WHITE PAPER

Cybersecurity nel settore Food & Beverage

Minimizzazione del rischio secondo CRITIS
siemens.com/industrialsecurity

SIEMENS

La crescente digitalizzazione delle aziende e la conseguente interconnessione di quasi tutti i settori generano un enorme potenziale economico. Oggi oltre 20 miliardi di dispositivi e macchine sono già connessi tramite Internet. Entro il 2030 questo numero crescerà fino a circa mezzo trilione. La digitalizzazione e la connettività possono essere motori per la crescita e la prosperità, ma l'aumento della connettività crea anche nuove vulnerabilità a cui è necessario rispondere in modo rapido e coerente.

Questo vale anche per le aziende del settore food & beverage

Nel 2017 una delle più grandi aziende del settore food & beverage al mondo è stata vittima di un ransomware Trojan. Il malware "Petya" ha attaccato i sistemi informatici di tutto il mondo e ha bloccato i loro utenti per estorcere denaro per il riscatto. Secondo le stime dell'azienda, l'attacco informatico ha comportato una perdita di ricavi pari a circa 140 milioni di dollari. Ci sono voluti giorni prima che i sistemi più importanti fossero operativi e diverse settimane prima che i sistemi rimanenti fossero utilizzabili.

Questo e altri incidenti simili avvenuti negli ultimi anni hanno spinto i legislatori di numerosi paesi ad adottare norme e regolamenti in materia di sicurezza informatica. Tali norme hanno lo scopo di proteggere le infrastrutture critiche in modo da garantire l'affidabilità dell'approvvigionamento per i cittadini dei paesi e la stabilità per i paesi stessi.

In Germania, ad esempio, nel luglio 2015 è entrata in vigore la "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (Legge per migliorare la sicurezza dei sistemi informatici). Questa legge richiede che i gestori di infrastrutture critiche (CRITIS) attuino determinate misure. Tra gli "operatori di infrastrutture critiche" ci sono anche le aziende del settore food & beverage, perché gli attacchi informatici contro questo settore non solo interrompono la produzione e causano danni finanziari, ma possono anche comportare rischi per la salute.

La priorità principale è prevenire gli errori di fabbricazione e la manipolazione della produzione ed evitare una perdita di immagine. Misure di sicurezza adeguate non sono un lusso, sono una necessità.

Indice

I legislatori regolano la sicurezza informatica in tutto il mondo

Da luglio 2015, la legge tedesca sulla sicurezza informatica richiede la segnalazione di incidenti di sicurezza che interessano determinate infrastrutture critiche. Nel corso del tempo, gli operatori CRITIS saranno inoltre tenuti a rispettare gli standard minimi di sicurezza informatica. L'attuazione di queste norme si basa in particolare sugli standard IEC 27001 e IEC 62443. I produttori di componenti di automazione e di rete e i gestori di impianti devono implementare misure di sicurezza informatica all'avanguardia. Il termine giuridico "stato dell'arte" è utilizzato perché l'esperienza ha dimostrato che lo sviluppo tecnologico progredisce più rapidamente della legislazione. Lo stato dell'arte in un dato momento può essere determinato sulla base di standard nazionali o internazionali esistenti come DIN e IEC o sulla base delle best practice per il settore specifico.

Stato dell'arte secondo IEC 62443

I documenti IEC 62443 sono organizzati come segue:

- IEC 62443-1 include terminologia, concept, casi d'uso e modelli.
- La norma IEC 62443-2 si rivolge agli operatori di impianti e descrive attività come l'implementazione di un sistema di gestione della sicurezza e la gestione delle patch.
- IEC 62443-3 descrive le tecnologie di sicurezza per i controller e i componenti di rete.
- La norma IEC 62443-4 si rivolge ai produttori e formula procedure per la protezione del processo di sviluppo e di altre attività.

Questa divisione delle informazioni mostra che la sicurezza informatica è vista come un processo completo e che gli standard di sicurezza devono essere rispettati durante lo sviluppo dei componenti.

Il Food Safety Modernization Act (FSMA) della FDA negli Stati Uniti include standard simili che comprendono, tra le altre cose, una combinazione di monitoraggio, opzioni di intervento e verifica delle misure di sicurezza informatica. In Gran Bretagna, la PAS 96:2017 regola le misure di sicurezza e prevenzione contro gli attacchi all'industria del food & beverage.

Fondamentalmente, ciò che tutte le leggi e gli standard hanno in comune è che sono composti da una combinazione di standard tecnici, obblighi di segnalazione degli incidenti e monitoraggio della conformità agli standard.

Figura 1: documenti della norma IEC 62443

Cybersecurity: un processo in continua evoluzione

Una protezione efficace dagli attacchi informatici non si ottiene con un'implementazione una tantum delle misure di sicurezza: è un processo continuo.

A seguito di un'analisi dei rischi (valutazione) di un processo automatizzato, è necessario implementare misure per ridurre al minimo i rischi (implementazione). Queste misure devono essere monitorate e si deve verificare continuamente se le misure devono essere riviste a causa di un cambiamento dello scenario di minaccia (gestione). Le misure necessarie sono tanto varie quanto i rischi valutati. In base al livello di automazione, alla tecnologia utilizzata e alla connettività OT (tecnologie operative) e IT (tecnologie informatiche), gli esperti di sicurezza sviluppano meccanismi di sicurezza appropriati su misura per ogni azienda e i suoi processi.

Il gestore dell'impianto è sempre responsabile della sicurezza informatica. Anche se la gestione dell'impianto non è supportata in tutto o in parte dal personale dell'azienda a causa dell'outsourcing, il gestore dell'impianto è comunque responsabile. Anche le minacce dovute all'esternalizzazione devono essere valutate. In generale, si consiglia al personale di seguire corsi di formazione che aumentino la consapevolezza degli attacchi informatici e che consentano loro di rispondere in modo rapido e mirato in caso di emergenza.

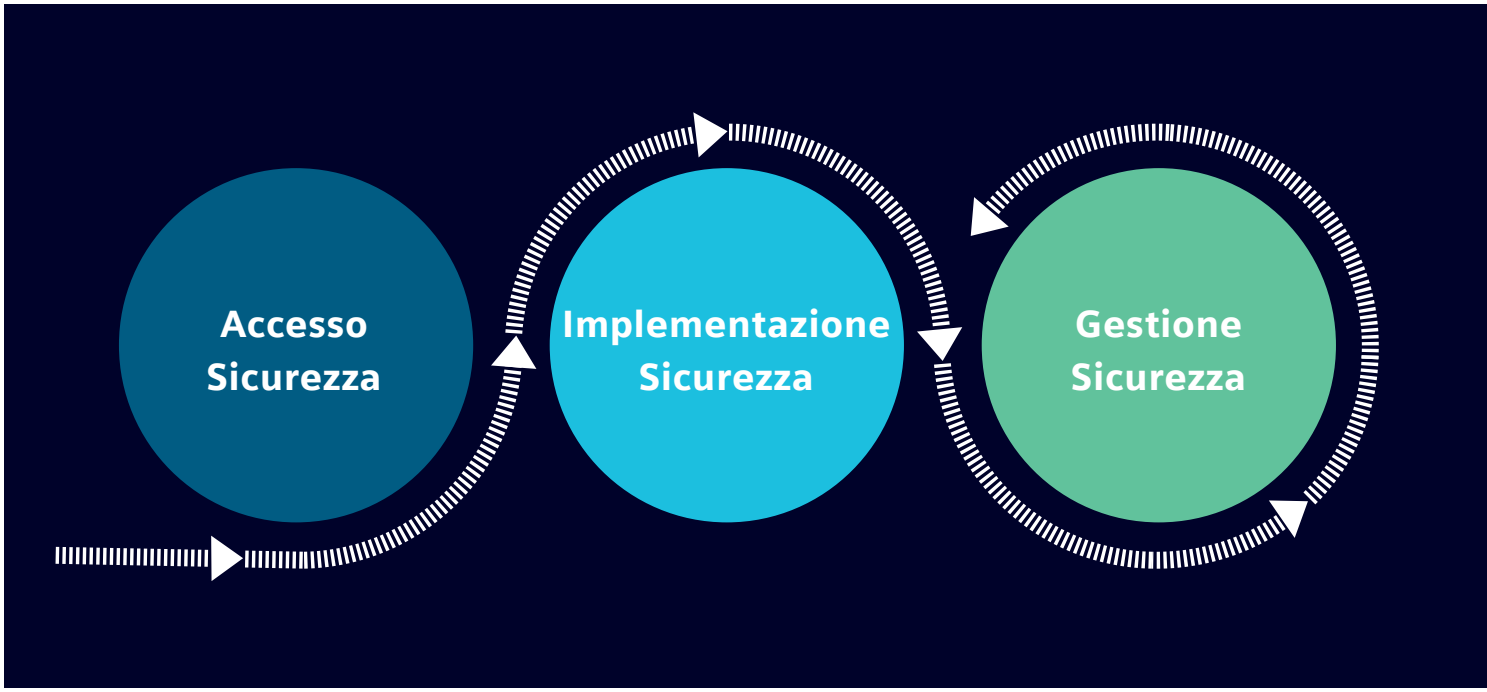

Figura 2: le tre fasi della sicurezza IT/OT o sicurezza industriale

Minacce – Obiettivi di attacco e tipi di aggressori

Quali sono gli obiettivi degli aggressori che cercano di superare le misure di sicurezza? Gli aggressori generalmente si dividono in quattro categorie.

Gli aggressori non addestrati ("script kiddies") utilizzano script finiti da Internet come mezzo semplice per attaccare vulnerabilità note "solo perché possono".

Gli aggressori addestrati ("hacker") lanciano attacchi più complessi a scopo di lucro e per estorcere denaro per il riscatto di dati crittografati.

Lo spionaggio industriale è solitamente praticato da addetti ai lavori che utilizzano le loro conoscenze specialistiche per rubare dati o danneggiare le aziende. In questo caso, gli (ex) dipendenti si rivolgono a un'azienda specifica.

Tecnicamente, **gli attacchi guidati dallo stato** sono i più pericolosi. Questi attacchi generalmente sfruttano vulnerabilità precedentemente sconosciute con vari obiettivi in mente: accesso a dati sensibili, manipolazione dei dati, interruzione dei processi di produzione o persino la distruzione di intere sezioni dell'impianto. Oltre al guadagno finanziario, la motivazione può anche essere quella di destabilizzare un paese, ad esempio attaccando l'approvvigionamento alimentare.

Minacce

L'Ufficio federale tedesco per la tecnologia dell'informazione (Bundesamt für Sicherheit in der Informationstechnik = BSI) ha identificato i dieci tipi di attacco più frequenti agli impianti industriali (Stato: BSI-CS 029 | Versione 2.0 dell'11 luglio 2018):

1. L'uso non autorizzato dell'accesso remoto alla manutenzione che consente l'accesso esterno ai sistemi di controllo industriale (ICS), spesso non sufficientemente protetti.
2. Attacchi online tramite l'IT dell'ufficio, che è generalmente connesso a Internet e può anche stabilire una connessione alla rete IC.
3. Attacchi a componenti standard come sistemi operativi, server di applicazioni o database che di solito contengono errori e vulnerabilità che gli aggressori possono sfruttare. Questi componenti possono anche essere implementati nei sistemi ICS, il che aumenta il rischio.
4. (D) Gli attacchi DoS alle connessioni di rete possono sovraccaricare i sistemi e interrompere la funzionalità della rete ICS o dell'ICS stesso.
5. L'errore umano e il sabotaggio da parte di responsabili interni o esterni sono una minaccia enorme. Anche la negligenza e l'errore umano minacciano la riservatezza e la disponibilità.
6. Il malware viene spesso introdotto tramite dispositivi di archiviazione rimovibili o componenti IT mobili di dipendenti esterni (ad esempio Stuxnet).
7. I comandi di controllo possono essere facilmente letti e importati perché la maggior parte dei componenti di controllo comunica tramite protocolli in chiaro, il che significa che la loro comunicazione non è protetta.
8. L'accesso non autorizzato ai componenti di rete è possibile se gli addetti ai lavori, o gli estranei che hanno violato le misure di sicurezza, accedono ai componenti utilizzando metodi di autenticazione e autorizzazione non sicuri.
9. Gli aggressori possono manipolare i componenti della rete per condurre attacchi man-in-the-middle o facilitare lo sniffing.
10. Il potenziale di guasti derivanti da influenze ambientali estreme o difetti tecnici non può mai essere completamente eliminato, ma il rischio e i danni conseguenti possono essere ridotti al minimo utilizzando componenti e misure di sicurezza appropriati.

Cybersecurity – Procedura dettagliata

L'elenco delle minacce mostra che possono essere utilizzati metodi molto diversi per lanciare attacchi e il processo deve essere protetto da questa vasta gamma di minacce. Lo standard industriale tedesco e la norma IEC 62443 definiscono un processo a più fasi per l'implementazione della cybersecurity.

1. La selezione degli oggetti serve a registrare e documentare tutti i sistemi dell'impianto, compresi i sottosistemi e il piano di rete.
2. Le minacce derivano da una serie di casi d'uso: ad esempio, il fatto che un sistema può essere attaccato tramite un accesso di manutenzione remoto.
3. La valutazione delle minacce identifica le minacce per ogni caso d'uso: ad esempio, l'accesso remoto alla manutenzione può essere utilizzato da una persona non autorizzata.
4. L'analisi dei rischi comporta l'identificazione di potenziali minacce sulla base di una matrice di rischio.

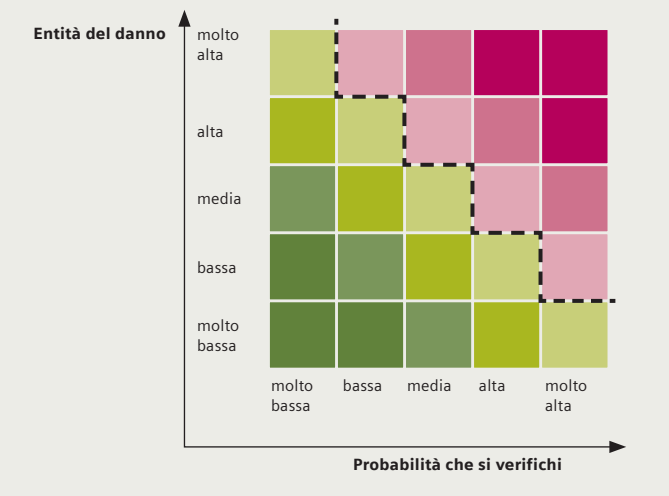

Figura 3: Matrice di rischio basata sullo standard BSI 200-3

Una minaccia con un'alta probabilità di verificarsi e un elevato danno potenziale appare nell'area rossa nell'angolo in alto a destra della matrice (rischio alto). Una bassa entità del danno e la probabilità di accadimento significano un basso rischio e appare nell'area verde nell'angolo in basso a sinistra. Lo standard BSI 200-3 fornisce una ripartizione esatta dell'entità del danno (grado in cui il funzionamento dell'impianto è limitato), della probabilità che si verifichi e del rischio.

5. Un processo per determinare le misure necessarie definisce opzioni concrete che vengono descritte in dettaglio nella sezione successiva.
6. L'implementazione delle misure include la programmazione e la pianificazione organizzativa dell'implementazione. Inoltre, comprende la definizione delle responsabilità e la chiara allocazione del budget per l'implementazione delle misure.
7. Per l'audit è necessario verificare le misure, completare la documentazione dell'impianto e compilare liste di controllo. L'efficacia delle misure deve essere verificata a intervalli regolari. Se vengono rilevati errori, ad esempio da rischi modificati o nuovi tipi di malware, l'intero processo deve essere riavviato, a partire dalla valutazione delle minacce.

Concetto di sicurezza

Poiché le minacce sono di natura diversa, possono avere origine interna o esterna e gli aggressori hanno livelli di competenza diversi, è importante creare un concetto di sicurezza multilivello per fornire un processo che offra la migliore protezione possibile. Ad esempio, anche se il firewall è stato violato perché l'aggressore è entrato fisicamente nell'impianto, è necessario proteggere i dispositivi terminali con meccanismi di sicurezza aggiuntivi.

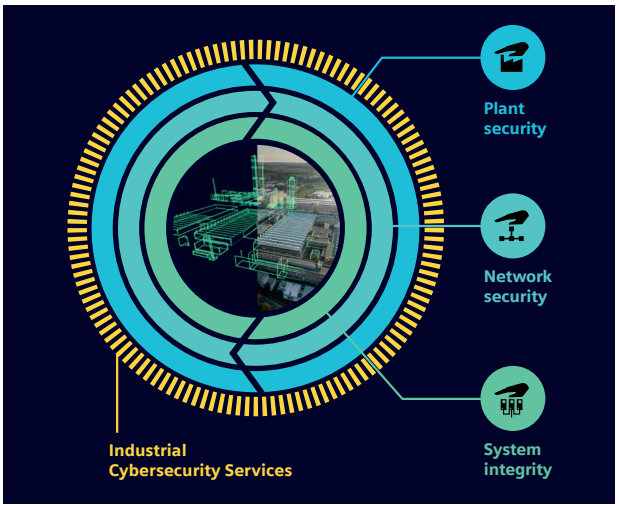

Figura 4: concetto di sicurezza "Defense in Depth"

La figura mostra un concetto di sicurezza multistrato che definisce la sicurezza dell'impianto, la sicurezza della rete e l'integrità del sistema come i tre livelli essenziali di una sicurezza efficace.

Misure di sicurezza dell'impianto

Le misure organizzative comprendono tutte le misure di protezione fisica dell'impianto. Oltre alla protezione dalle effrazioni, devono essere previste anche procedure per proteggere l'impianto dalle influenze ambientali.

Minacce
- Effrazioni/atti vandalici
- Accessi non autorizzati
- Inondazioni
- Incendi
- Fumo/polvere/gas corrosivi
- Fulmini/sovratensioni/EMC

Misure organizzative
A seconda delle minacce specifiche, è necessario adottare misure adeguate a proteggere l'impianto. Particolare attenzione è richiesta per le stazioni esterne (ad esempio, i magazzini) che di solito non sono occupate e sono monitorate a distanza dal centro di controllo. Le stazioni esterne devono essere protette contro le effrazioni e le porte e le finestre devono essere adeguatamente protette.

I contatti porta/finestra possono notificare al controllore l'apertura di porte o finestre e il controllore può informare il centro di controllo. Una telecamera IP può aiutare a rilevare gli aggressori e a monitorare l'edificio dal centro di controllo.

Le diverse aree produttive devono inoltre essere fisicamente separate mediante un controllo differenziato degli accessi. Ad esempio, i componenti critici devono essere protetti in un quadro elettrico chiuso a chiave (vedere anche pagina 14).

Le linee guida per le misure di protezione dell'accesso fisico determinano anche le misure di cybersecurity necessarie e la loro forza. Ad esempio, nelle aree a cui accedono solo persone autorizzate, le interfacce di accesso alla rete e i sistemi di automazione non devono essere protetti in modo così sicuro come nelle aree accessibili al pubblico.

Con la certificazione secondo la norma IEC 27001, le aziende possono ridurre i rischi per la sicurezza delle informazioni, rispettare meglio le normative e i requisiti di sicurezza pertinenti e promuovere una cultura interna della sicurezza.

Misure di sicurezza della rete

La rete deve essere strutturata per resistere il più possibile a potenziali attacchi, tenendo conto anche delle opzioni di accesso, della disponibilità e della protezione.

Opzioni di accesso
Di norma, le reti sono sistemi aperti con una connessione a Internet. Per la maggior parte degli operatori dell'impianto, l'accesso esterno ai fini della manutenzione, della diagnostica, dell'ottimizzazione, delle patch, degli aggiornamenti e di altre attività è diventato essenziale.

Disponibilità
Il processo automatizzato, che viene controllato, ad esempio, tramite la rete mediante la comunicazione PROFINET, deve essere eseguito indipendentemente dalle singole interruzioni di linea. I sistemi di monitoraggio nel centro di controllo devono essere in grado di continuare a monitorare il processo anche in caso di guasto dei singoli router.

Protezione
Il processo deve essere protetto da tutti i potenziali rischi che potrebbero minacciare la rete, inclusi accessi non autorizzati, malware e attacchi (D)DoS. Tutti i tipi di comunicazione diversi dagli accessi autorizzati e consentiti devono essere bloccati con misure appropriate.

La norma IEC 62443 richiede i seguenti elementi per la protezione della rete:
- Segmentazione dell'architettura di rete
- Isolamento o segmentazione dei componenti ad alto rischio
- Blocco delle comunicazioni non necessarie
- Accesso tramite firewall

Segmentazione della rete

La segmentazione della rete tramite firewall protegge dagli attacchi provenienti dalla rete. La rete è suddivisa in gruppi funzionali, ad esempio reti di produzione, rete di impianti e rete di uffici, e l'accesso è controllato con precisione da firewall.

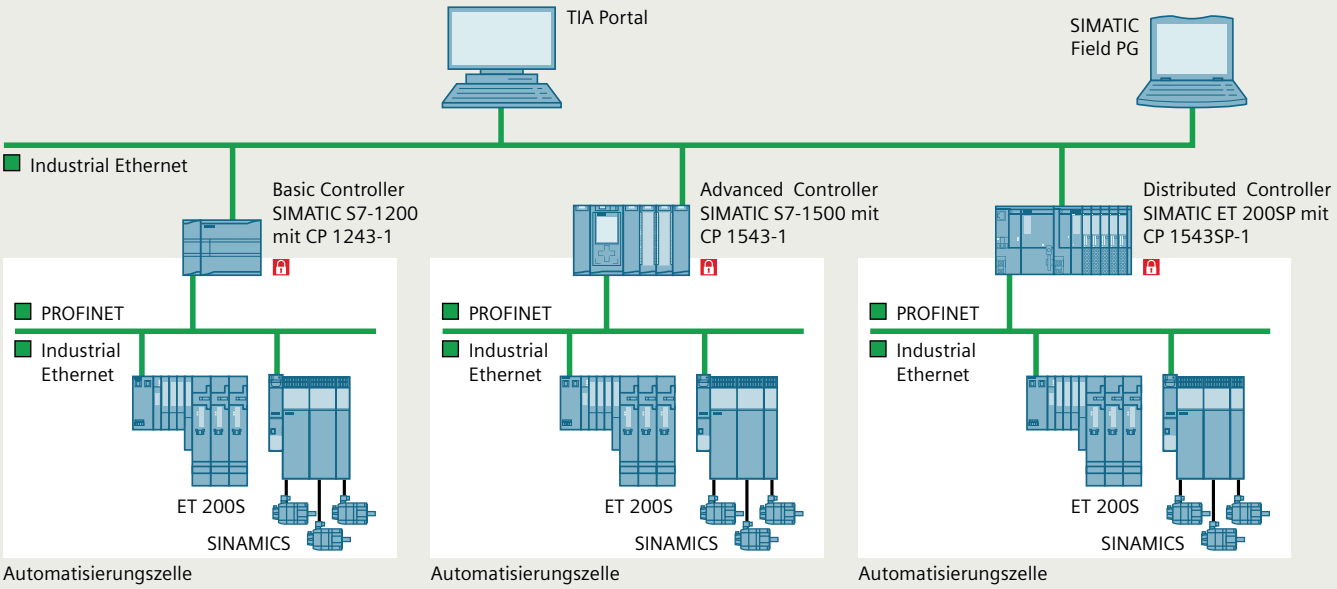

Figura 5: segmentazione della rete secondo la norma IEC 62443-2-1

Zona demilitarizzata (DMZ)
La Figura 5 mostra una configurazione di rete raccomandata dalla norma IEC 62443-2. Le celle di automazione nella parte inferiore sono combinate come unità funzionali e sono separate dalla rete dell'intero impianto da un firewall. La rete dell'impianto nella parte in alto contiene tutti i dispositivi di livello superiore importanti per il funzionamento dell'impianto, come il centro di controllo e i server. L'interfaccia tra la rete dell'impianto e quella dell'ufficio è nuovamente separata da un firewall. Qui è possibile impostare una o più zone demilitarizzate (DMZ). In una DMZ, i dispositivi delle reti di livello superiore e inferiore non comunicano direttamente tra loro. Comunicano invece tramite un server che, ad esempio, recupera lo stato dell'impianto dalle celle di automazione e rende disponibili queste informazioni alla rete di livello superiore. La rete dell'ufficio è inoltre protetta da Internet da uno o più firewall.

In questo esempio, la configurazione crea tre pareti di protezione per le celle di automazione che controllano il processo. La rete dell'ufficio, potenzialmente interessata dall'introduzione più frequente di malware (ad esempio tramite chiavette USB), è separata dalla cella di automazione da due firewall. Più un dipendente lavora vicino alla cella di automazione, più è importante che sia costantemente informato sui problemi di cybersecurity.

Accesso remoto e stazioni esterne distribuite

Il collegamento di stazioni distribuite esterne rappresenta una sfida particolare. Se da un lato queste stazioni devono essere in grado di funzionare autonomamente, dall'altro devono poter essere monitorate dal centro di controllo. La rete di una postazione deve essere protetta e l'accesso alla postazione deve essere sicuro, anche se è collegata tramite una rete separata o una connessione aziendale. L'outstation può essere collegata via cavo (come ADSL o SHDSL) o via radio (ad esempio, LTE, UMTS). Il modem deve contenere un firewall ed essere compatibile con VPN.

Per aumentare la sicurezza, la connessione VPN può essere configurata per l'accesso remoto secondo la norma IEC 62443 affinché il tunnel venga stabilito solo quando un tecnico in loco attiva la VPN sul modulo.

Connessioni wireless tramite WLAN
Occorre prestare particolare attenzione alla trasmissione wireless tramite WLAN o altre tecnologie. Nel caso della comunicazione cablata, un aggressore deve avere accesso fisico ai cavi o ai componenti della rete per poter leggere i dati o manomettere il traffico di dati. Con la comunicazione wireless, le onde radio si diffondono su un'area più ampia, rendendo più facile un attacco.

Se nella cella di automazione è necessaria una WLAN, per l'automazione è necessario configurare una WLAN separata. La WLAN dell'ufficio deve essere gestita attraverso diversi punti di accesso WLAN per mantenere la segmentazione della rete.

Misure organizzative per una WLAN
Il punto di accesso deve essere installato in modo che sia inaccessibile o protetto in un armadio di controllo chiuso e le antenne WLAN devono essere installate a distanza. Ciò impedirà agli aggressori di accedere fisicamente al punto di accesso. Anche la frequenza WLAN deve essere selezionata con attenzione, perché altre applicazioni che utilizzano la stessa frequenza possono interferire con la trasmissione in modo simile ai jammer, o addirittura interromperla completamente.

Meccanismi tecnici di sicurezza per una WLAN
La crittografia WPA2 è l'attuale stato dell'arte. I metodi di crittografia meno recenti (WEP e WPA) non devono più essere utilizzati perché non sono sicuri e sono facili da decifrare. La password e l'SSID predefiniti devono essere modificati e l'SSID nascosto.

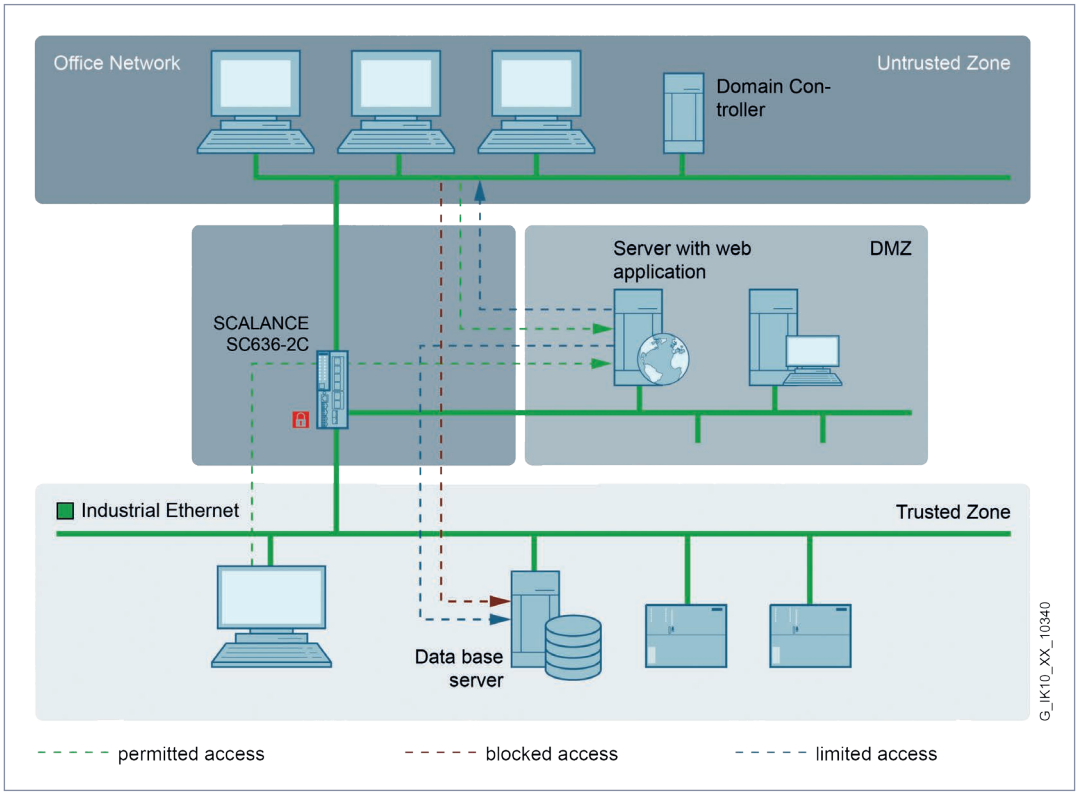

Figura 6: collegamento di un PC di servizio locale tramite una porta DMZ su SCALANCE S615

Requisiti generali per elementi di rete

Lo standard internazionale per la configurazione e la gestione sicura dei componenti di rete secondo lo standard IEC 62443 raccomanda le seguenti caratteristiche e meccanismi di sicurezza per la configurazione e la protezione dei dispositivi.

Protezione degli accessi e gestione degli account
Per proteggere i componenti di rete da accessi non autorizzati, deve essere possibile gestire e, se necessario, bloccare gli account per i quali è stato abilitato l'accesso.
È necessario supportare le seguenti funzionalità:

- Configurare le opzioni di accesso
- Identificare gli utenti/renderli identificabili tramite account
- Impostare/modificare/chiudere gli account tramite un gestore centrale
- Documentare gli account e gli utenti degli account
- Eliminare o bloccare gli account inutilizzati
- Verificare regolarmente i diritti di accesso
- Modificare le password predefinite

I requisiti di protezione dell'accesso possono essere implementati per mezzo di componenti di gestione degli utenti (UMC). Con gli UMC, vengono creati diversi account utente su un server centrale noto come UMC ring server. I progetti TIA Portal possono utilizzare questi utenti e a questi utenti possono essere concessi i diritti di accesso ai componenti e ai partecipanti della rete.

Controllo degli accessi: autenticazione
Quando si accede a un componente, deve essere possibile identificare l'utente che vi accede. L'autenticazione deve fornire i seguenti meccanismi:

- Accesso possibile solo se l'utente è stato autenticato (o se c'è un controllo di accesso sufficiente)
- Solidi meccanismi di sicurezza per l'accesso amministrativo
- Registrazione di tutti gli accessi ai sistemi critici
- Identificazione di tutti gli utenti di accesso remoto
- Linee guida per l'accesso remoto, logout automatico dopo un periodo di inattività
- Accesso remoto bloccato dopo ripetuti accessi non riusciti
- Riautenticazione durante l'accesso remoto dopo un periodo di inattività
- È necessario impostare un meccanismo di autenticazione anche per la comunicazione tra attività

Questi requisiti si riferiscono a sistemi diversi e devono quindi essere presi in considerazione per l'intero impianto. Per l'accesso remoto, ad esempio, i requisiti possono essere soddisfatti da SINEMA Remote Connect perché, tra l'altro, il logout automatico dopo l'inattività e il blocco di un IP dopo diversi tentativi di accesso falliti sono già implementati e gli accessi remoti vengono sempre registrati. Nel TIA Portal è possibile concedere agli utenti l'accesso al progetto e separatamente alla configurazione di sicurezza. Poiché la configurazione della protezione richiede diritti di accesso propri, viene soddisfatto anche il requisito di una protezione aggiuntiva per l'accesso amministrativo.

Controllo accessi: Autorizzazione

Per autorizzazione si intende la concessione di diritti specifici agli utenti precedentemente autenticati: ad esempio, l'accesso a un componente. La norma IEC 62443 cita i seguenti punti in merito all'autorizzazione:

- Metodo logico o fisico per l'autorizzazione all'accesso
- Accesso al sistema o alle informazioni basato sui ruoli
- Il diritto di accesso ai dispositivi di sicurezza deve essere un diritto distinto
- È necessario configurare più livelli di accesso per i sistemi critici

Gestione della rete

SNMP, ora supportato da tutte le interfacce di rete, può essere utilizzato per la gestione della rete. Insieme al server SINEMA, è possibile utilizzare SNMP per monitorare la rete e le sezioni dell'impianto collegate tramite una VPN. In questo modo è possibile gestire tutte le sezioni della rete e rilevare più rapidamente i guasti.

Piano di rete

Per documentare l'impianto e mostrare le interconnessioni tra i partecipanti è necessario un piano di rete fisico, una vista topologica. Questo piano di rete doveva indicare gli indirizzi (IP e MAC), le connessioni delle porte e le posizioni di installazione. Si può stampare dal TIA Portal o utilizzare lo strumento di pianificazione della rete SINETPLAN.

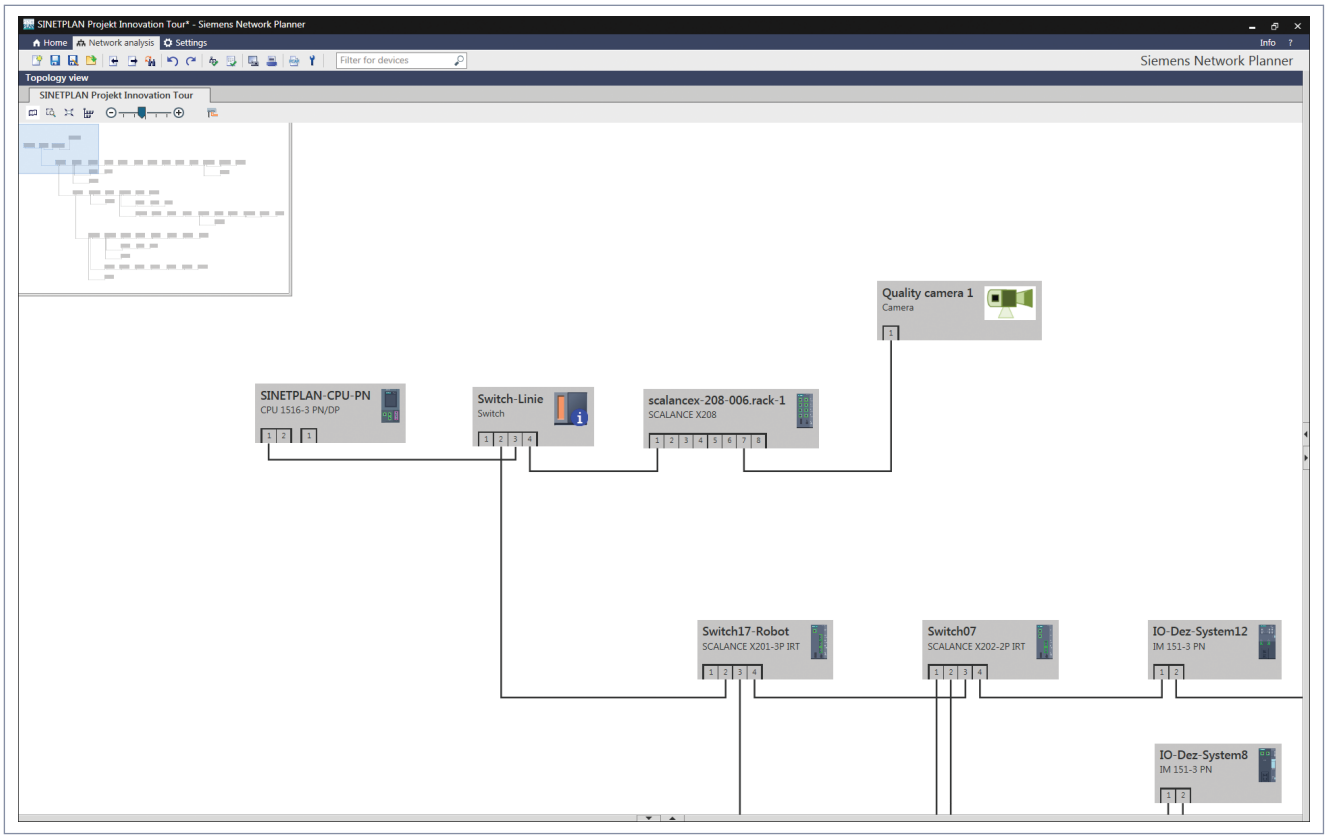

Figura 7: rete topologica in SINETPLAN

Misure di integrità del sistema

Integrità del sistema significa garantire l'autenticità e la genuinità dei dati e dei programmi all'interno di un sistema. Non è consentito modificare il programma o manomettere i dati (sia nel canale di comunicazione sia nel sistema) o copiare il programma o i dati senza autorizzazione. Anche le competenze in materia di controllo dei processi devono essere protette.

Accesso al programma
Anche la programmazione dei controllori (PLC) fa parte della sicurezza informatica, motivo per cui l'accesso al progetto e agli uffici deve essere protetto. In genere il progetto può essere protetto utilizzando il registro di Windows. A partire dal TIA Portal V15, è possibile criptare l'intero progetto. Ciò significa che il progetto può essere aperto solo con un nome utente e una password aggiuntivi, il che garantisce la sicurezza quando più persone lavorano contemporaneamente allo stesso progetto.

Protezione dell'accesso alla CPU
È possibile impostare password diverse in base ai diversi livelli di accesso alla CPU, in modo che solo il personale qualificato abbia accesso completo.

Server Web
Sempre più soluzioni di controllo utilizzano l'accesso tramite server Web, spesso utilizzati anche per l'accesso remoto. In questo caso, anche i server Web devono essere completamente protetti. HTTPS è la versione sicura di HTTP ed è la scelta preferita. L'autenticazione e l'autorizzazione richieste dallo standard di settore possono essere ottenute configurando diversi utenti e livelli di accesso.

Comunicazione sicura
Se il controllore comunica al di fuori della sua cella di sicurezza, questa comunicazione deve essere criptata. L'attuale stato dell'arte è la crittografia TLS, che può essere utilizzata nell'S7-1500 tramite OPC UA o una connessione TCP.

Un'altra opzione per la crittografia consiste nell'utilizzare firewall integrati per impostare una connessione VPN. Il tunnel VPN viene stabilito tra i firewall e la comunicazione tra le celle di automazione viene trasmessa tramite la rete di livello superiore in forma crittografata e decrittografata dalla rete di destinazione.

Misure di sicurezza sui PC industriali
I PC utilizzati nell'ambiente industriale (IPC) richiedono misure speciali perché sono direttamente esposti a diverse minacce, inclusi i dispositivi di archiviazione infetti, mentre le chiavette USB non possono essere collegate direttamente a un controller. Le seguenti misure servono a proteggere un IPC dagli attacchi di cybersecurity.

Account utente
Si consiglia di configurare gli account amministratore e utente. Solo l'amministratore è autorizzato a modificare le impostazioni di sicurezza o a (dis)installare software. L'utente standard non è in grado di eseguire queste funzioni, il che impedisce l'installazione di malware durante le normali operazioni.

Configurazione delle linee guida
Con l'aiuto di Microsoft Management Console, è possibile stabilire linee guida per l'uso dei dispositivi di archiviazione, il controllo del sistema e altro. Un documento che descrive queste linee guida e le modalità di definizione è disponibile online all'indirizzo:
support.industry.siemens.com/cs/ww/en/view/109475014

Filtro di scrittura avanzato (EWF)
Questa funzione è disponibile sui SIMATIC IPC: Protegge una parte del file system dalla modifica dei dati reindirizzando l'accesso in scrittura alla RAM. Quando l'IPC viene riavviato, il file system viene riportato allo stato originale. Il malware introdotto non è più presente dopo un riavvio.

Firewall
I firewall standard (firewall Windows) forniscono già un'importante protezione di base. Devono assolutamente rimanere attivati. Utilizzando regole appropriate, i firewall devono essere configurati in modo tale che solo i dati degli utenti possano essere comunicati e che tutte le altre comunicazioni siano bloccate.

Protezione dai virus
Il software antivirus è in grado di rilevare virus e malware. In Siemens, utilizziamo un'installazione McAfee per la nostra automazione. Un server di gestione gestisce i client antivirus sui sistemi PC e fornisce le firme antivirus più recenti. Il server di gestione può anche notificare gli allarmi al personale di servizio tramite e-mail.

Prodotti certificati IEC 62443
I controller, i PC e gli altri sistemi selezionati per l'uso devono contenere meccanismi di sicurezza e devono essere stati testati per individuare eventuali vulnerabilità. Questi test sono standardizzati: ad esempio, un certificato Achilles indica che il sistema è stato sottoposto a test di carico e vulnerabilità. I produttori possono anche eseguire uno sviluppo sicuro del prodotto per garantire un elevato livello di qualità per i loro prodotti. Il processo di sviluppo di Siemens è stato testato e ha superato il test IEC 62443-4:
siemens.com/press/PR2016080373DFEN

Misure relative al personale

Le migliori misure di sicurezza tecniche e organizzative sono inutili se i dipendenti di un'azienda sono negligenti. Ecco perché i corsi di formazione e la chiara definizione delle aree di responsabilità sono parte integrante della cybersecurity. La norma IEC 62443 raccomanda che il nuovo personale venga sottoposto a screening per determinarne l'affidabilità e valutare se è in grado di adempiere alle proprie responsabilità. È inoltre necessario determinare l'affidabilità del personale esistente. Anche il personale esterno può partecipare ai corsi di formazione, ma deve sempre essere accompagnato e supervisionato da personale qualificato dell'azienda.

Responsabilità
Lo standard di settore prevede che gli operatori di infrastrutture critiche (CRITIS) designino l'organizzazione UP KRITIS come contatto per la cybersecurity. In genere si consiglia di affidare la sicurezza informatica a un individuo o a un gruppo all'interno dell'azienda.

Formazione
Devono essere offerti corsi di formazione periodici che coprano la corretta gestione dei sistemi installati, dei dispositivi di archiviazione rimovibili e del software. Deve essere previsto anche un corso di formazione sulla risposta agli incidenti e a tutte le altre potenziali minacce. Lo standard di settore richiede esplicitamente che gli amministratori siano formati sulla corretta gestione dei componenti di rete per garantire che le configurazioni vengano eseguite correttamente.

Piano di emergenza e recupero

Lo standard del settore richiede un concept per la gestione di un'emergenza quando è emersa una minaccia e il processo è stato interrotto. Questo concetto è noto anche come gestione della continuità operativa. È necessario rispondere alle seguenti domande:

- Qual è il tempo di inattività massimo accettabile?
- Come può il processo continuare a funzionare indipendentemente dal sistema di controllo/ dall'ufficio?
- In che misura le altre sezioni dell'impianto possono compensare l'alimentazione?
- Come verrà revisionato il sistema interessato?
  - Attraverso gli esuberi
  - Tramite un backup
- Come si eviterà il ripetersi di questo errore?
  - Reporting
  - Ottimizzazione

Siemens ProductCERT
Siemens dispone di un team di esperti di sicurezza che funge da punto di contatto per i clienti e i loro esperti di sicurezza quando rilevano una vulnerabilità di sicurezza. Questo team, noto come Product Computer Emergency Response Team (ProductCERT), valuta e analizza immediatamente le vulnerabilità di sicurezza segnalate.

Avvisi di sicurezza Siemens
Siemens ProductCERT esamina tutti i problemi di sicurezza segnalati e pubblica avvisi sulle vulnerabilità di sicurezza validate che coinvolgono direttamente i prodotti Siemens e che richiedono un aggiornamento del software, un upgrade del software o un'altra azione da parte dell'operatore dell'impianto. Sfrutta questa fonte di informazioni per valutare gli effetti di una vulnerabilità della sicurezza. Siemens affronta apertamente le proprie vulnerabilità in modo che tu possa reagire prima che queste vulnerabilità ti colpiscano. Rimani aggiornato iscrivendoti ai nostri feed RSS: siemens.com/global/de/home/produkte/services/cert.html#Benachrichtigungen

Quadro generale

Una sicurezza industriale completa richiede che vengano presi in considerazione tutti i livelli di protezione. Le misure di sicurezza devono essere tanto diverse quanto i rischi potenziali. Un approccio end-to-end e più linee di difesa possono proteggere in modo affidabile gli impianti industriali. Per semplificare questo complicato problema per l'industria, Siemens offre un portafoglio di soluzioni personalizzate specificamente mirate alla sicurezza degli impianti industriali e delle tecnologie operative.

La figura seguente rappresenta un'architettura di rete tipica per un impianto di bevande analcoliche. Mostra i livelli in cui sono state implementate le misure di sicurezza descritte in questo documento secondo le raccomandazioni dello standard IEC-62443.

Perché scegliere Siemens?
Siemens offre una base affidabile per soluzioni di automazione sicure e innovative.

In Siemens:

- Conosciamo la digitalizzazione,
- Conosciamo il settore Food & Beverage,
- Ci intendiamo di comunicazione industriale,
- Comprendiamo la sicurezza industriale,
- Offriamo processi e prodotti di sicurezza comprovati e certificati.

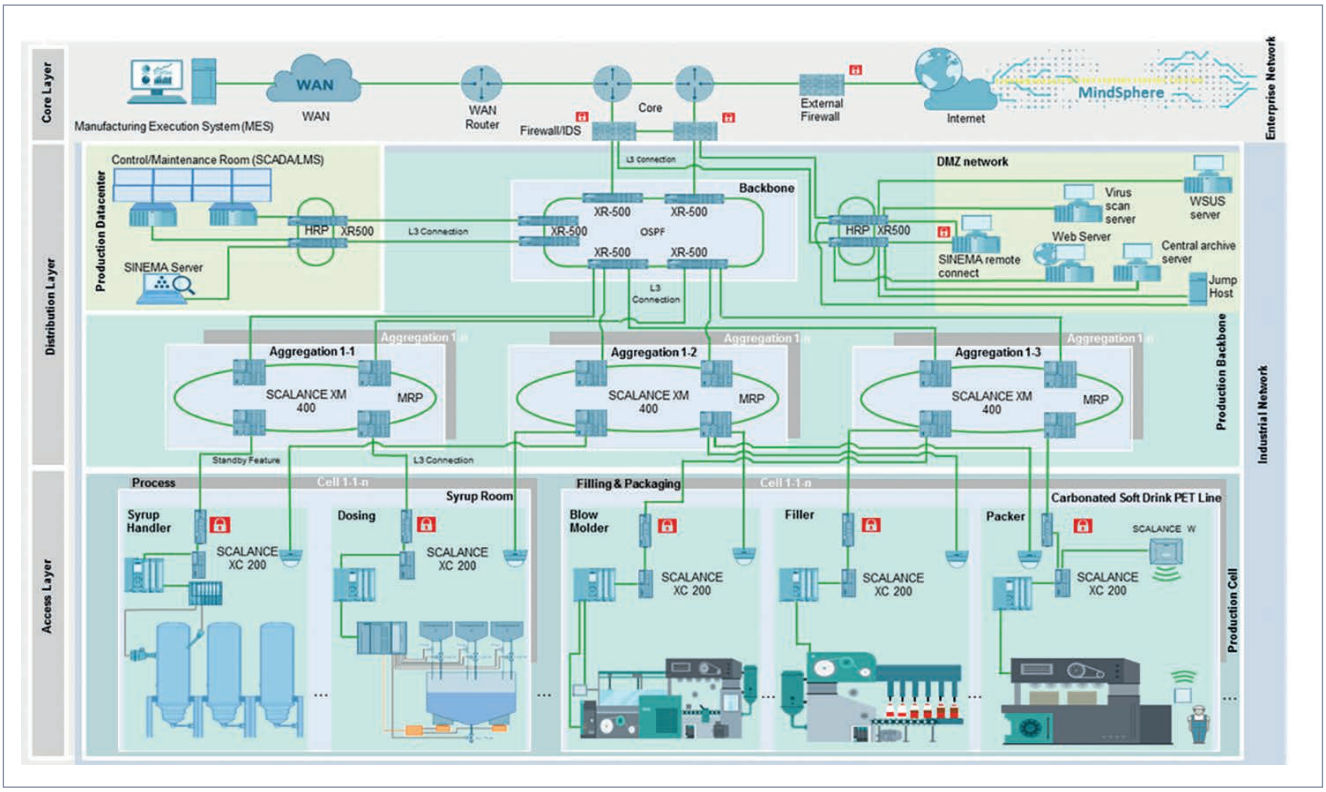

Figura 8: architettura di rete di un impianto di bevande analcoliche

Termini e abbreviazioni

Autenticazione
Il rilevamento e l'identificazione di un utente o (nel caso di impianti collegati in rete) di un altro sistema.

Autorizzazione
Il diritto di accedere a un sistema o a una sezione (software) di un sistema o di un programma.

Cybersecurity
Tutte le misure tecniche per la protezione di un impianto, compresa la protezione della rete, la parte hardware del sistema e il monitoraggio degli incidenti.

Processo
Il processo di produzione vero e proprio, ad esempio la produzione di formaggio o l'imbottigliamento, indipendentemente dal fatto che si tratti di un processo discreto o continuo.

Rete privata virtuale (VPN)
Una VPN fornisce una connessione crittografata tra gli utenti VPN. Viene anche definito gruppo VPN. Una VPN assomiglia a un tunnel in cui il traffico dati può essere inviato da entrambe le direzioni. Nel tunnel, il traffico dati viene trasmesso in forma crittografata e al termine del tunnel, ovvero sull'altro dispositivo VPN, viene consegnato in forma decrittografata. I dispositivi terminali non devono supportare la crittografia poiché questa viene eseguita dai dispositivi VPN.

Pubblicato da
Siemens AG

Digital Industries
Factory Automation
Vertical Sales Food & Beverage
Lindenplatz 2
20099 Amburgo
Germania

Per ulteriori informazioni, contatta
E-mail: fb.communications@siemens.com

Articolo n. DIFA-B10284-00-7600

Per gli Stati Uniti pubblicato da
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
Stati Uniti