www.ServiTecno.IT

esperti in Cyber Security Industriale

- Education & Awareness
- Design
- Anomaly detection & asset management
- Scada Security
- Continuità Operativa
- Configuration management
- ICS Cyber Security per Industria 4.0 & Utility 4.0

ServiTecno – Industrial Cyber Security

Education & Awareness

ServiTecno sostiene da sempre l'approccio della ***Security by Design*** che in ambiente produttivo e di fabbrica, dove la ***disomogeneità dei sistemi*** è all'ordine del giorno, è da sempre più efficace della Security by Products.

Uno degli aspetti fondamentali in questo caso è certamente ***l'istruzione*** e la ***conoscenza delle problematiche*** che chi ha limitate competenze in ambito digitale deve acquisire anche solo per poter redigere e rispettare le policy di sicurezza che non possono mancare in un piano di Cyber Security Industriale (e non).

Enzo M. Tieghi, esperto di Industrial Cyber Security durante un corso

Quali sono le minacce che affrontiamo oggi e che affronteremo domani**? A cosa possono portare**? Differenti figure e profili aziendali possono approcciare il problema dal loro punto di vista, ecco perché abbiamo proposte di corsi e workshop specifici: dagli operatori che lavora sulla linea, fino a supervisori e manager, abbiamo la proposta giusta per voi.

LA PROPOSTA DI SERVITECNO: il programma per Corsi Avanzati saranno concordati con il cliente

Il percorso ***STANDARD*** è composto da ***½ giornata lavorativa (più un seguito eventuale di 8h)*** ed avrà un taglio strettamente legato al settore di business e alle tipologie di tecnologie utilizzate: in ogni caso tratterà i seguenti macro-argomenti.

1) Intro e ***Terminologia***
2) ***Analisi*** e Valutazione dei rischi
3) Normative, Standard Industriali e ***best practices*** internazionali
4) ***Metodologie di protezione*** HW/SW: Antimalware, IDS/IPS, Firewall, ecc.
5) Introduzione a ***tool e strumenti*** per la protezione di reti e sistemi industriali
6) ***Segmentazione della rete e segregazione in Zone*** & Conduit, secondo ISA99/IEC62443

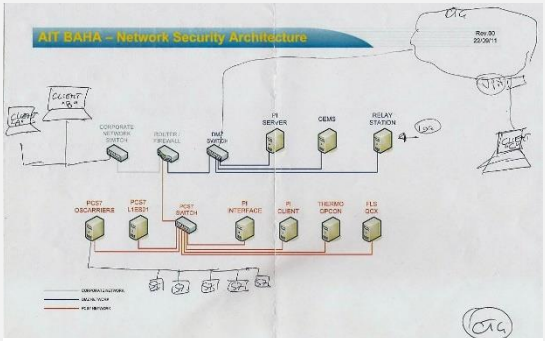
WWW.SERVITECNO.IT – ***info@servitecno.it*** – TEL +39-02.486141

DESIGN

Il "disegno" della rete e dell'architettura in generale rappresenta il primo importantissimo passo verso un'applicazione sicura.

Quando si progetta una nuova rete bisogna ben tenere a mente quali saranno **caratteristiche, priorità e vulnerabilità**: in questo caso si parte con un grande vantaggio che è quello di poter "disegnare" il sistema partendo da un foglio bianco e con tutte le nozioni per creare un'infrastruttura sicura.

Intervenire su un'architettura esistente potrebbe essere più complicato, ma anche in questo caso si parte **mappando tutte le connessioni** (attività non banale nell'epoca dell'IoT) **e i terminali** di sistema ed individuando le criticità.



Architettura di rete "prima e dopo": lo schema dell'architettura era stampato, il risultato finale ha diverse aggiunte

Così sarà possibile procedere con un'adeguata **suddivisione in Zone/Conduit** e **selezionare le tecnologie necessarie alla loro protezione**: questa analisi servirà a **porre la RETE su fondamenta solide** e soprattutto a costruirla a **compartimenti stagni**, come una nave.

Anche nel caso in cui una problematica si verifichi in una parte dell'impianto o del sistema, potremo **proteggere il resto dell'architettura isolandolo e mantenendo produttivo l'impianto**.

LA PROPOSTA DI SERVITECNO:

ServiTecno può fornire consulenza altamente specializzata per analizzare la situazione esistente, necessità e vincoli al fine di "disegnare" e/o "ridisegnare" una rete più sicura

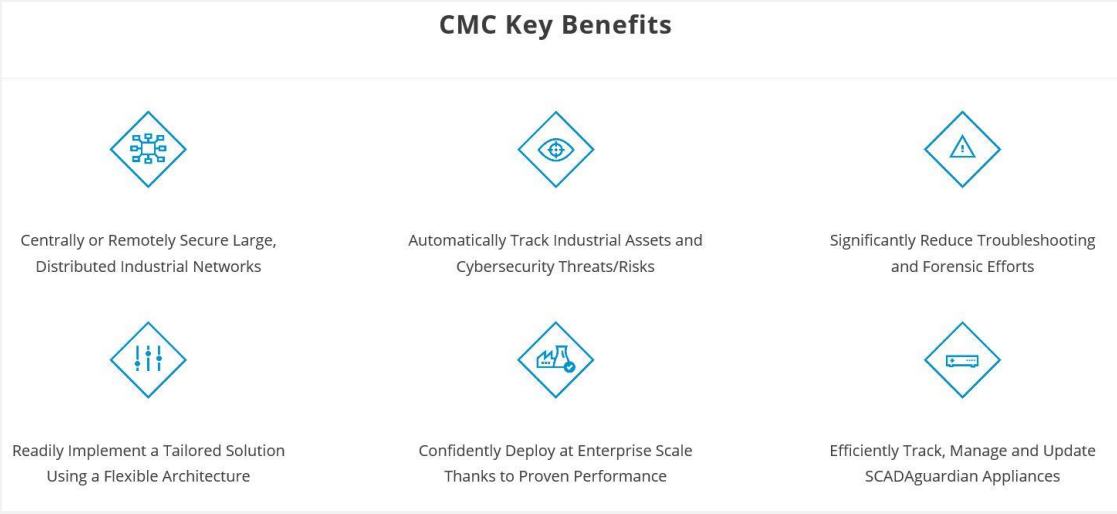
ANOMALY DETECTION e MONITORAGGIO degli ASSET

Una volta mappata l'intera architettura esistono tool in grado di analizzare i suoi comportamenti in maniera più precisa e regolata.

I sistemi di controllo e di automazione di fabbrica sono studiati e programmati per comportarsi in modo "prevedibile".

Nel caso in cui sopravvengono allarmi o problemi sull'impianto, ci sono procedure automatiche o guidate dall'operatore che sono state "previste" e che devono essere eseguite con la corretta sequenza: **se sull'impianto insorge un problema "inaspettato" si crea la cosiddetta "anomalia"**.

Potrebbe essere un fatto assolutamente "lecito", ma alcune anomalie potrebbero essere avvisaglie di malfunzionamenti o addirittura sabotaggi indotti da "incidenti informatici", anche correlando eventuali concatenazioni (AI, Machine Learning, etc…): ecco quindi che oggi sono disponibili sul mercato ***sistemi di "Anomaly Detection" che possono rappresentare un primo livello di "early warning"*** a ***protezione di reti e sistemi*** di controllo ed a tutela dell'impianto controllato.



LA PROPOSTA DI SERVITECNO:

NOZOMI NETWORKS

WWW.SERVITECNO.IT – *info@servitecno.it* – TEL +39-02.486141

ServiTecno – Industrial Cyber Security

SCADA SECURITY

L'utilizzo dello **SCADA** come piattaforma nei progetti per l'integrazione dei **sistemi aziendali non deve però sottovalutare gli aspetti relativi alla Cyber Security**: di seguito alcune delle aree tematiche "care" a ServiTecno che permettono di aumentare la resilienza dei sistemi SCADA avendo come obiettivo lo SCADA Sicuro.

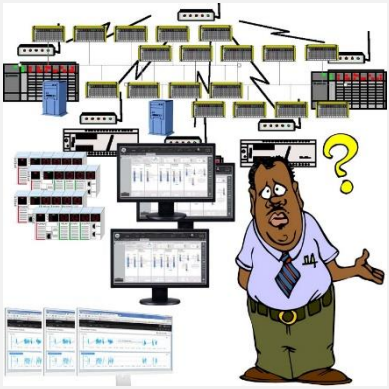
- ***Network architecture***: Non tutti gli SCADA hanno la stessa architettura di rete, le abituali architetture dei prodotti di mercato possono avere un impatto sulla Cyber Security anche molto differente.
- ***Firewall, Segmentation & Segregation***: La segmentazione della rete in zone & conduit è alla base di tutte le strategie di messa in sicurezza dei sistemi ICS.
- ***Common Vulnerabilities & Exposures detection (CVEs)***: Il controllo delle vulnerabilità e le falle.
- ***Zero Days detection***: Il controllo delle vulnerabilità e le falle di sicurezza particolarmente gravi non ancora note e rese pubbliche.
- ***Change Management & Change Control***: La gestione, il controllo e l'archiviazione delle modifiche, delle release, etc…
- ***Disaster Recovery***: Il veloce recupero e ricostituzione della stazione SCADA a seguito di un incidente.
- ***White List Hardware***: La definizione di una lista di dispositivi, che sono considerati sicuri.
- ***White List Software***: La definizione di una lista di software che sono considerati sicuri.
- ***New Versions, Upgrades & Sandbox***: Gestione programmata di test per software improvement, patches, release e versioni.
- ***ThinClient***: Uso di hardware speciale per la realizzazione di interfacce operatore sicure.
- ***Deep Packet Inspection (DPI)***: Modalità di analisi del contenuto dei pacchetti di dati al fine di individuare contenuti non aderenti a precisi criteri definiti in precedenza
- ***Anomaly Detection***: La verifica di anomalie presenti nel network
- ***Availability (Redundancy, High Availabilty and Fault Tolerance)***: La capacità del sistema SCADA di rimanere attivo senza interruzioni (down-time).
- ***Antivirus***: Gli specifici antivirus che hanno caratteristiche compatibili con il sistema SCADA
- ***Criptazione & VPN***: L'utilizzo di criteri di criptazione e tunnelling per la comunicazione sicura fra gli elementi dell'architettura SCADA

LA PROPOSTA DI SERVITECNO:

GE Digital

WWW.SERVITECNO.IT – *info@servitecno.it* – TEL +39-02.486141

Configuration Management



Come gestire gli applicativi di decine o centinaia di PLC, SCADA, etc...

Un **impianto produttivo** o comunque un **processo** è **gestito da dispositivi di campo (PLC, HMI-SCADA, robot, ICS, DCS, motion, etc...)**, **supervisori a bordo macchina o in control room** e dispositivi per la remotizzazione delle informazioni: ognuno di questi dispositivi e applicativi ha una sua "storia" fatta di configurazione, programmazione e variazioni dettate da necessità che variano nel tempo.

Come si gestiscono dunque gli applicativi di tutti questi dispositivi e pc di produzione?

Cosa succede se un operatore o un manutentore devono modificare questi applicativi? Chi tiene traccia della variazione? Qual è la versione corretta dell'applicativo?

Crea la tua "CASSAFORTE" degli applicativi: saprai sempre dove trovare l'ultima versione

Dotarsi di una piattaforma per **Change Management & Version Control** vuol dire:

- **OGNI SINGOLA VARIAZIONE VIENE TRACCIATA**, dunque è possibile risalire ad ogni singolo dettaglio a riguardo: chi l'ha fatta, quando, perché.
- **IL BACKUP DEGLI APPLICATIVI E' SEMPRE DISPONIBILE**: verificare quale versione sta girando o ripristinarne una precedente sarà semplicissimo.
- La domanda da porsi oggi è: **IN QUANTO TEMPO SONO IN GRADO DI RIPARTIRE DOPO UN INCIDENTE INFORMATICO?** È facile intuire come una "repository" contenente tutte le versioni aggiornate degli applicativi possa ridurre all'osso i Tempi di Ripartenza.

LA PROPOSTA DI SERVITECNO: MDT SOFTWARE

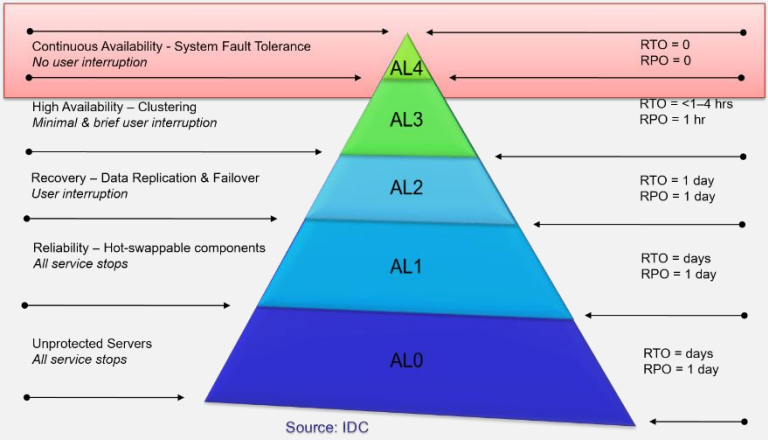
Continuità Operativa (e Business Continuity)

Nel Settore Manifatturiero ***un'ora di fermo impianto*** può costare fino a **30.000 euro** (in alcuni casi anche molto di più): questo per quanto riguarda la mancata produzione: è bene però ricordare che ***un DOWNTIME non pianificato può costare fino a 10 volte*** rispetto ad una fermata programmata (per manutenzione, controllo, test, etc...). Riassumiamo brevemente tutti i costi:

- *Costo del lavoro*
- *Costo del prodotto*
- *Costo di avvio*
- *Costo collo di bottiglia*
- *Aspettative di vendita*
- *Costo per ora*
- *Produzione ridotta*
- *Rottame*
- *Costi di assistenza*
- *OEM, consulenza e assistenza*
- *Tooling, cambio formato*
- *Sostituzioni e riparazioni*

Accrescere la disponibilità dei sistemi fino al raggiungimento dell'Alta Disponibilità (99,99% e oltre) è una questione di metodo: applicare soluzioni di ridondanza con macchine virtuali risulta più semplice e sicuramente più economico che basare la propria DISPONIBILITA' sulla potenza dei server.

QUANTO VALE LA
DISPONIBILITA' DEI SISTEMI?

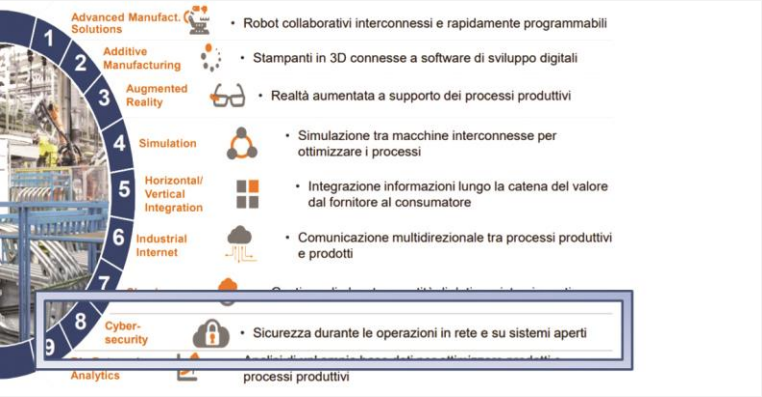


LA PROPOSTA DI SERVITECNO:

Stratus Technologies

Industria4.0, Utility4.0 e Cyber Security

Smart Manufacturing, ***Smart Grid***, ***Smart City*** sono termini e concetti oramai noti a tanti, come lo sono ***IoT ed Industrial IoT*** (Internet of Things).



Anche nel ***piano strategico pubblicato nel 2017 dal Governo Italiano*** (come in molti altri paesi), ***la Cyber Security è uno dei "pilastri"*** (tecnologie abilitanti) che devono essere presenti e presidiati per garantire il successo dei progetti di digitalizzazione in ottica 4.0.

Nel ***Piano Industria4.0*** (come anche nelle Utility4.0), si parla di Industrial Internet, di Cloud, di BigData & Analytics e soprattutto ***integrazione verticale/orizzontale tra i sistemi***, tutti aspetti che hanno come presupposto la ***"connettività" tra impianti***, ***reti***, ***sistemi di gestione*** e ***architetture in Cloud***.

"Collegare in modo sicuro gli oggetti industriali" come PLC, RTU, etc…è da decenni (ben prima che si cominciasse a parlare di Internet of Things, Industria4.0 o Industrial Internet) una sfida che affrontiamo mettendo al servizio dei Clienti (Utilizzatori Finali, ma anche System Integrator, Costruttori di Macchine e Impianti) competenza, metodologie, prodotti innovativi e tecnologie "best-in-class".

Con quanto previsto nei Piani Industria4.0/Utility4.0 si possono ottenere incentivi e benefici fiscali (come gli ammortamenti maggiorati) che permettono di abbreviare i tempi di ritorno sull'investimento.

White papers e documentazione disponibile su www.servitecno.it