Università degli Studi di Padova
Facoltà di Ingegneria dell'Informazione

Corso di Laurea Magistrale in Ingegneria Informatica

Misure di cyber-security per sistemi di controllo industriale

Laureando
Alessandro Panciera

Relatore
Prof. Carlo Ferrari

Co-relatore
Ing. Massimiliano Veronesi

07/04/2014

Anno Accademico 2013/2014

Come ogni mio traguardo,
dedicato alla mia famiglia

Sommario

I sistemi di processi di automazione si sono evoluti da computer isolati e reti chiuse a sistemi interconnessi e applicazioni integrate con sistemi informatici aziendali che scambiano informazioni attraverso i vari canali di comunicazione all'interno della rete stessa, ma anche verso l'esterno.
L'aumento del livello di interoperabilità ha permesso un numero significativo di benefici, tra i quali l'aumento della sorveglianza delle attività di processo e l'integrazione tra sistemi di impianto e della sala controllo. Questi vantaggi, in particolare, permettono di abbattere drasticamente i costi complessivi di sostenimento e consentono monitoraggio remoto dei processi stessi. E' possibile definire degli standard per modelli, termini e scambi di informazione che consentono all'insieme degli operatori del sistema di condividere informazioni in modo consistente e performante.
Tuttavia, questa facilità di condivisione e la diffusione di standard commerciali hanno permesso la crescita di vulnerabilità, ad un errato trattamento dei dati sensibili e ad attacchi di hacking sempre più mirati e crescenti, introducendo in questo modo potenziali rischi all'azienda che utilizza il sistema. Essendo l'attrezzatura dei sistemi di automazione direttamente connessa al processo, la perdita di segreti commerciali e l'interruzione nel flusso di informazioni non sono l'unica conseguenza di un'eventuale breccia nella sicurezza. La potenziale perdita di produzione dovuto al blocco di sistema, danni all'ambiente, violazioni dei regolamenti e compromissione della salvaguardia degli operatori sono solo alcune delle più gravi conseguenze.
In questa tesi verranno trattati gli aspetti di progettazione e design di una rete aziendale esistente focalizzando l'attenzione sui problemi legati allo sviluppo e al mantenimento della sicurezza dell'apparato informatico della stessa, enunciandone i fattori di rischio, le conseguenze e le soluzioni proposte e adottate.

Indice

Lista delle figure

Elenco delle tabelle

1 Il sistema di controllo e le sue vulnerabilità

Prima di procedere con una definizione delle pratiche e procedure che stabiliscono la sicurezza di un DCS (Distribute Control System), è necessario fornire una descrizione sommaria dei concetti e della struttura di cui è composto il sistema di riferimento.
Nel procedere della panoramica verranno presentati con maggiore dettaglio solamente gli aspetti tecnici e architetturali che vanno ad influire considerevolmente sulla sicurezza del DCS.

1.1 Architettura e funzionalità di un sistema di controllo

Nell'ambito dell'automazione industriale, i sistemi di controllo distribuito (DCS) rappresentano la soluzione più adottata per i grandi impianti di processo (raffinerie, impianti chimici, centrali di produzione di energia, etc.). Essi svolgono in modo integrato sia le funzioni implementate nei PLC (Programmable Logic Computer), per il controllo di base, che quelle dello SCADA (Supervision Control And Data Acquisition), per la supervisione. Un DCS è una rete di controllori automatici costituito da diversi sottosistemi, tra cui quello di acquisizione e di elaborazione dei dati, in grado di scambiare autonomamente informazioni con il campo (processo o impianto) in architettura decentralizzata. In altre parole non esiste un unico computer controllore di tutto il sistema, ma diversi controllori dislocati per sezioni di impianto e opportunamente segregati, le informazioni scambiate dai sottosistemi vengono raccolti da opportune stazioni operatore. La perdita di un accentratore non inficia la capacità di mantenere controllato il sistema (tra gli altri benefici, non ne consegue lo shutdown accidentale dell'impianto). L'architettura tipica e semplificata di un sistema di controllo distribuito si compone come in Figura 1 e si basa su una divisione a livelli definita dallo Standard ANSI\ISA 95[1] e sull'esperienza operativa di Yokogawa, azienda di rifermento per lo sviluppo della tesi.

Livello 0

Partendo dai dispositivi alla base della struttura informatizzata troviamo le interfacce che comunicano con il campo direttamente, tramite le schede elettroniche di acquisizione e comando, o con i 'bus di campo', i quali scambiano informazioni con i trasmettitori e gli attuatori[2]. Su questo livello viaggiano l'insieme delle variabili di processo (process device) e delle variabili di controllo che rappresentano l'impianto oggetto del sistema di controllo. E' uno strato che non verrà trattato nell'analisi della cyber-security di impianto essendo estraneo alla logica di rete, ma collegato direttamente al proprio controllore (dispositivo di livello 1) responsabile del controllo.

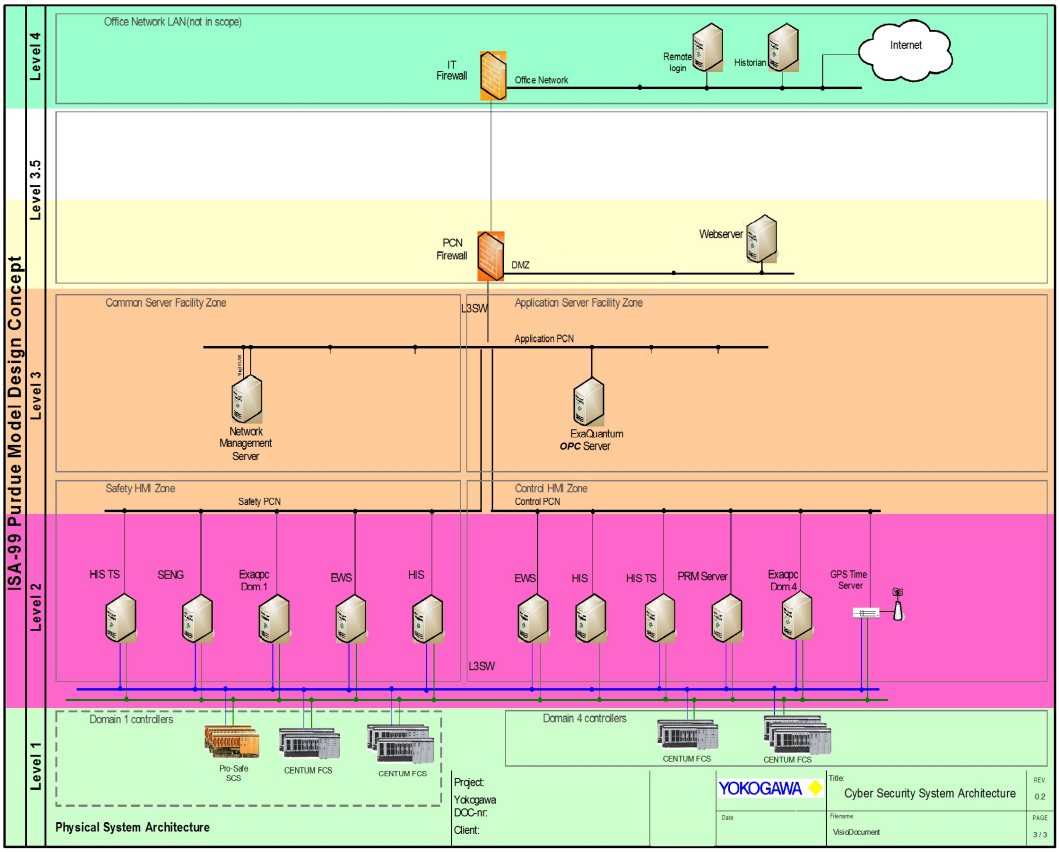


Figura 1: Architettura di un DCS;

Livello 1

In questo punto della rete l'indirizzamento e la comunicazione fra i controllori avviene nei bus di I\O tramite i primi livelli dello standard del modello ISO\OSI (Physical e Data Link layer). Su questa architettura di base si appoggiano tutti i protocolli (proprietari e non) che contraddistinguono i dispositivi attualmente nel mercato.
Alcuni prodotti commerciali, come quelli sviluppati da Siemens, hanno raggiunto un grado di diffusione nei vari impianti sparsi per il globo tale da proporsi come standard di comunicazione. Nonostante le conseguenze di abbattimento dei costi e di integrazione tra i dispositivi che una standardizzazione di questo tipo porterebbe nel mercato, è evidente che la conoscenza diffusa di un protocollo offre, ad un eventuale hacker, informazioni maggiori sul sistema, sia per produrre un attacco, sia per celare la propria presenza.
Nel paragrafo seguente viene presentato un attacco ad impianti di questo tipo che sfrutta in particolar modo le debolezze dei prodotti Siemens (nel 2012 sono stati identificate più di 40 vulnerabilità legate ai prodotti sviluppati da

questo vendor[3]).

Livello 2

Al di sopra dei controllori vi sono le workstation, identificati come HMI (Human/Machine Interface) o HIS (Human Interface Station), quest'ultime svolgono il ruolo di supervisori sfruttando le strutture dati e il database condiviso e distribuito fra i componenti della rete. L'accesso ai dati dei livelli inferiori permette la storicizzazione a lungo termine per generare strategie avanzate di controllo del processo (APC).
Switch e router all'interno del network di processo hanno caratteristiche particolari per l'instradamento e la gestione dei conflitti con il fine di ridurre il carico e massimizzare la disponibilità della comunicazione all'interno della CAN (Control Area Network). Una configurazione tipica di questa tipologia di reti prevede la ridondanza dei bus di comunicazione e delle apparecchiature di rete (i.e. nel bus 1 circola la comunicazione tra controllori e supervisori, nel bus 2 si svolge lo scambio dati lasciando una porzione della banda come backup per il bus 1).
Tuttavia un sottodimensionamento del traffico della rete, una configurazione superficiale dei dispositivi o la presenza di path critici possono agevolare il blocco di porzioni o, ancor peggio, della totalità del processo. Un attacco DoS (Denial of Service), in presenza di questo tipo di errori di progettazione, potrebbe essere facilitato dalla formazione di particolari anelli per paralizzare il traffico di rete e, di conseguenza, l'intera comunicazione fra dispositivi in campo.

OPC

L'OPC (Ole for Process Control, o più recentemente rinominato dalla OPC Foundation[1] in Open Platform Communication) è uno standard nell'ambito dell'automazione industriale da quando le funzionalità di supervisione vengono implementate su workstations gestite da noti sistemi operativi commerciali.
Si tratta, di fatto, di un pacchetto software di *middleware* a supporto dell'architettura distribuita dei sistemi di controllo per la diffusione dei dati, questi verranno poi utilizzati da applicazioni che possono accedere alla stessa rete ethernet. In particolare sono disponibili diversi formati a seconda che il dato sia di tipo numerico (OPC DA utilizzato per i dati di processo) o stringa (OPC AE, utilizzato per allarmi ed eventi); infine esiste anche la

[1] OPC Foundation [4](Object Linking and Embedding for Process Control Foundation) è un consorzio industriale che genera e mantiene standard per la connettività di dispositivi nell'ambito dell'automazione industriale e di sistemi riferiti all'ambiente di controllo dei processi. Lo standard specifica la comunicazione dei dati, degli allarmi e eventi, dello storico fra i sensori, la strumentazione, i controllori, i pacchetti software e i dispositivi di notifica.

condivisione via OPC di dati non real-time ma già storicizzati. In ogni caso il flusso delle informazioni è sempre quello che prevede il funzionamento di un OPC-Server (eventualmente ridondato) in grado di convertire in formato OPC i dati disponibili sulle stazioni operatore. I pacchetti superiori non devono far altro che integrare la funzionalità di OPC-Client in modo da poter attingere dal server dati di interesse per l'espletamento della loro funzione.
Lo standard prevede che ad ognuno venga associato il Timestamp e un Quality-Code indicativo della bontà del valore conseguente al processo di comunicazione. Talvolta il fornitore del DCS provvede al creare librerie aggiuntive di funzioni utili per poter prelevare i dati dal proprio sistema in modo più agevole ed efficace[5], tuttavia il protocollo possiede dei deboli meccanismi di autenticazione che lo rendono un ancor più facile bersaglio.
Le specifiche dell'OPC di cui tratteremo da questo punto in avanti saranno basati su tecnologia DCOM[6] sviluppata da Microsoft per adattarsi in modo trasparente alla famiglia di sistemi operativi Windows.

Livello 3 e successivi

Salendo la struttura di un ulteriore livello, troviamo tutta la componentistica software che, tramite tool realizzati *ad hoc*, permettono il monitoraggio e la gestione dei sistemi del livello inferiore. I dispositivi che possiedono questi strumenti di elaborazione dati, tipicamente, possono interagire anche con la rete aziendale. La posizione di confine tra rete di campo e rete d'ufficio rende queste macchine un obiettivo allettante per eventuali attacchi atti a diffondere i malware nei livelli sottostanti e infettare il processo vero e proprio.
I dispositivi di questo livello, tipicamente macchine server, fanno parte di quella categoria di dispositivi che, grazie alle loro capacità computazionali e software installato, permettono l'utilizzo di un'ampia gamma di *exploit* tipici delle reti aziendali utilizzati nelle web-application come SQL Injection e bug di Cross-Site Scripting (XSS). La connessione a queste HIS avviene, tipicamente, a causa di una configurazione non completamente sicura della DMZ[2] con conseguenze dirette sulla sicurezza dell'ambiente della rete di controllo.

1.2 Caratteristiche dei malware e delle vulnerabilità nei sistemi di controllo

Differenziandosi dalle normali rete IT (Information Technology) sparse per il globo, i DCS sono caratterizzati, come accennato nel capitolo precendente,

[2]DMZ (DeMilitarized Zone): un segmento isolato di LAN raggiungibile sia da reti interne sia esterne, ma caratterizzata dal fatto che gli host posizionati sulla DMZ hanno possibilità limitate di connessione verso la rete interna. Nel nostro caso la DMZ separa la rete IT dalla PCN.

Anno	Vulnerabilità
2005	1
2007	3
2008	5
2010	11
2011	64
2012	98

Tabella 1: Vulnerabilità registrate negli anni[3];

da debolezze diverse del sistema che, tuttavia, sono una diretta conseguenza delle falle legate all'ambiente IT.
Come conseguenza del boom del networking degli anni 90, sempre più i sistemi SCADA dovevano integrarsi con le reti aziendali fornendo a quest'ultime informazioni sullo stato e sull'andamento dei processi. Nello spirito dell'economia e nella necessità di avere in tempi brevi queste informazioni, i componenti software e hardware offerti nel mercato per l'ambito IT vennero riadattati per offrire le funzionalità nei DCS; in particolare la struttura su cui si appoggiano le reti d'ufficio odierne di questi impianti viene affiancata e, sotto opportune condizioni e segregazioni, comunica direttamente con la rete di controllo di processo. Con questa apertura del sistema orientata verso l'esterno, tutte le garanzie e convinzioni offerte dai sistemi chiusi svaniscono. La rete DCS si trova, a questo punto della sua evoluzione, strutturata con tecnologie di rete e software tipicamente impreparati a gestire i pericoli derivanti dall'interoperabilità con il traffico esterno. Sempre più troviamo sistemi che utilizzano gli standard di comunicazione (TCP\IP) tipici delle reti IT, includendo database SQL e browsing web per la visualizzazione delle informazioni nei thin-client, senza che questi vengano trattati con le accortezze del caso. Mentre i firewall mantengono le loro caratteristiche, sempre più applicazioni richiedono accessi alla CAN, portando con esse la richiesta di una nuova connessione e, di conseguenza, una nuova breccia nella rete di processo.
Una scarsa sensibilità verso le tematiche di sicurezza informatica può portare ad alcune errate scelte progettuali tra cui le piu diffuse sono:

- Assenza di antivirus e update sever;
- Controllori configurati per il real-time e non per il networking;
- Noncuranza dei punti di accesso (primari e secondari) della rete;
- Mantenimento prolungato di connessioni aperte;
- Nessun blocco sugli ingressi dei supporti di massa;

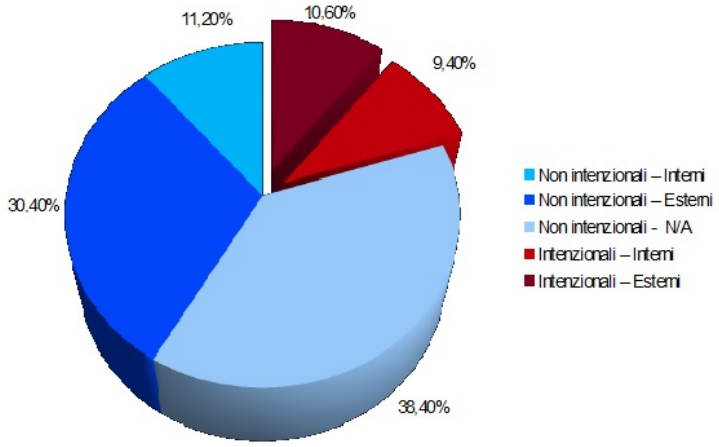


Figura 2: Grafo percentuale della tipologia di incidenti nei DCS(2011)[7];

Un'analisi effettuata dalla *Positive Technologies* illustra una panoramica della situazione del livello di protezione dei centri industriali mondiali. Più del 40% dei sistemi SCADA sono insicuri e di facile accesso dalla rete, di questi più di un terzo delle debolezze del sistema sono dovuti ad errori interni di configurazione o sull'utilizzo di password di default.
Con il worm Stuxnet (le cui caratteristiche vedremo più avanti) l'attenzione sulla tematica di sicurezza ha avuto un aumento considerevole; la scoperta di nuove vulnerabilità, con crescita esponenziale a partire dal 2010, è una chiara testimonianza di questa nuova tendenza. Il report fornisce anche una classificazione del tipo di vulnerabilità che affliggono questi sistemi, sui tempi che intercorrono tra l'individuazione dell'exploit e la sua patch e sulla classificazione dei rischi. Interessante notare tra le statistiche la percentuale di ICS (Industrial Control System) accessibili direttamente da Internet (di cui l'Italia, in seconda posizione, ne copre il 6% sul totale mondiale) di cui il 42% viene segnalato come vulnerabile e solo il 17% ne è dichiarato sicuro. La maggior parte dei difetti di sicurezza individuati sono dovuti a errori di configurazione (tipicamente password di default e restrizioni degli accessi) e ricoprono circa il 40% delle vulnerabilità, seguita da latenza nell'installazione di patch e da errori di natura più complessa.
Questi, e molti altri, difetti di progettazione, uniti ai vari bug dei software conosciuti o meno (*zero-day attack*[3]), hanno offerto negli ultimi anni delle facili porte di accesso per eventuali attaccanti esterni e interni. Osservando

[3]Zero-day attack: attacco che sfrutta la finestra temporale di vulnerabilità che esiste a partire dal momento in cui una vulnerabilità viene sfruttata e termina quando lo sviluppatore pubblica una patch di protezione da quell'attacco.

la Figura 2 si può comprendere come i vari *flaws* individuati non compromettano la sicurezza del sistema solamente dal mondo esterno e della criminalità informatica, ma anche la fragilità del sistema stesso al suo interno, ad opera degli stessi operatori (ben intenzionati), viene condizionata da questa situazione.
L'analisi di alcuni dei maggiori worm che si sono presentati negli anni, affliggendo intenzionalmente, o per diffusione spontanea, le reti industriali di tutto il mondo, risulta tuttavia essere molto utile per capire dove e come proteggere il proprio sistema con conseguenze dirette anche sul contenimento degli incidenti interni. Partendo da esempi reali di disastri economici e ambientali, attribuiti all'influenza dei virus, e evidenziando i motivi e gli errori progettuali che hanno portato alla loro diffusione nei DCS, si può iniziare a porre le basi da cui partire per parlare di cyber-security e di politiche di salvaguardia.

2003 - Slammer

SQL Slammer Worm (W32.SQLExp.Worm[8]) è stato uno dei primi worm ad affliggere i DCS connessi alla rete con un attacco di tipo DoS. Sfruttando un bug di buffer overflow, colpiva i sistemi con il servizio in esecuzione Microsoft SQL Server 2000 e Microsoft Desktop Engine (MSDE) 2000. Slammer inviava a ripetizione 376 bytes alla porta UDP 1434 destinata al servizio SQL Server Resolution intasando la rete.
Un esempio reale, che ne testimonia la pericolosità, si riferisce all'infiltrazione del worm nella rete privata della centrale nucleare di Davis-Besse in Ohio nel Gennaio del 2003[9]. In questo caso Slammer mise fuori uso il sistema di monitoraggio della sicurezza per 5 ore. Nonostante la protezione della rete verso le minacce esterne da parte del firewall, il worm è riuscito a bypassarlo penetrando nella rete interna tramite una linea non completamente protetta alla quale si era collegato un ignaro operatore commerciale. Dall'intranet, il worm si è diffuso nella rete d'impianto dove ha trovato dei server Windows non aggiornati alle ultime patch diffuse.
Secondo quanto riportato nella documentazione dell'incidente, gli operatori della sala di ingegneria non avevano installato le patch per coprire la vulnerabilità MS-SQL su cui faceva leva Slammer per la sua infezione, nonostante il rilascio dell'aggiornamento nei precedenti sei mesi.

2008 - Conficker

Conficker, come Slammer, rientra tra quei worm sviluppati per il mondo IT che hanno avuto pesanti conseguenze nel mondo dei DCS. Virus scoperto nel Novembre 2008 che mira a dispositivi con sistema operativo Microsoft Windows, utilizza un *exploit* sul servizio che permette il controllo dell'esecuzione di codice in remoto (RPC), per infettare le macchine[10].

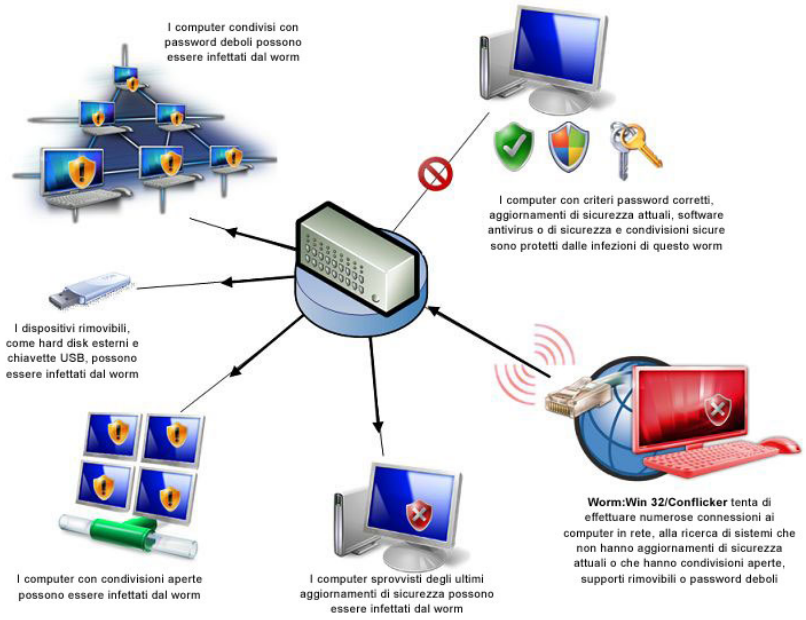


Figura 3: Caratteristiche di diffusione del Conficker[11]

L'infezione si propaga bombardando gli altri pc nel dominio, vedi Figura 3, sfruttando debolezza nelle password(*dictionary attack*[4]) per ottenere un escalation dei privilegi. Ottenuti i privilegi di amministratore, si diffonde sulle risorse di rete condivise fino a creare una botnet difficilmente individuabile a causa della cifratura avanzata della comunicazione (hashing SHA in cascata ad un RC4 a 512 bit o, in alternativa un MD6) e perché incorpora dei meccanismi di autodifesa per disabilitare i servizi di antivirus e aggiornamento.
Tuttavia, per la natura aggressiva di Conficker, il traffico di rete e gli accessi alle workstation sono pesantemente rallentati, primo sintomo che permette l'individuazione dell'infezione.
Attualmente esistono delle varianti (A,B,C,D e E) che hanno perfezionato e corretto il worm nel corso degli anni, adattandolo a mano a mano che nuove patch venivano rilasciate.
Ancora oggi, se almeno una macchina nel sistema non presenta l'aggiornamento Windows MS08-067 installato, il sistema intero è vulnerabile al diffondersi di questo virus.

[4]Dictionary attack: tecnica di attacco alla sicurezza di un sistema informatico mirata a rompere un codice cifrato o un meccanismo di autenticazione provando a decifrare il codice o a determinare la passphrase cercando tra un gran numero di possibilità e tramite una serie continuativa e sistematica di tentativi di inserimento della password.

2010 - Stuxnet

A differenza dei virus precedentemente elencati, Stuxnet si impone come primo worm concepito per attacchi mirati ai sistemi di controllo industriali e con la capacità di modificare il codice dei PLC[5]. In particolare, la storia dei principi di cyber-sicurity pro-attiva nei DCS, che vedremo a partire dal prossimo paragrafo, nasce in risposta all'avvento di Stuxnet.
Caratterizzato da una complessità del codice considerevole (tornato a far parlare di se con lo scandalo sul *cyber warfare* ad opera di Edward Snowden che conferma la paternità del virus ad opera del governo degli Stati Uniti in collaborazione con l'Intelligence Israeliana[12]), dalle dimensioni maggiori rispetto agli altri malware (circa 500 KB), ed essendo il primo della sua specie, richiede, per la comprensione delle debolezze dei DCS, un'analisi tecnica maggiore.
Stuxnet faceva leva su un ampia gamma di flaws e tecniche di hacking per entrare nel sistema e diffondersi nei vari livelli della rete:

- **4 *zero-day vulnerability***:
  - MS10-046 pratica un exploit sull'auto detection del sistema per la replicazione nella variante da dispositivo USB verso il PC, e nel caso opposto (da PC verso USB), permette il propagarsi dell'infezione;
  - MS10-061 permette la diffusione in LAN tramite flaw nella *Spooler* delle stampanti condivise con Windows;
  - MS10-092 e MS10-073 si occupano di ottenere un escalation dei privilegi tramite un exploit del Task Scheduler che permetteva di mandare in esecuzione il virus, nasconderlo all'analisi del sistema e, contemporaneamente, farlo eseguire con privilegi superiori.
- **Diffusione tramite RPC come il Conficker**: sfrutta gli stessi exploit del processo tramite il protocollo SMB (Server Message Block).
- **Installazione di rootkit[6]e codice per l'hooking[7] in Windows**: Stuxnet ha la capacità di nascondere i propri file copiati nelle unità rimovibili proprio grazie a queste tecniche di hacking.

[5]Programmable Logic Controller (PLC): controllore programmabile utilizzato per l'automazione dei processi elettromeccanici, come il controllo dei macchinari delle linee di montaggio di fabbriche, raffinerie e settori industriali in genere. Un PLC è un esempio di un sistema *hard real-time*.

[6]Rootkit: software malevolo progettato per celare l'esistenza di processi o programmi ai normali metodi di *intrusion detection* e perpetrare l'accesso al dispositivo tramite l'ausilio di *backdoor*.

[7]Hooking: insieme di tecniche utilizzate per alterare i comportamenti di O.S. e applicazioni intercettando funzioni, messaggi o eventi software.

- **Installazione di rootkit e infezione nei PLC**: per la prima volta nella storia dei malware vi è un tentativo mirato di prendere controllo dei PLC del processo. Il passaggio per ottenere il controllo passa, prima di tutto, tramite la sottomissione di macchine Windows su cui è eseguito il software WinCC[8]. Quando il virus trova un sistema di questo tipo, cerca di connettersi al suo database tramite una password hardcoded[9] memorizzata nel WinCC software. Una volta connesso vengono effettuate due azioni; per primo viene inviato del codice SQL malevolo al DB per permettere a Stuxnet di trasferirsi in quel dispositivo. Successivamente modificherà le *view* esistenti aggiungendo codice in modo da essere eseguito ad ogni accesso.
  Il passo successivo consiste nell'attacco diretto al PLC S7 Simatic (prodotto Siemens) che si adopera di monitorare, controllare ed eseguire comandi sul processo industriale. La libreria s7otbxdx.dll è responsabile della gestione dei blocchi di codice del PLC; rimpiazzando quest'ultimo con il file .dll del virus, Stuxnet è in grado di monitorare esso stesso la scrittura e lettura dei blocchi nel PLC, infettarlo con dei propri blocchi di codice e di mascherare la propria infezione nello stesso.

Alla lista si aggiungono anche particolarità che non fanno propriamente parte delle attività di hacking, ma che comunque meritano di essere nominate per dimostrare l'unicità del malware sviluppato. Si trattano delle tecniche di propagazione in rete tramite routine di *P2P*(*peer-to-peer*) per l'aggiornamento, il furto di certificati legittimi, la presenza di un interfaccia per i comandi e il controllo del virus e la capacità di fallire nel caso in cui le operazioni di replica avessero allarmato il sistema rivelando la presenza[13].
Il bilancio dei dispositivi che hanno subito l'infezione da parte di Stuxnet (circa 100.000 computer distribuiti su 22 sistemi industriali) non è significativamente elevato come la diffusione che hanno raggiunto Conficker e Slammer (più di 15 milioni di dispositivi), tuttavia la particolarità dei metodi di infezione e la capacità di rimanere nascosto alle tecniche di difesa del sistema lo rendono un interessante oggetto di studio per lo sviluppo di sistemi industriali più sicuri e per la revisione delle norme e procedure di sicurezza. Da segnalare la diffusione del virus concentrata nel Medio Oriente, con la conseguente manomissione di svariati siti di lavorazione di materiale radioattivo (Uranio in particolare) e ingenti danni socio-economici.

[8]SIMATIC WinCC: sistema SCADA e HMI della Siemens. Utilizzato per monitorare e controllare il processo. Utilizza Microsoft SQL Server per il logging e programma di interfaccia.

[9]Hardcoded: caratteristiche di un programma, definite e fissate al momento della creazione dell'eseguibile. Modificabili solamente tramite operazioni di reverse engineering.

2011 - Duqu

Si suppone nato dallo stesso codice sorgente di Stuxnet, Duqu si propone come nuova generazione di malware *Stuxnet-like*. A differenza del precursore, questo virus si pone con un obiettivo totalmente differente, quello di raccogliere dati sensibili e registrare le attività da infrastrutture industriali e produttori di sistemi. Il fine è quello di raccogliere informazioni sul design che potrebbero aiutare ad orchestrare un futuro attacco, incluso gli impianti del sistema di controllo industriale.
Come mostrato in Figura 4, il worm inizia il proprio insediamento nel primo dispositivo attraverso un 0-day exploit di Microsoft Word. Il proseguire dell'installazione è un processo lungo ma accurato e discreto che si pone l'obiettivo di non lasciare tracce del proprio passaggio ed offuscare la propria presenza. Durante il processo di caricamento di Duqu, solo la parte che risiede in memoria risulta essere decriptata. Il resto della diffusione sfrutta gli stessi exploit e tecniche di hacking e mascheramento precedentemente viste con Stuxnet. Duqu, nel suo ciclo di vita, cerca di comunicare fornendo

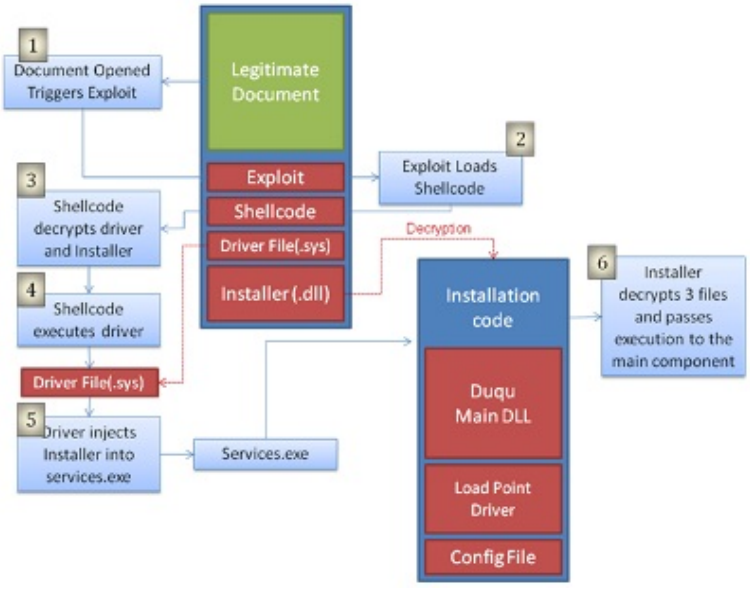


Figura 4: Processo di installazione di Duqu[14];

informazioni e aspettando comandi, la messaggistica verso l'esterno avviene tramite incapsulamento nella porta 80 (HTTP) e 443 (HTTPS), mentre le comunicazioni interne sono fatte tramite protocollo SMB sfruttando un architettura Peer-to-peer. Quest'ultima si adopera di incanalare la comunicazione verso l'esterno da una solo PC infettato in una zona poco controllata della rete aziendale.
Il pacchetto incapsulato contiene un protocollo specifico di Duqu simile al

TCP e i dati al loro interno vengono cifrati con AES-CBS, poi compressi usando LZO, e in seguito compressi una seconda volta utilizzando un algoritmo personalizzato.
Notizie della presenza del malware e di sue varianti sono state segnalate in Germania, Belgio, Filippine, India e Cina. Mentre di Stuxnet è stata scoperta la paternità, Duqu risulta ancora oggi di origine sconosciuta.

2012 - Flame

Flame fa parte della categoria di malware dedicata allo spionaggio industriale più che al *cracking* di sistemi; molto simile come struttura a Duqu e Stuxnet, si differenzia da loro per la complessità del codice (definito come 20 volte più complicato[15]) e per le considerevoli dimensioni rispetto a tutta la categoria (circa 20 MByte).
La natura modulare, con la possibilità di controllo remoto e di estensione delle funzionalità, suggerisce che il malware fosse stato progettato per mantenere la minaccia nei sistemi hackerati per lunghi periodi di tempo. Il bersaglio di questo worm rimangono i sistemi con prodotti Microsoft, condivide con Stuxnet il sistema di replicazione nella rete (exploit dello Spooler, Autorun e Shortcut di Windows) alla quale ne aggiunge un ulteriore basandosi sul recupero delle credenziali dal Domain Administrator[10].
Il design di Flame punta sul furto di informazioni sensibili attraverso file audio (anche conversazioni Skype), screenshot, keystroke logging[11] e bluetooth.
Le funzionalità di Flame però non si fermano qua, grazie ad un modulo di Scripting Interpreter vi è la possibilità di aggiungere da remoto nuove funzionalità (strutturato come un *app-store*[16]), cifrare la comunicazione tramite un modulo di Secure Shell Communication e utilizzare il DB Server, Web Server e Proxy installati al suo interno (per dettagli tecnici più specifici consultare l'analisi tecnica della CrySyS Lab[17]).
Flame è stato individuato per la prima volta in Ungheria e nella zona Medio Orientale, come per Stuxnet, colpendo raffinerie petrolchimiche.
La Symantec, nel proprio documento tecnico[15] ha rilasciato alcune precauzioni e linee guida (*best practices*) per difendere il sistema che coinvolgono il firewall (*dropping* di default di tutte le connessioni verso l'interno), il rafforzamento delle password e della gerarchia dei privilegi, l'hardening (disabilitare l'AutoPlay e modalità Read-Only), aggiornamenti (soprattutto a quelle macchine critiche che offrono servizi attraverso il firewall: HTTP, FTP, mail e DNS server), training e quant'altro.
Tuttavia, come già discusso in precedenza, molti accorgimenti elencati non

[10]Domain Administrator (DA): gruppo logico di computer con sistema operativo Microsoft Windows che condividono un database di directory centrale; contiene gli account utente e informazioni di protezione per le risorse in tale dominio.

[11]Keystroke logging: attività con la quale si monitora la sequenza dei tasti premuti in un certo intervallo di tempo.

riescono ad essere applicati ad una realtà più critica come quella dei sistemi industriali; ad esempio l'isolamento di un dispositivo talvolta non può essere fatto affatto, l'installazione di alcune patch possono andare ad influire negativamente sul processo e alcune macchine con funzionalità da client per la rete di controllo fungono da server per la rete di processo non potendo limitare servizi e porte.
Nella sezione successiva vedremo alcuni dei principi e delle norme di comportamento sulla sicurezza di questa diversa categoria di sistemi di rete.

2 Principi di Cyber-Security

Come discusso nel capitolo precedente, i sistemi industriali possono essere bersaglio dello stesso tipo di cyber-attacchi subiti dalle reti general-purpose, e il semplice impiego delle contromisure concepite e sviluppate per queste ultime non può rappresentare una soluzione di sicurezza efficace. La diversità nasce principalmente, oltre che dalla tipologia di software utilizzato, da una differenza nella priorità che si attribuisce ai requisiti principali di *safety*[12] e *security*:

- **availability**, la disponibilità all'accesso da parte di altre entità;
- **integrity**, la salvaguardia dell'integrità dell'informazione;
- **confidentiality**, la garanzia che l'informazione non sia disponibile ai non autorizzati;

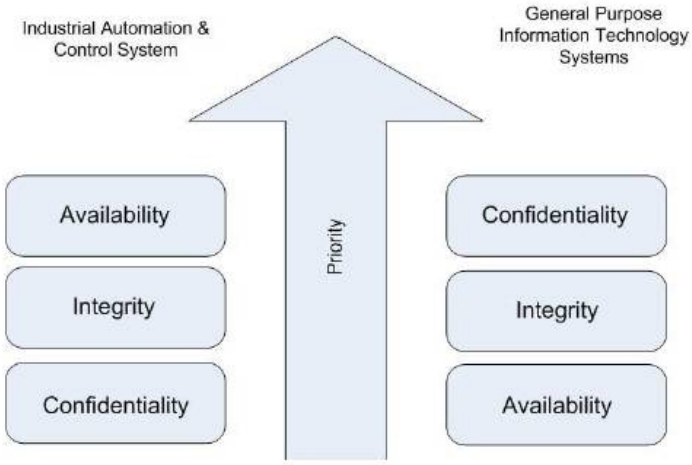


Figura 5: Differenze di priorità tra IT e ICS;

Quando gli ICS erano ancora sistemi chiusi la riservatezza delle informazioni circolanti nella rete non risultava essere un problema; spesso e volentieri il sistema non veniva tutelato da questo punto di vista concentrandosi sulla robustezza dell'ICS. Con le problematiche di riservatezza e l'hacking del sistema, la confidentiality sui dati risulta acquisire un importanza maggiore

[12] safety: nell'ambiente industriale viene inteso come quello stato di funzionamento dell'impianto in cui prevale la sicurezza degli ambienti, del personale e garantisce la continuità di produzione. Nel caso degli ICS viene spesso assicurata a discapito della sicurezza dell'infrastruttura informatica (e i dati in esso contenuti) che viene definita con la terminologia di *security*. Tuttavia i due termini nella realtà pratica hanno una forte componente di correlazione.

	IT	ICS
Affidabilità	Guasti occasionali tollerati	Interruzione intollerabile
Conseguenze di rischio	Perdita di dati	Danni alla produzione, persone e strumentazione
Performance	Richiesta throughput elevata, ritardi e jitter tollerati, dispositivi con alta capacità computazionale	Throughput moderato tollerato, preoccupazione per i ritardi, dispositivi customizzati e con capacità computazionale limitata
Recovery	Reboot, le procedure di safety non sono mandatorie	Richiesta di tolleranza ai guasti, obbligatoria l'analisi dei rishi
Security	Poca separazione tra internet e intranet, priorità sulla sicurezza del server centrale	Sicurezza fisica, isolamento tra rete IT e rete di impianto, priorità sulla stabilità dei dispositivi
Upgrade	Aggiornamenti semplici e automatizzati	Aggiornamenti di software eseguiti con cautela (spesso dopo essere stati testati) e effettuato da utilizzatori specializzati
Comunicazione	Protocolli standard	Sistemi con protocolli misti (proprietari e standard)
Tempo di vita dei componenti	3-5 anni	15-20 anni per i controllori, 5-8 anni per tutto il resto
Accesso ai dispositivi	Tipicamente in luoghi facilmente accessibili	Posizionati generalmente in zone remote

Tabella 2: Differenze di comportamento tra ambiente IT e ICS;

e una correlazione più stretta anche con le caratteristiche di disponibilità e integrità dell'informazione[18].
Le caratteristiche di sicurezza che vedremo qui di seguito si rifanno alle norme della guida NIST[13][20] che considerano sistemi generici, ma che, a differenza dell'approccio ANSI/ISA 99, offre della documentazione aggiuntiva nei temi di *risk analisys* e affrontano esplicitamente la sicurezza della rete di processo.

2.1 Information Security Management System

Information Security Management System (ISMS) è un processo iterativo che coinvolge tutti gli aspetti di un'organizzazione industriale (spesso si parte dalla versione stilata per il mondo IT per poi adattarla all'ambiente di processo). Viene utilizzato come modello di base per l'evoluzione del sistema e della sicurezza su di esso sviluppata; come più volte sottolineato, la sicurezza è un processo continuo che richiede un'attenta sorveglianza e ag-

[13]NIST (National Institute of Standards and Technology) è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie. Fa parte nel Dipartimento del Commercio e il suo compito è la promozione dell'economia Americana attraverso il lavoro con l'industria per sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio[19].

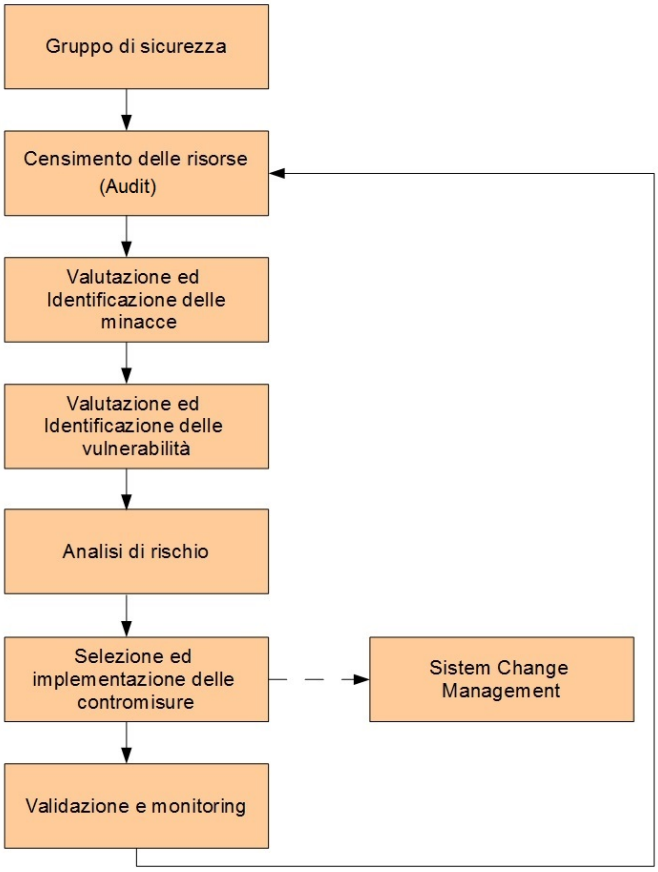


Figura 6: Procedura per la costruzione di un ISMS;

giustamenti progressivi.
Un ISMS moderno deve prevedere due livelli complementari di intervento. Il livello di sistema, luogo in cui si collocano tutte le tecniche di analisi e gestione del rischio che richiedono un alto grado di astrazione; a questo ambito appartengono anche le metodologie e gli strumenti di definizione delle politiche di sicurezza e le soluzioni concepite per la relativa gestione. Un'idea generale delle norme e procedure di comportamento di questa prima fase di definizione dell'ISMS vien presentata dalle sezioni di *Audit*, *Analisi e valutazione dei rischi* e *Policy*. Queste fasi dovrebbero essere il più possibile indipendenti dalle tecnologie utilizzate per segregare la rete e dall'architettura utilizzata, dovrebbe omettere le procedure di implementazione e di processo.
A livello di componente si trovano invece le contromisure che possono essere adottate per l'implementazione delle politiche di alto livello, ovvero i meccanismi di prevenzione, identificazione e reazione. Questa parte viene trattata

con maggior specificità nella parte dedicata alla soluzione della rete in esame; per quanto riguarda la parte sul *Security Control* relativa a normative e preoccupazioni generali trattate sul NIST viene fatta una panoramica sui punti saldi delle apparecchiature di rete su cui gli enti di sicurezza globali si stanno focalizzando per rispondere al bisogno crescente di sicurezza nelle reti di impianto.

2.1.1 Audit e definizione di policy

Il primo passo nella creazione di normative e di un sistema orientato alla sicurezza è quello di condurre una verifica dei sistemi di controllo per capire esattamente come è strutturata la sicurezza attuale e dove le vulnerabilità potrebbero presentarsi. Prima di stabilire le politiche e le specifiche di sicurezza aziendali per la protezione di un ICS, si passa attraverso una fase, denominata di *audit*, in cui si procede alla creazione di una serie di liste dettagliate di quali dispositivi, quali protocolli e applicazioni sono in esecuzione nella rete (*whitelisting*), chi ha accesso a questi device, da dove e quali sono le azioni su di essi eseguibili e gli accessi consentiti a questi utenti.

Strategia Deny-All

Una buona politica con cui vengono create le regole di base è quella di consentire l'accesso minimo ai dispositivi e di proibire tutti gli altri. Le norme pratiche stabilite nel Security Control con questo tipo di policy applicate limitano lo spazio di manovra per qualsiasi accesso illegale al sistema. Anche nei firewall e nell'hardening dei dispositivi viene adottata questo tipo di strategia.

2.1.2 Analisi e valutazione di minacce, vulnerabilità e rischi

Questa fase raggruppa elementi tra di loro correlati in serie. Si procede con la definizione di tutte le minacce che potrebbero affliggere il sistema, le possibili vie di accesso e la classificazione dei danni che questi ingressi potrebbero causare. Da questa base di partenza vengono affrontate le analisi delle vulnerabilità; la descrizione del sistema (topologia, protocolli, moduli sw\hd installati ecc.) è integrata con quella delle vulnerabilità conosciute, in termini di prerequisiti per il loro sfruttamento e relative conseguenze. Lo strumento di analisi acquisisce la descrizione e identifica gli attacchi che possono essere condotti sfruttando le vulnerabilità presenti.
La valutazione dei rischi viene effettuata tramite una stima sulla probabilità del verificarsi di *threat*, alle vulnerabilità che sfruttano e alle conseguenze in termini di perdita di business che il fermo dell'impianto causerebbe, i costi di riavvio e i danni a persone e ambienti. Se l'impianto non è in grado di permettersi spese per la copertura di tutte le sue vulnerabilità è utile stilare

una classifica o un piano d'azione in tal senso per procedere gradualmente nell'applicare le misure di cyber-security.

2.1.3 Strategia Defense-in-Depth

Minacce al sistema di informazione sono sotto evoluzione quotidiana, pertanto un singolo prodotto o tecnologia non è pronto a proteggere adeguatamente e completamente un ICS. Una strategia più consona al nostro sistema, conosciuta come *Defense-in-Depth*, consiste nell'utilizzare due o più meccanismi e strati di sicurezza che si sovrappongano e monitorare la rete ad ogni suo livello, fino alle profondità della rete interna a contatto con i PCN.
Anche se uno strato di difesa dovesse crollare per attacchi o per disfunzioni, il livello di sicurezza adiacente (sovrastante o sottostante) continuerà a fornire una protezione parziale allo strato in cui il sistema ha ceduto in attesa del ripristino.
Come mostrato in Figura 13, con questa strategia, vogliamo che le misure di protezione siano composte da più di un controllo di sicurezza per la tutela del sistema ed in particolare si fa riferimento a tre strati di difesa.

- **Network Boundary Security**
  E' un punto di contatto tra la rete di controllo e la rete esterna, come la rete aziendale, e previene l'ingresso delle minacce esterne nella rete di controllo.

- **Internal Network Security**
  La funzione di questo livello è di ridurre i danni che si possono verificare nella rete di controllo il più possibile. Uno dei principali obiettivi è quello di dividere la rete di controllo in varie zone e costruire la rete in modo da non permettere che danni in una sezione si propaghino nelle altre.

- **End Point Security**
  E' un provvedimento atto all'esclusione delle vulnerabilità nei dispositivi terminali. Le procedure di hardening sono un chiaro esempio di questa tipologia di difesa.

2.2 Security Control

Il passo successivo dell'ISMS consiste nel configurare correttamente i dispositivi di rete per mantenere salvaguardate queste policy. Le preoccupazioni principali del Security Control sono quelli di assicurare l'integrità dei dati, mettere in sicurezza gli accessi remoti e autenticare ogni dispositivo che comunica nella rete.
Al termine non rimane che il costante monitoring delle regole implementate per assicurarsi la loro effettiva efficacia nei comportamenti della rete.

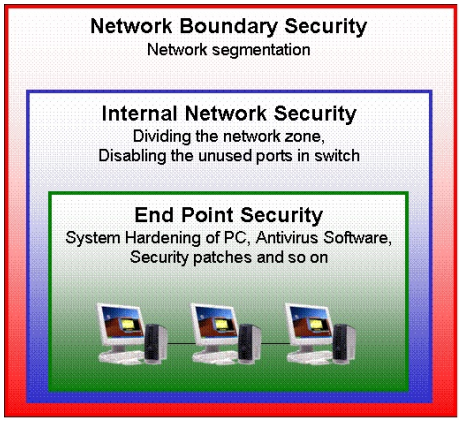


Figura 7: Esempio di strategia Defense-in-Depth;

2.2.1 Architettura di rete

Il documento di riferimento fornisce una descrizione sommaria della strumentazione e delle politiche degli strumenti per la protezione dell'architettura della rete per il controllo di processo. La panoramica prende in esame aspetti procedurali, software e hardware senza entrare nello specifico dell'implementazione, ma illustrando le alternative compatibili con i prodotti COTS[14].

Segmentazione e segregazione

Riprendendo le politiche introdotte dalla strategia Defense-in-Depth, lo standard definito in ISA 99 ha deciso che una buona linea di condotta per la definizione dell'architettura è quella di separare la rete di controllo per aree (*zone*), facendole comunicare fra loro tramite collegamenti (*conduits*) opportunamente controllati e dimensionati. La politica di segregazione è basata sulla strategia Deny-All.
Le segmentazioni delle zone possono essere orizzontali e verticali. Nel primo caso si tenta di creare una suddivisione netta tra rete aziendale, DMZ e rete di process control[15]; in particolare non viene definito alcun condotto che permetta una comunicazione diretta tra rete aziendale e rete di controllo senza attraversare i condotti connessi alla DMZ.
La segmentazione orizzontale viene applicata per suddividere (tipicamente per funzionalità o dislocazione fisica) la PCN in zone in modo da impedire,

[14]COTS (Commerce Of The Shelf): componenti hardware e software disponibili sul mercato per l'acquisto da parte di aziende di sviluppo interessate a utilizzarli nei loro progetti.

[15]La struttura di base presa in esame si rifà ad una segregazione tramite un firewall ad almeno tre vie. I vantaggi di questa configurazione, oltre ad evincersi nel proseguire del testo, verranno descritti nell'analisi tecnica dell'architettura del sistema preso in esame.

filtrando il traffico nei canali di collegamento, che la corruzione di una porzione della rete possa propagarsi.
Segmentazione e segregazione vengono garantite nella maggior parte dei casi attraverso l'utilizzo di VLAN. I device non appartenenti alla stessa VLAN saranno invisibili ai membri delle altre. Se un dispositivo di una VLAN deve comunicare con computer in altre reti virtuali, questo deve essere fatto attraverso dispositivi di almeno livello 3 (i.e. router) che permettono di limitare le tempeste di broadcast e sorvegliare meglio la situazione nella rete. Le VLAN separano in questo modo i flussi di traffico, spesso sovradimensionati nel throughput per il carico della CAN, pur passando attraverso gli stessi dispositivi di livello 2 (i.e. switch) tipicamente e largamente utilizzati nella rete di processo per la loro velocità di inoltro ed il prezzo relativamente contenuto. Un esempio di segregazione consiste nel separare la comunicazione del DCOM (PCN), quella del NMS (Network Management System) e degli altri protocolli assegnando porte e indirizzi di rete differenti.
Da segnalare il fatto che gli switch, in tal senso, sono suscettibili ad attacchi come MAC-spoofing[16], table overflow, VLAN hopping[17] e gli attacchi contro i protocolli dello Spanning tree, a seconda del dispositivo e della sua configurazione. Questi attacchi, tuttavia, non possono essere effettuati in remoto e richiedono accesso fisico locale allo switch.

Firewall

Molto spesso le aziende fanno troppo affidamento al firewall posto a separare la rete esterna dalla rete IT di stabilimento, non sapendo che ben il 50% della pirateria informatica bypassa il firewall e attacca la rete dall'interno. Nei sistemi DCS con un sistema di sicurezza che pone un occhio di riguardo alla protezione della rete di controllo, viene posizionato un ulteriore firewall a più vie come strato di difesa e separazione tra rete IT e PCN. Nel caso di firewall a più di 2 vie si utilizza tipicamente un ramo uscente dal firewall per posizionare una DMZ.
Il firewall può essere equipaggiato con pacchetti software di complessità e prestazioni variabili che offrono protezioni a livelli differenti:

- **Packet Filtering**: Feature di base che controlla la formattazione dei datagrammi TCP e IP; parametri della ACL (*Access Control List*) tipici sono destinazioni, sorgenti e protocolli consentiti per i messaggi. E' una funzionalità *stateless* che non aggiunge latenze significative all'inoltro;

[16] spoofing: tecnica con cui un attaccate si finge un altro dispositivo nella rete modificando il proprio indirizzo di rete. Sia esso a livello MAC, IP o livelli superiori.
[17] VLAN hopping: la possibilità di iniettare frame per porte non autorizzate sfruttando errori di configurazione negli switch. Le tecniche più utilizzate sono lo Switch spoofing o il doppio incapsulamento.

- **Stateful Inspection**: A differenza della feature precedente, questa permette di tenere traccia delle connessioni attive e legittime a livello 4 (TCP). Controllando il numero di messaggi e connessioni permette di difendere la rete da tecniche rudimentali di DoS[18] e Spoofing;
- **Deep Packet Inspection (DPI)**: Utilizzato per l'ispezione di pacchetti a livello *Application* (tipicamente HTTP, SMTP, DNS e FTP);
- **Application-Proxy Gateway**: Un ulteriore protezione del livello 7 viene garantita da questa feature che si adopera di inglobare nelle connessioni funzionalità proxy e offrire autenticazione aggiuntiva per valutare l'affidabilità dei tentativi di connessione. Tuttavia necessita di un maggiore dispendio di risorse computazionali e aumenta le latenze;
- **Network Address Translation (NAT)**: offre la traduzione dei socket (coppia IP-porta) per nascondere la struttura di rete interna e le porte dei servizi aperte evitando la fase di attacco di *network reconaissance*;

La configurazione del firewall richiede un ampia conoscenza sul sistema ICS da salvaguardare, se non settato correttamente diventa un apparato inutile. Alcuni prodotti software del mondo ICS non sono stati pensati per dare importanza alla sicurezza del sistema. Prendendo come esempio chiave la comunicazione instaurata dagli OPC server con i client si può osservare come il protocollo di comunicazione non sia stato pensato per collaborare con le apparecchiature per la protezione della rete; infatti, il protocollo, apre dinamicamente un numero di porte non ben specificato tra la 1024 e la 65535 per instaurare la comunicazione rendendo impossibile la gestione dei sistemi in tal senso. In questi casi viene suggerito l'utilizzo di software per il tunnelling e limitare il range di porte aperte dagli OPC.

Intrusion Detection and Prevention System (IDPS)

Talvolta ad un firewall è associata anche la funzione rilevamento delle intrusioni (IDS), un sistema basato su euristiche che analizza il traffico e tenta di riconoscere possibili attacchi alla sicurezza della rete, e può anche scatenare reazioni automatiche da parte del firewall (Intrusion prevention system, IPS)[22]. Quest'ultima funzionalità ha la capacità di riconfigurare automaticamente i sistemi; tuttavia, uno strumento automatizzato come questo, potrebbe essere utilizzato per influenzare negativamente l'andamento di un ICS. Falsi positivi possono anche ostacolarne il funzionamento.
L'analisi viene fatta su eventi nella rete come i modelli di traffico (*IDS network-based*, tipicamente installato sui firewall), o di un sistema, le voci di registro o gli accessi ai file (*IDS home-based*), in modo che possano

[18] Tuttavia non protegge da un tentativo di esaurire la capacità computazionale e di memoria del firewall stesso.

identificare un intruso o il tentativo di penetrare in una rete. Gli IDS garantiscono che le attività insolite (*anomaly detection-based*), come ad esempio nuove porte aperte, schemi di traffico inusuali, o modifiche ai file critici del sistema operativo vengano registrate e portate all'attenzione del personale addetto alla sicurezza[23].

2.2.2 Antivirus

Gli utenti finali e fornitori di sistemi di controllo industriale hanno espresso la preoccupazione che la distribuzione di software antivirus possa interferire con il funzionamento dei processi di controllo *time-critical*. Queste preoccupazioni sono uno dei motivi per il quale l'antivirus non è stato più ampiamente adottato, o pesantemente sottodimensionato, nella fase di configurazione quando si tratta del settore dell'automazione industriale; a tal proposito una sezione speciale della documentazione redatta dal NIST[24] fornisce delle analisi tecniche che hanno lo scopo di contribuire a ridurre al minimo l'impatto sul sistema, siano essi workstation che macchine server.
Qui di seguito vedremo brevemente quali parametri di giudizio possono essere utilizzati per adattare l'utilizzo di un antivirus alle esigenze industriali, stabilirne le configurazioni ottimali e evitare carichi indesiderati sul sistema senza compromettere la sicurezza dello stesso.

- **Motore di scanning**
  Definendo le politiche di attivazione quali apertura (lettura) o chiusura (scrittura) di un file, oppure selezionando le estensioni dei file da analizzare. Le modalità di attivazione si dividono in due categorie principalmente:
  - **Active (on-access) scanning** esamina i file, i dispositivi e le aree di accesso ogni qualvolta vi sia una modifica o cambiamento. Questa modalità non ha bisogno del supporto dell'utente e rimane in background nel sistema.
  - **Manual (on-demand) scanning** analizza porzioni di memoria o gruppi di file selezionati. Questa fase computazionalmente onerosa utilizza una percentuale maggiore di tempo di CPU in modo da ridurre i tempi d'esecuzione, ma la conseguenza di uno scanning troppo accurato potrebbe essere il lock esclusivo a risorse per tempi troppo lunghi.
- **Tecniche di scanning**
  I software antivirus commercialmente più diffusi offrono tre tecniche:
  - **Matching delle firme**: tecnica che confronta le firme (*hashing* di porzioni di codice) della banca dati dei virus identificati e analizzati e il codice da verificare. Non individua virus scritti con codice "nuovo".

  - **Analisi euristiche**: tecnica che cerca di sopperire alle limitazioni del metodo precedente. L'antivirus valuta il codice assegnando dei pesi al comportamento dello stesso, se il peso eccede una certa soglia questo viene segnalato come malevolo. Le tecniche euristiche sono computazionalmente più onerose e sono prone ai falsi positivi.
  - **Behavior blocking**: tecnica progettata per concentrarsi sull'individuazione di comportamenti di attacco (quali tentativi di aprire porte). Si differenza dall'euristiche che analizzano il comportamento di codice.

- **Tecniche di rimozione**
  Ciascuno comportamento, qui sotto elencato, attivo sui file corrotti richiede un'analisi delle conseguenze sulle applicazioni per il processo.
  - **Pulizia e ripristino**, spesso richiede l'avvio di procedure per il recupero della configurazione di backup nel caso di corruzione di registri o modifiche permanenti.
  - **Rimozione**, quando possibile.
  - **Quarantena**, per salvaguardare la continuità dei processi.
  - **Notifica**, tecnica che richiede una certa attenzione da parte del personale, tipicamente poco adatta alla rete di processo degli ICS.

La scelta della configurazione di un antivirus sulla base delle precedenti caratteristiche deve passare attraverso la considerazione della presenza di falsi positivi e falsi negativi. Nel primo caso, l'esecuzione di un programma utile (o, peggio, indispensabile al sistema) potrebbe essere interrotto, eliminato o messo in quarantena bloccando il sistema; nel caso opposto, con una soglia di interesse troppo lasca si potrebbe permettere ad un virus di confondersi fra i programmi concessi.

2.2.3 Autenticazioni

Generalmente gli utilizzatori di ICS non hanno un regolamento adeguato per le politiche di accesso ai sistemi. Inoltre, raramente forniscono adeguate capacità di amministrazione, tra cui, in primo luogo, granularità di accesso basato sui ruoli (identificare gli utenti specifici). Tipicamente un utente se ha accesso, può eseguire tutte le operazioni senza restrizioni, una volta autenticato. A causa della memoria limitata, la maggior parte dei dispositivi di controllo non conservano i log degli eventi informatici. Questa mancanza di registrazione ha impedito negli anni che incidenti informatici vengano analizzati rispettando i requisiti per il monitoring degli eventi previsto dagli enti standardizzanti.
Un'autenticazione avviene generalmente tramite 4 sistemi di identificazione, ciascuna con i propri punti di forza e debolezze intrinseche:

- **Password**: oltre alle policy di generazione della password, per la sua complessità dovrebbe essere tenuto in considerazione il metodo di cifratura e di *message digest* utilizzato (soprattutto il metodo di invio nell'etere utilizzato nelle autenticazioni remote). Una considerazione particolare deve essere fatta anche per i casi di allarme dell'impianto, momenti in cui il giudizio e le abilità dell'operatore possono ritenersi sotto stress.

- **Challenge\response**: utilizzabile per il riconoscimento di dispositivi.

- **Token**: dispositivo che sostituisce il sistema di password tramite generazione di chiavi. Essendo un dispositivo fisico potrebbe essere sottratto e garantire l'accesso.

- **Impronta biometrica**: deve essere tenuto in considerazione in un installato di questo tipo la presenza di errori di falsi-positivi e falsi-negativi con una certa soglia di precisione.

Una sicurezza più forte può essere applicata tramite l'utilizzo di una combinazione di due o più dei metodi elencati.

2.2.4 Accessi remoti e sicurezza del mezzo trasmissivo

Il metodo di funzionamento che garantisce un accesso dalla rete esterna e che, al tempo stesso, si difende dal maggior numero di vulnerabilità, semplificando la gestione del firewall, si compone di una combinazione di due collegamenti. Una prima connessione viene instaurata tra l'utente che vuole accedere alla rete e il server nella DMZ, previa autenticazione e cifratura del percorso. Una seconda linea viene aperta dal server della DMZ al dispositivo che si intende controllare\monitorare ripassando per il firewall, ma con diverse politiche di controllo.
Il server della zona demilitarizzata può effettuare controlli sulla formattazione di richieste per bloccare intrusioni e manomissioni. I controlli applicati vanno ad osservare l'assegnazione di privilegi, i tentativi di accesso non riusciti, il sistema di notifica, la notifica di accesso, il controllo della sessione corrente (blocco della sessione, e la terminazione della stessa in caso di anomalie). Spesso l'utilizzo di due diverse cifrature e protocolli di comunicazione introduce un aumento della protezione dell'impianto, in quanto gli exploit utilizzati sul primo potrebbero non funzionare sul secondo protocollo, e viceversa.

VPN

Un metodo di cifratura dei dati di comunicazione nel primo segmento degli accessi alla rete interna viene effettuato tipicamente attraverso una VPN[19]. Le tecnologie che implementano connessioni di questo tipo più utilizzate e considerate solide sono:

- **IPSec**, la modalità *Tunnel* è preferibile a quella di *Transport* per la cifratura dell'header e i parametri di sicurezza sul percorso di rete. IPSec tuttavia richiede requisiti software e dei test sulla compatibilità dei sistemi prima di essere messo in atto.

- **SSL\TLS**, l'utilizzo di questo *socket layer* elimina la necessità della distribuzione di software nei client, modifiche ai server interni e costosa manutenzione e supporto desktop (i.e. HTTPS con web server e browser client). Ha lo svantaggio di cifrare a partire dal livello transport e quindi di mantenere in chiaro le informazioni sul routing di rete.

- **SSH**, utilizzato al posto del protocollo Telnet privo di cifratura.

Cifratura livello di rete di controllo

L'uso della crittografia in un ambiente ICS all'interno della CAN non viene usualmente praticato a causa della latenza nella comunicazione dovuta al tempo supplementare, alla dimensioni dei messaggi e alle risorse di calcolo necessarie per cifrare, decifrare e autenticare ciascun messaggio. Alcuni dispositivi potrebbero essere troppo datati per supportare una determinata crittografia, presentando un'ulteriore limitazione alla compatibilità.
L'AGA[20] aveva in corso di sviluppo uno standard (AGA-12 in origine, poi diventato uno standard dell'ente IEEE 1711-2010) per la cifratura della comunicazione dei collegamenti basato su un sistema IPSec-like con cui proteggere il segmento di rete fra due dispositivi *bump-in-the-wire*[21]. Un'ulteriore prospettiva è rappresentata dal protocollo di sicurezza di livello 2, MACsec, il quale però, attualmente, rimane dalle potenzialità limitate a causa della bassa compatibilità con i prodotti e con protocolli (i.e. Spanning Tree Protocol).

[19] VPN (Virtual Private Network): rete di comunicazioni privata che circola su infrastrutture di trasporto pubbliche. Una VPN può essere vista come l'estensione di una LAN aziendale che collega tra loro siti interni all'azienda stessa dislocati nel territorio, sfruttando l'instradamento tramite IP realizzando di fatto una rete LAN virtuale e privata, ma su scala geografica.

[20] AGA (American Gas Association): Organizzazione commerciale americana che rappresenta le aziende di fornitura di gas naturale e altri con un interesse nella produzione di apparecchi a gas, standard, nonché per la produzione di gas.

[21] Bump-in-the-wire: dispositivi di rete, come ad esempio switch, che supportano il protocollo IPSec.

2.2.5 Patch management

Gli aggiornamenti dovrebbero essere adeguatamente testati per determinare l'accettabilità di effetti indesiderati. Non è raro per le patch di avere un effetto negativo su altri software. Un aggiornamento può rimuovere una vulnerabilità, ma può anche introdurre un maggior rischio dal punto di vista produttivo o di sicurezza. Un altro problema è che molti ICS utilizzano vecchie versioni di sistemi operativi che non sono più supportati dal produttore, di conseguenza, le patch disponibili potrebbero non essere applicabili.
Una politica di installazione delle patch ben assodata consiste nel procedere all'update, prima con macchine di test e zone a basso rischio di safety, e poi, a mano a mano che il sistema si dimostra stabile, procedere verso le aree a rischio più elevato fino alla copertura totale del sistema.
Il passaggio delle patch dal fornitore alla rete interna, nei sistemi più *cyber-security-oriented*, avviene attraverso un server intermedio posizionato nella DMZ. Lo scopo di queste configurazione è quello di eliminare l'esistenza di collegamenti diretti fra rete esterna e interna.

2.2.6 Monitoring

Ultima fase, ma non per questo motivo meno importante, nella gestione del sistema di sicurezza consiste nel monitoring continuo del sistema da parte degli operatori. Il monitoraggio dei sensori, file di log, IDS, antivirus, patch management, software di gestione delle policy e altri meccanismi di sicurezza deve essere fatto su una base periodica e in tempo reale sul sistema, dove possibile.
Un servizio di monitoring di alto livello riceve allarmi, fa una rapida analisi iniziale del problema e agisce per avvisare il personale della struttura per intervenire. Oltre alla gestione del sistema e dei vari allarmi, può partecipare attivamente al mantenimento degli standar di security tramite analisi proattive. I metodi più utilizzati si compongono in:

- **Red Team**[22], istruendo i membri sulla criticità del sistema;
- **Tool di Scanning**, anche se spesso lo scanning attivo di questi strumenti influenza il corretto funzionamento dei DCS;

Una volta determinate le nuove vulnerabilità nel sistema, queste verranno reintrodotte nella fase di audit dell'ISMS per forgiare nuove policy e ripercorrere il ciclo di protezione del sistema.

La seziona appena discussa non vuole proporsi come procedura definitiva

[22]Red Team: gruppo scelto per espugnare le difese del sistema. Tipicamente utilizzato nei sistemi ICS per effettuare analisi di penetratio testing

per attuare misure di cyber-security su qualsiasi sistema ICS, ma vuole offrire in breve sintesi la conoscenza dei pacchetti software, delle metodologie più sicure e della strumentazione hardware presenti in commercio attualmente. Tutto questo al fine di fornire il giusto grado di conoscenza sia ad un agente esperto di sistemi IT, che necessita di sapere l'influenza che la sua strumentazione può avere sulla rete di controllo, sia un professionista dell'automazione industriale, che richiede le conoscenze per difendere il proprio sistema senza dover apprendere tutti i concetti e teorie informatiche.
Per il lavoro di implementazione e definizione delle policy e delle misure di cyber-security applicate verranno utilizzate le procedure conformi al documento Yokogawa *TI 33Y01B30-01E*[21], vendor del sistema per l'impianto in esame.
L'analisi tecnica viene effettuata sulla base della situazione dell'impianto coadiuvata dalle metodologie proposte dal documento Yokogawa e dal NIST.

3 Caso industriale in esame

Il sito industriale su cui, da questo momento in avanti, si farà riferimento nel documento di tesi è la raffineria ENI R&M di Porto Marghera (Venezia). Il lavoro di analisi e installazione per l'impianto viene fatto seguendo le linee guida dell'azienda Yokogawa che ha fornito il DCS, per la quale opero come stagista. Con la migrazione ad una nuova serie di macchinari e software, il gruppo Yokogawa ha deciso, forte di una lunga esperienza maturata nel settore industriale e alla luce dei rischi di sicurezza affrontati dagli impianti di vecchia generazione, di implementare con maggior veemenza le proprie misure di cyber-security con il fine di tutelare l'*end-user* da eventuali fermi accidentali, e non, dell'impianto.
Partendo dalla base del ciclo di rinnovamento e introduzione delle norme di sicurezza, è necessario verificare la presenza di un Information Security Management System applicato all'impianto. ENI Venezia dovrà avere anch'esso un proprio ISMS per il sistema di automazione; e anche i clienti partner commerciali dovranno avere delle proprie security policy da integrare alle attività di ISMS.
Seguendo le procedure descritte nell'ISMS, la prima fase di svolgimento consiste nel prendere visione dell'architettura corrente, di effettuare un censimento delle apparecchiature e dispositivi utilizzati, ed è essenziale, soprattutto in questa fase, individuare le policy, linee guida e procedure previste nel sistema fino ad ora. In conformità con le indagini statistiche presentate nelle sezioni precedenti e alla luce delle analisi effettuate, un sistema, nonostante sia stato configurato al suo meglio al momento della realizzazione, con normative obsolete o non pienamente applicate, con scarsa manutenzione e monitoring scostante, tende nel tempo a non garantire più la sicurezza e la protezione presente e offerta al momento della messa in atto.
La situazione presentata al momento dell'analisi fa riferimento ad uno stato intermedio della migrazione dell'impianto. Il sistema ha completato l'upgrade al software di DCS CENTUM VP R5.03[23] ed è in attesa di una configurazione finale tramite l'applicazione delle nuove norme e dispositivi per la sicurezza. In questa prima sotto-sezione si prende nota della situazione procedurale e normativa della raffineria.

3.1 Policy e procedure

L'impianto non presenta della propria modulistica e politiche riguardanti specificatamente la gestione della rete e dei dispositivi. Alcune policy di sicurezza derivanti dalle procedure del mondo IT sono state riscontrate nel setting delle password e sul lock di servizi nelle macchine desktop client. Tuttavia altri servizi nelle workstation necessitano di avviare delle sessioni

[23]CENTUM VP (Vigilant Plant)) R5.03: è l'ultima versione Yokogawa di un sistema integrato di controllo distribuito del processo di produzione (DCS).

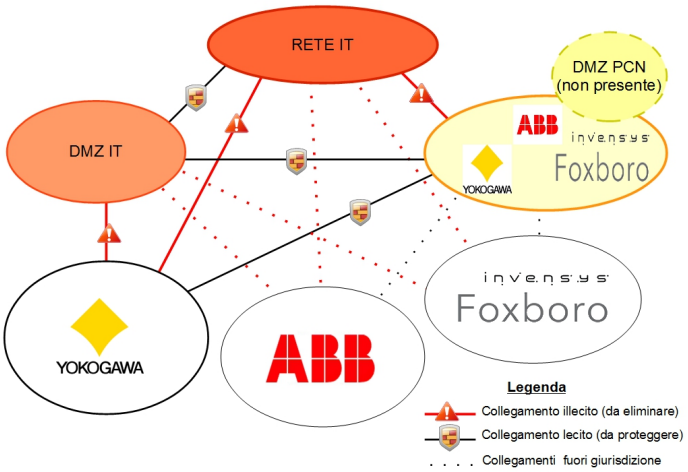


Figura 8: Situazione di zone e condotti attuale in ENI Venezia;

di comunicazione con la strumentazione in qualità di macchine server per la PCN e, pertanto, non ottengono alcun lock dei servizi (whitelisting e blacklisting assenti).
Allo stesso modo la gestione degli account è poco performante sui dispositivi in questione; esistono solo due tipologie di account accettati, l'operatore, con funzioni limitate al relativo ambito lavorativo, e l'admin user che ottiene pieni privilegi nell'utilizzo della macchina. Non esistendo livelli di utenza intermedi la conoscenza della password di amministrazione viene condivisa dai *vendor*, dai *contractor* e dai manutentori e utilizzatori di medio-alto livello del sistema.
Yokogawa non essendo l'unico sistema presente all'interno dell'impianto, convive e condivide porzioni di rete con altri 2 sistemi di automazione industriale di gestione appartenente ai *vendor* Invensys e ABB. Fatto che merita considerazioni ulteriori nella fase di design della nuova architettura, nella richiesta di nuova strumentazione compatibile e nel dimensionamento del firewall per il carico di rete; tuttavia anche nella fase di audit dell'impianto non si può ottenere una documentazione tecnica specifica delle altre reti a causa di regolamenti di privacy. Le altre reti di processo, in assenza di informazioni specifiche, vanno considerate non sicure alla stregua della LAN di stabilimento nei confronti della PCN di Yokogawa. Questa considerazione va a supporto della divisone e della segregazione delle zone della rete stabilito nello standard ISA 99, tuttavia non è presente alcuna documentazione che motiva e supporta l'utilizzo di questa separazione logica e funzionale.
Le zone fino ad ora individuate sono riassunte nella Figura 8. Nella fase di descrizione dell'architettura vedremo più attentamente come sono gestiti i

condotti che collegano le varie sezioni.
L'hardening sui dispositivi registrati sotto la responsabilità di Yokogawa sono coperti da una procedura minima prevista in fase di messa in esercizio nell'impianto comprensiva della disabilitazione delle porte degli switch e di un MAC filtering nei collegamenti. E' importante notare che i dispositivi di sicurezza, quelli di comunicazione di rete e le linee sono ridondati; una pratica comune utilizzata in tutti gli impianti industriali per garantire le esigenze di *availability* e *integrity* richieste.
Le attività di monitoring non sono previste, fatta eccezione per le attività di manutenzione ordinaria e straordinaria ad opera di Yokogawa sui propri sistemi in caso di guasti o malfunzionamenti. Tuttavia queste attività non hanno sempre scadenza regolare e non richiedono necessariamente una valutazione dello stato o presa visione dei log della totalità del sistema. Riepilogando la situazione del sistema è la seguente:

- Policy assenti o derivate dal lato prettamente IT;
- No whitelisting dei servizi necessari;
- No blacklisting dei servizi nella rete di stabilimento (strategia Deny-all non applicata);
- Procedure di hardening standard nel lato PCN e derivate dall'upgrade Yokogawa;
- Account poco performanti;
- Aggiornamenti senza procedure;
- Monitoring on-demand;

E' evidente che la tutela della sicurezza della rete PCN non è tenuta in considerazione dai gestori della rete e non esiste una documentazione efficiente e dedicata alla cyber-security completa dello stabilimento. Vedremo ora come ad una scarsa burocrazia normativa in materia, corrisponda anche una carenza nella configurazione e nella presenza di strumentazione *security-care* orientata alla PCN.

3.2 Valutazione tecnica

L'approccio di valutazione dell'intero apparato informatico industriale, che ho deciso di praticare nel sito, utilizza lo schema della strategia defense-in-depth, già affrontato nella relativa sezione, come base per affrontare l'analisi tecnica della rete di stabilimento.
Si procederà con una valutazione dell'architettura e delle barriere di difesa border-line del sistema, per poi passare a dedicare l'osservazione nella rete interna della PCN fino ad una considerazione della sicurezza negli end-point.

Questa metodologia scelta mi permettere di discernere le procedure utilizzate e osservare se per ciascun livello di protezione esistono errori di configurazione, gravi mancanze in termini di difesa del sistema o installazioni che, nonostante siano efficienti, non sono supportate da una relativa documentazione e collocamento nelle policy d'impianto.
Per ogni punto e problematiche sviluppate corrisponderà una descrizione delle vulnerabilità generate dalla mal configurazione del sistema. L'argomento verrà ripreso nella sezione successiva per la costruzione figurativa di alcuni esempi di attacchi funzionali.

3.2.1 Architettura e difesa esterna

La rete, al momento dell'analisi, è strutturate come in Figura 9. La suddivisione logica è l'esatta trasposizione delle zone evidenziate nel paragrafo precedente, ciò nonostante la separazione viene demandata ad un unico firewall che si adopera di suddividere le reti. Gli eventuali problemi di crash di quest'ultimo sono risolti ridondandolo con un medesimo firewall collegato alla linea di backup della rete, tuttavia, i problemi di latenza possono affliggere entrambi i firewall (doppia rete, doppio traffico). Un ulteriore motivo di rallentamento del traffico viene a crearsi nel caso della generazione delle VLAN. Il firewall, con funzionalità di routing nelle vie, visiona il contenuto dei pacchetti e, inoltrandoli alla giusta sottorete, vengono marchiati con l'identificativo della corretta VLAN per l'instradamento negli switch.
Il tronco di rete in cui convivono sistemi differenti non separa i vari OPC in diverse VLAN ma sono attualmente identificati nella stessa subnet (128.2.1.0/24). La rete mista ha lo stesso dominio di indirizzamento delle reti ABB e Invensys, all'interno della propria PCN ciascun vendor possiede i propri indirizzi(126.2.1.0/24 per la futura subnet Yokogawa). L'organo di sicurezza IT ha preferito rendere sicuro il tratto che collega il client Cim-IO[24] con il software ExaOPC[25] a discapito di una maggiore segregazione.

In particolare posizionando i server OPC nella stessa macchina del server Cim-IO sulla rete "mista" (anche se contenuta nel dominio Yokogawa), non vengono aperti continui flussi di comunicazione verso la PCN attraverso il firewall che creerebbero passaggi per eventuali malware da una rete all'altra. Questi buchi nel passaggio sarebbero spesso mantenuti per tempi prolungati (nell'ordine tipico dei 3 minuti) per garantire una comunicazione robusta

[23]La configurazione del firewall IT esterno non è di mia competenza, si assume a priori che possieda una configurazione sufficiente a bloccare gli attacchi più semplici, ma insufficientemente predisposto alla difesa degli attacchi mirati alla rete PCN. Oltretutto come abbiamo visto nei vari esempi di attacchi, questo firewall borderline non è efficace per tutti gli attacchi che partono già dall'interno della rete LAN di stabilimento.

[24]Cim-IO: Software di proprietà della AspenTech per la storicizzazione del database e dei file della rete di processo elaborati dall'OPC. Il client deve essere in comunicazione con l'OPC.

[25]ExaOPC: Software Yokogawa per l'utilizzo delle funzionalità di OPC.

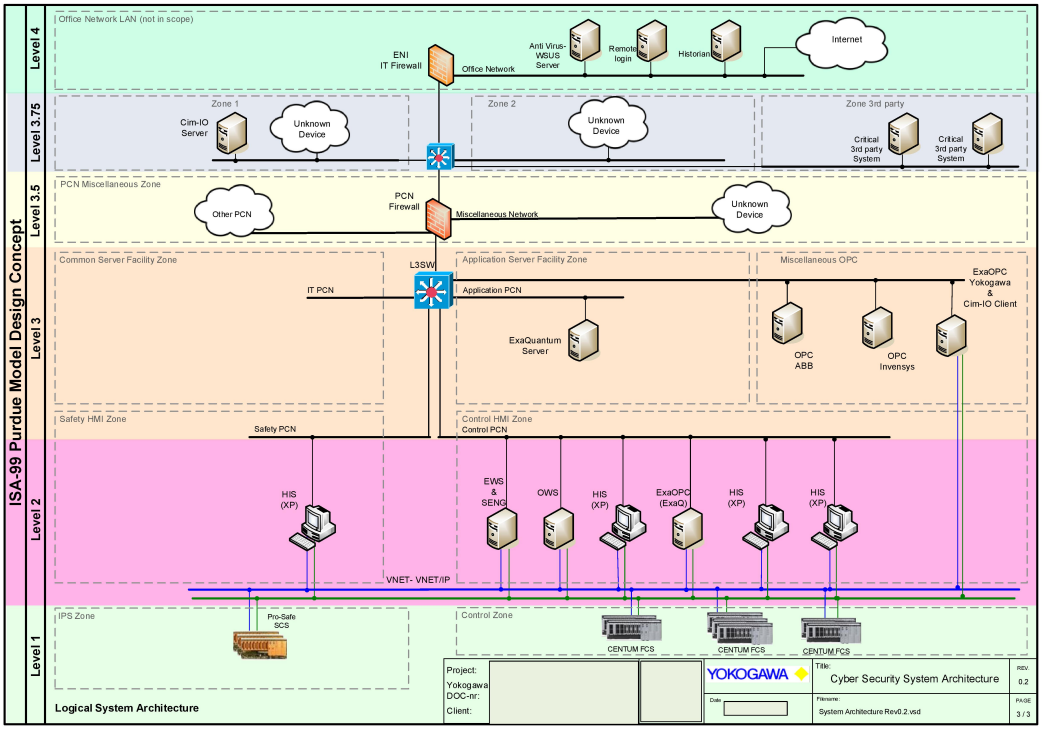


Figura 9: Design dell'architettura pre-intervento di ENI Venezia;

nelle trasmissioni OPC con conseguente dispendio di risorse del firewall, sia per mantenere la traccia delle connessioni attive, sia per contenere la fragilità del sistema. Tuttavia questa scelta progettuale posiziona dispositivi con diverse proprietà, software e politiche di sicurezza nella stessa rete. La comunicazione in questo tratto non è regolamentata da alcuna politica (gestione per condotti) e non è segregata.
E' opportuno evidenziare tuttavia un bilanciamento in positivo nelle prestazioni, il numero di percorsi nel firewall è limitato e non subisce rallentamenti dagli OPC, tuttavia la libertà nelle comunicazioni in entrata indifferentemente dal vendor potrebbero essere cause di dispute in caso di danni alla rete.

Tra le vie uscenti dal firewall non è presente alcuna DMZ di supporto alla PCN e pertanto non offre servizi di appoggio per "intermediare" i servizi di accesso remoto, aggiornamento delle patch e la distribuzione dell'antivirus, che, fra l'altro, non è presente al di sotto del firewall IT. I servizi in tal senso non sono bloccati a prescindere dal firewall ma vengono analizzati dal software di Deep Packet Inspection. Un tipo di architettura di questo tipo non concede una scalabilità delle regole con conseguente diminuzione dei pacchetti filtrati e l'aumento progressivo dei percorsi e sessioni generabili

Proprietà Software	Descrizione
ACL	Presente (requisito minimo firewall commerciali)
Deep Packet Inspection	Presente
Stateful Packet Inspection	Non presente
Connections per second	9000
Packets per second (64 byte)	85000
3DES/AES VPN throughput	100 Mbps
Proxy	Non presente
VPN	IPSec trasparente
Configurazione specifica per OPC	Assente
Suite filtri dedicati a Yokogawa	Non presente, regole generiche per il tratto Others PCN - PCN Yokogawa
Supporto al Natting	Non presente
IDPS	Non presente
Filtri porte presenti	HTTP(80), FTP(20-21), SMTP(25), DNS e DCOM(135), Telnet(23)

Tabella 3: Dati tecnici del Checkpoint Firewall-1 (applicazione software) presente in stabilimento;

attraverso, con conseguente crescita di diffusione di malware nella PCN. L'analisi dei pacchetti diminuirebbe, ma nel caso di introduzione di applicativi per lo Stateful Packet Inspection, l'analisi dei flussi diventerebbe gravosa con conseguente deperimento delle prestazioni.

3.2.2 Configurazione dispositivi di rete e difesa interna

Messe da parte tutte le accortezze sul firewall e sulle comunicazioni verso le reti esterne, è necessario calarsi nell'analisi al dettaglio della rete PCN sotto la gestione di Yokogawa. La comunicazione dei dispositivi si divide in 3 sottoreti (più la connessione per l'equalizzazione), ciascuna delle quali opera su diversi ambiti della gestione del processo:

- **Vnet e Vnet\IP**: Distribuisce le informazioni nella rete di processo per la coordinazione delle attività in tempo-reale. La rete VNET funzione con un protocollo di comunicazione proprietario di Yokogawa che, fino ad ora, non ha riportato bug sfruttabili per il controllo dei DCS. Per cooperare con software e prodotti non-Yokogawa, adeguarsi agli standard e favorire l'interoperabilità, tuttavia, parte della comunicazione viene convertita su una rete mista VNET\IP[26]. Ai fini di

[26] Vnet\IP: è una control network che viaggia a 1-Gbps per i sistemi di controllo di produzione che ingloba funzioni di comunicazioni generali e fornisce un'alta affidabilità, stabilità e comportamento real-time delle comunicazioni. Utilizza il protocollo IP per comunica-

garantire una linea di difesa comune, entrambe le reti vengono trattate come reti con protocollo di comunicazione IP.
Alcune funzionalità di sicurezza nelle schede di rete (Vnet\IP NIC) offrono una protezione contro lo spoofing, il tampering dei dati e l'escalation di privilegi aumentando la sicurezza tra le HIS e i controllori. Il router proprietario AVR10D di Yokogawa utilizzata per la conversione tra le due reti ha una certificazione Achilles[27] di primo livello sulla sicurezza e robustezza del sistema.

- **PCN e Equalizzazione**: Rete in cui circolano le informazioni utilizzate dal DCS per coordinare e sorvegliare la produzione. A differenza della Vnet, non utilizza protocolli di comunicazione a supporto del real-time, ma predilige la robustezza del sistema. Come visto sulla sezione dedicata agli OPC, il protocollo di comunicazione utilizzato è il DCOM.
  L'equalizzazione che viaggia in parallelo si adopera di gestire la sincronia tra i dispositivi per supportare la fase di coordinazione delle operazioni e mantenere una valenza temporale nei dispositivi di storicizzazione (timestamp).

- **NMS**: Raccoglie dati sullo stato della rete e sulla comunicazione dei dispositivi dell'instradamento. Il protocollo di comunicazione è il SNMP, standard per la gestione di rete, comune anche agli ambienti IT. Al momento la rete Yokogawa non possiede un server di gestione di questa rete ma sono comunque attivi i servizi per la gestione da IT.

La separazione tramite VLAN di queste tre reti permette un bilanciamento del carico migliore dando priorità ai pacchetti critici per il processo, piuttosto che alle comunicazioni di storico e gestione di rete. Anche dal punto di vista della protezione e della sicurezza questa segregazione offre molti vantaggi; un'infezione che sfrutta un exploit del protocollo SNMP diffuso nella rete NMS potrebbe essere confinato negli indirizzi senza inficiare la comunicazione dei dispositivi sugli altri livelli. Altri vantaggi potrebbero essere quelli di limitare la portata degli attacchi DoS nella rete (limitazione di banda per la comunicazione) e nascondere ad un attacco di *reconaissance* alcuni dispositivi connessi solamente per certi servizi e porzioni di rete. Ovviamente per supportare queste funzionalità è necessario avere dei dispositivi nell'architettura che supportino i Multiple Spanning Tree per la gestione dei più percorsi di rete. Uno switch che non supporta a dovere questo protocollo di instradamento rischia di creare dei loop nella comunicazione.

zioni general-purpose e conformi al CPF-10 per il profilo real-time delle comunicazioni Ethernet (RTE) definito nello standard IEC 61784-2.

[27] Yokogawa ha ricevuto la certificazione Achilles Level 1+ per tre differenti apparecchiature di controllo AFV10D, AVR10D e SSC50D. I test sono stati condotti in Febbraio 2007 dalla Wurldtech Security Inc. a Vancouver, Canada[26].

Gli switch diventano dispositivi critici per un intruso che ha accesso fisico alla rete interna. Da questa posizione favorevole è possibile per un attaccante rendere vane molte delle difese costruite ai bordi della rete e minare l'integrità delle connessioni, *sniffare* la rete (che non ha un sistema di cifratura) ed inserirsi nella comunicazione tramite tecniche di spoofing e Men-in-the-middle. La disabilitazione delle porte di ingresso e il lock dei MAC possibili per la comunicazione (MAC filtering degli switch) sono solo alcuni accorgimenti tipici e che non richiedono grandi competenze tecniche, ma che, in questo punto della rete, potrebbero fare veramente la differenza tra un sistema violabile ed uno sicuro.

3.2.3 Protezione end-point

La valutazione della sicurezza dei singoli dispositivi è l'ultimo punto cruciale per la protezione del sistema. L'importanza di questa barriera di difesa, oltre alle ovvie ragioni sulla salvaguardia della macchina singola, è motivata dal fatto che l'infezione di una macchina, dei suoi servizi e l'accesso a privilegi elevati, potrebbe bypassare quelle difese di rete edificate minuziosamente e diffondersi nel sistema intero.
A tal proposito viene costruita una scheda per l'analisi delle workstation e dei server riassunta brevemente nelle Tabelle 4 e 5. E' facile constatare che la sicurezza delle singole macchine non rispetta i parametri qualitativi di sicurezza prefissati. In particolare l'assenza di un antivirus e di un hardening minimo sono da considerarsi deleteri per il sistema. Per quanto riguarda il sistema operativo installato e gli aggiornamenti è importante notare che, dall'Aprile 2014, Windows XP non sarà più supportato da Microsoft per il rilascio di patch[27]. Un worst-case scenario di questa notizia sarà il proliferare di virus che sfrutteranno flaws del sistema che non saranno più coperti da nuovi aggiornamenti.

L'aggiornamento costante delle macchine è un altra priorità per la protezione del sistema che non viene trattata regolarmente. Nonostante ci siano dei meccanismi di update di base, questi non sono eseguiti con una metodologia di diffusione sicura. Le pratiche più utilizzate sono l'installazione tramite dispositivo removibile (che senza un antivirus di scansione potrebbe trasportare dei malware), oppure tramite la diffusione nel network a partire da un server di update centrale contenuto nella rete IT. I problemi di quest'ultima procedura sono l'apertura di porte e connessioni diretti tra rete IT (considerata non sicura dalle ipotesi iniziali) e PCN nel firewall senza passare attraverso un luogo intermedio di protezione (DMZ).
L'autenticazione degli utenti viene gestita da Windows e dal sistema DCS CENTUM VP. Tuttavia le policy e gli account presentano i problemi elencati in precedenza, assenza di un sistema di gestione centrale e larga diffusione della conoscenza delle password di amministratore.

Proprietà	Descrizione
Sistema Operativo	Microsoft Windows XP
Antivirus	Nessuno
Aggiornamento Patch	Manuale e a scadenze non fissate o gestito da Update Server nella rete IT
Hardening applicato	Nessuno

Tabella 4: Valutazione della sicurezza di workstation prima dell'intervento;

Proprietà	Descrizione
Sistema Operativo	Microsoft Windows Server 2003 e Unix-based
Antivirus	Nessuno
Aggiornamento Patch	Manuale e a scadenze non fissate o gestito da Update Server nella rete IT
Hardening applicato	Nessuno

Tabella 5: Valutazione della sicurezza dei Server prima dell'intervento;

3.3 Valutazione delle vulnerabilità e di minacce al sistema

Sulla base dei buchi precedentemente scoperti vengono indicati nella Tabella 6 alcuni attacchi funzionalmente distruttivi per il sistema. Per ciascuno di essi vengono presentate le vulnerabilità incontrate che favoriscono quella specifica tipologia di attacco. Per ragioni di sicurezza dell'impianto, per obblighi contrattuali e responsabilità operative ed economiche, non si è potuto provare alcuna tipologia di attacco al sistema; anche lo scanning passivo con prodotti commerciali generici (*Metasploit* e *BackTrack* in primis) influenzano negativamente l'operatività dei controllori e della strumentazione in campo. Oltretutto non si è voluto descrivere in dettaglio un'eventuale procedura specifica di attacco per evitare di fornire conoscenze potenzialmente dannose ad un lettore malintenzionato. E', tuttavia, ragionevolmente giusto pensare che questa tipologia di attacchi, che sfruttano debolezze sia hardware che software, siano effettivamente applicabili con effetti catastrofici nella produzione dell'impianto, nella salvaguardia degli operatori e nell'integrità dei macchinari impiegati.

Attacco		Flaws sfruttati
Passivo	Sniffing	• Accessi fisici non protetti • Comunicazione non cifrata

Continua a pagina seguente

Attacco		Flaws sfruttati
	Port Scanning	• Protocolli TCP e UDP consentiti verso la rete PCN
	Network Scanning	• ICMP valido oltre il firewall • Assenza di router nella PCN per il controllo del broadcast di pacchetti
Attivo	Spoofing (account e device)	• Nessun controllo incrociato su MAC e IP • Nessuna autenticazione di livello superiore • Account limitati • Nessuna cifratura • Nessun monitoring periodico degli accessi
	Reply attack	• Sessioni aperte e assenza chiave di sessione • Nessuna autenticazione di pacchetto
	Brute force (Account)	• Password fragili • Nessun sistema di controllo per gli accessi centralizzato
	Brute force (Remote) e connection hijacking	• Sessioni aperte e assenza chiave di sessione • Connessioni remote direttamente connesse alla PCN
	SQL-injection	• DCOM con password in chiaro • DB MySQL legato alla comunicazione DCOM • Comunicazione non cifrata • Account DB fragile • Nessun Antivirus • Sistema con latenza nell'installazione di patch

Continua a pagina seguente

Attacco		Flaws sfruttati
	DDoS	• Accessi fisici non protetti • Nessuna segregazione della PCN • DCOM con connessioni prolungate (esaurimento delle risorse del firewall) • ICMP valido
	Spyware	• Nessun hardening (lock USB) • Nessun Antivirus • Servizi attivi • Protocolli SMTP, FTP, Telnet e HTTP consentiti direttamente verso la PCN • Nessun report dei log periodico
	Malware e Trojan	• Nessun hardening (lock USB) • Nessun Antivirus • Servizi attivi • Protocolli SMTP, FTP, Telnet e HTTP consentiti direttamente verso la PCN • Nessun report dei log periodico • Sistema con latenza nell'installazione di patch • Facile escalation di privilegi (account Admin frequentemente utilizzato)

Tabella 6: Attacchi praticabili sulla base dei flaws evidenziati;

In aggiunta alla tipologia di attacchi elencati ed evidenziati in Tabella 6, qualsiasi altro strumento di penetrazione, nonostante la presenza del firewall, può essere mascherato e incapsulato nei pacchetti al livello application come HTTP e SMTP. L'assenza del filtro è una conseguenza della mancanza delle funzioni SPI che non tengono traccia del flusso delle connessioni. Un hacker potrebbe sfruttare porte aperte su connessioni remote attive per aggiungere al payload di quest'ultime nuovi pacchetti malevoli senza essere ulteriormente filtrato dalla rete di impianto.
Nel Dicembre 2013 il sistema CENTUM di Yokogawa ha riportato, ad opera

di un report investigativo della Rapid7[28], la presenza di alcune falle nel sistema di accesso remoto di cui è necessario prendere provvedimento, almeno fino al rilascio di tutte le patch. Alcune sono già state sistemate dagli aggiornamenti di Marzo 2014 del sistema, altre verranno rilasciate nei prossimi mesi. L'exploit degli eseguibili incriminati, se soggetto ad attacchi alle porte su cui sono in ascolto, porterebbe a sfruttare i problemi di buffer e stack overflow andando a permettere l'esecuzione di codice malevolo.

[28]Rapid7: Azienda che offre soluzioni di sicurezza IT. Effettuano analisi delle minacce (penetration testing e incidentd detection e investigation) ai sistemi con una veloce raccolta dati completa di tutti gli utenti, beni, servizi e reti.

4 Soluzione proposta

Sulla base del NIST e dei documenti Yokogawa viene stilato l'FDS[29] su cui si basa la proposta tecnico commerciale al gruppo ENI R&M responsabile della gestione dell'impianto a Venezia; le proposte di sicurezza e le configurazioni introdotte nel bando vanno a completare la migrazione al sistema di controllo (DCS) di ultima generazione. Nei prossimi paragrafi si discuteranno le scelte progettuali dando enfasi agli aspetti che più sono stati argomento di discussione e cruciali nella fase di scelta delle tecniche di difesa adottate. Non è incluso nel documento in questione la gestione della sicurezza fisica dell'impianto (accesso agli armadi server e switch di rete da parte di hacker), pertanto la protezione dagli attacchi diretti con accesso è vincolata alle scelte del cliente. E' importante notare che alcune porte di switch (come quella seriale) non possono essere disabilitate e che alcuni dispositivi, se resettati, perdono la configurazione e ripristino la password di default. Tuttavia questa parte della sicurezza non dipende da Yokogawa ed esula dall'obiettivo di questa tesi.

4.1 Principi e criteri

L'FDS Yokogawa basa le proprie regole e suggerimenti in linea con la strategia Defense-in-Depth. Dal punto di vista gestionale viene introdotto un documento ufficiale che regolamenta l'utilizzo di un ISMS come procedura di base che dovrebbe coinvolgere i gestori della rete IT, della rete di processo e della produzione e business. La raccomandazione è di applicare su tutte le reti di impianto un sistema di gestione di questo tipo.
Le modalità operative sul sistema dipendono dal grado di intervento sullo stesso concesso dai clienti a Yokogawa. A fronte dell'esperienza acquisita nella gestione della rete di processo si consiglia di operare in *Stregthened mode*, che si prefigge lo scopo di proteggere da attacchi di rete, manipolazioni dirette ai computer e furto di dati. Le quattro categorie sotto il controllo IT sulla quale vengono concesse libertà di intervento e un certo grado di influenza sulle configurazioni sono:

- Controllo degli accessi;
- Tuning del Firewall;
- Stop dei servizi Windows;
- Setting di alcuni apparati IT;

[29]FDS (Functional Design Specification): è un documento utilizzato dalle aziende in una fase di pre-sviluppo in cui si traducono tutte le note, i concetti e le applicazioni per soddisfare tutti i requisiti. Come minimo, un FDS conterrà un elenco organizzato di requisiti che possono essere utilizzati per lo sviluppo, il test e il client sign-off.

Con la questa modalità, le impostazioni di default dei dispositivi vanno riconfigurate dagli operatori manualmente.

4.2 Architettura proposta

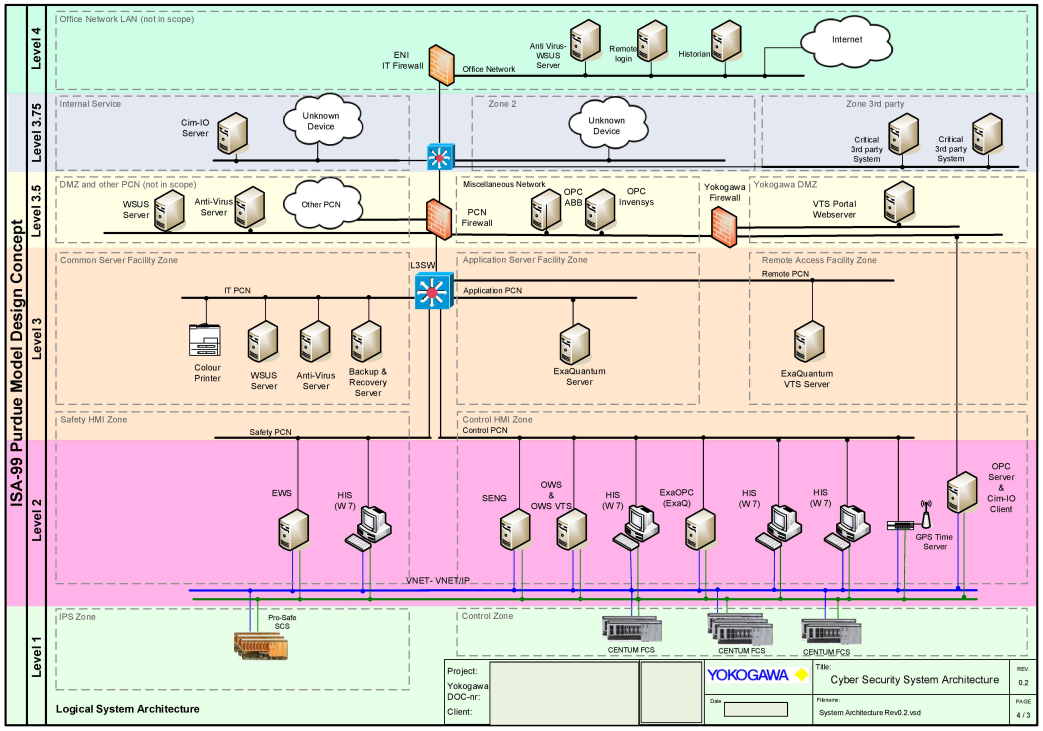


Figura 10: Nuova Architettura ENI Venezia;

Il nuovo design dell'architettura di rete in Figura 10 si basa sulla decisione di offrire maggiore protezione ai server OPC e alla rete Yokogawa rimuovendo la zona in cui più sistemi vanno a convergere per comunicare con le relative PCN appartenenti a ciascun vendor. Questa protezione viene offerta con l'introduzione di un secondo firewall in una rete contenente una varietà non specificata di utilizzatori ,di una DMZ relativa alla gestione della connessione remota (di utilizzo esclusivo di Yokogawa) e dalla presenza di un'ulteriore DMZ di utilità comune dedicata al flusso downstream degli aggiornamenti e allo scambio di informazioni con gli storici IT.
Il motivo fondamentale dell'aggiunta di un firewall in cascata a quello principale rivolto alla PCN è l'impossibilità di muovere l'OPC dal tronco di rete della subnet 128 (sotto il controllo dei responsabili IT) alla rete di processo Yokogawa. Essendo in una posizione compromettente dal punto di vista della sicurezza, dovuto alla presenza di più sistemi concorrenti di cui si ignorano i segreti commerciali e contratti di utilizzo della rete, si è preferito tutelarsi

con una barriera di difesa aggiuntiva. Tuttavia, con la presenza di un firewall sottodimensionato rispetto alle esigenze del traffico di rete, è possibile aggiungere una via uscente dallo stesso e configurarla in modo da essere utilizzata come DMZ ad utilizzo esclusivo dei server Yokogawa.
Una segregazione ulteriore con VLAN era prevista per separare i vari OPC nella relativa sezione, ciò nonostante, dal momento in cui si intende aggiungere una DMZ dedicata, la soluzione perde di efficacia, anche se offre uno strato di sicurezza in più che potrebbe essere utilizzato nella fase di configurazione del secondo firewall per limitare l'analisi del traffico. Per quanto riguarda la struttura della PCN, la segregazione orizzontale consiste nel rendere operative delle VLAN per segregare i vari vendor nella propria sottorete. Gli switch, se correttamente configurati e protetti (anche fisicamente), permettono di mantenere l'isolamento tra le reti. Il diffondersi dei malware verrebbe limitato all'impacchettamento della propria VLAN, tuttavia, come visto nella sezione relativa, non previene da attacchi eseguiti in loco che potrebbero aggirare gli switch e permettere il broadcasting malevolo.

4.2.1 Firewall, DMZ e connessioni remote

Il fulcro della protezione della rete PCN si basa sul Checkpoint Firewall di proprietà e responsabilità di gestione di Eni. Le attività che si sono dovute operare sono riassunte nella Tabella 7 e mostrano una variazione nella tipologia di traffico a cui è stato concesso di transitare dopo l'intervento di completamento della migrazione del sistema. I pacchetti software di ispezione del traffico di questo dispositivo non sono mutati.
Per limitare l'influenza eccessiva di Yokogawa da quest'ultimo e suddividere le responsabilità operative si è deciso, come discusso nei paragrafi precedenti, di introdurre un secondo firewall per la generazione di una DMZ privata e ad uso esclusivo dei server Yokogawa. In questa DMZ vengono concessi i servizi di controllo remoto da parte degli operatori Yokogawa, mentra la DMZ condivisa nella PCN offre la diffusione delle patch, degli upgrade di firme e dell'antivirus. Per evitare la tipologia di attacchi che sfruttano connessioni attive nel percorso, e avendo una maggiore libertà di manovra, si è deciso di configurare il firewall Yokogawa con l'aggiunta di software per il Stateful Packet Inspection, per il Natting e che supportino le connessioni autenticate con IPSec con un Application-Proxy Gateway. In questo modo è possibile aumentare l'autonomia e l'automatizzazione dell'amministrazione del sistema diminuendo gli sforzi del personale Yokogawa che, per ovvi motivi di locazione e amministrativi, non può avere un operatore fisso posizionato all'interno dell'organico della raffineria. Il sistema migliore per il monitoring è costituito da un Versatile Terminal Server (VTS) che offre un servizio web-based per la connessione da remoto. Quando un client nella rete aziendale, o da reti esterne nel caso di VPN, richiede una visualizzazione del DCS CENTUM, la richiesta sarà processata dal Web Server nella DMZ. In

Percorsi considerati	Servizi e comunicazioni concesse	
	Pre-intervento	**Post-intervento**
IT - PCN YOKO	Aggiornamenti e comunicazione Cim-IO	Nessuno
IT - PCN MISTA	N.P.*	Comunicazione Cim-IO ABB, Invensys e Yokogawa**, Server remoto Yokogawa**
IT - DMZ PCN	N.P.*	Aggiornamenti (donwload da rete)
DMZ PCN - PCN YOKO	N.P.*	Aggiornamenti (diffusione interna)
DMZ PCN - PCN MISTA	N.P.*	Aggiornamenti (diffusione interna)
PCN MISTA - PCN YOKO	N.P.*	Comunicazione OPC** e Controllo remoto **
TRA PCN	Comunicazione OPC	Nessuno

**Non esiste una DMZ uscente dal firewall al bordo della PCN.*
***Attraverso il nuovo Firewall Yokogawa e DMZ Yokogawa*

Tabella 7: Variazione delle regole nelle vie passanti per il Firewall;

questo caso il client non ha accesso diretto alla PCN, ma solo alla DMZ. Il server VTS inoltrerà la richiesta all'Application Server all'interno della rete di controllo (HIS con le funzioni per supportare il terminale) e rimanderà la risposta al client nella rete di partenza. Cambiando il protocollo utilizzato e appoggiandosi alla DMZ si evita di diffondere conoscenze aggiuntive sullo stato della rete al di fuori della stessa.

4.2.2 Antivirus

Mentre gli Antivirus (AV) sono una pratica comune e di facile impiego per l'ambiente IT, il loro utilizzo negli ICS può richiedere l'adozione di particolari pratiche di management sulla migrazione, nonché controlli di compatibilità e impatto sulle prestazioni del sistema.
Non esistendo un sistema di protezione di questo tipo dedicato alla rete di processo, è necessario affidarsi a soluzioni commerciali general-purpose e optare per una configurazione manuale il più possibile livellata sui requisiti e necessità del sistema. Il prodotto importato nella definizione della rete è il McAfee, recentemente diventato *recommended solution (provide)* dei prodotti Yokogawa. I pacchetti software utilizzati sono il VirusScan Enterprise (VSE) versione 8.8 per la protezione nella singola macchina (stand alone). Per la gestione client-server nella rete è stato rifiutato da Eni l'utilizzo del software McAfee ePolicy Orchestrator (ePO).
Sempre con un occhio di riguardo sulle prestazioni e il rispetto dei tempi di risposta dei dispositivi, la configurazione dell'antivirus deve tener conto anche dei pacchetti software dedicati e con informazioni sensibili alla gestione dei DCS (ExaOPC, CENTUM, Pro-Safe, ecc...) e ignorarli nelle fasi di scan. La motivazione di questa politica va a ricercarsi sull'utilizzo in mutua

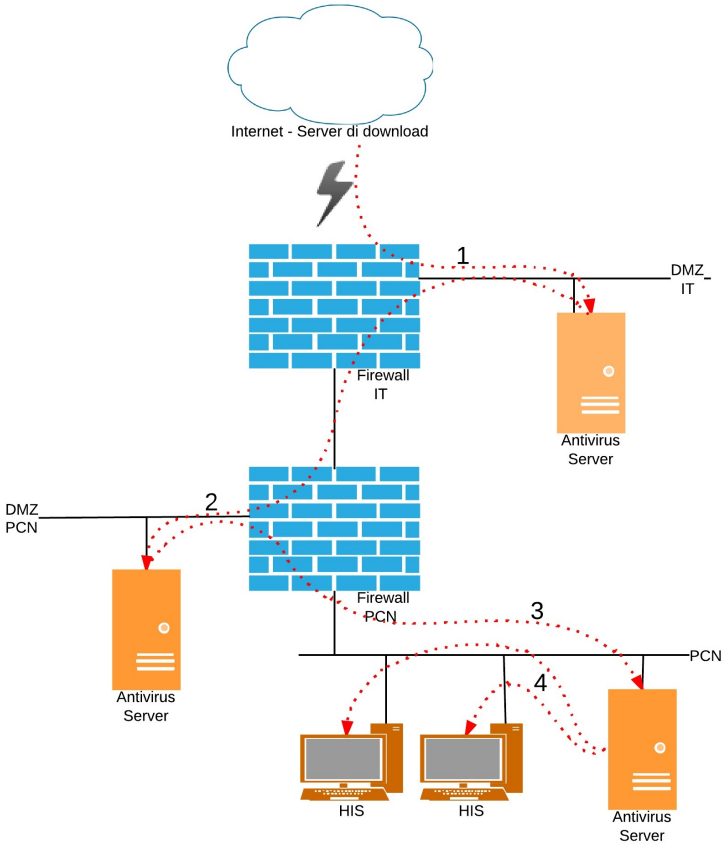


Figura 11: Distribuzione del software e delle firme dell'Antivirus nella rete di controllo di processo;

esclusione delle risorse che, senza una corretta politica di dealloccamento e di gestione delle priorità, potrebbe mandare in lock il processo di gestione del DCS. Un ulteriore considerazione nasce anche dal metodo di generazione e confronto del file scannerizzato e la lista .DAT con le firme dei virus. La verifica avviene tipicamente andando a confrontare comportamenti (i file Yokogawa hanno diritti elevati per la scrittura in zone riservate di memoria) e porzioni di codice (tramite hashing del file), a causa di queste caratteristiche i vendor degli antivirus non assicurano che un programma legittimo non venga identificato come virus (falso positivo). Alla luce di questo problema si ripetono le considerazioni sul comportamento dell'AV nella rimozione.
Il metodo di scansione utilizzato è l'on-acces per distribuire il carico di lavoro in background e non influenzare le prestazioni della CPU. Il controllo viene effettuato all'accesso per i file catalogati con meno criticità dal siste-

ma, mentre per quelli sensibili si prevede di analizzare il comportamento e nella fase di scrittura. La natura real-time predilige l'accesso immediato dei processi sensibili. E' buona norma, tuttavia, prevedere delle scansioni manuali (più onerose in termini di occupazione di CPU) schedulate nei vari fermi dell'impianto per assicurare una pulita fase di backup del sistema. Le funzioni di predizione di nuovi virus basate su tecniche euristiche sono state disabilitate (o impostate al minimo) per evitare che, oltre al dispendio di risorse, vengano rilevati troppi falsi positivi. Essendo un sistema fortemente statico nelle applicazioni utilizzate al suo interno non è necessario andare a sovrastimolare l'analisi del sistema e ad ottenere una sovrabbondanza di log. Se la segregazione tra le tipologie di codice e l'esclusione dell'analisi di materiale critico è stata operata con successo, sui i file e comportamenti che vengono rilevati come minaccia possono essere operate misure di eliminazione più drastiche, altrimenti si consiglia di operare ad una quarantena e alert dell'operatore dedicato alla sorveglianza.
L'installazione e il setting risulta essere insufficiente per la protezione se non supportato da un adeguato ciclo di update del software e delle firme dei virus. A tal proposito si suggerisce un sistema di diffusione degli aggiornamenti con uno schema a cascata come in Figura 11.

1. Scaricamento di firme e aggiornamenti dal sito web centrale Yokogawa al server nella DMZ della rete IT;

2. Dopo la diffusione sulla rete IT (se presente) e la conferma di stabilità del prodotto installato si procede al download sul server Yokogawa nella DMZ della PCN;

3. In seguito ad accertamenti sulla sicurezza viene inviato all'ultimo server per la distribuzione all'interno della PCN Yokogawa;

4. Si procede alla diffusione del codice da installare con metodologie predefinite. Tipicamente sono due le tecniche utilizzate per lo spreading degli aggiornamenti:

    - Punto di partenza su macchina meno critica e diffusione per livelli crescenti di criticità;
    - Diffusione per settori, sempre con criteri di scelta a priorità crescente;

Il rilascio degli aggiornamenti installabili a livello globale viene effettuato da una macchina server di proprietà Yokogawa dopo aver testato su simulatori l'effettiva compatibilità con i sistemi e garantire, pertanto, un certo grado di affidabilità in compatibilità con gli standard qualitativi supportati. Gli aggiornamenti (soprattutto per i file contenente le firme dei virus) devono essere eseguiti ad intervalli regolari e a scadenze giornaliere\settimanali al fine di mantenere un database *up-to-date* delle firme dei virus.

Il processo di aggiornamento di queste firme spesso impiega un dispendio di risorse di sistema, ma per tempi sufficientementi brevi. E' una buona norma programmare l'update in giornate in cui la rete è poco carica ma con presenza di operatori per il monitoraggio. L'assenza di un sistema di gestione centrale per la diffusione e il monitoraggio degli Antivirus installati è una grande debolezza del sistema; senza di esso è molto più difficile gestire l'installazione delle patch, gestire i file di log e rilevare minacce in tempi brevi. Senza una notifica dall'organo centrale, in caso di malfunzionamenti, è impossibile risalire all'origine del danno e provvedere ad evitare il ripresentarsi del problema.

4.2.3 WSUS Patch Server e management

Il secondo elemento software, dopo l'AV, da posizionare nella DMZ (il server fisico potrebbe contenere tutti e due i software) è il sistema di diffusione delle patch Windows Server Update Services (WSUS). Oltre alla limitazione negli accessi che un dispositivo di diffusione singolo comporta in una rete di questo tipo, il WSUS permette di avere un controllo centralizzato sullo stato di aggiornamento delle macchine per evitare il presentarsi di divari nelle configurazioni o la presenza di device con software datato. Altro fatto da considerare è la tipologia di aggiornamenti installati, essi non possono essere scaricati direttamente dal Windows Software Center, ma devono essere selezionati da un pool di upgrade opportunamente testati dal centro operativo di Yokogawa in Giappone. Come per la diffusione delle firme dell'antivirus, così per le patch di Windows si segue un procedimento di download a cascata come in Figura 12. I vari step sono i seguenti:

1. Scaricamento delle patch dal sito web centrale Yokogawa al server nella DMZ della rete IT;

2. Dopo la diffusione sulla rete IT (se presente) e la conferma di stabilità del prodotto installato si procede al download sul server Yokogawa nella DMZ della PCN;

3. In seguito ad accertamenti sulla sicurezza viene inviato all'ultimo server per la distribuzione all'interno della PCN Yokogawa;

4. Si procede alla diffusione delle patch da installare con metodologie predefinite. Tipicamente sono due le tecniche utilizzate per lo spreading graduale degli aggiornamenti:

    - Punto di partenza su macchina meno critica e diffusione per livelli crescenti di criticità;
    - Diffusione per settori, sempre con criteri di scelta a priorità crescente;

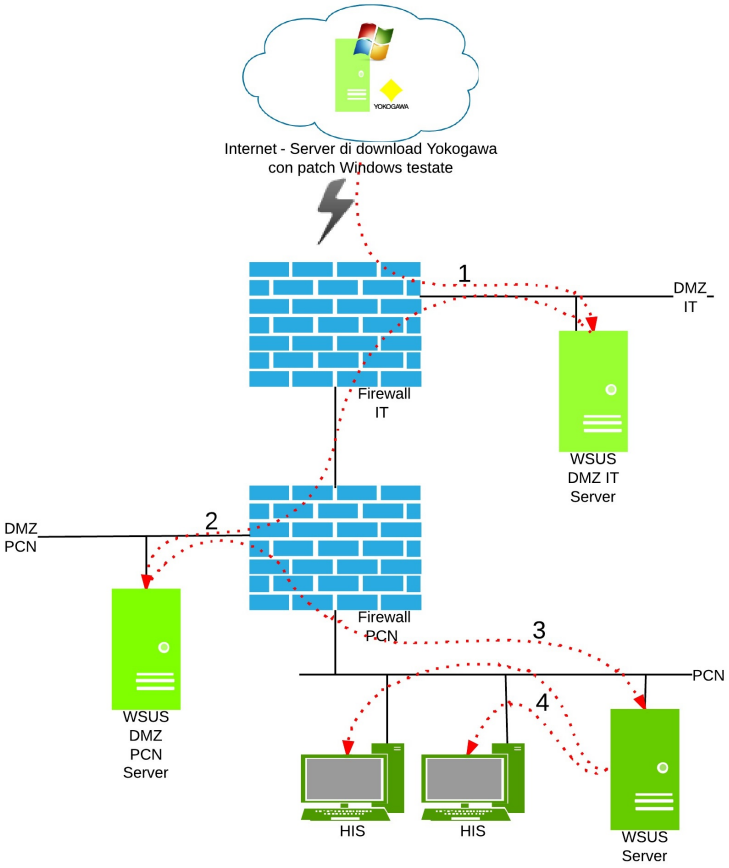


Figura 12: Distribuzione delle patch Windows nella rete di controllo di processo;

Lo scheduling delle patch ha una criticità tipicamente minore a quella dell'Antivirus in quanto mantiene nel breve termine vulnerabilità agli *0-day attack*, a differenza degli AV che se non aggiornati possono mettere il sistema in una situazione di debolezza rispetto ad attacchi *well-known*.
L'aggiornamento avviene in background e occupa percentuali di CPU ridotte per mantenere la continuità dei processi in esecuzione. Possono essere definiti dei gruppi per la tipologia di aggiornamenti e diversificare le criticità per la diffusione degli update tramite l'organo di management nella rete PCN.

4.2.4 Dispositivi della rete di processo e loro configurazioni

L'interesse per la rete di processo non si riduce alla semplice installazione di antivirus e diffusione delle patch nel sistema. Le configurazioni dedicate

di switch e router per ottenere un buon grado di fault tolerance e limitare il delay della rete dovuto all'aggiunta di software risulta essere un punto cruciale nel porre le fondamenta della rete. Mentre il firewall permette un controllo di soli quei pacchetti che gli passano attraverso (tempi di risposta variabile nell'ordine del secondo o minuto), per i dispositivi all'interno della rete che devono avere tempi di risposta inferiori (tempi di risposta nel decimo e centesimo di secondo) non è possibile effettuare ispezioni dei pacchetti a livelli troppo elevati e con pratiche troppo accurate. L'amministrazione con VLAN, come visto, permette di confinare le varie nature ed effetti di un problema (guasti compresi) ed è un primo passo avanti nel controllo della rete. Configurazioni di ACL e tabelle di routing diversificate per pacchetti e protocolli sono le altre tecniche suggerite e largamente impiegate nella strumentazione per il *forwarding* di rete.

La Figura 13 mostra come l'overlapping di tecniche di difesa (previsto dal

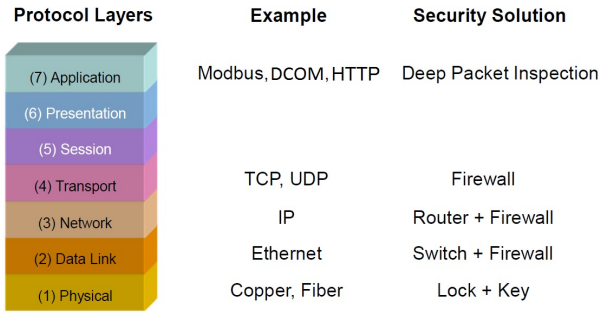


Figura 13: Tecniche adottate nei vari livelli dello stack OSI.

Defense-in-Depth) vada a coprire un pò tutti i livelli considerati nella comunicazione. Ora vedremo come l'introduzione di upgrade software e hardware permette al DCS di ottenere miglioramenti nella qualità della trasmissione senza andare a peggiorare la sicurezza dell'apparato, anche se non propriamente dedicati allo scopo. Una configurazione pensata con uno sguardo alla cyber-security permette comunque al sistema di focalizzarsi sui compiti attribuiti per il controllo di processo; dal momento in cui si vanno ad eliminare tutti i rallentamenti per l'offerta di servizi inutilizzati si possono dedicare maggiori risorse computazionali all'elaborazione di altri task utili al nostro scopo.

Upgrade dispositivi di stabilimento

Con l'introduzione della nuova versione CENTUM VP del sistema di gestione DCS sono necessari alcuni accorgimenti per l'upgrade dei dispositivi. Per compatibilità dei sistemi e aumento delle prestazioni e della capacità di elaborazione, i vecchi computer e server per la gestione della rete di processo vengono sostituiti con nuove macchine. L'aggiornamento del sistema ha

permesso di mantenere un maggior grado di compatibilità con i sistemi in utilizzo, di rinnovare il processo di update con i prodotti Microsoft prima dell'interruzione di Windows XP e di coprire tutti i flaws legati all'impiego di sistemi operativi datati.

Macchina	**Proprietà HW**	**Proprietà SW**
Stazione Server OPC	PowerEdge R720, proc. Intel Xeon E5-2640 (2,50GHz, 6C, cache 15MB, 7,2GT/s QPI, 95W, Turbo), 2 4GB RDIMM, 1.333 MHz, a bassa tensione, dual rank, x8	Windows Server 2008 R2 SP1, Attivo alimentazione controller BIOS impostazione
Stazione Ingegneria	PowerEdge T320, proc. Intel Xeon E5-2440 (2,40GHz, cache 15MB, 7,2GT/s QPI, Turbo, 6C, 95W), 2 4GB RDIMM, 1.333MHz, a bassa tensione, single rank, x4	Windows Server 2008 R2 SP1, Impostazione BIOS a elevate prestazioni
Stazione Desktop	Precision T3600 (635W), proc. Intel Xeon Processor E5-1620 (Quad Core, 3.60GHz Turbo, 10MB), 8GB (4x2GB) 1600MHz DDR3 ECC RDIMM, graph. Dual 1 GB ATI FirePro V4900 (2cards w/ 2DP & 1DVI-I each) (2DP-DVI & 2DVI-VGA adapter) (ELGA14B)	Windows 7 Professional (64Bit), Ripristino sistema operativo Dell Backup and Recovery Manager Windows 7, Dell Precision Performance Optimizer

Tabella 8: Caratteristiche tecniche workstation installate;

Hardening e OPC

La sicurezza delle singole macchine rientra nella sezione di hardening della rete e nella fase di protezione degli end-point. Ovvero si occupa di stabilire norme e regolamenti rivolte a limitare le capacità superflue dei dispositivi contenuti nella rete di processo e di provvedere al setting delle stesse secondo i parametri determinati. Sembrerebbe una limitazione delle capacità operative del sistema, tuttavia è opportuno considerare come un qualsiasi servizio che non rientra nella whitelist, un qualsiasi programma installato senza richiedere il consenso dell'amministratore e scritture su parti di sistema impropri siano atteggiamenti che non hanno ragione di esistere in una rete di impianto dai comportamenti fortemente deterministici; previa la possibilità di creare falle e errori imprevisti. Rivedendo nel dettaglio la configurazione del firewall Yokogawa è possibile scorrere una breve lista dei servizi concessi. Nella Tabella 9 sono elencate le porte TCP e UDP aperte per la generazione di flussi comunicativi, in particolare per la comunicazione DCOM viene indicato il range di porte concesso al protocollo.

Dallo stesso principio con cui si forgiano le regole nel firewall per l'OPC si può procedere alla generazione dei servizi da bloccare e quelli consentiti all'interno di ciascun computer e server nella rete. Il principio fondamentale del ragionamento per le configurazione rimane quello di considerare che se

Setting	**HIS&ENG**	**Domain Server**	**File Server**
Di base	Deny All	Deny All	Deny All
Eccezioni	• TCP:135 (RPC/DCOM) • TCP:443 (HTTPS) • TCP:445 (Direct Hosting) • TCP:1131 (ProSafe-RS) • TCP:1433 (SQL Server) • TCP:20100-20200 (Monitoring)* • TCP:20500-20550 (DCOM) • TCP:34405 (ProSafe-RS) • UDP:1037 (ProSafe-RS)	• TCP:88 (Kerberos Authentication) • TCP:135 (RPC/DCOM) • TCP:389 (LDAP) • TCP:445 (Direct Hosting) • TCP:20500-20550 (DCOM)* • UDP:53 (DNS) • UDP:88 (Kerberos Authentication) • UDP:389 (LDAP)	• TCP:445 (Direct Hosting)

** Le porte UDP:1250, 52302 e TCP:20109, 20111, 20171 sono sottoposte ad una sorveglianza speciale per debolezze del sistema CENTUM.*

Tabella 9: Nuovi filtri dedicati alla comunicazione dell'OPC per il nuovo firewall Yokogawa (Strengthened mode)[28];

ad un servizio non è concesso di circolare nella rete, per lo stesso motivo non ha ragione di esistere attivo su una stazione. Viene ora presentata una lista dei servizi disattivati\stoppati nelle stazioni e i benefici che si ottengono dal blocco impostato.

- NetBIOS, questo servizio potrebbe fornire ad un eventuale attaccante la lista di servizi attivi sulla macchina;
- DHCP Client, stoppandolo si blocca la possibilità di una modifica di DNS e IP dinamici per la comunicazione di rete (tutti i servizi basati su quest'ultimo cessano di funzionare);
- Windows Error Reporting, evita l'uscita dalla rete di informazioni sui log;
- IP Helper, non si permette la comunicazione con protocollo IPv6;

- IPSec Policy Agent(tranne che su quei terminali su cui è prevista la comunicazione tramite VPN);
- Offline Files, evita di mantenere le informazioni sui file condivisi in una memoria cache;
- Remote Registry (possiede enormi falle nella sicurezza);
- Secondary Logon;
- Shell Hardware detecher, elimino le notifiche di eventi di AutoPlay;

Altri accorgimenti software utilizzati riguardano il setting del sistema operativo e dell'utilizzo di alcune sue funzionalità. In particolare la disabilitazione dell'account di admin, la modifica dell'autenticazione dell'ambiente CENTUM e l'hiding dell'ultimo username con cui ci si è loggati al sistema sono alcuni degli accorgimenti base con cui impostare l'OS.
Nonostante la disabilitazione di accessi USB e tramite lettori CD e DVD si rende necessario anche il blocco dell'esecuzione automatica di programmi tramite *autorun*; in particolare la restrizione evita che quei malware che superano le difese (mail infette e non riconosciute) tentino di replicarsi ancor prima di essere passati in rassegna dall'Antivirus. Windows ha altre configurazioni di default che devono essere modificate per rendere ciascun PC performante a servire la rete e raccogliere informazioni. Le policy di audit e gli eventi da registrare devono essere configurati con conseguente dimensionamento dei file log in relazione e della sovrascrittura, vengono presi provvedimenti per il lockout degli account in caso di fallimento e, soprattutto, viene utilizzato il software SysKey per aggiungere un ulteriore strato di cifratura alle password ed evitare il cracking offline tramite dictionary e brute force attack.
L'intera gamma di accorgimenti elencati viene ripresa all'interno del documento TI 30A15B31-01E (visionabile dal solo personale Yokogawa) e costituisce la base tecnica su cui operare cyber-security a livello di end-point.

4.2.5 Funzionalità aggiuntive, account e monitoring

I pacchetti software e dispositivi hardware previsti dalla migrazione di per se non fanno parte dei prodotti dedicati alla sicurezza del sistema. Tuttavia, sotto opportune customizzazioni e impostazioni di sistema, persino strumentazione secondaria ad i propositi imposti può offrire funzionalità operativamente efficaci ad evitare ed individuare intrusioni. Vengono qui di seguito presentate i middleware DCS impiegati da Yokogawa e l'Active Directory per la gestione delle risorse condivise in rete. Senza la configurazione idonea, non solo si perdono i vantaggi appena elencati, ma è palese il rischio di favore la diffusione di informazioni sensibili. In particolare la condivisione di informazioni con Active Directory potrebbe portare alla diffusione incontrollata

di malware che sfruttano privilegi di rete. Vediamo ora invece i vantaggi che questi sistemi offrono.

CENTUM VP e Prosafe-RS

I pacchetti software Yokogawa CENTUM VP e Prosafe-RS[30], nelle loro ultime versioni, offrono la possibilità di essere gestite negli accessi e nei permessi come gruppi di Windows. I due sistemi possono essere mantenuti separati negli accessi in modo da offrire una maggior segregazione e controllo sul software e sul log degli utenti.

Active Directory

I servizi di Active Directory (AD) forniscono un set di servizi di directory che sono inclusi in Windows Server come parte integrante delle funzionalità del Domain Controller[31]. Un *directory service* è un servizio di rete che identifica tutte le risorse (dati utente, stampanti, server, database, policy, ecc...) e i servizi per la diffusione delle stesse in una rete windows che permette di renderle accessibili ai vari utenti e applicazioni. Nell'Active Directory le risorse sono organizzate in una struttura logica. Raggrupparle in questo modo permette di trovarle secondo il loro nome piuttosto che secondo la loro posizione fisica rendendo la struttura trasparente agli utenti.
Il componente fondamentale dell'AD che supporta il sistema di indirizzamento logico e di gestione delle subnet viene gestito dal Domain Name System (DNS) relativo che si occupa della treduzione dei nomi. Il DNS è configurato utilizzando zone di inoltro e reverse lookup. Le zone di forward-lookup traducono i FQDN (Fully Qualified Domain Name) in indirizzi IP. Le zone di reverse lookup funzionano al contrario, esse traducono gli IP in nomi FQDN. Attribuendo un nome logico e non un indirizzamento fisico al componente di rete si permette di nascondere la locazione del servizio nella subnet e di permettere all'AD e DNS di filtrare le richieste interne in base a nomi e IP precedentemente validati e autorizzati.
Grande parte delle funzionalità degli AD si occupano di AAA (Authentication, Authorization, Accounting), ed è importante verificare a quale livello queste sono implementate. Gli user account sono autenticati confrontando i valori di username e password con quelli contenuti nelle informazioni di directory. Se i campi sono corretti, viene permesso l'accesso. Gli account del computer sono autenticati correttamente quando un utente si è loggato. Gli account per cui non si richiede una password inviano un'unica stringa, assieme all'account del computer, per essere autenticata dai domini. Questo metodo serve ad assicurare che solamente ai dispositivi autorizzati venga

[30]Prosafe-RS: sistema di controllo di sicurezza basato su architettura CENTUM VP.

[31]Domain Controller (DC): Server che risponde alle richieste di autenticazione per la sicurezza (log-in, controllo dei permessi, ecc.) nell'ambito di un dominio in ambiente Windows.

permesso il login al dominio, tuttavia è un comportamento che dovrebbe essere eliminato in favore di una politica degli accessi più restrittiva.
Dopo che l'autenticazione ha avuto luogo, computer e utente sincronizzano le rispettive informazioni di autorizzazione. Quest'ultima contiene un'estesa lista di diritti attraverso la directory che sono assegnati all'AD object. Per esempio, ad un utente possono essere proibiti i diritti di amministratore nella macchina su cui sta lavorando in locale. La fase di accounting avviene ogni qualvolta un object richiede o invia informazioni al DC. Questa azione viene memorizzata nel log e può essere controllata in tempi successivi dall'amministratore di sistema. La definizione degli account in Eni è generica e non aiuta la consultazione dei log; un suggerimento (e tale per ora rimane, la modifica deve partire dall'amministrazione dell'organico) è quello di aggiungere account e gruppi intermedi per le classi di utenza (operatore, genio, reparto ingegneria, manutenzione, ecc...) e abilitare per ciascuno una classe di servizi utilizzabili e limitare la conoscenza dei privilegi forniti dall'amministratore al minor numero di user. Per maggiori informazioni sulle tipologie di account creabili e sulle Policy si rimanda a pagina 24 del file FDS in appendice C.

4.3 Vulnerabilità residue e miglioramenti ottenibili

A causa delle necessità di consistenza della rete e della continuità di processo, molte delle innovazioni e degli upgrade necessari non sono stati considerati attuabili nel breve termine. Per un completo sviluppo delle attività di cyber-security Eni ha stanziato budget ed investimenti nel lungo termine che richiedono, tuttavia, ulteriori valutazioni legati all'andamento del processo e allo stato della rete. In altri casi l'assenza di software per il monitoring precedente alla migrazione, in grado di sostenere e tenere traccia nel corso degli anni di eventuali situazioni di pericolosità e di danno, ha creato una carenza di informazioni e conoscenze per la quale non è possibile sostenere al meglio le scelte effettuate e analizzare al meglio il sistema e rilevare comportamenti malevoli dello stesso. Partendo da questa base spinosa, però, è possibile dedurre e proporre alcuni miglioramenti che, a fronte di interventi strutturali futuri e schedulabili in maniera più organica, porterebbero enormi benefici sul fronte della sicurezza e della responsività del processo.

Architettura ideale

Il primo intento per ottenere una rete di processo ideale è quello di confinare ciascun vendor nella propria PCN. Rimuovere la parte di rete mista è il primo obiettivo di questa proposta, in particolare in questo modo si aumenta la scalabilità del sistema, infatti, per ciascun nuovo elemento della rete Yokogawa che verrà aggiunto negli anni, non è necessario andare a modificare le regole del firewall rivolto alla PCN di Eni. Al tempo stesso non

ha più ragione di esistere il firewall Yokogawa inserito nel tronco di rete. Le regole di quest'ultimo andrebbero riprodotte sul firewall principale e mai più modificate. La rete otterrebbe anche meno rallentamenti interni dovuti alla comunicazione fra OPC e device. Questione spinosa, tuttavia, risulta la comunicazione tra OPC e database storico Cim-IO che aprirebbero una serie di porte nel firewall con flusso continuo appesantendone la capacità operativa. A tal proposito si consiglia l'impiego di un strumento software per il tunnelling della comunicazione e limitare così il numero di porte aperte. Il software già impiegato in varie attività da parte di Yokogawa sarebbe il MatrikonOPC Tunneller[32].
Il nuovo design di rete, nel modo in cui è stato appena descritto, avrebbe una rappresentazione architetturale simile a quella in Figura 14. Nel modello, così definito, sono stati aggiunti altri strumenti hardware (server e firewall) di cui si motiva la scelta qui di seguito. Annessi ad essi i relativi servizi software che contribuiscono a migliorare lo stato della rete, sia in termini di sicurezza, sia mantenendo i vincoli real-time operativi. Con la rimozione

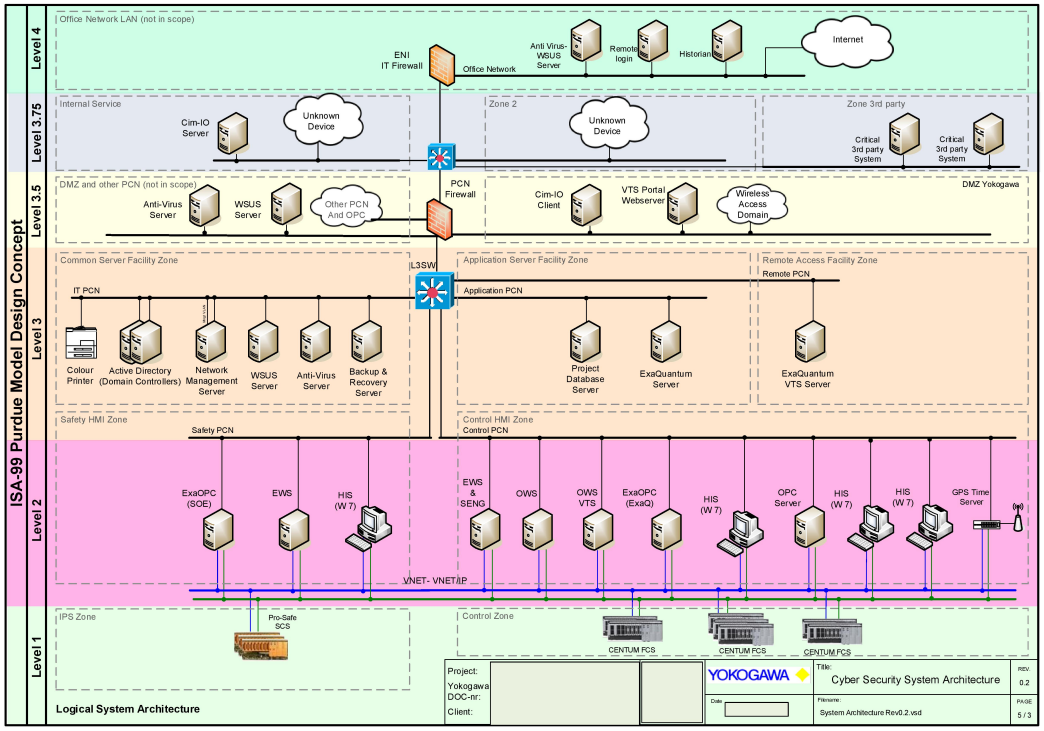


Figura 14: Architettura migliorata di ENI Venezia;

[32]MatrikonOPC Tunneller: software di proprietà della Matrikon Inc., forniscono apparecchiature e prodotti per la connettività dati basati sullo standard OPC. www.matrikonopc.com.

del firewall dedicato Yokogawa e posizionando tutti i server precedentemente segregati è necessario tutelare i server in questa nuova DMZ da accessi esterni. Il Web Application Firewall (WAF) situato in testa al firewall PCN permette di ridurre il carico di lavoro su quest'ultimo e di ripristinare le vecchie prestazioni. Il WAF, in particolare, analizza con maggior intensità il traffico HTTP utilizzato per le connessioni remote, spesso rivolte a server web relativamente insicuri e con una moltitudine di richieste di accesso a Database e storico dei dati. E' particolarmente indicato in questa situazione prevenendo attacchi di tipo cross-site scripting e SQL injection, tipicamente utilizzati per inserire codice malevolo nelle interrogazioni al Server.
Con un server dedicato si possono introdurre anche IDS stateful e provvedere a dotarli di eurista per individuare i comportamenti sospetti e agire proattivamente alle problematiche che si verificano. Mentre molti si oppongono all'utilizzo nella rete di processo di sistemi di prevenzione delle intrusioni (IDPS) o qualsiasi altro tipo di protezione pro-attiva perché pericolosi per la stabilità del processo, in una situazione di questo tipo, bilanciando opportunamente l'intervento, si potrebbe beneficiare delle nuove funzioni intelligenti senza compromettere l'intero apparato. Importante da segnalare il fatto che non tutte le reti (interamente o parzialmente) possono sostenere la protezione pro-attiva e che deve essere una dotazione valutata caso per caso.
Un ulteriore dotazione hardware della rete di processo che è stato pensato appositamente per la protezione della rete industriale è il Tofino[33]. Questo dispositivo, inserito in un tronco di rete permette di monitorare l'attività del network in modo assolutamente trasparente, senza richiedere indirizzo IP. I benefici sono ovviamente la possibilità di monitorare in maniera approfondita la rete come mai era stato fatto in altri impianti del genere, oltre a eliminare ulteriori punti di ingresso della rete non previsti e limitare le infezioni. Il vantaggio principale è la possibilità di evitare che attacchi di tipo DDoS possano interrompere il funzionamento della rete nella sua interezza. L'efficacia di un attacco malevolo di questo tipo viene di conseguenza limitata dalla presenza di questi dispositivi.
Il trattamento delle informazioni del malware dovrebbe essere gestito da un organo centrale tramite il McAfee ePolicy Orchestrator (ePO, versione 5.1 la più recente). I lati positivi di questo strumento software per la gestione client-server nella rete sono molteplici:

- Gestione distribuita e ottimizzata di aggiornamenti di software e firme;
- Organo centrale di controllo dei log degli antivirus dell'impianto;
- Strumenti aggiuntivi e avanzati per report e diagnostica;

Con l'upgrade di alcuni server e postazioni, nelle zone borderline e meno critiche, verificando con un periodo di test il dispendio di risorse, si consiglia

[33]Tofino: prodotto commerciale della Byres Security Inc. (BSI) acquisita nel 2011 dalla Belden Inc. e Hirschmann.

di aumentare l'attività degli algoritmi euristici per rendere il sistema pronto a reagire ai virus di nuova generazione.
La cifratura della comunicazione rimane una questione spinosa per la rete PCN e la necessità di contenere i tempi di comunicazione, come visto nella relativa sezione. In tal senso dovrebbe essere prioritario per gli organi di ricerca e sviluppo trovare un meccanismo di cifratura che permetta alla rete di mantenere una responsività del sistema adeguata e al contempo fornire una protezione della sicurezza dei dati soddisfacente. DCOM offre pacchetti di funzionalità di privacy ed integrity, ma che richiedono un accurata predisposizione dei pacchetti software che ne fanno utilizzo, tuttavia sono comunque insufficienti per le capacità di analisi di un hacker con esperienza di cracking di cifrature.
Rimanendo tuttavia, fino ad ora, delle considerazioni di protezione teoriche si rimanda ad un'analisi di esperti per far fronte ad eventuali falle di sistema. Mentre gli strumenti per il vulnerability assessment in commercio si potrebbero rivelarsi dannosi per l'integrità della rete, un RedTeam, nonostante di solito vengano rifiutati per intervenire negli ICS, con esperienze di Penetration Testing rivolte a sistemi fragili, potrebbero aiutare ad eliminare una buona parte delle vulnerabilità residue senza inficiare negativamente nel processo.
Qualsiasi software aggiuntivo disponibile alla sorveglianza della rete, tuttavia, è uno strumento potente, e spesso sufficiente, nelle mani di un operatore attento alla cyber-security, se adeguatamente addestrato ed educato a mantenere un costante interesse su questi aspetti della rete. Vediamo qui ora qualche esempio specifico di tool suggerito spesso da Yokogawa nei propri interventi.

4.3.1 Network Management Server

Nella PCN Yokogawa non è previsto, a causa del numero esiguo di macchine rispetto ad altri impianti e alla tipologia di servizio offerto, l'utilizzo di un Network Management Server (NMS). Questa combinazione di hardware e server viene utilizzata generalmente per monitorare e amministrare la rete e la sua moltitudine di componenti. La ricerca di fallimenti, rallentamenti, l'interruzione di servizi e la relativa notifica al server centrale permette di ricevere risposte nel breve termine sullo stato della rete. L'abilità di intercettare i problemi rapidamente è di importanza cruciale; il personale operativo della rete può fare affidamento su una mappa grafica della rete che ne evidenzia lo stato operativo dei dispositivi più critici come router e switch.
Nel caso di un impianto come quello di Venezia, composto da una trentina di elementi di rete (tra router, switch e terminali), sembrerebbe superfluo avere un sistema di amministrazione così avanzato (che permette oltretutto di snellire il traffico SNMP); tuttavia, dal punto di vista del mantenimento della cyber-sicurity e il supporto contante del sistema, per la difesa dei virus

di rete si pone come uno strumento fondamentale. Il monitoring e il rilevamento dei malware, che spesso tendono a sviluppare traffico aggiuntivo nella rete, potrebbe trarre vantaggio dall'aggiunta del NMS.
In compatibilità con i sistemi Yokogawa, come comprovato in altri impianti, è consigliato l'utilizzo del software WhatsUp Gold che supporta anche le funzionalità da Domain Controller collaborando con la rete Windows.

4.3.2 Exaquantum

L'Exaquantum è il PIMS[34] che supporta la produzione e l'andamento registrato dal DCS CENTUM. Oltre ai già elencati benefici di accountability offerti da altri prodotti della rete, ci sono alcune migliorie del sistema che vanno a coprire i flaws del sistema.

- Il servizio SQLServer viene eseguito come QuantumUser (al posto di LocalSystem);
- Database e store procedure hanno accessi limitati e i Database di Demo sono rimossi dal sistema (punti di accesso per attacchi);
- SQL e Exaquantum non hanno diritti di amministratore;

Più che una serie di prodotti focalizzati alla sicurezza, si intende, con questo paragrafo, offrire velocemente una panoramica su alcuni prodotti Yokogawa con funzionalità security-care e i miglioramenti continuamente portati avanti in tal senso.

[34]Plant Information Management System (PIMS): raccoglie e integra le informazioni relative ad un processo di produzione da fonti diverse. I compiti importanti del PIMS sono: raccogliere, consolidare e storicizzare i dati in tutta l'azienda, l'analisi delle prestazioni di produzione, qualità del prodotto, capacità di processo e conformità alle normative.

5 Conclusioni

L'ambiente della gestione della produzione industriale ha avuto negli ultimi anni dei profondi cambiamenti dal punto di vista dell'interconnessione dei dispositivi e della gestione delle risorse. Inizialmente separata dal mondo IT, la rete di impianto ha ottenuto un'apertura progressiva verso la rete globale approfittando dei benefici nell'aumento della responsività del sistema e nella salvaguardia della produzione, a discapito della protezione delle infrastrutture di rete. La sicurezza dei mezzi informatici, in questo ambito industriale, risulta essere spesso trattata in secondo piano, e con mezzi inadeguati, rispetto alle altre esigenze che vanno ad influenzare direttamente l'ambiente produttivo. La presenza di questo fenomeno di discrepanza di gestione e di investimento è spesso il risultato di scelte di business atte a soddisfare la crescita del processo nell'immediato senza un'adeguata presa visione dei rischi e del degrado progressivo della rete nel lungo termine. Il più delle volte la scarsa sensibilità in materia non viene supportata strumentalmente dalla presenza di risorse per determinare l'impatto di un eventuale cyber-attacco, il grado di sicurezza coperto e la presenza di falle nel sistema. Con questa tesi si tenta di allargare ulteriormente il punto di contatto tra il mondo IT e quello dei processi industriali. Il proposito principale è quello di offrire informazioni e indicare la strada da percorrere in materia di security ad un esperto di automazione di impianto, generalmente carente di conoscenze del mondo informatico, e, al tempo stesso, fornire una maggiore sensibilità alle caratteristiche della rete di impianto ad un gestore IT.
Si evince, tuttavia, che la rete di impianto, con le sue caratteristiche e peculiarità, non è in possesso di mezzi sufficientemente preparati (o configurabili) ad affrontare tutta la gamma di attacchi di rete. Un intervento di ricerca e sviluppo in tal senso, con nuove teorie sui sistemi, firewall dedicati e cifrature sviluppate *ad hoc*, potrebbero portare ad una customizzazione maggiore nella gestione dei protocolli e alla copertura di vulnerabilità legate alla rete di processo. La sicurezza al momento non è costituita da una metodologia e strumentazione perfetta, ma è un sistema vivo che si dovrebbe adattare all'evolversi della tecnologia attorno a se, al pari degli altri strumenti utilizzati per il processo. E' pertanto necessario, oltre all' R&D di nuovi meccanismi di difesa, fornire una *forma mentis* per il personale operativo per coprire il gap strumentale e delle performance tra le nuove tecniche di attacco e diffusione dei malware e la prontezza nella difesa del sistema. Una mentalità pro-attiva acquisita, un sistema di autovalutazione e penetration testing della sicurezza e un processo di monitoring integrato nel sistema sono combinazioni vincenti che potrebbero aiutare a colmare il divario e mostrare anche al più stoico industriale i benefici di una politica ciclica di cyber security. La sicurezza è un sistema che si autoalimenta in certe sue fasi e che, soprattutto in questi casi, può fare la differenza non solo economica, ma anche per la vita e la salvaguardia di personale e ambienti.

6 Bibliografia

[1] http://www.isa-95.com/subpages/technology/isa-95.php;

[2] Massimiliano Veronesi, Sistemi di controllo distribuito;

[3] Gleb Gritsai, Alexander Timorin, Yury Goltsev, Roman Ilin, Sergey Gordeychik, Anton Karpin, Scada Safety in number v1.1, Positive Technologies;

[4] http://www.opcfoundation.org/Default.aspx;

[5] http://www.opcfoundation.org/Products/Specifications.aspx?CM=-1;

[6] http://www.microsoft.com/com/default.mspx;

[7] http://www.securityincidents.org/;

[8] http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-979;

[9] http://www.securityfocus.com/news/6767;

[10] Confiker Working Group, Lesson Learned;

[11] http://www.microsoft.com/it-it/security/pc-security/conficker.aspx#EKE;

[12] http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/;

[13] Nicolas Falliere, Liam O Murchu e Eric Chien, W32.Stuxnet Dossier, Symantec Security Response;

[14] W32.Duqu The precursor to the next Stuxnet, Symantec Security Response;

[15] http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99&tabid=2;

[16] http://www.symantec.com/outbreak/?id=flamer;

[17] Laboratory of Cryptography and System Security (CrySyS Lab), Flamer: A complex malware for targeted attacks, Budapest University of Technology and Economics Department of Telecommunications;

[18] L. Durante, A. Valenzano, CYBERSECURITY E RETI INDUSTRIALI, Consiglio Nazionale delle Ricerche (CNR),Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni (IEIIT);

[19] http://it.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology;

[20] Keith Stouffer, Joe Falco, Karen Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 1;

[21] Technical Information(TI) TI 33Y01B30-01E, Security Standard of System Product, Yokogawa Electric Corporation;

[22] Enzo M. Tieghi, Introduzione alla protezione di reti e sistemi di controllo e automazione, Clusit;

[23] Architecture for secure scada and distribute control system networks, white paper, Juniper Network;

[24] Joe Falco, Steve Hurd, Dave Teumim, Teumim Technical, Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts, NIST special publication 1058;

[25] Technical Information(TI) TI 30A15B31-01E, Security Standard of System Product, Yokogawa Electric Corporation;

[26] http://www.wurldtech.com/product_services/certify_educate/achilles_certifications/;

[27] http://windows.microsoft.com/en-us/windows/end-support-help;

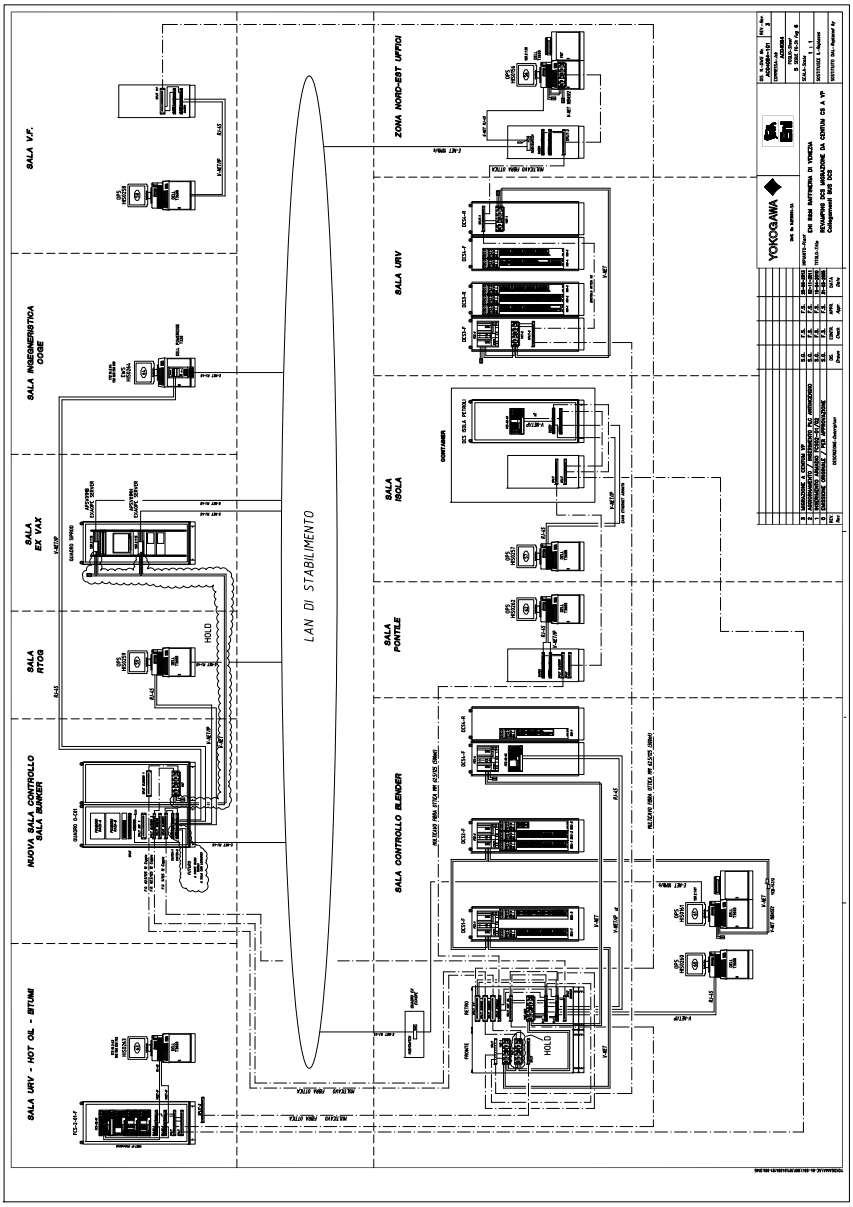
[28] IT Security Guide for System Products (CENTUM),TI 30A15B31-01E (Internal Use Only)[35];

[29] Eric Byres, P.E. Dr. Dan Hoffman, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems;

[35] Alcuni dei documenti di riferimento della bibliografia possono non essere pubblicamente disponibili in quanto di proprietà di Yokogawa Electric Corporation e contenuti con restrizioni di riservatezza nell'intranet aziendale.

7 Appendici

7.1 Appendice A: CAD rete di processo ENI R&M Venezia



7.2 Appendice B: Bozza di FDS proposto ad ENI.

Progetto: _____ ENI IT Security

Functional Design Specification – IT Security

REVISION CHANGE DETAILS

Rev.	Date	By	Checked	Approved	Description
0	4/Dec/2013	AP	PC	MV	First issue

TABELLA DEI CONTENUTI

FDS
ENI IT Security
Progetto: 14B120019
Doc. Name: 14B120019_FDS
Rev 0

1 Introduzione

1.1 Funzione del Documento

I sistemi di automazione di processo si sono evoluti dai singoli computer isolati con sistemi operativi proprietari e reti di sistemi interconnessi a delle applicazioni che impiegano componenti COTS (commercial off the shelf). Questi impianti sono stati integrati con sistemi aziendali e altre applicazioni business attraverso reti di comunicazione. L'aumento del livello di integrazione permette un numero significativo di benefici al business, tra I quali:

- Aumento della visione delle attività dei sistemi di automazione (stato dei dispositivi e del processo, pianificazione della produzione) e un sistema di integrazione con il processo a partire dal livello commerciale, il quale contribuisce ad affinare l'abilità con cui condurre analisi, abbattere costi di produzione e migliorare la produttività.
- Integrazione nei sistemi produttivi che permette un maggior accesso diretto a informazioni sull'andamento economico, permettendo una maggiore reattività nel gestire l'impresa.
- Interfacce che riducono i costi complessivi di sostenimento e consentono supporto remoto dei processi produttivi.
- Monitoraggio in remoto dei sistemi di automazione di processo che permettono una veloce soluzione delle problematiche.

E' possibile definire degli standard per modelli, termini, e scambi di informazione che permettono all'insieme degli operatori del sistema di condividere informazioni in modo consistente. Tuttavia, questa facilità di condivisione permette la crescita di vulnerabilità ad un errato trattamento dei dati e ad attacchi da individui con intenti malevoli introducendo potenziali rischi all'azienda che ne utilizza il sistema di automazione di processo.

Il sistema di automazione di processo opera in un ambiente complesso. Organizzazioni stanno incrementando la quantità di informazioni condivise attraverso rapporti commerciali e sistemi industriali; partner in un settore di business possono essere in competizione in un altro. Tuttavia, essendo l'attrezzatura dei sistemi di automazione direttamente connessa al processo, la perdita di segreti commerciali e interruzione nel flusso di informazioni non sono l'unica conseguenza di una breccia nella sicurezza. La potenziale perdita di produzione, i danni agli ambienti, la violazione dei regolamenti e compromissione della salvaguardia degli operatori sono solo alcune delle più gravi conseguenze. Queste possono avere esiti al di là dell'organizzazione mirata e possono gravemente danneggiare l'infrastruttura della regione o nazione ospitante.

Le minacce esterne non sono le uniche preoccupazioni: un membro dell'organico, con buone conoscenze e intenti malevoli o, semplicemente, un gesto frutto dell'errore umano possono rappresentare un serio rischio alla sicurezza. Dato che un sistema d'automazione è spesso integrato con altri sistemi di business, modificare o testare sistemi in opera può portare ad effetti indesiderati sulle operazioni di sistema.

Combinando fattori interni ed esterni, è facile notare che il pericolo potenziale di permettere accessi non autorizzati o l'accesso dannoso al sistema industriale è tutt'altro che un problema di facile soluzione.

Infatti, nonostante i cambiamenti tecnologici, e l'influenza positiva per il business, queste problematiche aumentano i rischi legati alla sicurezza. Così come le minacce al business sono in crescita, così anche le necessità di una maggior sicurezza.

Questo documento descrive le soluzione che saranno applicate da Yokogawa con l'intento di implementare una soluzione di IT Security nella sede Eni R&M di Venezia. Questo documento tratterà gli stessi argomenti visti nel corso dei controlli di sicurezza e comprenderà raccomandazioni basate sull'esperienza e le procedure Yokogawa.

La soluzione dettagliata in questo documento è basata su sistemi operativi Windows (Windows 7 Professional e Windows Server 2008) e tecnologie sviluppate con i prodotti Yokogawa.

1.2 Obiettivo del Documento

L'approccio generale di Yokogawa System Security Design segue gli standard/report tecnici come BS ISO/IEC 27001/27002 e ISA SP99. Per l'impianto ENI R&M Venezia, Yokogawa prende in considerazione anche il documento ENI XXXXXXXXXXXXX

Le soluzioni per mettere in sicurezza un sistema di controllo:

- Firewall
- Antivirus Server
- WSUS Microsoft OS Patch Server
- Active Directory Server
- Hardening di Server e workstation

La soluzione per il mantenimento del business sarà basata su:

- Network Management Server (NMS)

Nei capitoli seguenti è possibile trovare dettagli per ogni soluzione prevista per l'impianto ENI Venezia.

Documenti di riferimento e Standard

Per i documenti si faccia riferimento ai numeri fra parentesi [].

Ref.	Titolo del Documento	Documento No.
[1]	Information Security Management Systems	BS ISO/IEC 27001
[2]	Information technology-Security techniques-Code di practice for information security management	BS ISO/IEC 27002
[3]	Security for Industrial Automation and Control Systems Part1: Terminology, Concepts, and Models	ANSI/ISA-99.00.01-2007
[4]	Security Technologies for Industrial Automation and Control Systems	ANSI/ISA-TR99.00.01-2007
[5]	Integrating Electronic Security Into the Manufacturing and Control Systems Environment	ANSI/ISA-TR99.00.02-2004,
[6]	Guide to Industrial Control Systems (ICS) Security (SECOND PUBLIC DRAFT)	NIST SP800-82
[7]	Security Standard di System Product	TI 33Y01B30-01E
[8]	Production IT Security Standard	XXXXXXXXXXXXXX

2 Termini e Abbreviazioni

2.1 Abbreviazioni

AD	Active Directory
AMADAS	Analyzer Management And Data Acquisition System
ANSI	American National Standards Institute
COTS	Commercial off the Shelf
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
ERP	Enterprise Resource Planning
FAST/TOOLS	Advance Process Control Management software
FCS	Field Control Station
FDS	Functional Design Specification
FGS	Fire and Gas System
FTP	File Transfer Protocol
GSGW	Generic Subsystem Gateway
HIS	Human Interface Station
HIS-TS	Human Interface Station – Terminal Server
HIS-ENG	Human Interface Station – Engineering Station
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
ICCP	Inter-Control Centre Communications Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute di Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	The Instrumentation, Systems and Automation Society
ISMS	Information Security Management System
ISP	Internet Service Provider
ESSID	Extended Service Set Identity
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control (address)
NetBIOS	Network Basic Input/Output System
NTLM SSP	Windows NT LAN Manager Security Support Provider

NTP	Network Time Protocol
OPC	OLE for Process Control
OS	Operation System
PAS	Process Automation System
PCN	Process Control Network
PLC	Programmable Logic Controllers
POC	Proof Of Concept
PRM	Plant Resource Manager
RBNS	Role Based Name Space
RDAS	Rotating Disc Analytical System
RPC	Remote Procedure Call
RTU	Remote Terminal Units
SCS	Safety Control Station
SENG	Safety Engineering Station
SER	Sequence di Events Recorder
SIOS	Software for Innovative Open Solutions
SIS	Safety Instrumented System
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SCADA	Supervisor Control And Data Acquisition
SOE	Sequence di Events
SQL	Structured Query Language
TCP	Transmission Control Protocol
TDAS	Tank Data Acquisition System
TS	Terminal Server
UDP	User Datagram Protocol
WSUS	Windows Server Update Services

Definizioni

- **Process Automation System**

  Sistema di Livello 1 fino a Livello 3 di un tipico modello di un architettura di rete

- **Sistema di Controllo di Processo**

  Sistema di Controllo Distribuito

- **System Data Highway**

  Bus di controllo, Yokogawa Vnet/IP

3 Misure di Controllo di Base sulla Sicurezza

Strategia di Base per la Gestione della Sicurezza

Minacce alla sicurezza sono in costante evoluzione. Peraltro, questi rischi non sono confinati alle reti esterne come le reti aziendali, ma anche a quelle interne, come quelle PCN. Per questa ragione è importante implementare una strategia di difesa che vada in profondità (***Defence-in-Depth***).

Come mostrato in **Figura 3-1**, con questa strategia, vogliamo che le misure di protezione siano composte da più di un controllo di sicurezza per la tutela del sistema. Attraverso l'uso di questo tipo di sistema multi-livello, ciascuno strato continuerà ad offrire protezione anche nel caso in cui un altro venga distrutto, in modo da salvaguardare con maggior fermezza i dispositivi.

- **Network boundary security**

E' un punto di contatto tra la rete di controllo e la rete esterna, come la rete aziendale, e previene l'ingresso delle minacce esterne nella rete di controllo.

- **Internal network security**

La funzione di questo livello è di ridurre i danni di minacce che si verificano nella rete di controllo il più possibile. Per esempio, divide la rete di controllo in varie zone e costruisce la rete in modo da non permettere che danni in una zona non abbiano effetto in altre.

- **End point security**

E' un provvedimento atto all'esclusione delle vulnerabilità nei dispositivi *end-point*. Questa metodologia comprende, per esempio, installazione di patch di sicurezza e disabilitazione della lettura dei dispositivi USB.

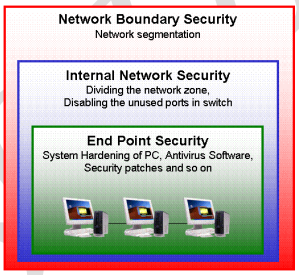


Figura 3-1:Strategia Defence-In-Depth

3.1 Physical security

Il primo strato di difesa è la sicurezza a livello Fisico (Physical security). Se un individuo con intenti malevoli può connettere il proprio portatile alla rete interna dell'impianto o aver accesso ad un computer, il sistema sarà considerato sotto attacco. Con la sicurezza a questo livello viene creata una prima linea di difesa. Nell'impianto ENI Venezia tutti i computer avranno una password di accesso e tutte le porte non utilizzate dalla rete saranno disabilitate. Tuttavia, se un hacker ha la possibilità di accedere fisicamente ad un computer, quest'ultimo potrebbe avere la possibilità di scoprire la password tramite *guessing attack* , e probabilmente proverà ad ottenere un reset della password di Windows utilizzando un qualsiasi software commerciale disponibile. Allo stesso modo gli altri dispositivi della rete, come switch e persino firewall, non sono salvaguardati da persone con accesso fisico al dispositivo. Alcuni switch hanno una porta per l'accesso alla console che non può essere disabilitata. Una qualsiasi persona con accesso fisico allo switch e con la conoscenza della procedura per il recupero della password può facilmente introdursi nella rete. Ci sono alcuni switch con un bottone di reset che, quando premuto, si riavvieranno con le specifiche di costruzione di default, che ovviamente include anche la password di default. Per questa ragione l'accesso

fisico può essere considerato come una delle maggiori preoccupazioni per la sicurezza dell'impianto. In ENI Venezia il controllo degli accessi alle stanze dove sono collocati ICS e attrezzature di reti è ad opera di Eni (Non Yokogawa).

4 Necessità di un Information Security Management System

Le minacce alla sicurezza sono in continua evoluzione e ne emergono di nuove giorno dopo giorno. Pertanto le misure di sicurezza adottate devono essere rivalutate ogni volta. Questa procedura viene chiamata Information Security Management System (ISMS). E' un sistema di gestione basato sulla valutazione dei rischi. In questo capitolo verranno spiegate le procedure per formare un ISMS di un sistema di automazione.

La procedura seguente viene utilizzata per la costruzione di un ISMS.

- Organizzazione della commissione di sicurezza
- Identificazione delle attività
- Identificazione e valutazione dei rischi
- Identificazione e valutazione delle vulnerabilità
- Valutazione dei rischi (Risk assessment)
- Valutazione e attuazione delle misure di gestione della sicurezza
- Valutazione e attuazione delle misure di gestione dei cambiamenti nel sistema
- Monitoraggio continuo e analisi

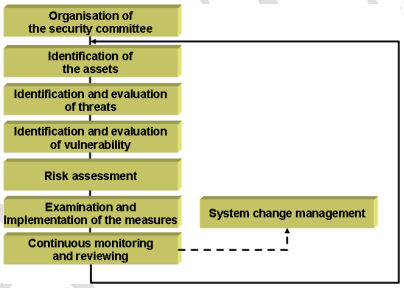


Figura 4-2: Procedura per la costruzione di un ISMS

Ogni azienda o organizzazione / dipartimento dovrebbe avere l'ISMS precedentemente illustrato. L'impianto ENI Venezia dovrà avere anch'esso un ISMS per il proprio sistema di automazione. E anche i clienti dovranno avere delle proprie security policy per le attività di ISMS. Yokogawa supporterà il cliente alla realizzazione delle proprie security policy.

4.1 Organizzazione della commissione di Sicurezza

Il comitato di sicurezza si impegna ad indirizzare le attività dell' ISMS. Qualsiasi cliente ha bisogno di organizzare la commissione di sicurezza. Si prega di prendere nota di quanto segue quando è organizzato.

4.1.1 Organo di Gestione

L'obiettivo della sicurezza è di proteggere le proprietà dell'impresa. Questo significa che la gestione è responsabile di questo. In più, è necessario ottenere la collaborazione di chiunque sia coinvolto nelle attività di produzione in ordine di rafforzare efficientemente le misure di sicurezza. Pertanto, l'organo gestionale

dovrebbe esprimere la propria opinione sulle attività di sicurezza chiaramente e prendere esso stesso l'iniziativa.

4.1.2 Organizzazione delle Funzionalità Incrociate

L'organo di sicurezza è composto dalla rappresentanza di tutte le divisione coinvolte nelle attività di produzione. Per esempio, possiamo assumere un organizzazione con le seguenti suddivisioni.

- Produzione
- Gestione del sistema di automazione del processo
- Gestione del sistema IT
- Gestione Business
- Manutenzione

4.2 Identificazione delle Risorse (beni e attività)

In questa procedure, le risorse da proteggere sono elencate, il titolare è identificato e l'importanza delle risorse (criticità) sono valutate.

Le risorse sono al centro di un programma di sicurezza. Esse sono il soggetto della protezione. In ordine per apprendere a pieno i rischi di un ambiente basato su un sistema di automazione, è come prima cosa necessario creare un inventario delle risorse e beni che richiedono protezione. Quest'ultimi possono essere classificati come risorse fisiche, logiche o umane.

4.2.1 Risorse Fisiche

Questa categoria include qualsiasi componente materiale o gruppo di componenti appartenenti ad un organizzazione. Nell'ambiente industriale, questi possono includere sistemi di controllo, componenti fisici della rete e dell'apparato di trasmissione, muri, stanze, edifici, materiali, o qualsiasi altro oggetto fisico che in qualche modo è coinvolto nei processi di controllo, monitoring, o analisi dei processi produttivi o generalmente in supporto al business. Le più importanti risorse fisiche sono quelle che compongono l'apparecchiatura che è sotto il controllo del sistema di automazione.

4.2.2 Risorse Logiche

Risorse logiche sono di carattere informativo. Esse possono includere proprietà intellettuali, algoritmi, prassi proprietarie, conoscenza di processo specifiche, o altri elementi informatici che vanno a formare le abilità organizzative di operare o fare innovazione. In oltre, questo tipo di risorse possono includere l'opinione pubblica, fiducia degli acquirenti, o altri provvedimenti che, se danneggiati, hanno effetti diretti nel business. Le risorse logiche possono trovarsi nella forma di memoria personale, documenti, informazioni contenute su supporti fisici, o documenti elettronici di memorizzazione che si occupano del bene informativo. Possono includere anche risultati di test, dati di conformità alle normative, o qualsiasi altra informazioni che possa essere considerata sensibile o proprietaria, o che potrebbe sia fornire che produrre un vantaggio competitivo. Perdita di attività logiche spesso causano effetti a lungo termine dannosi per l'organizzazione.

Le risorse di un processo di automazione sono una forma speciale di questa categoria. Esse contengono la logica di automazione utilizzata nell'esecuzione del processo industriale. Questi processi sono altamente dipendenti dalla ripetitiva o continua esecuzione di precisi e ben definiti eventi. La compromissione delle attività di processo può provenire sia da risorse fisiche (distruzione di dispositivi) che non (modifiche non autorizzate), e potrebbe comportare ad una perdita dell'integrità o della disponibilità del processo stesso.

4.2.3 Risorse Umane

Le risorse umane includono le persone e le conoscenze e abilità che esse possiedono associate alle loro attività produttive. Possono includere certificazioni, conoscenze specifiche sull'apparechiattura, o altre attività non incluse nei processi di produzione o capacità necessarie durante le emergenze. Raramente le infrastrutture sono completamente automatizzate e l'interruzione dell'attività degli operatori può avere un impatto maggiore nella produzione anche se i sistemi fisici e logici rimangono relativamente intatti. Per

esempio, un erroneo allarme nell'impianto può indurre il personale a iniziare lo spegnimento e l'evacuazione dell'impianto anche senza nessun disturbo effettivo nelle risorse fisiche o logiche nel sistema di automazione e di controllo. Qualsiasi incidente o attacco che va a ledere una persona può essere considerato una minaccia alle risorse umane.

Come esempio, sono mostrati qui di seguito alcuni livelli di classificazione dei rischi.

- Criticità A: Molto Alto
- Criticità B: Alto
- Criticità C: Basso
- Criticità D: Molto Basso

4.3 Identificazione e Valutazione delle Minacce

Qui facciamo chiarezza sulle minacce potenziali alle risorse sopra elencate.

Nel procedere a effettuare una lista delle minacce è necessario pensare secondo i seguenti punti di vista.

Accesso illegale alla proprietà da parte di persone con intenti malevoli

- All'interno dell'azienda
- All'esterno dell'azienda
- Tramite accesso di rete
- Accesso diretto alla proprietà (operazioni dirette alla strumentazione nel luogo della proprietà)

Accesso illegale alla proprietà da parte di software con intenti malevoli

- Tramite accesso di rete
- Tramite dispositivo removibile

Accesso illegale accidentale alla proprietà dovuto a errori o negligenza nelle operazioni

Il livello dei possibili casi delle minacce sarà valutato. Un esempio di classificazione può essere il seguente

- Livello A: Alta possibilità.
- Livello B: Media possibilità.
- Livello C: Bassa possibilità.

4.4 Identificazione e Valutazione delle Vulnerabilità

In questa procedura la vulnerabilità di ciascuna risorsa o di ciascun dispositivo, nel luogo di collocazione, necessita di essere identificato accuratamente. La vulnerabilità è determinata dalla situazione o dalle condizioni in cui le minacce possono avere effetto sulle risorse.

Alcuni esempi di vulnerabilità.

- Difetti delle policy di sicurezza o delle procedure di installazione
- Mancanza di protezione fisica
- Difetti nel setting del Firewall posizionato in un punto di connessione alla rete esterna.
- Incompletezza dei file di pattern di un software anti-virus (pattern non aggiornati)
- Incompletezza delle patch (security patch non aggiornate)
- Incompletezza del backup (Il sistema non ha una versione di backup)
- Mancanza di conoscenza nelle procedure di sicurezza di operatori e personale

5 Requisiti dell'Architettura di Rete

Il design della rete ENI raccomandato (vedi Figura 4-1) è diviso in tre segmenti: Rete d'Ufficio, PCN e DMZ. Tra queste reti, il traffico è controllato e minacce dalle reti esterne sono bloccate. Accessi al server e alla DMZ sono permessi solo dalla Rete d'Ufficio.

5.1 Design dell'Architettura di Rete

La seguente immagine raffigura l'architettura generale raccomandata della rete dell'impianto di Eni Venezia. Parte di questa rete esiste già, altre parti saranno implementate durante questo progetto. Questa architettura fa riferimento al *modello di Purdue* e ne aggiunge la DMZ (Livello 3.5) al modello. Per ragioni di chiarezza nella figura seguente le connessioni alla rete per la gestione non sono visualizzate. L'architettura di rete è visionabile in dettaglio nel documento riguardante la System Network Architecture.

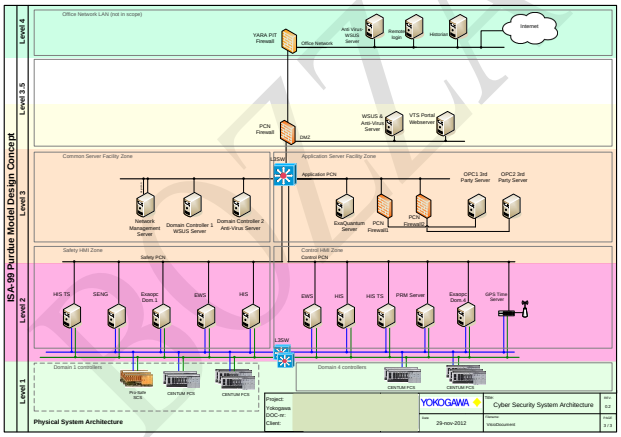


Figura 5-1 Eni Venezia Architettura di Rete raccomandata "esempio"

5.2 Modello di Purdue ISA-99

Il modello Purdue è utilizzato come riferimento per definire le relazioni significative che avvengono tra le entità di un ambiente architetturale, e per lo sviluppo di standard coerenti o specifiche che supportino questo ambiente. Gli standard architetturali definiscono l'ambito da un punto di vista logico:

- Il Modello Logico mostra i livelli dei dispositivi e dei sistemi collocati dal Livello 1 fino al Livello 3 del modello di Purdue ed evidenzia come differenti requisiti e vincoli di sicurezza sono validi per diverse porzioni del contesto generale.
- Il Modello Fisico descrive la gerarchia dall'infrastruttura fisica fino alle applicazioni

- I Modelli Concettuali servono a illustrare gli standard architetturali.
- Ogni sistema dovrebbe essere propriamente allocato all'interno di ogni livello del modello di Purdue.

Livello 1 – Controllo Locale o di Base

Il Livello 1 include le funzioni coinvolte nel rilevamento e nella manipolazione del processo fisico. L'attrezzatura di monitoraggio del processo legge i dati dai sensori, esegue algoritmi se necessario, e conserva lo storico del processo. Esempi di sistemi di monitoraggio possono essere un sistema di misurazione dei serbatoi, schermi per l'emissione continua, e indicatori di temperatura. L'apparecchiatura di un controllore di processo è simile. Legge dati dai sensori, esegue gli algoritmi e manda le informazioni a un elemento di destinazione (valvole di controllo o unità di smorzamento). Il controllore di Livello 1 è direttamente connesso ai sensori e agli attuatori di processo.

Il Livello 1 include controllori per flusso continuo, di sequenza, controllori batch e discreti. Molti controllori moderni includono tutti i tipi elencati in un singolo dispositivo.

Inoltre, incluso in questo livello, vi sono i sistemi di sicurezza e protezione che sorvegliano il processo e permettono, in automatico, a quest'ultimo di raggiungere uno stato di sicurezza nel caso in cui ecceda i limiti di tolleranza. Questa categoria include anche sistemi che allertano l'operatore di imminenti condizioni critiche.

I sistemi di sicurezza e protezione sono stati tradizionalmente implementati utilizzando controllori separati fisicamente, ma in tempi recenti è diventato possibile realizzarli utilizzando un metodo conosciuto come "separazione logica", all'interno di un'infrastruttura comune.

Apparecchiature di Livello 1 includono :

- Controllori per Distributed Control System (DCS)
- Safety Instrumented System (SIS)

Livello 2 – Controllo di Vigilanza dell'Area

Il Livello 2 comprende le funzioni coinvolte nella supervisione e nel controllo del processo fisico. CI sono tipicamente una moltitudine di zone e attività di produzione in un impianto quali la distillazione, la conversione, la miscelazione in una raffineria o, nel caso di un servizio di fornitura elettrica, turbine e strutture di raffreddamento.

Il Livello 2 tipicalmente include le seguenti funzioni:

- Operatore Human-Machine interface (HIS)
- Operatori per Allarmi e Avvisi (Alarms&Alerts)
- Funzioni di controllo di vigilanza
- Interfacce con I livelli superiori della rete (OPC-PIMS)

Livello 3 –Controllo delle Operazioni di Produzione

Il Livello 3 include tutte le funzioni coinvolte nell'amministrazione del flusso di lavoro al fine di produrre i prodotti finali desiderati. Esempi includono produzione di spedizione, pianificazione della produzione, garanzia di affidabilità e ottimizzazione del sito di controllo a livello. Vengono consolidati dati e informazioni grezze dal PCN Livello 2, elaborati prima di essere utilizzati dalla rete a Livello 4 come sistemi ERP MES. Contribuisce pertanto all'integrazione verticale tra la rete di stabilimento Livello 4 e il PCN Livello 2.

Le attività Livello 3 includono:

- Report di Produzione
- Dati su produzione, inventario, materiali grezzi, manodopera, ricambi e consumi energetici.
- Data collection e analisi off-line per funzioni di supporto ingegneristico
- Funzionalità statistiche
- Programma dettagliato di produzione
- Ottimizzazione dei costi per aree di produzione individuali

Livello 3.5 – DMZ

DMZ fornisce dati sicuri da e verso la PCN e permette la gestione del traffico proveniente dal Livello 4 verso il sistema di controllo (Livello 3 e inferiori). Per realizzare questa protezione, i seguenti sistemi saranno inclusi nella DMZ.

- Firewall
- Versatile Terminal Server (VTS) per funzionalità di Controllo Remoto
- Antivirus / Windows Server Update Service Server (WSUS)

Livello 4 – PCD esterne

Livello 4 include reti esterne al dominio PCD Yokogawa. Reti che sono incluse in questo livello sono

- Rete di terze parti
- Rete d'ufficio

Tutt'oggi reti di Controllo di Processo sono spesso connessi alle reti d'ufficio degli operatori, le quali, a loro volta, possiedono una connessione internet. Il motivo di queste connessioni può essere quello di mandare i dati dello storico alla rete aziendale, inviare aggiornamenti verso la PCN, connettersi in remoto o per altri validi motivi.

Come per l'accesso fisico è necessario limitare gli accessi alla PCN al solo personale autorizzato. Non è possibile generalmente limitare gli accessi sui singoli individui, tuttavia vi sono altri accorgimenti per attuare le restrizioni. E' di comune utilizzo la pratica di chiudere gli accessi basandosi sulla destinazione e sorgente tramite l'utilizzo del firewall.

5.3 Design del Firewall

Introduzione

Il firewall è la linea di difesa da intrusioni da altre reti. Di default un firewall bloccherà tutto il traffico fra le reti. Con un firewall il traffico tra due, o più, reti può essere regolato.

Le regole contenute nell' Access Control List (ACL) consentono l'accesso da :

- Una sorgente specifica(computer) a una destinazione fissa (computer);
- Un insieme specifico di sorgenti(più computer) a una destinazione fissa (computer);
- Un insieme di sorgenti ad un insieme di destinazioni;
- Per un protocollo specifico;

Queste regole possono essere applicati con l' Access Control List anche su un router (Switch L3), ma con l'ACL è comunque possibile che dati non voluti(o previsti), che comunque soddisfino le condizioni, passino attraverso il dispositivo.

Per esempio, se un computer nella PCN non richiede informazioni ad un computer in un'altra rete, l'ACL permetterà il passaggio della risposta, se le condizioni precedenti sono verificate.

I Firewall aggiungono alle capacità dell'Access Control List anche le funzionalità di *stateful packet inspection*.

Questo significa che oltre agli attributi verificati dall'ACL, il Firewall controlla anche lo stato della connessione. Così se un computer nella rete di Controllo di Processo non ha richiesto informazioni ad un computer in un altra rete, la risposta verrà bloccata dal firewall.

Il modello di firewall utilizzato per il progetto ad Eni Venezia sarà un XXXXXXXXXX. Un firewall sarà posizionato al livello 3.5, in modo da collegare i router del livello 3 ai livelli superiori. Il software Matrikon OPC Tunneller può essere installato nei server Exaopc per limitare il numero di porte aperte nelle connessioni attraverso il firewall.

Demilitarized Zone (DMZ)

Come precauzione aggiuntiva per i dati tra le varie reti e la PCN verrà creata una zona *demilitarizzata (DMZ)*. La Figura 5-2 mostra l'applicazione VT Portal, la quale consente l'accesso *web based* dalle altre reti verso la PCN.
Quando un client nella rete aziendale richiede una visualizzazione del CENTUM, la richiesta sarà processata dal Web Server nella DMZ. In questo caso il client non ha accesso diretto alla PCN, ma solo alla DMZ. Il server contenuto in quest'ultima inoltrerà la richiesta all'Application Server all'interno della rete di controllo e rimanderà la risposta al client nella rete di partenza.

5.4 Sicurezza degli Switch

Anche se l'accesso fisico al dispositivo di rete è a posto, impostazioni di protezione verranno applicate agli interruttori di rete. Le tre impostazioni per migliorare la sicurezza della rete sono:

- Disabilitare porte inutilizzate;
- MAC filtering;
- Segregazione del traffico tramite VLAN (LAN Virtuale).

Saranno installati in Eni Venezia swtich Netgear (Da definire a cura di ENI modelli utilizzati), in modo da implementare PCN e NMS (Network Management System). Per la rete PCN il colore delle connessioni sarà blu, per NMS i cavi saranno rossi.

Disabilitare porte inutilizzate

Non tutte le porte degli switch vengono utilizzate. Questo può avvenire per requisiti particolari o perchè semplicemente lo switch possiede più porte di quelle necessarie. Quando l'accesso fisico non è limitato solamente al personale autorizzato, un portatile può facilmente essere connesso ad una delle porte inutilizzate, e garantire in tal modo l'accesso al Livello 2 della rete.
L'accesso a queste porte inutilizzate sarà pertanto disabilitato.

MAC filtering

Network Interface Card (NIC) costituiscono un univoco indirizzo fisico, il quale non può essere impostato dall'utente. Gli switch di rete fanno uso dell'indirizzo MAC (Media Access Control) e della sua univocità per aumentare la sicurezza degli altri switch.
Questa funzionalità proibisce che computer non autorizzati ottengano un accesso alla rete quando si connettono ad un cavo di rete dello switch.
Negli switch configurabili viene applicato il MAC filtering; questo assicura che solo i pacchetti inviati all'indirizzo MAC assegnato alla porta vengano inoltrati. Se l'indirizzo MAC connesso a questa porta cambia (come per esempio se il NIC, o l'host, vengono rimpiazzati), il precedente MAC connesso rimane assegnato a quella porta, e tutti i pacchetti indirizzati verso il nuovo MAC saranno scartati dallo switch.
Per un *non-intelligent* switch tali misure possono non essere applicabili, in questo caso alcune misure di sicurezza fisica devono essere prese al fine di prevenire accessi non autorizzati alle porte (per esempio installando lo switch in un armadio chiuso a chiave).
Il lato negativo di utilizzare questo metodo è che se un dispositivo di rete viene rimpiazzato senza considerare il MAC filtering, potrebbero esserci delle conseguenze e risoluzioni non necessarie di problemi nel sistema.

Virtual Local Area Networks (VLAN)

Una VLAN sono un gruppo di host che si comportano come se fossero connessi allo stesso segmento di rete, anche se possono essere connessi alla stessa rete fisica. Gli Host non appartenenti alla stessa VLAN saranno invisibili agli altri membri delle altre VLAN. Se un dispositivo di una VLAN deve comunicare con computer in altre VLAN questo deve essere fatto attraverso un router (Switch Livello 3).
Nonostante non sia un requisito funzione per le Vnet/IP l'utilizzo di VLAN in un singolo ambiente di dominio, queste possono essere utilizzate per ragioni di sicurezza.
Se affiancata ad una rete Vnet/IP vi sono delle reti Ethernet per altri utilizzi come PCN, OPC e management degli switch. E questi passano attraverso lo stesso switch, le VLAN possono essere utilizzate per separare i flussi di traffico.

Le implementazione delle VLAN offrono i seguenti benefici;

- Gruppi virtuali (Remoti, Common e Applicativi etc.)
- Protezioni avanzate della rete (ulteriori segregazioni di rete)

Riduzione del traffico delle trasmissioni di rete (Latenza ridotta)
La Figura 5-2 mostra un esempio schematizzato della comunicazioni fra le reti. In questo esempio il Firewall Yokogawa controlla e instrada il traffico di rete fra le VLAN.

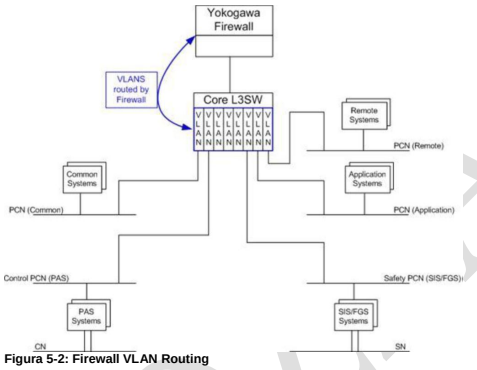


Figura 5-2: Firewall VLAN Routing

6 Applicazioni di Base per la Sicurezza

Sicurezza applicata a Yokogawa

Differenti provvedimenti sono stati introdotti per garantire la sicurezza dei sistemi di produzione Yokogawa. Questo capitolo descrive la generica Application Security che utilizza le funzioni di sicurezza Windows, e le funzioni di sicurezza specifiche dei prodotti.
Il setting delle Application Security che utilizzano le funzioni di sicurezza di Windows vengono supportate dalle versioni CENTUM VP R5.03 e ProSafe-RS R2.03. La Configurazione di Application Security protegge dalle minacce il computer tramite procedure di hardening.
Le minacce gestite dall' Application Security possono essere suddivise come segue:
1. Attacchi alla rete.
2. Attacchi diretti tramite manipolazione dei computer.
3. Furto di dispositivi e di dati.

Tre differenti modelli di sicurezza sono disponibili (vedi Tabella 6-1 Modelli di sicurezza) per trattare questi tipi di attacchi. Questi modelli supportano differenti configurazioni di sistema e operazioni.

Modello	Feature
Legacy	Questo modello non rafforza la sicurezza. Da priorità alla collaborazione con altri prodotti .
Standard	Questo modello è orientato alle maggiori operazioni di sistema e collaborazione con altri sistemi. E' in grado di contrastare minacce (1) e (2).
Strengthened	Questo modello è utilizzato per far fronte a tutti e tre i tipi di attacco elencati. Le operazioni possono essere rallentate se si attua piena sicurezza.

Tabella 6-1 Modelli di sicurezza

Per contrastare le minacce, le misure di sicurezza che possono essere implementate nell'ambiente IT dei prodotti Yokogawa sono suddivisi in quattro categorie.

Tipo di Sicurezza	Legacy	Standard	Strengthened
Controllo accessi	N/A	Applicabile	Applicabile
Tuning personalizzato del firewall	N/A	Applicabile	Applicabile
Stop servizi Windows non necessari	N/A	N/A	Applicabile
Cambiamento del setting dell'ambiente IT	N/A	Parziale	Applicabile

Tabella 6-2 Tipi di Sicurezza

I prodotti Yokogawa forniscono degli strumenti che in automatico configurano le impostazioni di sicurezza secondo i modelli di sicurezza. Quando viene selezionato il modello “Strengthened” alcune impostazioni dovranno essere configurate manualmente. In ordine di garantire la miglior protezione possibile, quest'ultimo modello sarà applicato per l'impianto di Eni Venezia.

CENTUM VP

Le impostazioni di sicurezza di CENTUM possono essere classificare in due funzioni, le funzioni di base di Application security delle funzioni di sicurezza di Windows e le funzioni specifiche di sicurezza di CENTUM VP.

Funzioni di Application Security di CENTUM VP

Le funzioni di Application security per rafforzare la sicurezza sono supportate da CENTUM VP. L'hardening di sistema dell'ambiente IT del CENTUM VP è realizzato utilizzando le Windows function. Per esempio, l'utilizzo degli strumenti di CENTUM VP e i permessi di accesso alle cartelle dei file sono gestite tramite controllo degli accessi per utenti e gruppi di Windows. Pertanto, è possibile applicare contromisure di sicurezza in tali circostanze che permettano agli utenti Windows come un operatore di loggarsi al PC per utilizzare gli strumenti relativi alla sua classe di utenza, ma impedirgli di utilizzare gli strumenti del gruppo di ingegneria.
Alcuni tipi di comunicazioni e porte possono essere disabilitate dal firewall e tramite il setting DCOM.

Modalità di autenticazione

Nel CENTUM VP R5.03 il sistema di autenticazione di Windows è incluso. Tuttavia l'impianto Eni Venezia non richiede questo tipo di autenticazione per gli operatori. Le policy di accesso in Eni sono che tutti gli operatori utilizzano lo stesso Windows user.

Prosafe-RS

Prosafe-RS supporta le funzioni di Application Security basate sulle security feature di Windows, anche le funzioni peculiari del CENTUM VP possono essere applicate nel sistema integrato ProSafe-RS/CENTUM. In aggiunta, ProSafe-RS ha delle specifiche funzioni per migliorare la sicurezza quale il Safety Instrumented System.

Funzioni dell'Application Security di Prosafe-RS

Le versione ProSafe-RS R2.03 e successive supportano le funzioni di Application security.
L'hardening di sistema dell'ambiente IT del ProSafe-RS è realizzato utilizzando le funzioni Windows. Inoltre, la funzione di sicurezza dell'applicazione può essere applicato sul sistema integrato ProSafe-RS/CENTUM VP. Pertanto, è possibile applicare le contromisure di sicurezza in tali circostanze, per consentire a un utente di Windows come ad esempio un ingegnere CENTUM VP di accedere al PC per utilizzare gli strumenti di ingegneria del VP Centum ma limitato all'avvio nell'utilizzo degli strumenti di ingegneria del ProSafe-RS.

Livello di Sicurezza SCS

Il livello di sicurezza delle SCS (Safety Control Station) indica il livello di protezione contro erronee scritture nella memoria delle postazioni o dei dispositivi.
Vi sono 3 livelli di sicurezza: due livelli online (livelli 1 e 2) e uno offline(livello 0). L'SCS limita i cambiamenti fatti dall'esterno in accordo con il livello di sicurezza. Il livello 2 è il più altro livello di sicurezza. Si raccomanda di lasciare l'SCS in questo stato, quando non sono necessari interventi di manutenzione o download sul controller.
Si raccomanda di installare uno switch hardware che permetterà o negherà la modifica del livello di sicurezza da un SENG. Questo permetterà di prevenire erronee scritture alla memoria dell' SCS. Lo switch verrà installato durante il prossimo shutdown dell'impianto.

7 Active Directory

I servizi di Active Directory Domain forniscono un set di servizi directory che sono inclusi in Windows Server come parte integrante delle funzionalità del Domain Controller. Un *directory service* è un servizio di rete che identifica tutte le risorse in una rete windows and permette di renderle accessibili a utenti e applicazioni. Active Directory Domain Services includono le directory, le quali immagazzinano informazioni sulle risorse, e i servizi che permettono di rendere queste informazioni disponibili e utili. Le risorse contenute nelle directory, come dati utente, stampanti, server, database, gruppi, computer, e policy di sicurezza, sono conosciuti come *object*.
Nell' Active Directory Domain Services, le risorse sono organizzate in una struttura logica. Raggruppare le risorse logicamente permette di trovarle secondo il loro nome piuttosto che secondo la loro posizione fisica. Finchè si attuano raggruppamenti logici, Active Directory Domain Services rende la struttura fisica di rete trasparente agli utenti. La struttura logica è composta da object, unità organizzative, domini, alberi e foreste.

Obiettivi di DC e AD in un ambiente di rete

Il compito del Domain Controller è quello di mantenere un livello di controllo sui domini Windows. Il Domain Controller elabora query del DNS e gestisce qualche funzionalità AAA di base. Molte di queste ultime funzioni sono direttamente manipolate dall'AD, queste funzioni saranno descritte in dettaglio nella prossima sessione.
Come menzionato precedentemente, AD fornisce una visione logica dell'intero ambiente di rete. Semplicemente memorizza in un repository gli oggetti di rete. Ancor più importante, l'AD fornisce all'amministrote alcune utility di gestione per questi oggetti.
Il compito del Domain Controller riguarda principalmente il mantenere un controllo sui domini Windows.

Fondamentali dell'AD

E' prioritario configurare e implementare un Microsoft Active Directory in un ambiente di rete, alcuni concetti fondamentali sono necessari per essere in grado di prendere decisioni critiche e giudizi sulla progettazione del design. Essi sono:

- La struttura dei domini
- Domain Name Services (DNS)
- funzionalità AAA

Struttura dei Domini

Nelle Active Directory, i siti mappano la struttura fisica della propria rete, mentre le foreste mappano la struttura logica o amministrativa dell'organizzazione.
I siti rappresentano la struttura fisica, o topologica, della rete. Sono formati da uno o più subnet basate su Internet Protocol (IP). Active Directory utilizzano le informazioni sulla topologia, memorizzati come sito e link nella directory, per costruire una replica topologica affidabile.
Una foresta contiene diversi alberi che possono contenere uno o più domini. I domini contengono tutti gli objects al loro interno su cui svolgeranno le operazioni di AAA. I diritti amministrativi sono contenuti all'interno del dominio e controllate dall'amministratore dello stesso.
Il livello di funzionalità del dominio definisce a quale versione server di Microsft Windows, il dominio è applicabile. Il seguente Fully Qualified Domain Name(FQDN) sarà implementato a Venezia: ENI-VE-PCN.local

Domain Name Services (DNS)

La funzione DNS ricopre un ruolo di importanza all'interno dell'Active Director Domain Services. Si occupa di tradurre gli indirizzi IP nel nome del dispositivo e vice versa. I domini dell'Active Directory sono nominati dal DNS. E' pertanto facile constatare che l'Active Directory utilizza il DNS come proprio sevice location protocol. I clients dell'Active Directory richiedenti di loggarsi alla rete richiedono al DNS di localizzare i controllori del dominio. Il Domain Name Space è più importante componente dell'Active Directory.
Ai domini dell'Active Directory vengono assegnati nomi del DNS. Conseguenza di questo fatto sono che le Active Directory utilizzano il DNS come protocollo per il servizio di locazione. I client che vogliono loggarsi alla rete chiedono al DNS di cercare i Domain Controller. Il Domain Name Space è il più significativo componente dell' Active Directory.

Il DNS è configurato utilizzando zone di inoltro e *reverse lookup*. Le zone di forward-lookup traducono i FQDN (Fully Qualified Domain Name) in indirizzi IP. Le zone di reverse lookup funzionano al contrario, esse traducono gli IP in nomi FQDN.

Funzionalità AAA

Grande parte delle funzionalità degli AD si occupa di AAA (Authentication, Authorization, Accounting) ed è importante verificare a quale livello queste sono implementate.
Gli user account sono autenticati confrontando i valori di username e password con quelli contenuti nelle informazioni di directory. Se i campi sono corretti, viene permesso l'accesso. Gli account del computer sono autenticati correttamente quando un utente si è loggato. In alternativa per gli account per cui non si richiede una password, un'unica stringa, assieme all'account del computer, viene inviata per essere autenticata dai domini. Questo metodo serve ad assicurare che solamente ai dispositivi autorizzati venga permesso il login al dominio.
Dopo che l'autenticazione ha avuto luogo, computer e utente sincronizzano le rispettive informazioni di autorizzazione. Quest'ultima contiene un'estesa lista di diritti attraverso la directory che sono assegnati all'AD object. Per esempio, ad un utente possono essere proibiti i diritti di amministratore nella macchina su cui sta lavorando in locale attraverso l'active directory. La fase di accounting avviene ogni qualvolta un object richiede o invia informazioni al DC. Questa azione viene memorizzata nel log e può essere controllata in tempi successivi dall'amministratore di sistema.
E' importante notare che l'autorizzazione non include i diritti NTFS(per la visione/modifica dei dati). I diritti NTFS sono assegnati tramite flag sui dati. Questo viene solitamente fatto dalla creazione di gruppi a cui sarà permesso l'azione richiesta. Questi diritti sono facilmente gestiti semplicemente aggiungendo o rimuovendo utenti dal gruppo appropriato.

Design architetturale AD

Il design della struttura dell'Active Directory coinvolge la strutturazione delle relazioni tra foreste, domini, e unità organizzative che si intendono sviluppare. Definendo attentamente la struttura logica dell'Active Directory di ENI, i costi di amministrazione possono essere minimizzati.
Per il progetto in ENI, le seguenti fasi devono essere seguite sequenzialmente per garantire l'ambiente appropriato per l'Active Directory e rispettare i requisiti di Yokogawa:
1. **Design Topologico –** Nella fase iniziale la struttura organizzativa viene esaminata e l'appropriato design della topologia di foreste e domini delle Active Directory vengono create. Decisioni sulle convenzioni sui domi devono essere concordate. Si prevede di creare un dominio che comprende tutti i PC e i server collegati a PCN, con il nome ENI-VE-PCN.local.
2. I**nfrastruttura dell'Active Directory** – Sulla base del design sulla topologia viene creata l'Active Directory. Decisioni sulla distribuzioni delle regole FSMO e sulla ridondanza dell'Active Directory ricoprono il ruolo più importante di questa fase. Come in Figura 7-1, due server saranno installati al livello 3, i quali agiranno da controllori DC ridondanti.
3. **DNS** design– La precedente decisione sulla topologia e sull'infrastruttura della Active Directory determina come il Domain Naming System (DNS) verrà configurato.
4. **Organizational Unit Structure** – Una struttura gerarchica dell'Organizational Unit (OU) è creata secondo gli standard ingegneristici. Le differenti OU conterranno tutti gli utenti, i gruppi, computer object in modo da poterne applicare le relative policy.
5. **Utenti e Gruppi** – Dopo che la struttura della OU è stata implementata, gli utenti vengono creati per l'accesso da parte dei lavoratori e i gruppi vengono costituiti per controllare gli accessi alle risorse di rete.
6. **Policies dei Gruppi** – Dopo la creazione di gruppi e utenti, questi vengono spostati nelle appropriate Organizational Units, le Group Policy Objects (GPOs) vengono create e collegate con le OU.

Account management

L'accesso alle risorse di rete nell'ambiente delle Active Directory viene fornito attraverso la creazione degli utenti e dei gruppi.

7.1..1 Users

Ci sono due possibilità di base nella creazione di account per l'accesso dei dipendenti. Il primo è quello di creare account per ogni tipo di dipendente. Questo comporta, per esempio, che un singolo account venga creato per tutti gli operatori degli HIS su cui loggarsi. La seconda possibilità è quella di creare account individuali per ogni singolo dipendente. Questo significa che se vi sono 10 operatori sugli HIS, 10 differenti user account verranno creati nel Active Directory.

Di default il software Yokogawa crea utenti definiti per i ruoli (per esempio 'Centum' user).
Entrambe le possibilità offrono dei pro e dei contro che sono mostrati nella tabella seguente.
Basandosi sul documento Production IT Security Standard (vedi riferimento [8]) è suggeribile la creazione di account personali.

How to manage accounts	How to operate	Operational advantages		Security strength	
Common account management	A Windows account is shared by several users.	High	Same operability as the conventional CENTUM system.	Low	Unfavourable because di high anonymity.
Individual account management	A Windows account is allocated to a user.	Low	More complex than the conventional operation because Windows logoff/logon is required when the user is changed.	High	Favourable because AAA can be controlled on a per user basis.

Tabella 7-1 Gestione degli account Windows

7.1..2 Gruppi

Gruppi delle Active Directory sono solitamente create per fornire accesso alle risorse di rete a tutti i membri di quel particolare gruppo. I membri del gruppo possono essere utenti del dominio o di altri gruppi.
Yokogawa ha creato una procedura standard per la generazione di gruppi di utenti e per la delegazione appropriata dei diritti degli stessi appropriati ai gruppi in un ambiente CENTUM.
I diritti assegnati a ciascun gruppo sono tenuti al minimo in modo da prevenire accessi illegali, falsificazioni, dispersione e distruzioni di dati critici. I gruppi e gli user account creati sono coperti attraverso le rispettive Installazioni Manuali le quali sono fornite entrambe con il CD di installazione.

Policy dei gruppi

Yokogawa suggerisce l'utilizzo di Group Policy Objects (GPO) per la gestione centralizzata e la configurazione di tutti i sistemi operativi Microsoft, applicazioni e setting degli utenti. In altre parole, le GPO controllano in parte cosa un utente può e non può fare in un computer tramite restrizione di tutte quelle azioni che potrebbero offrire dei potenziali rischi alla sicurezza.
La Tabella 7-2 elenca i requisiti delle policy per l'ambiente degli AD.

Requisiti delle Policy	Definizione	Requisiti
Password Policy	Lunghezza: imposta i requisiti sulla lunghezza della password	Impostata ad un minimo di 12 caratteri
Nota:Queste policy sulle password applicate al livello di Dominio applicano i loro effetti a tutti gli Utenti/Gruppi fatta ad eccezione per quelli coperti da Fine Grain password policy.	Complessità: imposta i requisiti sulla complessità della password	Combinazione di almeno 3 delle 4 insieme di caratteri: - Maiuscole, Minuscole, - Carattere numerico - Carattere speciale
	Limite temporale: imposta la durata minima e massima di una password. (Linea guida: dovrebbe essere impostata ad un time in cui l'account venga utilizzato prima che la password venga modificata.)	Impostata a: 90 Giorni (Max) e 30 Giorni (Min).
	Storico: Imposta il numero di volte dopo il quale una password può essere riutilizzata.	25 password vengono ricordate
Account lockout Policy	Login multipli: Imposta il numero di fallimenti di autenticazione consecutivi prima che un account venga bloccato	10 fallimenti di login consecutivi
	Tempo di attesa per lo sblocco automatico dell'account.	15 minuti.

Requisiti delle Policy	Definizione	Requisiti
Audit Policy	Impostazioni appropriate dell'auditing del sistema di sicurezza Windows.	Consigliato impostare successi e fallimenti dei log degli utenti e controllo degli eventi di sicurezza correlati basato sulla guida di IT security per prodotti IA (IT Security Guide for IA Products Yokogawa)
	Impostazione della dimensione massima del log che riguarda gli eventi di sicurezza.	Setting come segue: System (16,384 KB) Security (81,920 KB) Application (16,384 KB)
	Impostare le azioni da eseguire nel momento in cui il file di log raggiunge la dimensione massima impostata	Impostare l'azione di sistema a: "Overwrite events as needed" (Sovrascrivere gli eventi a necessità)
Patch Management Policy	Configurare il Setting di Update Automatico (Automatic Update Setting)	Impostare a: auto download e notifica con installazione manuale.
	Specificare la locazione dell'intranet Microsoft update service	Impostare il percorso all'IP e alla porta del server del Patch Management.
	Specificare la frequenza di update da Microsoft Windows	Abilitare quest'impostazione e tenere la frequenza di aggiornamento al valore di default (22 ore)
Disable USB Device Policy	Limitare l'utilizzo di dispositivi rimovibili disabilitando le porte USB. Questa politica previene l'attacco di virus veicolati da dispositivi USB e il furto dati da parte di utenti non autorizzati	Disabilitare dispositivi di memorizzazione di massa USB, CD / DVD-ROM e floppy.
HIS Security Policy	Network Security: Modificare il livello di Autenticazione LAN Manager	Impostazione delle policy basato sulla guida di IT security per prodotti IA (IT Security Guide for IA Products Yokogawa): Abilitare i cambiamenti di Autenticazione LAN Manager tramite l'utilizzo delle GPO
	Stop dei Servizi di Sistema inutilizzati: Questa Policy suggerisce di disabilitare tutti i servizi non necessari in esecuzione nel sistema e bloccare il la loro partenza all'avvio del sistema.	Impostazione delle policy basato sulla guida di IT security per prodotti IA : Utilizzzando la GPO, disabilitare i servizi non necessari dall'avvio.(Note: Riferendosi alla guida IT Security per info su quali servizi Windows stoppare in accordo con la piattaforma OS del client.)
	AutoRun : Questa policy limita i programmi illegali dall'eseguirsi automaticamente.	Policy basate sul documente IT Security Guide for IA Products (Yokogawa): Disabilitare AutoRun Opzione 1: Utilizzando GPO Opzione 2: Da CENTUM VP 4.03, queste impostazioni possono essere disabilitate eseguendo le IT Security Tool localmente nella macchina client. Gli strumenti di Setup IT Security si trovano nei supporti di installazione del CENTUM VP R4.03
	NetBIOS settings: La risoluzione dei nomi dovrebbe essere eseguita dal DNS in ambiente di dominio.	Impostazione delle policy basato sulla guida di IT security per prodotti IA : Disabilitare il NetBIOS Opzione 1: questa impostazione NON PUO' essere settata utilizzando GPO. Deve essere configurata manualmente nel client della macchina locale. Opzione 2: Dal CENTUM VP 4.03, questa impostazione può essere disabilitata con l'esecuzione in locale degli strumenti di IT Security nel client. I tool di setup solo localizzati nei media di installazione CENTUM VP R4.03.

Requisiti delle Policy	Definizione	Requisiti
	Software Restriction Policies: Le limitazioni software hanno la funzione di controllare l'esecuzione dei programmi.	Impostazione delle policy basato sulla guida di IT security per prodotti IA : Abilitare Restrizione Software Opzione 1: tramite GPO Opzione 2:Dal CENTUM VP 4.03, questa impostazione può essere disabilitata con l'esecuzione in locale degli strumenti di IT Security nel client. I tool di setup solo localizzati nei media di installazione CENTUM VP R4.03.
	HDD Password Settings: Setting delle password nel BIOS per proteggere l'HDD da manomissioni.	Impostazione delle policy basato sulla guida di IT security per prodotti IA : Queste impostazioni NON POSSONO essere fatte utilizzando GPO. Deve essere configurato manualmente nelle macchine in locale.
	Disabilitare/Cambiare l'account da Amministratore: Imposto per prevenire la costruzione di account creati all'installazione di Winsows che potrebbero essere dei facili bersagli per scoprire la password Disable/Changing the Administrator Account: Consigliato per prevenire la creazione di account all'installazione di Windows da bersagli facili per il cracking di password.	Impostazione delle policy basato sulla guida di IT security per prodotti IA Raccomandato: Rinominare l'Admin Account nel caso di Windows XP/2003/2008. Raccomandato: Disabilitare l'Admin Account nel caso di Windows Vista
	Oscurazione ultimo ID loggato Non mostrando i precedenti user name nella finestra di dialog di Windows Logon si può prevenire la perdita di un qualsiasi user name valido all'interno del sistema.	Impostazione delle policy basato sulla guida di IT security per prodotti IA. Abilitare l'opzione Hiding Last Logon User Name.

Tabella 7-2: Requisiti di Policy

8 Antivirus - McAfee 8.8

Un sistema di antivirus protegge una rete aziendale dai virus, Trojan, worm, spyware e qualsiasi altra combinazione di attacchi. Sorveglia tutti i punti terminali di una rete, il quale include laptop, workstation, e server di rete, per mantenere un grado di efficienza e stabilità della produzione e dei processi.
La soluzione antivirus che verrà installata in Eni Venzia è McAfee End-Point Protecton con VirusScan Enterprise (VSE) 8.8 (AV11000 Yokogawa) e ePolicy Orchestrator(ePO) 5.1. Questo antivirus supporta grazie al software ePO un architettura client-server, la quale permette una gestione centralizzata di tutti gli aspetti del software. La console di gestione sarà installata in uno dei nuovi server DC. L'installazione nei client si distribuirà a partire da questa macchina.

8.1 Server Anti-Virus

Il server anti-virus agisce come centro del software antivirus. Comunica con i client attraverso un sistema ad agenti. La console di management del server fornisce una visione centrale dell'intero sistema. E' la posizione centrale da cui è possibile gestire tutti i client/host attraverso il display della console. Attraverso il server, l'amministratore può configurare impostazioni come regole per la sicurezza, monitor e report sui client, verificare e scaricare l'ultimo aggiornamento disponibile, ecc.
Il software Anti-virus è efficace solamente con l'ultima versione della lista dei virus installata. Attraverso il server, l'amministratore è in grado di scaricare e distribuire il file contenente la lista aggiornata a tutti gli

host/client. La procedura di aggiornamento viene automatizzata per essere eseguita ad intervalli regolari. Il server immagazzina al suo interno l'ultima versione del file e le precedenti.
Una delle importanti funzioni del software anti-virus è lo scanning. Cerca attraverso l'hard disk, nei processi in corso nella CPU, ecc. componenti dannosi o indesiderati. Se elementi di dubbia natura sono trovati, lo scanner mostra una descrizione del file e le azioni da intraprendere su di esso. Lo scanning manuale e automatico sono configurati per essere eseguiti sia sui client/host, che nel server. Il server mette in quarantena i file sospetti e gli elementi non riparabili dei client/host.

8.2 Console di Management

La console di management viene utilizzata assieme al server per facilitare la gestione centralizzata. La console viene attivata attraverso il server che ospita l'anti-virus server software o in remoto attraverso un qualsiasi browser web. Tutte le configurazioni e i task di gestione vengono attivati attraverso la console.

8.3 Agent

L'agent è il componente che protegge i client/host contro minacce alla sicurezza. L'agent viene installato nella macchina client e scambia dati tra il server anti-virus e ciascun sistema di gestione. L'agente richiede/recupera aggiornamenti, assicura l'implementazione di task, applica le policy e inoltra gli eventi a ciascun sistema di gestione. Si mantiene aggiornato con l'ultima versione dei virus scaricata nell'antivirus server. L'agent può anche eseguire qualche procedura in locale come lo scanning e l'update del singolo dispositivo.

8.4 Design dell'Architettura di un AV

Un anti-virus server ha bisogno di essere collocato nella DMZ. Questo server viene utilizzato per scaricare gli aggiornamenti da un altro server simile collocato nella rete di ufficio ENI o da internet ad intervalli pianificati.

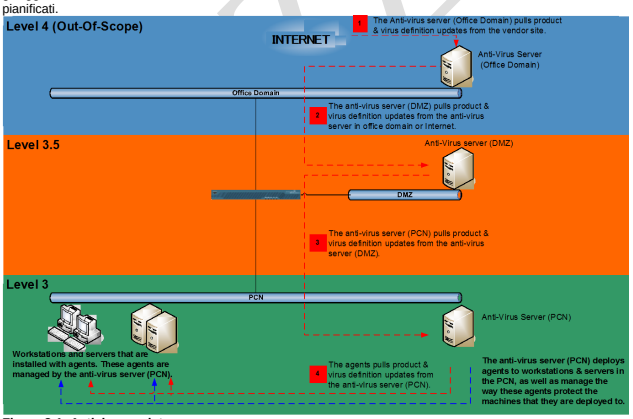


Figura 8-1: Antivirus update

1. L'anti-virus server (DMZ) richiede gli aggiornamenti dei virus e prodotti all'anti-virus server nella rete d'ufficio ENI o da internet.
2. L'anti-virus server (PCN) richiede gli aggiornamenti dei virus e prodotti all'anti-virus server (DMZ) a scadenze regolari.
3. L'agente richiede gli aggiornamenti dei virus e prodotti all'anti-virus server (PCN) a scadenze regolari.

8.5 AV Gruppi & Policy

Le impostazioni dei gruppi & policy nell'anti-virus software forniscono all'amministratore uno strumento migliore per gestire tutti i client nella rete e risultano essere un aiuto ulteriore nel garantire la sicurezza. Tuttavia, il setting di default nell'anti-virus software non dovrebbe essere utilizzato. Le impostazioni vengono customizzate per aderire ai bisogni di ciascun ambiente.

Gruppi

Raggruppare computer ha il compito di separare i differenti dispositivi in modo da applicare impostazioni comuni ai diversi ambienti. Abilita in questo modo l'amministratore a minimizzare il lavoro di customizzazione delle impostazioni su ciascun computer. Ogni gruppo può avere il proprio set di regole/policy predisposte.

Tabella 8-1: Gruppi

Gruppi	Descrizione
GENERAL	Questo gruppo ospiterà l'infrastruttura industriale IT dei computer (Domani controller, Backup server, NMS server, ecc.) e laptop wireless per qualsiasi applicazione di terze parti.
APPLICATION	Questo gruppo include tutte le applicazioni Yokogawa (Exaquantum, CENTUM, ProSafe-RS, ecc.) server e workstation.
EVALUATION	Questo gruppo contiene le applicazioni, server e workstation utilizzati per i test di valutazione.

Policy

Nell'anti-virus software, le policy devono essere configurate per bloccare/consentire alcune funzionalità software. Assegnando o modificando le policy, queste vengono applicate a cascata su tutti i client/computer di un gruppo in accordo con le necessità di utilizzo.

8.6 Scanning e Esclusione di Cartelle

Una delle più importanti funzioni dell'anti-virus è lo scanning engine. Il luogo dove verranno controllati tutti i file nel computer alla ricerca di virus/codice sospetto.
Sono disponibili diversi tipi di scanning dei dati. Le operazioni di scan sono configurate per essere eseguite automaticamente o manualmente e sono di due tipi :

- Scan completo
- Scan di auto protezione

Lo scan completo controlla tutti i file e cartelle nel computer su cui viene eseguito. Può essere configurato per essere eseguito manualmente dall'utente o avviato in automatico dalle policy configurate dalla console di management. Lo scan di auto protezione esamina quei file su cui si sta per eseguire un accesso da parte di computer su cui è necessario mantenere controlli continui e in tempo reale delle minacce. Può anche scannerizzare file nei settori di boot e processi già caricati in memoria.

Esclusione File/Cartelle

A causa dell'esistenza di alcuni file/cartelle critiche che potrebbero minare alla stabilità delle applicazioni, l'anti-virus ha bisogno di identificarle e escluderle dall'operazione di scan. Alcune policy vengono create per definire quali file/cartelle devono essere escluse. Queste regole vengono applicate ogni volta che una qualsiasi delle applicazioni di scan viene mandata in esecuzione.

Le seguenti cartelle sono escluse dallo scanning per il fatto che potrebbero essere potenzialmente scambiati per file infetti dall'anti-virus e, di conseguenza, rimosse. Il fatto di escluderle dallo scan ne limita la protezione da virus e altri rischi alla sicurezza.

- Tutte le cartelle di installazione di applicazioni software Yokogawa
- ExaOPC HDA file folder, CENTUM e ProSafe-RS project database folders

8.7 Schedule

Il software anti-virus offre delle agevolazzioni per l'amministratore per programmare alcuni task da mandare in esecuzione in automatico. Aggiornamenti giornalieri del file dei virus, scanning periodici dei client possono essere impostati per l'esecuzione automatica. La tabella seguente mostra un esempio d scheduling delle azioni.

Tabella 8-2: Schedule

Tipologia	Compiti da Automatizzare	Frequenza
Server	Download degli aggiornamenti	Giornaliera
Client	Download degli aggiornamenti	Giornaliera
	Scan definito dall'amministratore	Giornaliera

8.8 Metodologia di Installazione

Per far funzionare adeguatamente un anti-virus software, il file contenente la lista dei virus deve essere sempre il più aggiornato possibile ed essere installato in ciascuna workstation e tutti i server. Tuttavia, per evitare rischi di crash o reboot dei sistemi dovuto a certi update inconsistenti, l'amministratore deve pianificare un metodo per testare gli aggiornamenti scaricati. Questo obiettivo può essere raggiunto in diversi modi. L'ordine di installazione dell'anti-virus di un client deve essere considerato per gruppi come evidenziato nella sezione 8.5.1.
L'amministratore può utilizzare una macchina di test per gestire la fase di prova degli update. Il sistema deve essere aggiornato allo stesso livello della rete PCN (se possibile). Dopo questa fase, l'amministratore di sistema deve assicurarsi che gli update non causino nessun rallentamento o conseguenze evidenti. Al termine, l'admin deve procedere alla pianificazione della graduale installazione, partendo da quei dispositivi che offrono un minore impatto nelle operazioni giornaliere nell'impianto.
L'amministratore può raggruppare l'aggiornamento su più macchine tenendo a mente l'influenza che l'update causa al sistema ed ai suoi task giornalieri. Una volta certificata la non pericolosità dell'aggiornamento, l'update viene installato nel resto del sistema.

9 PATCH MANAGEMENT

Il gestore di Patch OS, chiamato anche Windows Server Update Services (WSUS), è il processo di controllo della distribuzione e manutenzione di versioni del software in ambienti di produzione. Aiuta a mantenere operativamente efficiente ed efficace, migliorare la sicurezza e la stabilità dell'ambiente di produzione. Se l'organizzazione non riesce a mantenere un livello di affidabilità tra il sistema operativo e le applicazioni software, è facile che insorga la presenza crescente di falle nella sicurezza, le quali, se sfruttate, potrebbero portare ad una massiccia perdita di risorse e proprietà intellettuale.
Applicare gli aggiornamenti per gli OS è un compito critico per l'ambiente della PCN. Considerazioni sulla sicurezza e sulla stabilità sono necessarie per l'approvazione dell'introduzione di una patch. Yokogawa ha un team di ricercatori che collabora con Microsoft per testare gli aggiornamenti sulle applicazioni Yokogawa prima che queste vengano rilasciate al pubblico. Eseguendo dei test in anticipo, Yokogawa è in grado di avvisare il partner commerciale sulla disponibilità dell'update per il relativo sistema di controllo in tempi brevi.
WSUS abilita l'admin IT all'accesso all'ultimo aggiornamento del prodotto Microsoft per i computer con in esecuzione i sistemi operativi Microsoft Windows Server 2008(R2), Windows 7 professional. Gli update dei prodotti possono spaziare dai Sistemi Operativi, applicazioni per server database e applicazioni d'ufficio. Utilizzando WSUS, l'amministratore di sistema può gestire la diffusione degli aggiornamenti rilasciati attraverso Microsoft Update ai computer della loro rete.

FDS
ENI IT Security
Progetto: 14B120019
Doc. Name: 14B120019_FDS
Rev 0

9.1 Windows Server Update Services (WSUS) Overview

WSUS fornisce una infrastruttura per il management costituita dai seguenti:

- WSUS Server (Administration Console)
- WSUS Client Computers

WSUS Server

I componenti server WSUS possono essere installati in un computer con i sistemi operativi Windows Server 2008. Il WSUS fornisce le feature che l'admin necessita per gestire e diffondere gli update attraverso la WSUS Administration Console. In aggiunta, un server WSUS viene scelto come sorgente ("upstream server") per l'aggiornamento degli altri WSUS server nell'organizzazione. In un implementazione WSUS, almeno un server WSUS nella rete deve essere connesso a Microsoft Update per rendere disponibile le informazioni di aggiornamento. L'amministratore determina, basandosi sulla configurazione e sicurezza della rete, quale server deve essere direttamente connesso alla sorgente di update Yokogawa.

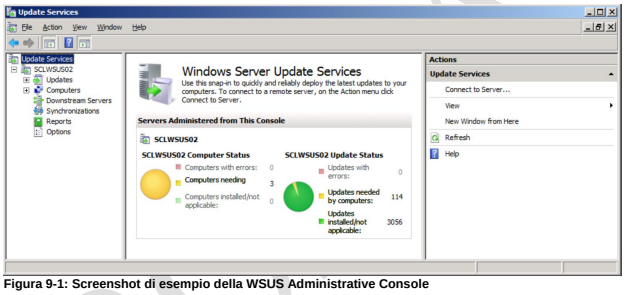


Figura 9-1: Screenshot di esempio della WSUS Administrative Console

WSUS Client Computer e gli Automatic Updates

Automatic Updates è un componente dei computer client sviluppato negli OS Windows. Abilita sia server che client a ricevere aggiornamenti dal server WSUS in esecuzione.
L'admin può configurare i comportamenti di Automatic Updates utilizzando i gruppi di policy in una ambiente gestito dalle Active Directory.
Il servizio di Automatic Updates viene eseguito in background in modo da renderne impercettibile e minimale l'impatto sulle funzionalità dell'impianto.

9.2 Design Architetturale WSUS per Eni Venezia

Un server Microsoft WSUS viene pposizionato nella DMZ. Viene configurato in modalità downstream e replica periodicamente gli update scaricati dal server upstream precedentemente introdotto.
Un server Management Microsoft WSUS (macchina che ha anche il ruolo di DC) viene posizionata nella rete PCN. Viene utilizzato per le seguenti funzioni:

- console amministrativa con il quale approvare gli update per i clietn WSUS.
- Download aggiornamenti dal server downstream Microsoft WSUS nella DMZ a intervalli regolari.

Tutti i computer Yokogawa forniti (definiti come client WSUS) nella PCN, DMZ avranno il servizio di Automatic Update configurato in modo da scaricare gli aggiornamenti approvati dal server WSUS Management ad intervalli regolari.

Nei casi in cui l'upstream server Microsoft WSUS non è disponibile, il server in downstream nella DMZ può essere riconfigurato in modo da scaricare direttamente dal sito Microsoft gli aggiornamenti in programma.

9.3 Update dei Prodotti

Poichè gli aggiornamenti approvati sono postati regolarmente nel sito web di Yokogawa nella sezione Microsoft security update, l'admin deve fare controlli settimanali nel sito web prima di approvare un aggiornamento nel server di management WSUS. Solo gli update approvati ed elencati nella sezione degli aggiornamenti Microsoft del website Yokogawa sono stati testati in compatibilità con la suite di soluzioni Yokogawa.

9.4 Gruppi

L'obiettivo dei raggruppamenti è quello di separare computer che richiedono differenti aggiornamenti. Per esempio, se un update critico è incompatibile con un applicazione ma compatibile con un altra, l'amministratore più assicurarsi che la patch venga distribuita nei soli dispositivi compatibili.
Ogni client WSUS viene assegnato ad un gruppo all'interno del server di gestione WSUS. I gruppi sono disposti in modo gerarchico. Alla radice dell'albero vi è un gruppo chiamato All Computers. Quest'ultimo viene creato di default con l'installazione del server e non può essere rimosso. Tutti i gruppi figli saranno creati a partire da questo gruppo.
Quando il servizio di Automatic Update dei client WSUS viene configurato per controllare gli aggiornamenti nel server management WSUS, questi client sono assegnati automaticamente ad un gruppo Unassigned Computer. Questi vengono poi manualmente ridiretti nei differenti gruppi figli in base alla categoria di applicazioni in esecuzione al loro interno.
La tabella successiva mostra i gruppi figli che vengono creati in base alle categorie delle applicazioni. Questa lista viene stilata sulla base delle informazioni della sezione di Microsoft Security Update nel sito web Yokogawa.

Tabella 9-1: Gruppi Figli Create sul WSUS Management Server

Gruppi Figli	Descrizione
CENTUM	Patche sono soggette ad approvazione dell' YHQ prima di essere applicate.
ProSafe-RS	
PRM	
Solution-based Software (Exaopc,Exapilot,Exaplog,Exasmoc, Exarqe,Exaquantum,Exaquantum/Batch)	
Fast/Tools	
IT-Related systems	Patch NON sono soggette ad approvazione dal YHQ. Tutte le patch possono essere installate.

9.5 Schedules

La seguente tabella mostra un esempio di tempistiche delle varie procedure automatizzate che avranno luogo nello svolgimento di processo giornaliero.

Tabella 9-2: Esempio di Schedule di Task Automatizzati WSUS

Tipi	Task Automatizzati	Frequenza	Tempo di Svolgimento
WSUS downstream server	Synchronization [1] schedule	Giornaliera	8pm
WSUS management server	Synchronization schedule	Giiornaliera	10pm
WSUS clients	Automatic Updates detection frequency	Intervalli di 22 ore	*NA*
	Auto download e notifica per l'installazione	*NA*	*NA*

Nota [1]: La sincronizzazione avviene quando il server WSUS scarica aggiornamenti (metadati e file) da una sorgente. Scarica anche nuove classificazioni e categorie dei nuovi prodotti, se presenti. Quando il server WSUS si sincronizza per la prima volta, procede al download di tutti gli aggiornamenti specificati. Dopo la prima sincronizzazione, il server

provvederà a scaricare gli update dalla sorgente degli aggiornamenti, così come le revisioni dei metadati per gli aggiornamenti esistenti e secondo le scadenze degli stessi.

9.6 Metodologia di Installazione

L'installazione delle patch dell'OS in un sistema individuale devono essere eseguite manualmente da personale Yokogawa. La strategia di approccio, che necessita di essere formalizzata, richiede che l'installazione delle patch nel sistema non causino nessun impatto al processo nel causo di una richiesta di reboot. Una panoramica delle patch MS approvate da Yokogawa può essere trovato nel seguente sito web: http://www.yokogawa.com/vps/update/msup/vps-msup-en.htm.
Dopo che sono state notificate le nuove patch approvate, l'admin può testarle con una macchina di test o in un gruppo di sistemi meno critici. Il sistema selezionato per la prova deve, a questo punto, essere lasciato funzionare per almeno una settimana. Questa procedura serve ad assicurarsi che le patch dell'OS installate non causino problemi al sistema in opera a cui sono destinate.

9.7 WSUS Reporting

Il server di gestione WSUS colleziona informazioni sugli eventi di update nella rete e li visualizza, quando vengono richiesti, in svariati formati di report. Quando un report viene creato, quest'ultimo viene visualizzato in una finestra separata. Una copia viene salata in un formato per l'archivio web o può essere stampata.
Non vi sono configurazioni richieste per la generazione dei report. Questi vengono semplicemente collocati nella sezione dei report del server di management WSUS. Essi sono generati manualmente da questa sezione come e quando l'amministratore lo richiede, mostrando lo stato di un determinato evento di aggiornamento.

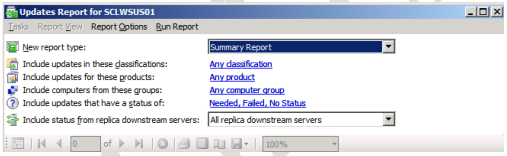


Figura 9-3: Screenshot di un Report vuoto

10 NETWORK MANAGEMENT SYSTEM

Un NMS è una combinazione di hardware e software utilizzato per monitorare e amministrare i componenti della rete. Il sistema monitora costantemente i computer ricercando rallentamenti o fallimenti e notificando all'amministratore in caso di interruzioni via email e allarmi.

10.1 Architettura del Network Management Systems

L' NMS viene posizionato nella zona comune dei server (Common Server Facility Zone) in cui ottiene ed elabora gli eventi dai dispositivi di gestione nella rete. Gli eventi ricevuti dai server e altre risorse critiche possono essere inoltrate a un entità di gestione. Le seguenti funzioni sono incluse nello standard di gestione delle entità:

- Network discovery
- Mappatura della topologia dei dispositivi gestiti
- Gestore di eventi
- Raccolta dati sulle prestazioni e grafici
- Management data browser

L'entità di gestione della rete può essere vista come la console principale per le operazioni di rete. L'abilità di intercettare i problemi rapidamente è di importanza cruciale. Il personale operativo della rete può fare affidamento su una mappa grafica della rete che ne evidenzia lo stato operativo dei dispositivi più critici come router e switch.
I dispositivi controllati (come computer di sistema e altri) eseguono un software che li abilita a inviare avvisi di allarme ogni qualvolta si presenta un problema (per esempio, quando una o più soglie di controllo vengono superate). Una volta ricevuto l'allarme, le entità di gestione sono programmate per reagire per eseguire una o più azioni incluse operazioni di notifica, shutdown del sistema, registrazioni di eventi e tentativi di autoriparazione.
La Figura 10-1 ritrae una tipica architettura di management di una rete.

- Entità di Management : interrogano i dispositivi per controllare i valor di alcune variabili. La richiesta avviene tramite un polling degli agenti. Può agire in automatico o per volontà dell'utente.

- Agenti: sono moduli software che prima di tutto compilano informazioni sui dispositivi gestiti nei quali risiedono, successivamente memorizzano le informazioni in un database, e infine inviano quest'ultime (in anticipo o di conseguenza) alle entità di management attraverso la rete NMS con il relativo protocollo di comunicazione. Quest'utlimo è costituito dal noto Simple Network Management Protocol (SNMP) e dal Common Management Information Protocol (CMIP). Nel caso del SNMP, un agente di servizio SNMP viene utilizzato e nessun software addizionale necessita di essere installato come agente.

- Management proxy: sono entità che forniscono informazioni a nome di altre entità. Un proxy di management aiuta a localizzare il polling dell'SNMP e le trappole di ricezione riducendo così il traffico SNMP attraverso le dorsali di rete e collegamenti WAN. Può fare l'elaborazione locale per riassumere i dati che possono poi essere inviati a NMS.

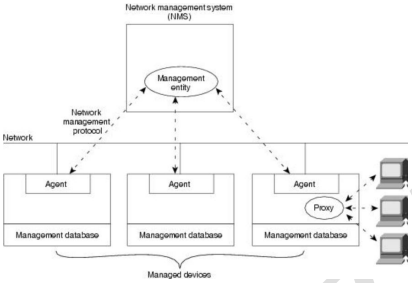
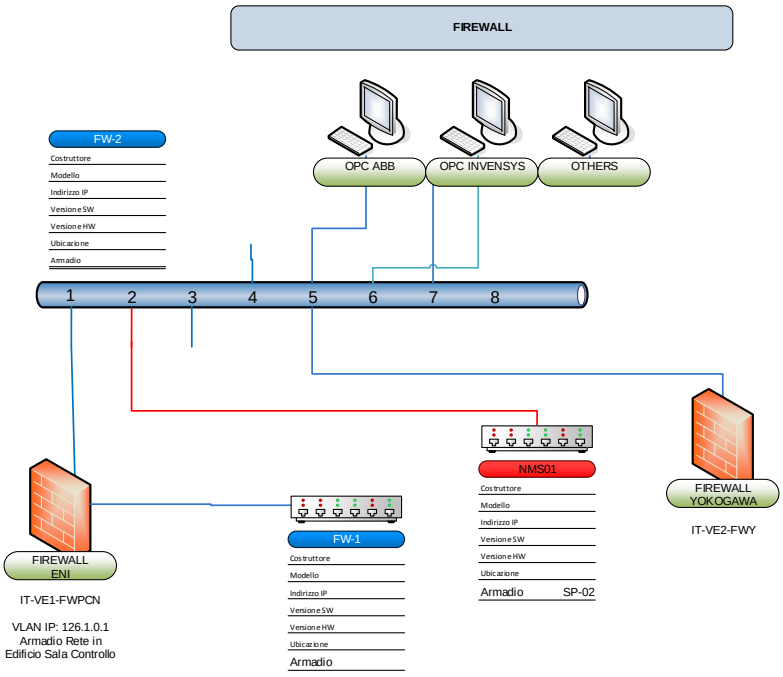


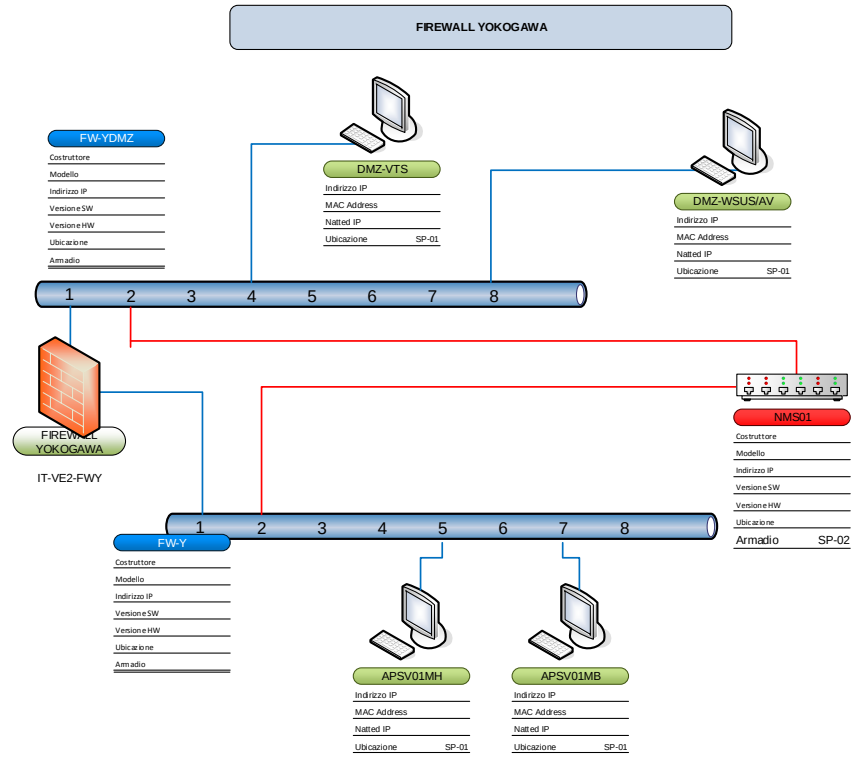
Figura 10-1: Architettura di Network Management

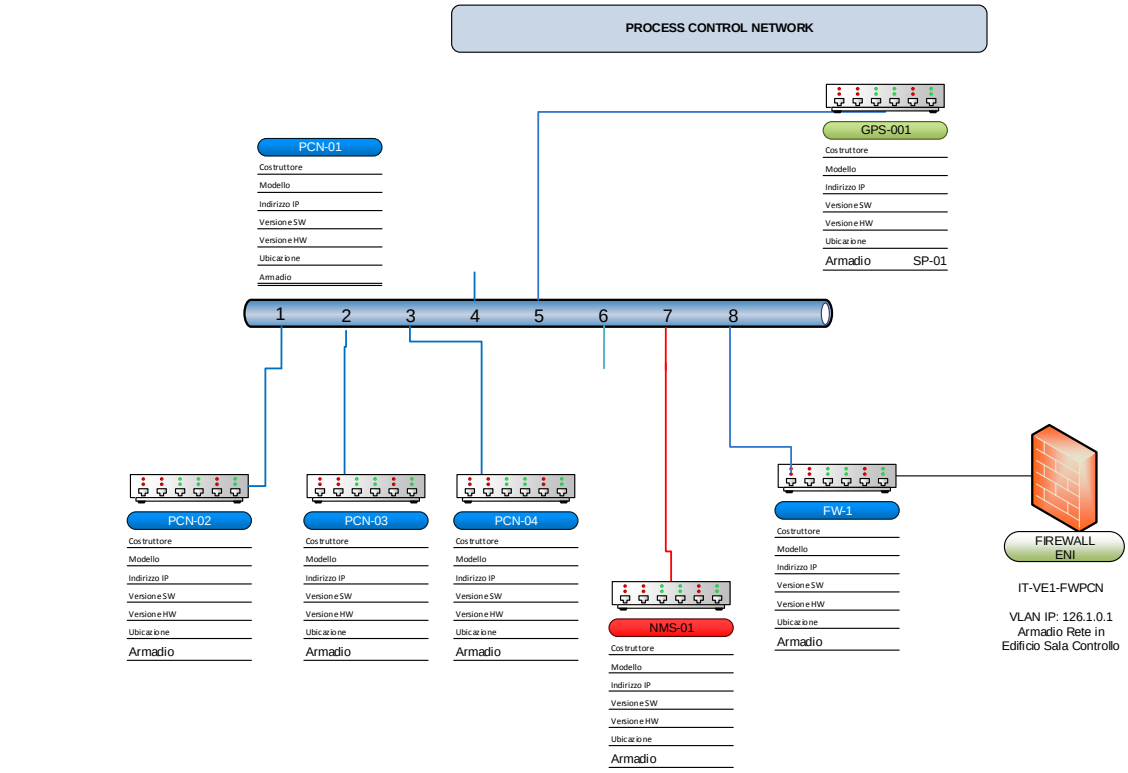
10.2 Soluzione di Network management per il sito di Eni Venezia

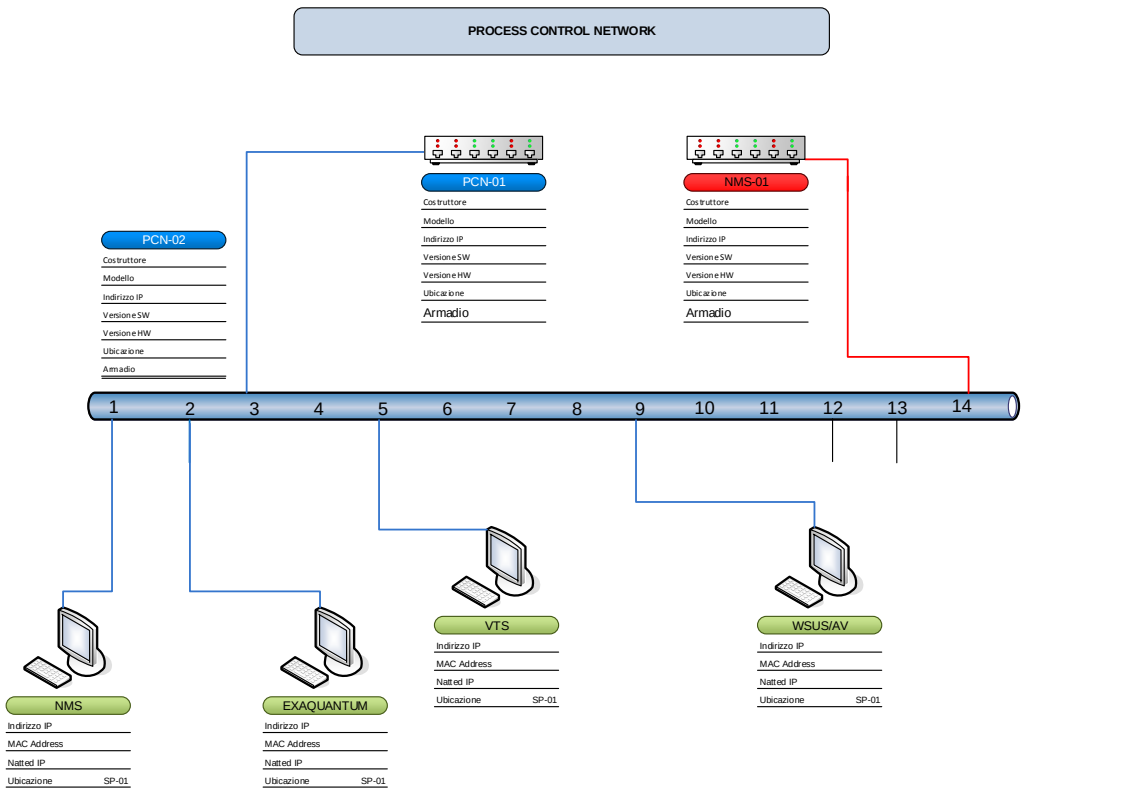
Per il sito di Eni Venezia, l'NMS si basa sul software WhatsUp Gold, installato nel server di network management. Questo server agisce anche da Domain Controller. WhatsUp Gold monitorerà tutto l'attrezzatura della rete e i PC connessi alla PCN e alla rete Vnet/IP utilizzando il Network Management System.

7.3 Appendice C: Architettura di rete Yokogawa

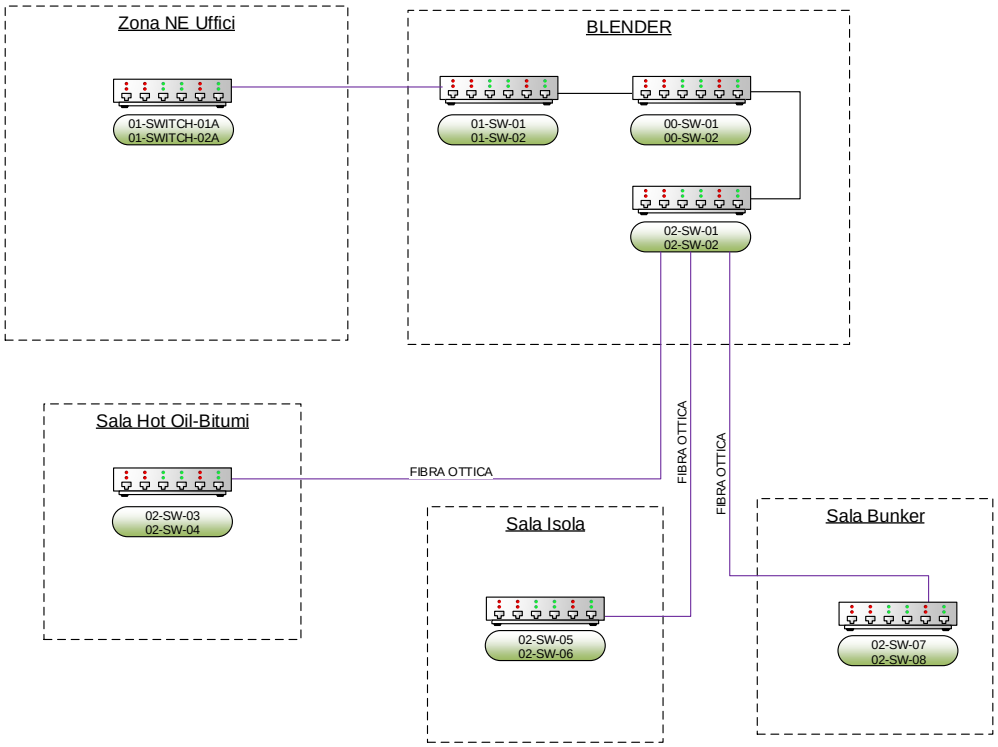




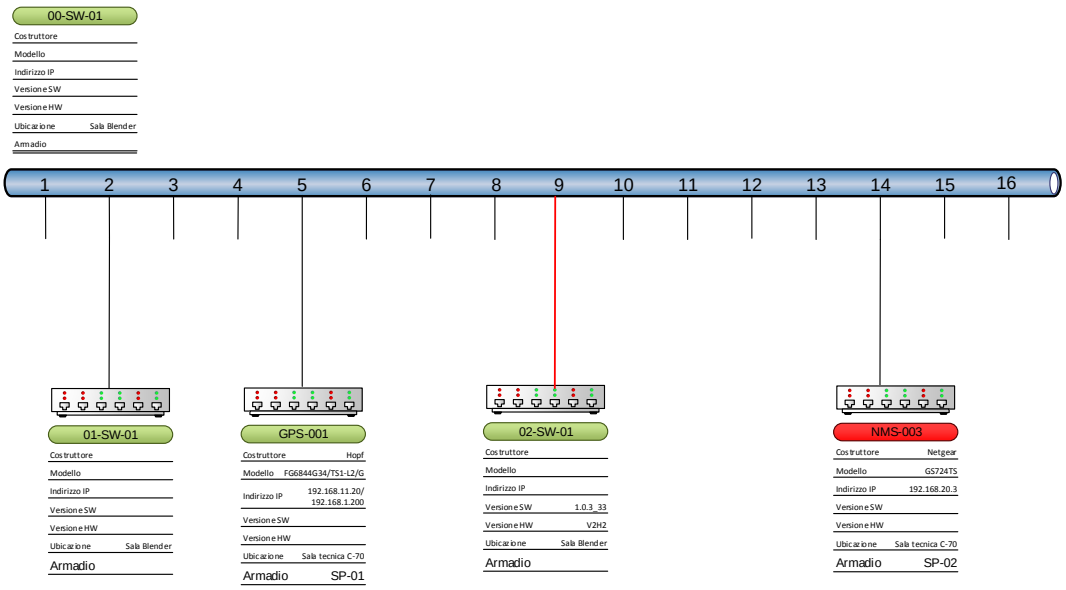

PROCESS CONTROL NETWORK
PCN-01
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione
Armadio
GPS-001
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione
Armadio SP-01
1 2 3 4 5 6 7 8
PCN-02
PCN-03
PCN-04
NMS-01
FW-1
FIREWALL ENI
IT-VE1-FWPCN
VLAN IP: 126.1.0.1
Armadio Rete in Edificio Sala Controllo

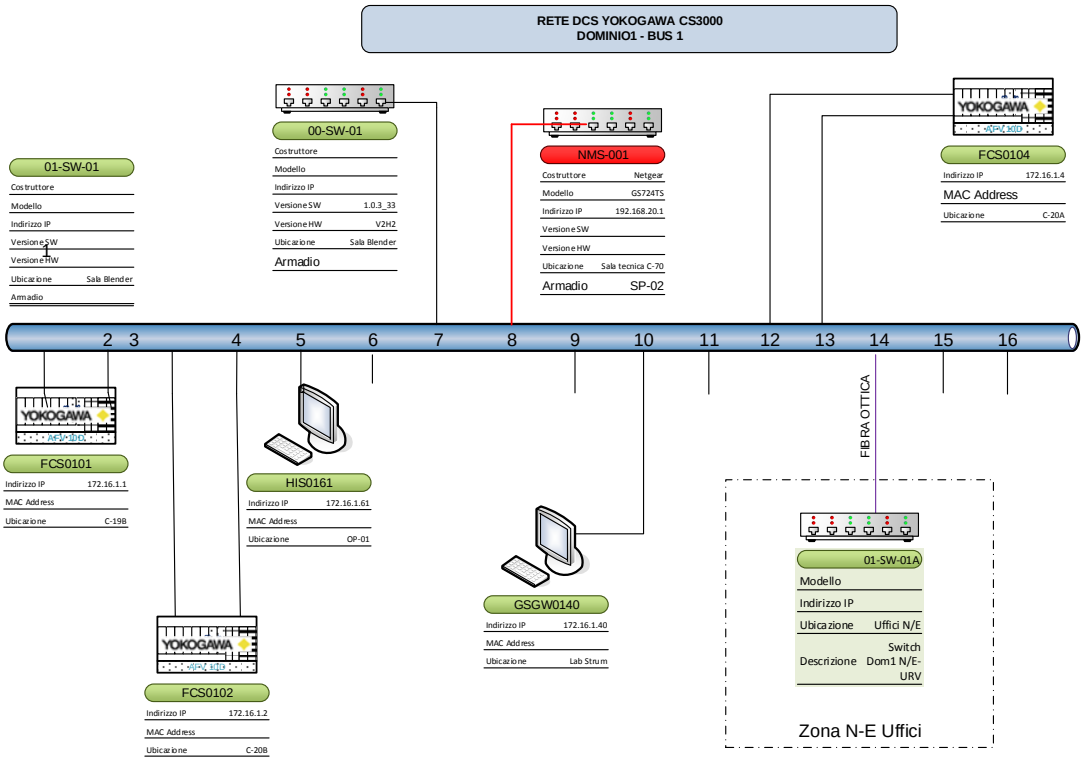

PROCESS CONTROL NETWORK
PCN-02
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione
Armadio
PCN-01
NMS-01
1 2 3 4 5 6 7 8 9 10 11 12 13 14
NMS
Indirizzo IP
MAC Address
Natted IP
Ubicazione SP-01
EXAQUANTUM
VTS
WSUS/AV

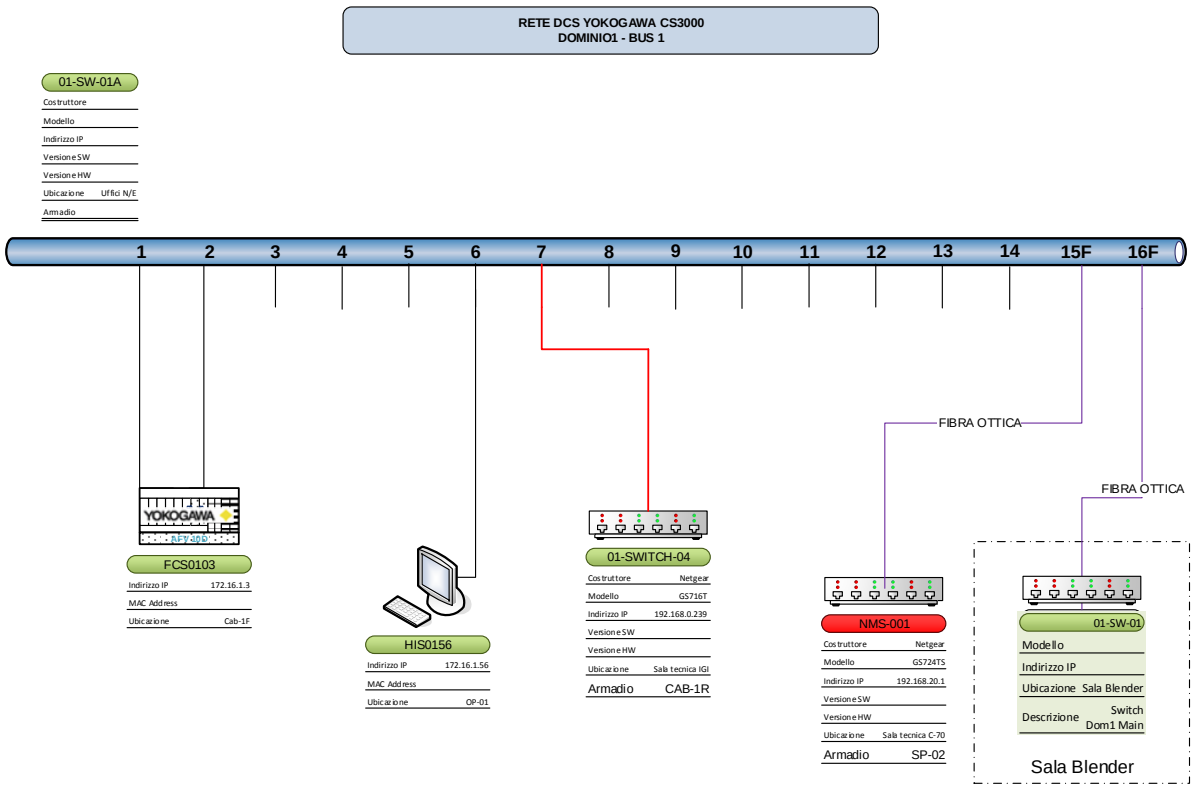
Vista Globale VNET – VNET/IP

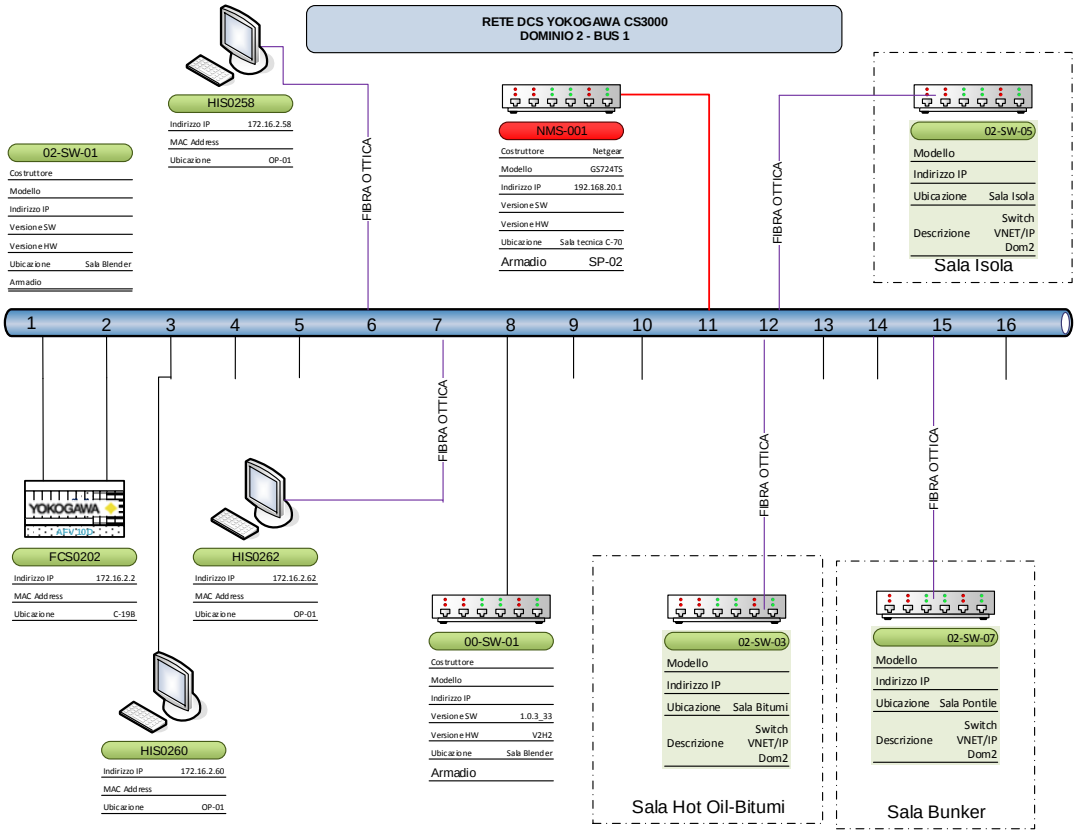


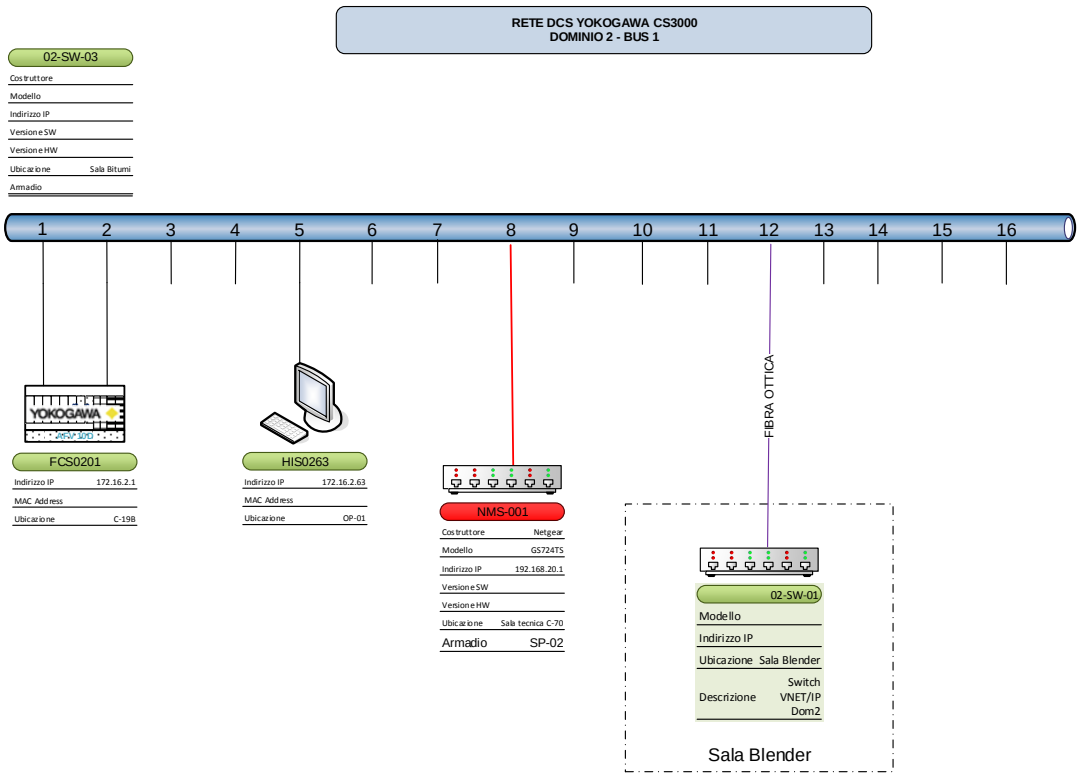
RETE DCS YOKOGAWA CS3000
LAYER 3 - BUS 1

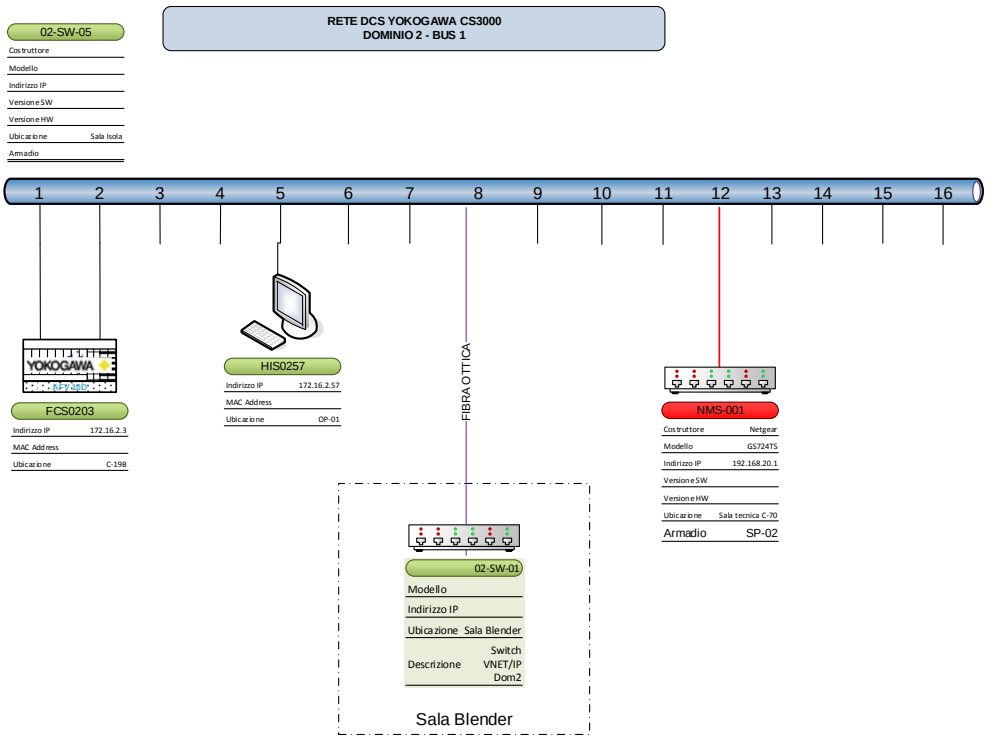


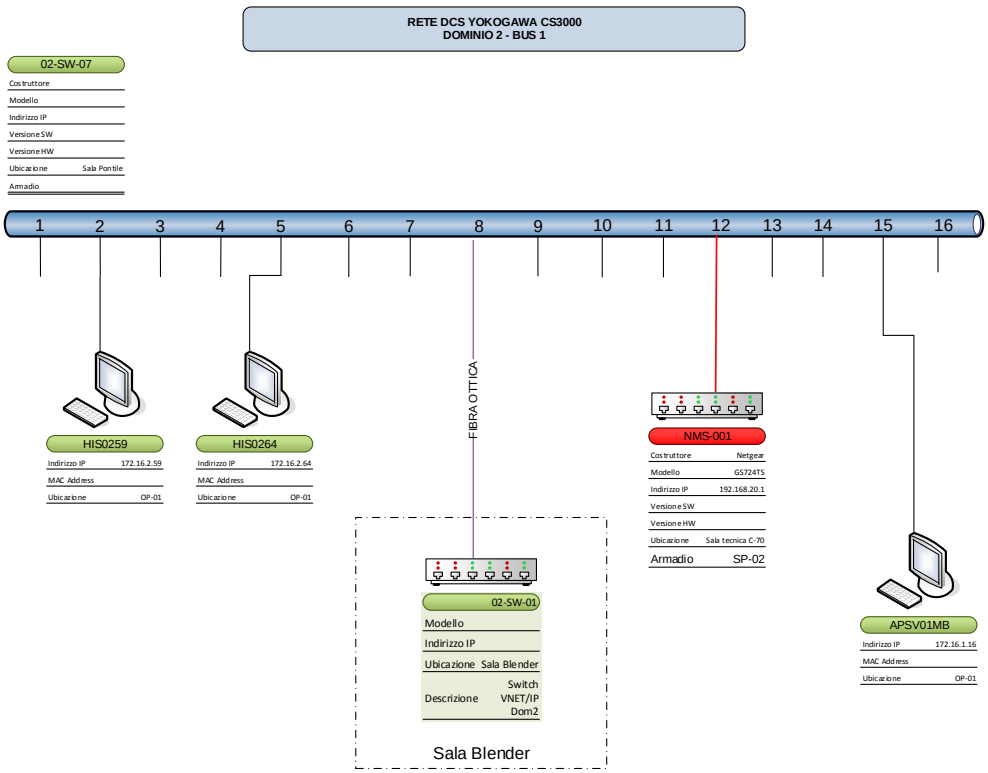

RETE DCS YOKOGAWA CS3000
DOMINIO1 - BUS 1
01-SW-01
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione Sala Blender
Armadio
00-SW-01
Costruttore
Modello
Indirizzo IP
Versione SW 1.0.3_33
Versione HW V2H2
Ubicazione Sala Blender
Armadio
NMS-001
Costruttore Netgear
Modello GS724TS
Indirizzo IP 192.168.20.1
Versione SW
Versione HW
Ubicazione Sala tecnica C-70
Armadio SP-02
FCS0104
Indirizzo IP 172.16.1.4
MAC Address
Ubicazione C-20A
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
FIBRA OTTICA
FCS0101
Indirizzo IP 172.16.1.1
MAC Address
Ubicazione C-19B
HIS0161
Indirizzo IP 172.16.1.61
MAC Address
Ubicazione OP-01
GSGW0140
Indirizzo IP 172.16.1.40
MAC Address
Ubicazione Lab Strum
FCS0102
Indirizzo IP 172.16.1.2
MAC Address
Ubicazione C-20B
01-SW-01A
Modello
Indirizzo IP
Ubicazione Uffici N/E
Descrizione Switch Dom1 N/E-URV
Zona N-E Uffici


RETE DCS YOKOGAWA CS3000
DOMINIO1 - BUS 1
01-SW-01A
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione Uffici N/E
Armadio
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15F 16F
FIBRA OTTICA
FIBRA OTTICA
FCS0103
Indirizzo IP 172.16.1.3
MAC Address
Ubicazione Cab-1F
HIS0156
Indirizzo IP 172.16.1.56
MAC Address
Ubicazione OP-01
01-SWITCH-04
Costruttore Netgear
Modello GS716T
Indirizzo IP 192.168.0.239
Versione SW
Versione HW
Ubicazione Sala tecnica IGI
Armadio CAB-1R
NMS-001
Costruttore Netgear
Modello GS724TS
Indirizzo IP 192.168.20.1
Versione SW
Versione HW
Ubicazione Sala tecnica C-70
Armadio SP-02
01-SW-01
Modello
Indirizzo IP
Ubicazione Sala Blender
Descrizione Switch Dom1 Main
Sala Blender


RETE DCS YOKOGAWA CS3000
DOMINIO 2 - BUS 1
HIS0258
Indirizzo IP 172.16.2.58
MAC Address
Ubicazione OP-01
NMS-001
Costruttore Netgear
Modello GS724TS
Indirizzo IP 192.168.20.1
Versione SW
Versione HW
Ubicazione Sala tecnica C-70
Armadio SP-02
02-SW-05
Modello
Indirizzo IP
Ubicazione Sala Isola
Descrizione Switch VNET/IP Dom2
Sala Isola
02-SW-01
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione Sala Blender
Armadio
FIBRA OTTICA
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
FCS0202
Indirizzo IP 172.16.2.2
MAC Address
Ubicazione C-19B
HIS0262
Indirizzo IP 172.16.2.62
MAC Address
Ubicazione OP-01
HIS0260
Indirizzo IP 172.16.2.60
MAC Address
Ubicazione OP-01
00-SW-01
Costruttore
Modello
Indirizzo IP
Versione SW 1.0.3_33
Versione HW V2H2
Ubicazione Sala Blender
Armadio
02-SW-03
Modello
Indirizzo IP
Ubicazione Sala Bitumi
Descrizione Switch VNET/IP Dom2
Sala Hot Oil-Bitumi
02-SW-07
Modello
Indirizzo IP
Ubicazione Sala Pontile
Descrizione Switch VNET/IP Dom2
Sala Bunker


RETE DCS YOKOGAWA CS3000
DOMINIO 2 - BUS 1
02-SW-03
Costruttore
Modello
Indirizzo IP
Versione SW
Versione HW
Ubicazione Sala Bitumi
Armadio
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
FCS0201
Indirizzo IP 172.16.2.1
MAC Address
Ubicazione C-19B
HIS0263
Indirizzo IP 172.16.2.63
MAC Address
Ubicazione OP-01
NMS-001
Costruttore Netgear
Modello GS724TS
Indirizzo IP 192.168.20.1
Versione SW
Versione HW
Ubicazione Sala tecnica C-70
Armadio SP-02
FIBRA OTTICA
02-SW-01
Modello
Indirizzo IP
Ubicazione Sala Blender
Descrizione Switch VNET/IP Dom2
Sala Blender





[35] L'architettura per ragioni di sicurezza e privacy non è presentata comprensiva di tutte le informazioni di indirizzamento e dispositivi hardware utilizzati.

Ringraziamenti

In questa sezione finale vorrei ricordare brevemente tutte le persone che mi hanno seguito in questa formativa esperienza di tesi e dedicare anche a loro questo mio traguardo.
Ringrazio il professor Carlo Ferrari per la sua disponibilità ad assecondarmi in questo percorso di formazione e conclusione della mia carriera universitaria. Ringrazio il correlatore Massimiliano Veronesi e i collaboratori della Yokogawa che più mi hanno sopportato nell'esperienza di stage, primo fra tutti del gruppo Paolo Cocco, senza il vostro aiuto probabilmente sarei ancora a leggere documentazioni e mandare email a vuoto. Ringrazio i miei genitori e i miei familiari che in qualsiasi occasione mi hanno supportato e assecondato a spada tratta, anche nelle scelte più azzardate. Ringrazio infine i miei amici (più o meno intimi, più o meno tutti sentitevi presi in causa) che negli anni sono cresciuti e cambiati con me rendendomi pronto ad affrontare qualsiasi prova nel mio percorso e che hanno dato un tocco di colore in più alle mie giornate.
Ringrazio tutti voi ora e vi ringrazierò ancora nonostante le botte che prenderò da voi dopo la proclamazione. Spero di ringraziarvi ancora in altri miei traguardi indipendentemente dalle strade che il destino ci riserverà.

Grazie di tutto.