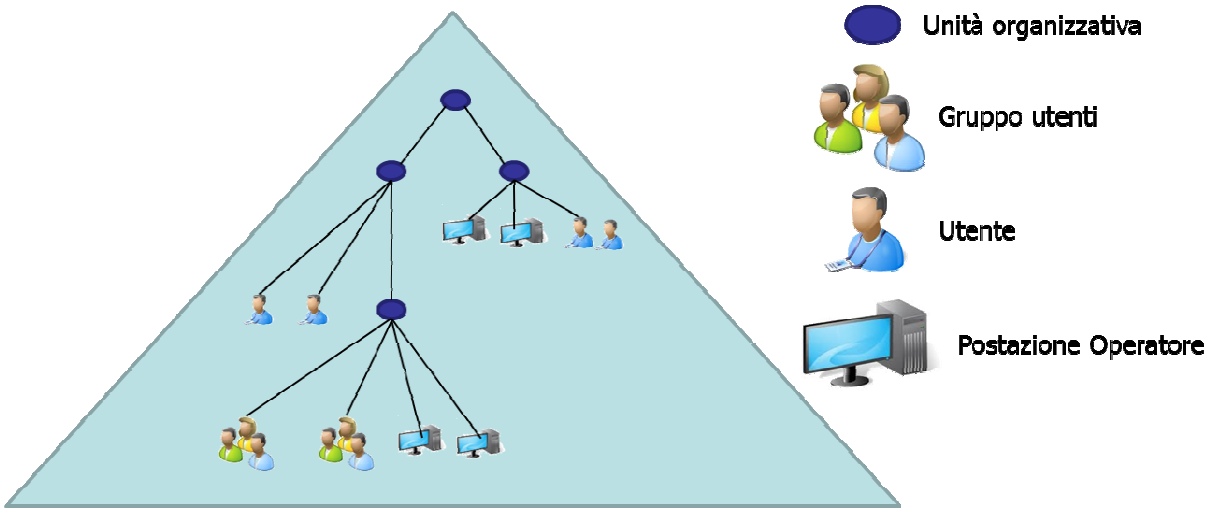

Fig. 4. Esempio di dominio

Tutti gli utenti della rete sono quindi registrati in un unico archivio centralizzato in cui vengono assegnate loro le autorità e definite le politiche di gestione delle password.

Il software del sistema di controllo permette quindi di definire un insieme di gruppi di utente aventi diverse autorità di gestione (impianti accessibili, amministrazione, configurazione, comandi, sola visualizzazione, ecc..) e di associarli a gruppi definiti nel dominio.

In questo modo si realizza un sistema di accesso e gestione delle autorità sicuro e centralizzato.

Al fine di coniugare i requisiti di sicurezza, centralizzazione e autonomia di funzionamento di ciascun CC sono stati implementati dei meccanismi di replica e ridondanza:

- in ogni CC sono definiti due server di dominio in ridondanza;
- un ulteriore sito, con funzionalità di *disaster recovery*, funge da archivio principale delle informazioni con funzioni di replica periodica verso gli altri siti.

3.3.3. Gestione dei rischi informatici base

In questo paragrafo sono descritte brevemente i requisiti e le tecniche adottate per gli aspetti legati alla sicurezza informatica *classica* o base, nel senso comune del termine. Si tratta di quelli aspetti dovuti all'impiego di piattaforme hw e sw di largo uso per le quali lo sviluppo di

agenti quali virus, cavalli di troia e altri moduli sw auto-replicanti da parte di ambienti ostili è frequente.

La gestione di più piattaforme hw e sw richiede di prevedere più sistemi paralleli ciascuno necessario per le varie funzioni, descritte di seguito, applicate alle varie piattaforme.

Hardening - particolare importanza nell'ambito della sicurezza informatica applicata ai sistemi di telecontrollo ricopre l'attività di hardening. Tale attività indica il processo di messa in sicurezza di un sistema attraverso la riduzione della sua "superficie d'attacco". Un sistema ha una superficie di attacco più ampia tante più funzionalità offre; in linea di principio un sistema con una singola funzione è più sicuro di un sistema con molte funzioni.
Con i requisiti richiesti ai moderni sistemi di telecontrollo non è più possibile limitare le funzionalità al solo controllo di processo e quindi è necessario agire in due direzioni implementando strategie di hardening hardware e strategie di hardening software.
Hardware hardening - In linea generale la strategia di hardening applicata all'hardware, implica la disabilitazione di tutte le periferiche non necessarie agli scopi del telecontrollo.
Per i server è consigliabile l'utilizzo di calcolatori di tipo industriale: computer cioè che anche dal punto estetico non presentino similitudini con i tradizionali computer di tipo desktop che "invogliano" anche i meno esperti a collegare le macchine con altri dispositivi esterni. Le soluzioni possibili sono i computer con montaggio a rack o i computer di tipologia blade. In entrambe le soluzioni le diverse porte di I/O sono poste in posizioni accessibili solo a sistemisti o a personale esperto. Un'ulteriore ed efficace misura di sicurezza è rappresentata dal fatto di inibire, nei settaggi di sistema, l'uso di porte di comunicazione (USB, Parallele, Bluetooth) dei server. In questo modo qualsiasi dispositivo si provi a collegare non sortirà alcun effetto.
Le postazioni operatore, cioè le macchine dalle quali vengono eserciti gli impianti, possono rappresentare un elemento potenzialmente più vulnerabile perché soggette all'uso di diversi

utenti. Anche in questo caso il ricorso a macchine “non convenzionali” può rappresentare la soluzione al problema. L’installazione di macchine “Thin Client” aiuta a realizzare il processo di hardening presentando all’operatore la sola tastiera e il solo mouse come unici dispositivi per poter interagire con il sistema.

Software hardening - proteggere la sola parte hardware del sistema non è sufficiente a garantire un adeguato livello di sicurezza sui sistemi informatici. Per questa ragione è necessario “ritagliare” la miglior configurazione possibile al fine di esercire i sistemi e di limitare al massimo la possibilità di attacchi software: in generale se un processo non esiste non e` possibile attaccarlo.

Si deve quindi procedere a disabilitare:

- tutti i servizi di sistema non necessari
- tutti i *device driver* non utilizzati dalla macchina
- tutti i protocolli di comunicazione non necessari.

Patching - la messa in sicurezza di un sistema informatico non è una attività “una tantum” ma è un processo di aggiornamento che deve essere costante nel tempo. Risulta necessario infatti prevedere una politica di aggiornamento continuo (patching) che permetta di mantenere i propri sistemi sempre aggiornati.

I sistemi operativi non nascono mai scevri da errori di scrittura del codice o da malfunzionamenti che vengono scoperti solo dopo la distribuzione e la messa in servizio. Gli autori di “malware” sono alla costante ricerca di nuovi metodi per “perforare” le sicurezze studiate da chi scrive sistemi operativi.

Ecco quindi che dotarsi di una robusta struttura di patching non è più una scelta opzionale ma una necessità.

Il processo di patching deve però tenere conto delle esigenze di funzionamento del sistema di supervisione del telecontrollo che deve funzionare senza soluzione di continuità 24 ore su 24.

E` quindi necessaria una stretta collaborazione tra gli amministratori del sistema e chi redige il codice degli applicativi che concorrono a formare il sistema di telecontrollo.

Alla notifica di rilascio della nuova release di Sistema Operativo relativa alla sicurezza, il fornitore del software di gestione del telecontrollo, si preoccupa di verificare la compatibilità di questa nuova versione con il proprio software grazie ad una campagna di test. In seguito a riscontri positivi il fornitore informa il cliente e dà il benestare all'installazione della patch sul sistema di telecontrollo.

Da parte sua il cliente può predisporre un sistema automatico di patching che costantemente verifica lo stato di aggiornamento del sistema rispetto allo stato ufficiale pubblicato dal costruttore del sistema operativo.

L'avvio dell'installazione delle patch non potrà essere quindi affidata ad un sistema completamente automatico ma dovrà essere sottesa al controllo umano: solo cosi si può avere la certezza che il sistema di telecontrollo mantenga l'adeguato livello di performance e sia costantemente aggiornato.

Antivirus - Il solo sistema di patching non può però essere sufficiente al fine di garantire un adeguato livello di sicurezza del sistema di telecontrollo. Come già illustrato in precedenza anche virus, "worm" e "cavalli di Troia" possono costituire una minaccia per la corretta gestione dei sistemi di telecontrollo. A tal proposito in tutti i sistemi di processo informatizzati deve essere installato un antivirus con aggiornamento centralizzato della "*signature*" (lista dei virus conosciuti) e della versione del motore di ricerca.

Analogamente a quanto descritto per il sistema di patching, è possibile organizzare anche per i software Antivirus una politica di aggiornamento automatico che si basa sul confronto tra quanto installato sul proprio sistema con quanto messo a disposizione dalle case produttrici. Anche in questo caso è indispensabile una stretta collaborazione con i fornitori del software per la gestione dei sistemi di telecontrollo.

Oltre a quanto affrontato per il sistema di patching, essendo tipicamente sistemi “tempo-reale” (*real-time*), è necessario definire una precisa lista di “esclusioni” per evitare che il software Antivirus pregiudichi il corretto funzionamento del software per la gestione del telecontrollo.

Ovviamente eventuali liste di esclusione dovranno essere concordate con l’amministratore del sistema sulla base delle informazioni acquisite dal fornitore o dall’esperienza operativa.

E` opportuno che il software installato debba, inoltre, consentire all’amministratore di sistema il monitoraggio dello stato di aggiornamento di motore di ricerca, lista dei virus conosciuti e la segnalazione in tempo reale di eventi di rilevazione di virus.

Vulnerability Assessment – la chiusura di consistenza sulle contromisure dedicate alla sicurezza informatica legata alle minacce derivanti da parti o moduli variamente replicanti e che infettano gli ambienti applicativi viene fatta attraverso un sistema di *Vulnerability Assessment* (VA) che possiamo vederlo come un sistema che esercita il nostro software con tutte le tecniche note di attacco informatico e individua i potenziali rischi, produce un dettagliato report che può includere le indicazioni di come proteggersi dalla minaccia individuata. Questo processo di VA normalmente è svolto in due passi: nel primo c'è una fase di scansione sistematica dello spazio IP assegnato all'operazione (fase di *Network Discovery*) in cui i nodi che in qualche modo sono in grado d'interagire con la rete vengono mappati e caratterizzati; nel secondo passo vi è il vero e proprio test di vulnerabilità che è un operazione che può risultare pesante in termini di prestazioni sia della macchina di VA sia su su quelle bersaglio, va quindi ben sintonizzata sulle esigenze e i rischi da cui si vuole proteggersi. Un ciclo completo di VA è previsto con ciclo semestrale od annuale. E' chiaro che il VA è utile, su reti particolarmente estese, come RDT, ad intercettare nuovi nodi posti in rete senza che la struttura organizzativa per la sicurezza ne fosse stata messa a conoscenza secondo le indicazioni previste nelle *policy*.

3.3.4. Gestione dei salvataggi e ripristini dei dati vitali

Per sistemi di telecontrollo geograficamente distribuiti devono essere implementate politiche di backup che permettano di recuperare rapidamente situazioni critiche.

Per questo tipo di sistemi la gestione di backup può essere suddivisa in due macro categorie:

- Backup finalizzati al ripristino di un computer all'interno di un centro di telecontrollo ("Backup locali");
- Backup finalizzati al recupero di una situazione di disastro: un intero centro di telecontrollo non è più utilizzabile per un evento improvviso ("Backup distribuiti").

Backup locali - per ogni centro di telecontrollo deve essere disponibile un sistema di backup (NAS, libreria o altro) in grado di archiviare i dati di configurazione degli SCADA, dei sistemi ausiliari e delle altre apparecchiature finalizzate alla tele conduzione degli impianti. Il salvataggio periodico dei dati deve poter essere posizionato anche fuori linea.

I sistemi di processo informatizzati devono essere dotati di un backup del contenuto delle partizioni di sistema ed applicative.

Al fine di realizzare questo tipo di soluzione può essere utile installare in ogni sito un sistema di tipo "*Write One Read Many*": sarà quindi compito dell'amministratore di sistema implementare la politica di salvataggio più adeguata da implementare con per ogni centro di telecontrollo.

Backup distribuiti - l'implementazione di questa politica di backup può risultare decisamente più complessa. Il presupposto è la necessità di ovviare all'indisponibilità di un intero Centro di Controllo per un periodo di tempo significativo (alcuni giorni). Il principio da implementare è quello di realizzare, in un sito remoto, una copia del sistema di telecontrollo.

Nel caso in cui i sistemi di telecontrollo di cui realizzare una copia siano diversi e geograficamente distribuiti, può essere delegato ad un unico sito, definito come Centro di Recupero del Disastro, la funzionalità di assumere il ruolo del sistema "in disastro".

Nei vari CC occorre prevedere il salvataggio delle configurazioni dei vari sistemi e il loro invio al Centro di Recupero del Disastro, dove un apposito server svolge la funzione di raccolta dei backup e “dispacciatore” verso le altre macchine.

Le attività di salvataggio dati e invio delle configurazioni sono svolte in modalità automatica e ciclica, secondo una periodicità configurabile da un apposito agente software.

In maniera analoga, un agente software sulla macchina di destinazione si preoccupa di “catalogare” e archiviare i dati ricevuti dai diversi centri di telecontrollo in modo da mantenere sempre allineate le configurazioni presenti nei centri di telecontrollo con la macchina del Centro di Recupero del Disastro.

Nel caso in cui si verifichi un evento che renda completamente indisponibile un centro di telecontrollo, sarà attivata, su richiesta di un operatore, un procedura automatizzata che configurerà le macchine presenti presso il Centro di Recupero del Disastro come “repliche” di quelle del centro di telecontrollo non più utilizzabile.

3.4. Sistemi di monitoraggio sul perimetro di sicurezza elettronica

Una parte fondamentale per garantire la prevenzione di intrusione informatiche è la gestione centralizzata dei sistemi antivirus, vulnerability assessment e di intercettazione e prevenzione delle intrusioni (IPS e IDS). L'insieme dei sistemi consente di correlare gli eventi che avvengono sul perimetro logico e all'interno del nostro sistema cosicché quello che può non essere un problema su un singolo sistema diventi un problema se si replica in rapida sequenza localmente o distribuito su più punti del sistema. Per esempio: non è segno di alcun problema l'accesso da remoto ad un server del CC di un singolo utente, ma lo è il tentativo in rapida sequenza di accesso a più server.

Il sistema di correlazione per la rivelazione delle potenziali intrusioni si basa su una rete di sonde informatiche e di firewall distribuite sul perimetro elettronico e all'interno della RDT nei punti critici. Punti critici sono: l'interconnessione con la rete geografica di ciascun CC o

l'interfaccia fra la più interna della RDT e le aree di transito o demilitarizzate (DMZ) dove vengono pubblicati i dati aggiornati in tempo-reale d'interesse degli utenti e applicazioni delle funzioni gestionali. Anche gli eventi derivanti dal sistema d'autenticazione di utenti ed applicazioni può rientrare tra gli eventi che entrano nel correlatore per il monitoraggio del rischio informatico (sistema di *Risk Monitoring* RM).

L'attivazione del sistema RM, su una scala di più livelli, consente di attivare il personale (processo di Security *Incident Management* SIM) che H24 supervisiona l'apparato di sicurezza della RDT. L'evento identificato automaticamente viene poi valutato congiuntamente tra gli esperti di sicurezza e gli esperti applicativi per poter stabilire se l'evento è effettivamente un tentativo di effrazione dei sistemi di sicurezza. Il processo SIM consente un monitoraggio H24 dei problemi di sicurezza informatica, garantendo un pronto intervento che può arrivare fino all'isolamento del segmento di RDT dove si è evidenziato il problema. La decisione sul tipo di azione da intraprendere viene presa ed attuata da una unità di crisi che viene attivata H24 se il personale reperibile giudica grave il rischio proveniente dal segmento di rete sotto analisi.

3.5. Sistema di monitoraggio degli apparati della rete di telecontrollo

Un sistema per il monitoraggio degli apparati di rete e sistemi dei supporti di telecomunicazione forniti dagli operatori di telecomunicazione sovrintende all'infrastruttura di rete per RDT.

La parte classica di Telecommunication Management Network (TMN) sarà integrata nei prossimi anni in un sistema in grado di supervisionare tutti gli apparati che concorrono a realizzare l'intera infrastruttura di telecontrollo ed automazione. Quindi non solo gli apparati classici di una rete informatica, quali router, firewall, switch, server, console, ma anche le apparecchiature di telecontrollo: RTU e IED. Per questo RTU e IED in generale dovranno

essere in grado di comunicare con il sistema di monitoraggio mediante protocolli adatti a tale scopo, come ad esempio Simple Network Management Protocol (SNMP).

Questo richiede l'arricchimento delle funzionalità delle RTU e nuovi IED, per questo ci attendiamo che il trasferimento del monitoraggio degli apparati di telecontrollo dagli SCADA, come avviene ora in modo classico, al sistema di monitoraggio dedicato richiederà alcuni anni e durante questo periodo conviveranno i due tipi di monitoraggio.

3.6. La gestione di chiavi e certificati elettronici

La sfida forse più ardua per la realizzazione di sistemi di telecontrollo e automazione di nuova generazione è costituita dalla realizzazione dell'infrastruttura per la gestione delle chiavi e dei certificati elettronici. E' questa una parte fondamentale per completare l'implementazione di un sistema conforme alla norma IEC 62351.

Per giungere a ciò e necessario disporre di una *Certification Authority* (CA). Potrebbe trattarsi di una di quelle che già operano su internet, anche Enel lo è. Ma la necessità di garantire l'adeguato grado di segregazione alle reti per il telecontrollo suggerisce di costituire delle infrastrutture separate. Potrebbe essere una delle entità che sovraintende e regola il mondo elettrico, come ad esempio il TSO (Transmission System Operator), che ciascuna rete nazionale ha e con il quale tutti gli operatori del mondo elettrico scambiano dati per consentire al TSO di svolgere il suo ruolo. Una soluzione di questo tipo sarebbe preferibile rispetto alla costituzione di CA autonome per ciascun sistema di sicurezza proprio per garantire anche l'interscambio di dati fra operatori del mondo elettrico e il loro TSO.

Il nostro sistema per il telecontrollo della generazione di fonti rinnovabili prevede la realizzazione dell'infrastruttura per la gestione di chiavi e certificati già dal 2012 con l'obiettivo di portare il servizio la prima connessione completamente conforme alla norma IEC 62351 nella prima metà del 2013.

A tale scopo è utile e necessario un ampio confronto fra i fornitori di sistemi SCADA e gli operatori del mondo elettrico per arrivare a soluzioni condivise nello spirito aperto della norma IEC.

4. Conclusioni

Nel valutare un sistema di controllo per gli impianti di generazione un tempo si esplodevano le problematiche inerenti i sistemi centrali SCADA dei centri di controllo, gli apparati RTU installati negli impianti e i protocolli da impiegare per far dialogare gli uni con gli altri al fine di consentire agli operatori dei centri di controllo di tele-condurre gli impianti.

L'impiego di tecnologie di vasto uso e di sistemi aperti ha posto il problema della sicurezza informatica come passo fondamentale per mantenere un alto grado di affidabilità del telecontrollo degli impianti.

SCADA, RTU e sistemi di telecomunicazione non sono più l'intera infrastruttura di tele-conduzione, ma ora è necessario disporre di un'infrastruttura complessa che preveda: autenticazione, prevenzione da intrusioni, gestione dell'aggiornamento di migliaia di apparati molte volte nell'arco della loro vita, gestione di firme digitali e così via.

Questa esigenza ha portato all'evoluzione di tecniche e tecnologie di sicurezza specifiche per il mondo del telecontrollo e l'automazione di cui si attende nei prossimi anni una continua crescita in termini di complessità e numerosità.

Ringraziamenti

Ringraziamo tutti i colleghi che in Enel e ABB 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.