FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

DAL 1945 IL VALORE DELL'INNOVAZIONE

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

Enel Produzione
Federico Bellio

ABB Power Sytems Division
Luca Cicognani, Stefano Doga

Introduzione

- 1978-1996: Telecontrollo impianti Enel
  - SCADA basato su hw, sw e protocolli proprietari
- 1997-2009: Telecontrollo impianti da fonte rinnovabile Enel Produzione
  - Dal 2001: hw, sw e di comunicazione di largo mercato, rete IP, Sistemi Operativi commerciali
  - Dal 2004: primo approccio alla sicurezza informatica sulla Rete Dati per il Telecontrollo (RDT) per l'interconnessione e accesso da intranet aziendale
- 2007: Comitato Tecnico 57 IEC WG15
  - norma IEC/TS 62351: *Power systems management and associated information exchange – Data and communications security.*

La memoria

- Scopo:
  - illustrare le linee e i principi generali che hanno guidato il gruppo di lavoro Enel nella stesura della *Policy sulla Sicurezza Informatica dei Sistemi di Processo Informatizzati.*
  - presentare, 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.

IEC 62351: sicurezza informatica e sistemi di controllo

- Firewall, protocolli criptati, Virtual Private Network (VPN) : da soli, inadeguati in molti casi
- Sicurezza da capo a capo (*end-to-end*):
  - accesso autenticato ai dispositivi sensibili
  - accesso autorizzato ai dati sensibili (mercato elettrico)
  - informazioni cronologiche malfunzionamenti
  - salvataggio e disponibilità dati per il ripristino
  - registrazione dati per ricostruire eventi cruciali.

IEC 62351: requisiti e minacce

- Requisiti di sicurezza fondamentali:
  - **Riservatezza** (*Confidentiality*): prevenire accesso non autorizzato informazioni;
  - **Integrità** (*Integrity*): prevenire modifica non autorizzata e furto informazioni;
  - **Disponibilità** (*Availability*): prevenire provocate indisponibilità servizi vitali e accesso autorizzato informazioni;
  - **Non-ripudiabilità o responsabilità** (*Non-repudiation or accountability*): prevenire rifiuto azione avvenuta o rivendicazione di un'azione non avventa.

- Minacce:
  - 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.

IEC 62351: attacchi informatici

- **Ascolto**: intrusione in una comunicazione, analisi traffico, intercettazione, indiscrezione da parte di personale, analisi supporti memorizzazione;
- **Modifica**: intercettazione e alterazione, rifiuto o impedimento modifica;
- **Interazione**: mascheramento, violazione di autorizzazioni, intrusione fisica, violazione dell'integrità, furto, ri-esecuzione di azioni;
- **Infezione**: *virus/worms*, cavalli di Troia, botole d'accesso (*trapdoor*), emulazione di servizi (*spoofing*);
- **Rifiuto**, **impedimento di servizio**: esaurimento di risorse indotto, fuori servizio di apparati o moduli software;
- **Post factum**: rifiuto d'azione eseguita, rivendicazione d'azione non eseguita, alterazione/furto, ripudio.

IEC 62351: contromisure

- Tecniche, tecnologie
  - sistemi di crittografia, certificati digitali, autenticazione
  - registrazione sicura eventi sicurezza
  - sistemi di prevenzione o di rilevazione delle intrusioni informatiche (IPS *Intrusion Prevention System*, IDS *Intrusion Detection System*)
  - sistema di firma digitale
- Servizi e ruoli aziendali
  - servizio per il rilascio e la gestione dei certificati digitali
  - gestione degli eventi (*incident*) di sicurezza
  - sistema di accertamento e segnalazione automatico delle vulnerabilità di sicurezza note (*Vulnerability Assessment*)
  - servizio per il salvataggio ed il ripristino dati vitali

IEC 62351: diversi approcci alla sicurezza

- Diversi approcci:
  - **perimetro della sicurezza fisica:** la sala calcolatori, sala controllo, sala telecomunicazioni, etc.
  - **perimetro della sicurezza elettronica**: confine logico sulla rete che contiene le infrastrutture (*cyber security*);
  - **il dominio di sicurezza**: unità organizzativa in una sezione, dipartimento o società dove i requisiti di sicurezza sono gli stessi o sottoposti al controllo della stessa unità
- Ambiti intersecati e non contenuti l'uno nell'altro: occorre attivare le contromisure su tutti tre i perimetri.

Security Policy

- Stabilisce i requisiti minimi di sicurezza
  - tecnologie disponibili sul mercato, protocolli ed applicazioni, caratteristiche dei sistemi di telecomunicazione e reti, criteri di assegnazione di utenze, parole chiave e certificati digitali al personale, alle applicazioni e ai dispositivi
- Ruolo divulgativo
  - rendere il personale cosciente di rischi e minacce.
- Documento *vivo*
  - al passo con gli aggiornamenti tecnologici

Valutazione del rischio

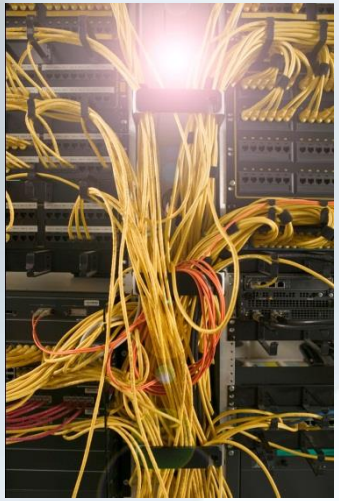
- Per ogni parte del sistema è necessaria una valutazione del rischio.
  - Analisi danno derivante da una effrazione al sistema di sicurezza (finanziario, per la sicurezza del personale e sociale)
  - Analisi costi da sostenere per realizzare e mantenere il sistema di sicurezza
- Precede la fase di sviluppo del sistema di sicurezza
  - requisito del sistema di sicurezza
  - stabilisce per ogni parte del nostro sistema il grado di sicurezza necessario a fronteggiare il danno

Sistemi di controllo: le sfide della sicurezza

- Criticità rispetto ad altri ambiti industriali/internet
  - Impedimento-di-servizio (*Denial-Of-Service* DOS): impedire ad un operatore autorizzato di agire su un interruttore di una sotto-stazione elettrica
  - Canali di comunicazioni di bassa capacità e apparati con limitazioni: potenza di calcolo, capacità di memoria
  - Siti remoti distribuiti, non presidiati, senza accessi internet: difficoltà implementare gestione chiavi digitali, la revoca dei certificati, etc.
  - Prudenza utilizzo comunicazioni senza fili: disturbi elettromagnetici, affidabilità

Sistemi di controllo e monitoraggio reti

- Attuali sistemi SCADA
  - Monitoraggio rete di acquisizione dati e apparati di telecontrollo.
  - Analisi a posteriori
  - Approccio inadeguato, possibili fuori servizi al sistema elettrico



- Prossimo futuro
  - gestione informazioni sempre più complessa
  - rete di (IED Intelligent Electronic Devices) capillare da monitorare
  - Sistemi dedicati per monitorare in tempo-reale rete, telecontrollo e automazione disgiunti dai sistemi SCADA

I cinque passi del processo di sicurezza

Audit revisione sistemi di sicurezza

Individuazione di rischi e minacce non fronteggiati adeguatamente

Assessment Valutazione del rischio

Analisi dei requisiti funzionali di un sistema e valutarne gli elementi di rischio e le contromisure da adottare in una logica costi-benefici

Training formazione per la sicurezza

Una continua azione di informazione a tutti i livelli per la sensibilizzazione sugli aspetti di sicurezza

Policy Norme di sicurezza

Stesura di norme aziendali che stabiliscono i requisiti per il progetto, lo sviluppo, la gestione e il mantenimento dei sistemi critici.

Deployment Sviluppo e realizzazione

Fase in cui i sistemi di sicurezza vengono acquisizione, realizzati, integrati, attivati e verificati

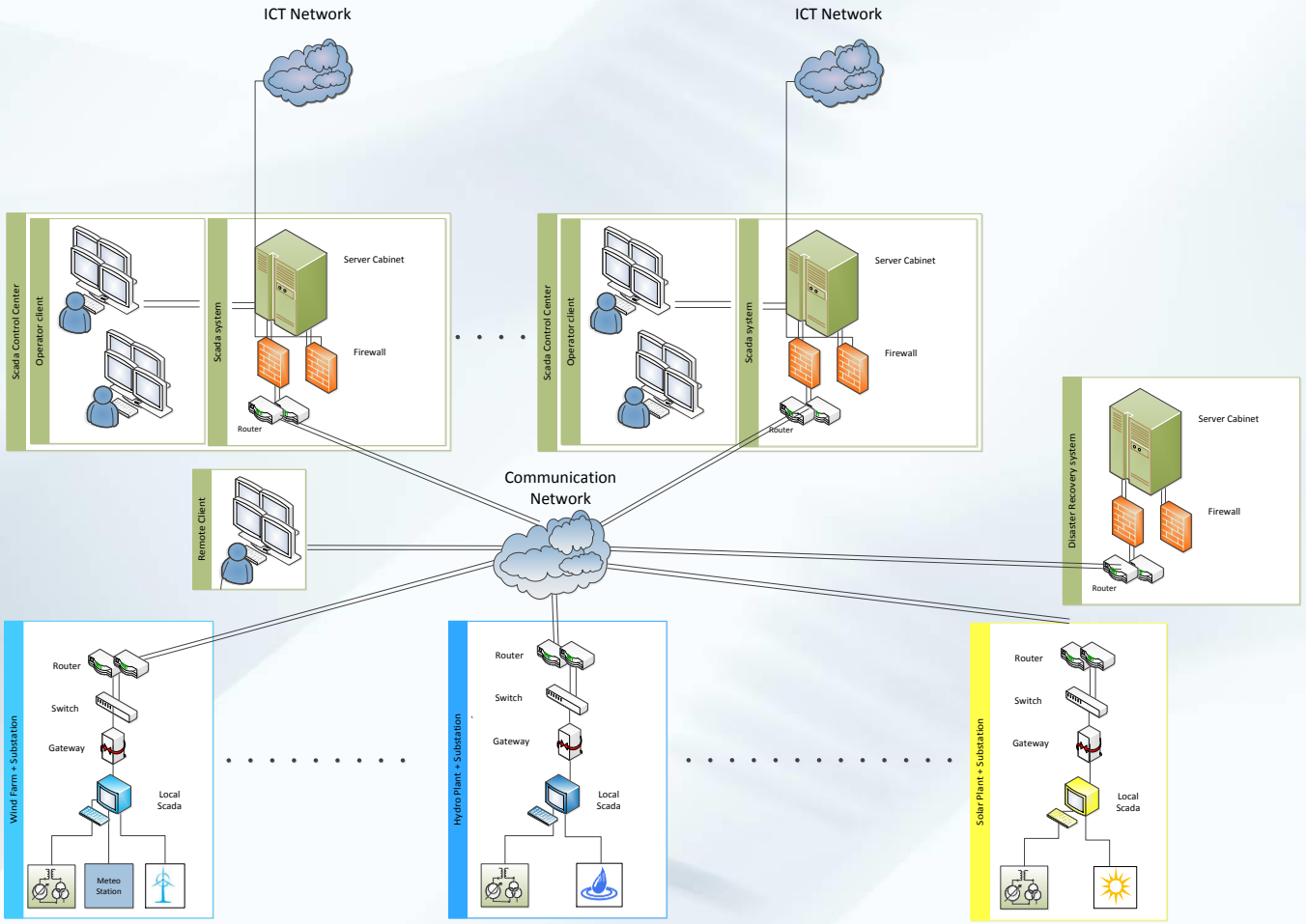
Politiche di sicurezza, domini di sicurezza

- Gruppo Enel:
  - sicurezza fisica e logica: dal mondo gestionale ai sistemi di automazione e telecontrollo
  - Separazione in **Domini di Sicurezza**.
    - Dominio gestionale
    - Dominio di telecontrollo ed automazione
      - Generazione dedicati alle fonti rinnovabili
      - Generazione da fonti fossili.
- Alcuni aspetti comuni ai due sotto-domini.
  - Sicurezza fisica (video-sorveglianza)
  - Medesima unità organizzativa.

Figure organizzazione professionali

- Suddivisione dei ruoli in tre categorie: giusto grado di separazione di competenze (SOD *Separation Of Duties*):
  - la gestione ed il controllo della sicurezza logica, assegnato al classico SOC (*Security Operation Center*) del ICT aziendale;
  - 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;
  - la gestione dei singoli sistemi in ambito locale, assegnato, volta per volta, al gruppo che gestisce il ciclo di vita dei singoli sistemi.

Il sistema: architettura



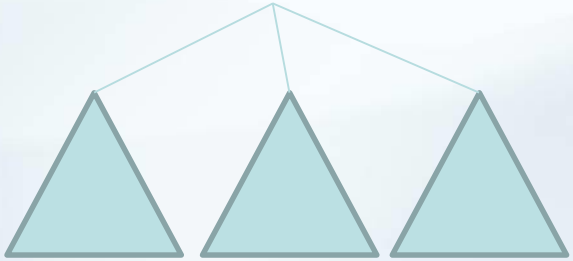
Il sistema: criticità

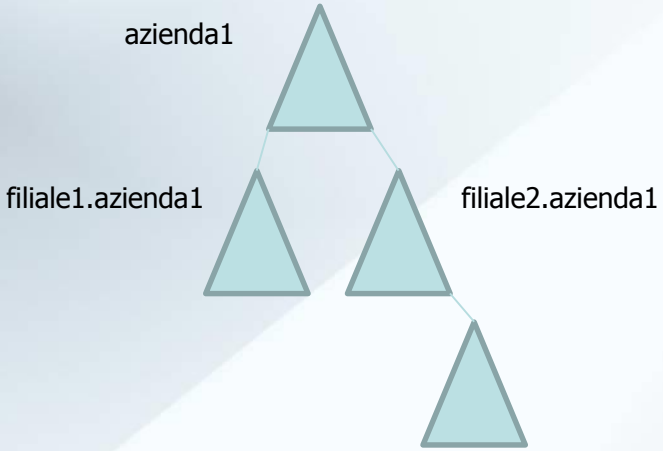
- Complessità sistema: criticità dal punto di vista della sicurezza informatica:
  - distribuzione geografica, reti locali ed elevato numero di sistemi da proteggere e controllare (server telecontrollo, server sistemi locali, postazioni operatore, ecc.);
  - necessità condivisione informazioni con altre strutture aziendali: apertura (controllata) della rete di telecontrollo verso la rete aziendale;
  - requisiti di alta affidabilità e prestazioni
  - gestione sofisticata del backup delle configurazione per ottimizzare la gestione del recupero del disastro.

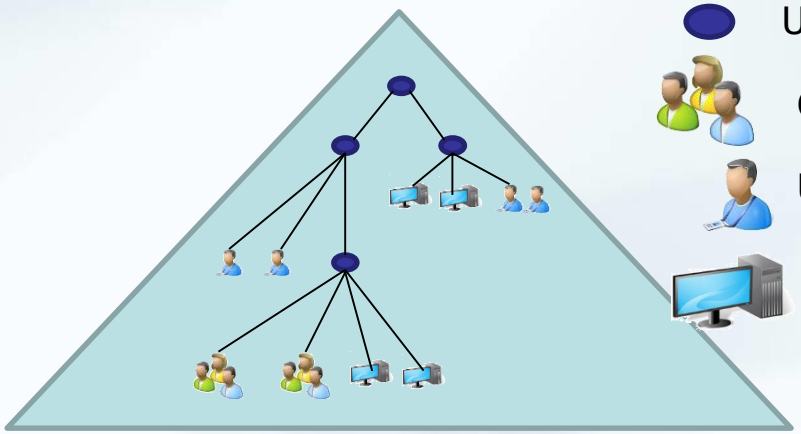
Infrastruttura di autenticazione: requisiti

- Gestire in maniera sicura e centralizzata il controllo degli accessi al sistema:
  - 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;
  - possibilità di ciascun CC di funzionare in autonomia dalla rimanente parte della infrastruttura.

Infrastruttura di autenticazione: foresta, albero di domini







Unità organizzativa

Gruppo utenti

Utente

Postazione Operatore

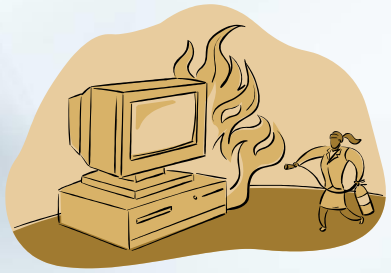
Rischi informatici di base

- Hardening: riduzione della “superficie d’attacco“
  - Hardware: disabilitare tutte le periferiche non necessarie
  - Software: disabilitare servizi, driver, protocolli non necessari
- Patching: aggiornamento costante nel tempo
  - Sistemi operativi, software di base
  - Affidabilità sistema telecontrollo: test preliminari, verifica
- Antivirus: gestione centralizzata “signature” e versione
  - Non pregiudicare corretto funzionamento sistema telecontrollo
- Vulnerability Assessment: esercitare il sistema
  - Scansione sistematica dello spazio IP assegnato
  - Test di vulnerabilità

Salvataggio e ripristino dei dati vitali

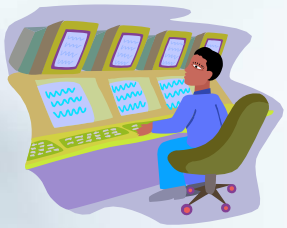
- **Locali:**
  - Sistema di backup per ogni centro di controllo (NAS, libreria o altro)
  - Archiviazione dati di configurazione (SCADA, sistemi ausiliari)
- **Recupero del disastro (Disaster Recovery)**
  - Indisponibilità intero centro di controllo periodo di tempo significativo
  - Criticità: diversi sistemi geograficamente distribuiti
  - Unico sito che dinamicamente assume le funzionalità del sistema “in disastro”: Centro di recupero del Disastro
    - salvataggio delle configurazioni vari sistemi
    - invio periodico al Centro di Recupero del Disastro
    - distribuzione dati salvati e procedura di attivazione

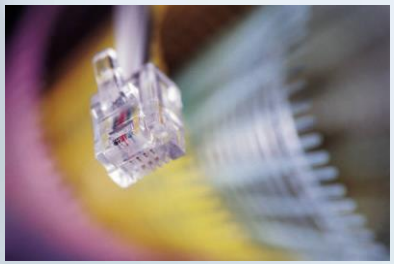
Monitoraggio perimetro di sicurezza elettronica



- Sistema di correlazione eventi
  - evento singolo innocuo, criticità se in rapida sequenza
  - rete di sonde informatiche distribuite sul perimetro elettronico e all'interno della RDT nei punti critici (interconnessioni, DMZ)
  - allarmi da sistema d'autenticazione
- Gestione incidente (*Security Incident Management SIM*):
  - Evento identificato automaticamente
  - Valutazione congiunta esperti di sicurezza e esperti applicativi
  - Pronto intervento (H24), isolamento del segmento RDT
  - Azione presa e attuata da unità di crisi

Monitoraggio apparati rete di telecontrollo





- Evoluzione *Telecommunication Management Network* (TMN) nel prossimo futuro:
  - supervisione tutti gli apparati infrastruttura di telecontrollo ed automazione: non solo router, firewall, switch, server, console, ma anche RTU e IED
  - RTU e IED: comunicazione con il sistema di monitoraggio - *Simple Network Management Protocol* (SNMP).
  - Trasferimento monitoraggio apparati telecontrollo da SCADA a sistema monitoraggio dedicato
  - Periodo di transizione in cui conviveranno i due tipi di monitoraggio.

Gestione chiavi e certificati elettronici

- Sfida più ardua
  - *Certification Authority* (CA): esistenti in ambito internet (anche Enel)
  - Ipotesi: ente terzo che sovraintende e regola il mondo elettrico, ad esempio il TSO (*Transmission System Operator*)
    - Evitare proliferazione CA, garantire interscambio dati fra operatori e TSO.
- Sistema per il telecontrollo fonti rinnovabili Enel
  - realizzazione infrastruttura gestione di chiavi e certificati dal 2012
  - obiettivo la prima connessione completamente conforme norma IEC 62351 nella prima metà del 2013.
- Utile e necessario confronto fra i fornitori di sistemi SCADA e gli operatori del mondo elettrico

Conclusioni

- Sistema di controllo tradizionale
  - sistemi centrali SCADA, centri di controllo,
  - apparati RTU installati negli impianti,
  - rete di comunicazione
- Sicurezza informatica: fondamentale per mantenere un alto grado di affidabilità del telecontrollo degli impianti.
- Non solo SCADA, RTU e TLC:
  - autenticazione, prevenzione da intrusioni, gestione aggiornamento migliaia di apparati, gestione di firme digitali, etc.
- Tecniche e tecnologie di sicurezza specifiche per il telecontrollo e l'automazione: nei prossimi anni 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 e dandoci consigli e ritorni utili ad una più esatta e completa descrizione dei temi trattati.