CYBERSECURITY FOR DISTRIBUTED ENERGY RESOURCES

Securing Industrial IoT (IIoT) – Asset Management (Electric Utilities, Oil & Gas Industry) – Identity and Access Management for Electric Utilities)

Autore: Aldo Pedico – Enterprise Security & Privacy

Contatto: pedicoaldo@gmail.com

Riporto parte dei risultati del progetto che NCCoE, *attualmente, sta ancora svolgendo sull'argomento. Ed io ho voluto realizzare questo documento per cercare di includere razionalmente gli aspetti riguardanti il Controllo:*

1. *delle risorse (*Securing the Industrial IoT: Cybersecurity for Distributed Energy Resources [**DER**]*);*
2. *degli accessi (*Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry*);*
3. *della identità digitale e dell'autenticazione* (Identity and Access Management for Electric Utilities);

nell'ambito dei sistemi industriali per la produzione di energia.

Inoltre, in questo documento ho voluto:

1. *evidenziare come gli scambi di informazioni tra* DER *su scala commerciale e di utilità e le operazioni della rete di distribuzione elettrica possono essere monitorati e protetti da alcune minacce e vulnerabilità alla sicurezza informatica;*
2. *fornire indicazioni su come migliorare le pratiche di gestione delle risorse OT sfruttando le capacità che potrebbero già esistere nell'ambiente operativo di un'organizzazione energetica e implementando nuove funzionalità;*
3. *fornire indicazioni sull'autenticazione degli individui che accedono alle risorse (*IDENTITY AND ACCESS MANAGEMENT [**IDAM**]*).*

Ma, soprattutto, porre l'attenzione alle minacce, indicate di seguito, che se si realizzano possono generare danni devastanti a scapito di tutta la comunità.

INDICE DEGLI ARGOMENTI

Titolo Pag.

1. ABSTRACT

---------- INDUSTRIAL IOT (IIOT)

L'INDUSTRIAL INTERNET OF THINGS (**IIoT**), *si riferisce all'applicazione di strumentazioni e sensori collegati e altri dispositivi nei macchinari e nei veicoli nei settori dei trasporti, dell'energia e di altre infrastrutture critiche.*

Nel settore energetico, le risorse energetiche distribuite *(*DISTRIBUTED ENERGY RESOURCES - DER*) come il solare fotovoltaico e le turbine eoliche includono sensori, sistemi di trasferimento dati e comunicazione, strumenti e altri dispositivi disponibili in commercio collegati in rete.*

I DER introducono scambi di informazioni tra il sistema di controllo della distribuzione di un'utilità e i DER per gestire il flusso di energia nella rete di distribuzione.

---------- OPERATIONAL TECHNOLOGY (OT) SOLUTION

*I sistemi di controllo industriale (*INDUSTRIAL CONTROL SYSTEMS - **ICS***) costituiscono una parte fondamentale dell'infrastruttura critica di una nazione. Le aziende del settore energetico si affidano a ICS per generare, trasmettere e distribuire energia e produrre, raffinare e trasportare petrolio e gas naturale.*
*Data l'ampia varietà di risorse ICS, come controllori logici programmabili e dispositivi elettronici intelligenti, che forniscono informazioni di comando e controllo sulle reti di tecnologia operativa (*OPERATIONAL TECHNOLOGY - OT*), è essenziale proteggere questi dispositivi per mantenere la continuità delle operazioni.*

Queste risorse devono essere monitorate e gestite per ridurre il rischio di un attacco informatico sugli ambienti di rete ICS.

Il **NCCoE** *del* **NIST** *sta rispondendo alla richiesta del settore energetico con una soluzione automatizzata di gestione delle risorse OT.*

Per rimanere pienamente operative, le entità del settore energetico dovrebbero essere in grado di identificare, controllare e monitorare efficacemente le proprie risorse OT.

---------- E-AUTHENTICATION AND DIGITAL IDENTITY (DI)

Per proteggere la generazione, la trasmissione e la distribuzione di energia, le società energetiche devono controllare l'accesso fisico e logico alle proprie risorse, inclusi edifici, apparecchiature, tecnologia dell'informazione (IT) e tecnologia operativa (OT).

Ossia, devono autenticare (E-AUTHENTICATION) le persone autorizzate ai dispositivi e alle strutture a cui le aziende stanno dando diritti di accesso con un alto grado di certezza.

Inoltre, devono applicare criteri di controllo degli accessi (ad esempio, consentire, negare, richiedere ulteriori informazioni) in modo coerente, uniforme e rapido su tutte le loro risorse.

*L'obiettivo di questo progetto è dimostrare un approccio tecnico convergente e basato su standard che unificano le funzioni di gestione dell'identità (*DIGITAL IDENTITY *[***DI***]) e degli accessi (*IDAM*) tra reti OT, sistemi di controllo dell'accesso fisico (*PHYSICAL ACCESS CONTROL SYSTEM *[***PACS***]) e sistemi IT.*

Queste reti spesso operano in modo indipendente, il che può comportare disparità di identità e informazioni di accesso, aumento dei costi, inefficienze e perdita di capacità e capacità di erogazione dei servizi.

Questo articolo ha la "presunzione" di offrire una breve indicazione tecnica per affrontare la sfida e incorpora anche una mentalità di valore aziendale identificando le considerazioni strategiche coinvolte nell'implementazione di nuove tecnologie.

2. CHALLENGE

---------- IIOT

La rete di distribuzione sta diventando una rete multisorgente di dispositivi e sistemi interconnessi guidati dalla comunicazione dati bidirezionale e dai flussi di potenza.

Questi flussi di dati e di alimentazione spesso si basano su tecnologie IIoT che sono collegate sia alle risorse di produzione di energia dei DER che a varie reti wireless.

Questi dispositivi EDGE *hanno un livello integrato di intelligenza digitale che consente di monitorare e tracciare le risorse DER e, attraverso i dispositivi Edge, condividere i dati sul loro stato e comunicare con altri dispositivi attraverso le reti DER e oltre.*

Un'utilità di distribuzione potrebbe dover comunicare in remoto con migliaia di DER, alcuni dei quali potrebbero non essere nemmeno posseduti o configurati dall'utilità, per controllare i punti operativi e monitorare lo stato di questi dispositivi.

La protezione delle comunicazioni DER sarà fondamentale per mantenere l'affidabilità della rete di distribuzione.

Qualsiasi attacco in grado di negare, interrompere o manomettere le comunicazioni DER potrebbe impedire a un'azienda di eseguire le azioni di controllo necessarie e potrebbe diminuire la resilienza della rete.

---------- OT SOLUTION

Molte aziende del settore energetico devono affrontare sfide nella gestione delle proprie risorse, in particolare quando tali risorse sono remote e geograficamente disperse.

Le organizzazioni potrebbero non disporre degli strumenti per fornire un elenco delle proprie risorse o potrebbero non sfruttare le capacità esistenti necessarie per produrre un inventario adeguato.

Gli inventari delle risorse esistenti possono essere istantanei, occasionali o puntuali, tali inventari possono essere difficili da mantenere e aggiornare manualmente, soprattutto considerando il cambiamento frequente.

Senza un'efficace soluzione di gestione delle risorse, le organizzazioni potrebbero essere esposte a rischi per la sicurezza informatica.

È difficile proteggere ciò che non si vede o non si conosce.

Mentre l'industria dell'energia elettrica aggiorna le vecchie infrastrutture per sfruttare le tecnologie emergenti, i servizi pubblici si stanno muovendo verso una maggiore convergenza tra tecnologia operativa (OT) e tecnologia dell'informazione (IT). Ciò consente a un numero maggiore di tecnologie, dispositivi e sistemi di connettersi alla rete per migliorare l'efficienza, fornire accesso ai dati spesso conservati in **silos** *e migliorare la produttività.*

Questa convergenza aumenta la sfida per i reparti OT e IT nella gestione efficiente ed efficace delle identità e dell'accesso.

Molte utility gestiscono sistemi IdAM (IDENTITY AND ACCESS MANAGEMENT) *frammentati e controllati da numerosi dipartimenti. Da ciò possono derivare diversi risultati negativi: 1) una mancanza di tracciabilità e responsabilità complessive riguardo a chi ha accesso alle risorse sia critiche che non critiche; 2) un aumento del rischio di attacco e interruzione del servizio e 3) l'incapacità di identificare potenziali fonti di un problema o di un attacco.*

Per proteggere meglio la generazione, la trasmissione e la distribuzione di energia, le aziende elettriche devono essere in grado di controllare e garantire l'accesso alle proprie risorse, inclusi sistemi OT, edifici, apparecchiature e sistemi IT.

---------- E-AUTHENTICATION AND DI

I sistemi IdAM per queste risorse spesso esistono in silos e i dipendenti che gestiscono questi sistemi non dispongono di metodi per coordinare efficacemente l'accesso a dispositivi e strutture attraverso questi silos.

*Ciò è inefficiente e può comportare rischi per la sicurezza delle aziende elettriche, secondo il parere delle società (***Utilities***) che hanno partecipato al progetto del sottosettore elettrico.*

Lo scenario è incentrato su un tecnico dell'utenza con accesso a più sottostazioni e alle unità terminali remote collegate alla rete dell'utilità.

Ad esempio, nel caso in cui il tecnico si dimette, un sistema IdAM convergente dovrebbe rimuovere in modo rapido e coerente l'accesso del tecnico a tutte le strutture e i sistemi.

Le aziende fornitrici di energia hanno bisogno di questa capacità per fornire alla persona giusta, l'appropriato grado di accesso alle risorse coerenti allo svolgimento delle sue funzioni e al momento opportuno.

3. SOLUTION

L'NCCoE ha realizzato un ambiente che rappresenta un'azienda di distribuzione interconnessa con DER. All'interno di questo ecosistema, esploriamo come gli scambi di informazioni tra DER e le operazioni della rete di distribuzione elettrica possono essere protetti da alcuni compromessi della sicurezza informatica.

La soluzione di esempio dimostra le seguenti funzionalità:

- ✓ COMUNICAZIONI E INTEGRITÀ DEI DATI *per garantire che le informazioni non vengano modificate durante il transito;*
- ✓ AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI *per garantire che solo i sistemi noti e autorizzati possano scambiare informazioni;*
- ✓ REGISTRO DEI COMANDI *che mantiene un registro indipendente e immutabile degli scambi di informazioni tra la rete di distribuzione e gli operatori DER;*
- ✓ RILEVAMENTO DI MALWARE *per monitorare lo scambio di informazioni e l'elaborazione per identificare potenziali infezioni da malware;*
- ✓ MONITORAGGIO COMPORTAMENTALE *per rilevare deviazioni dalle norme operative;*
- ✓ PROCESSI DI ANALISI E VISUALIZZAZIONE *per monitorare i dati, identificare anomalie e allertare gli operatori.*

Si indica come le organizzazioni produttrici di energia possano utilizzare commercialmente tecnologie disponibili coerenti con gli standard di sicurezza informatica, per affrontare le sfide: 1) stabilire; 2) migliorare e 3) automatizzare la loro gestione delle risorse OT.

Inoltre, si identifica una soluzione di gestione delle risorse OT che consiste nelle seguenti caratteristiche:

1. *la capacità di identificare e acquisire il maggior numero possibile di attributi delle risorse di base, come produttore, modello, sistema operativo (***SO***), indirizzi* **IP** *(Protocollo Internet), indirizzi* **MAC** *(*MEDIA ACCESS CONTROL*), protocolli, informazioni a livello di patch e versioni del firmware, insieme alle posizioni fisiche e logiche delle risorse;*
2. *identificazione, monitoraggio e avviso continui dei dispositivi appena connessi, dei dispositivi disconnessi e delle loro connessioni ad altri dispositivi (basati su IP e seriali);*

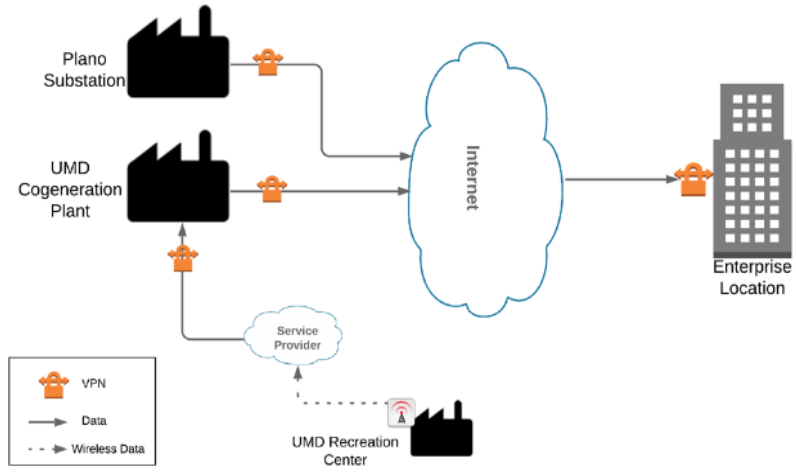
3. *la capacità di determinare la disposizione di un asset, compreso il livello di criticità (alto, medio o basso) e la sua relazione e comunicazione con altri asset all'interno della rete OT;*
4. *la capacità di allertare in caso di scostamenti dal previsto funzionamento degli asset.*

4. APPROACH

L'approccio include una valutazione e analisi del rischio, progettazione logica, sviluppo di build di esempio, test e mappatura del controllo della sicurezza.

Qui si evidenzia l'architettura e l'implementazione di esempio, inclusi elementi di supporto come un piano di test funzionale, analisi delle caratteristiche di sicurezza, lezioni apprese e considerazioni sulla build futura.

Figure 3-1 High-Level Topology



Sia la sottostazione di PLANO *che l'impianto di cogenerazione* UMD *sono collegati tramite Internet al laboratorio energetico NCCoE come sede dell'impresa.*

Ogni sito è connesso tramite una rete privata virtuale (VPN) multipunto e sempre attiva. Ciò consente all'NCCoE di aggregare i dati da più siti in un'unica posizione, emulando implementazioni multi-sito presenti nel settore energetico.

Il sito UMD è costituito anche da un sito remoto connesso tramite tecnologia wireless.

SCOPE

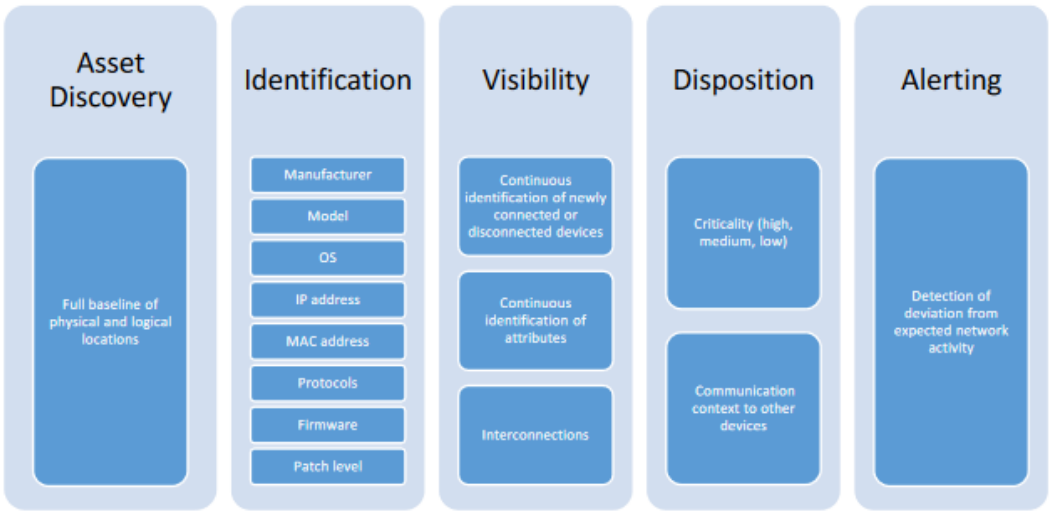
Ci concentriamo sulla gestione delle risorse OT, ovvero i dispositivi utilizzati per controllare, sia per monitorare e per mantenere la generazione, la trasmissione e la distribuzione di varie forme di energia sia dal punto di vista della sicurezza informatica.

Questi dispositivi includono PLC, IED, *workstation di ingegneria, storici e interfacce uomo-macchina (*HUMAN-MACHINE INTERFACE - HMI*).*

Il progetto affronta le seguenti caratteristiche della gestione patrimoniale:

1. ASSET DISCOVERY*: definizione di una linea di base completa di ubicazioni fisiche e logiche degli asset*
2. ASSET IDENTIFICATION*: acquisizione degli attributi delle risorse, come produttore, modello, sistema operativo, indirizzi IP, indirizzi MAC, protocolli, informazioni a livello di patch e versioni del firmware*
3. ASSET VISIBILITY*: identificazione continua di dispositivi appena connessi o disconnessi e connessioni IP (routable e non-routable) e seriali ad altri dispositivi*
4. ASSET DISPOSITION*: il livello di criticità (alto, medio o basso) di un particolare asset, la sua relazione con altri asset all'interno della rete OT e la sua comunicazione (inclusa la seriale) con altri dispositivi*
5. ALERTING CAPABILITY*: rilevamento di uno scostamento dal previsto funzionamento degli asset*

Figure 3-2 Asset Management Characteristics



L'ambito è anche l'esecuzione corretta delle seguenti funzioni di provisioning:

1. CONSENTIRE *l'accesso a un nuovo dipendente;*
2. MODIFICARE *l'accesso per un dipendente esistente;*
3. DISABILITARE *l'accesso per un ex dipendente.*

L'obiettivo, quindi, è eseguire tutte e tre le azioni da un'unica interfaccia che può fungere da fonte autorevole per tutti gli accessi gestiti all'interno di strutture, reti e sistemi di un fornitore di energia.

RISK ASSESSMENT

L'NCCOE *raccomanda che qualsiasi discussione sulla gestione del rischio, in particolare a livello aziendale, inizi con una revisione completa del* NIST SP 800-37, RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS.

La base per la nostra valutazione dei rischi associati alle sfide nella gestione delle risorse per OT deriva da NIST SP 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY, *Section 3.*

Abbiamo eseguito due tipi di valutazione del rischio:

1. ANALISI DEL RISCHIO INIZIALE *posta per il sottosettore elettrico nel suo insieme, che ha portato alla creazione del caso d'uso e delle caratteristiche di sicurezza desiderati, e*
2. ANALISI PER MOSTRARE AGLI UTENTI *come gestire il rischio di cybersecurity delle componenti introdotte dall'adozione della soluzione.*

THREATS

Se un'organizzazione non è a conoscenza delle risorse OT distribuite, è difficile proteggerle e qualsiasi altra risorsa potrebbe contenere vulnerabilità note o sconosciute. Tale mancanza di consapevolezza aumenta il rischio di sfruttamento di altre reti, dispositivi e vulnerabilità a livello di protocollo.

CISA ICS-CERT *insieme a* NIST SP 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS SECURITY, *identifica vari attori malintenzionati che possono rappresentare una minaccia per l'infrastruttura ICS.*

Questi includono:

1. **Servizi di intelligence stranieri**: *organizzazioni governative nazionali le cui attività di raccolta di informazioni e spionaggio cercano di danneggiare gli interessi della nazione;*
2. **Gruppi criminali**, *gruppi di criminalità organizzata che cercano di attaccare per guadagno monetario;*
3. **Hacker**, *considerati i più pubblicizzati; tuttavia, spesso possiedono pochissime abilità commerciali per produrre attacchi di lunga durata;*
4. **Terroristi** – *avversari che sono meno equipaggiati nelle loro capacità informatiche e quindi rappresentano solo una minaccia cibernetica limitata.*

Esempi comuni di vulnerabilità includono credenziali ***hardcoded****,* ***password*** *predefinite invariate e* ***anomalie*** *di crittografia.*

VULNERABILITIES

NIST SP 800-82 classifica le vulnerabilità ICS *(*INDUSTRIAL CONTROL SYSTEMS*) nelle seguenti categorie con esempi:*

1. **Politica e Procedura**: *politica di sicurezza incompleta, inappropriata o inesistente, inclusa la relativa documentazione, guide all'implementazione (ad es. procedure) e applicazione;*
2. **Architettura e Design**: *difetti di progettazione, difetti di sviluppo, cattiva amministrazione e connessioni con altri sistemi e reti;*
3. **Configurazione e Manutenzione**: *configurazione errata e scarsa manutenzione;*
4. **Fisico**: *mancanza o controllo degli accessi improprio, apparecchiature malfunzionanti;*
5. **Sviluppo software**: *convalida dei dati non corretta, funzionalità di sicurezza non abilitate, privilegi di autenticazione inadeguati;*
6. **Comunicazione e Rete**: *autenticazione inesistente, protocolli non sicuri, configurazione impropria del firewall. La conoscenza delle risorse distribuite è fondamentale per proteggere l'infrastruttura ICS di un'organizzazione e mitigare i rischi associati alle vulnerabilità basate sulle risorse.*

La conoscenza della posizione di una risorsa e la definizione del suo comportamento consentono di rilevare comportamenti anomali tramite il monitoraggio della rete che potrebbero essere il risultato di una vulnerabilità sfruttata con successo.

La capacità di rilevare in modo affidabile i cambiamenti nel comportamento delle risorse e la conoscenza degli attributi di una risorsa sono fondamentali per rispondere a potenziali incidenti di sicurezza informatica.

RISK

I rischi per la sicurezza relativi ai sistemi informativi sono quei rischi che derivano dalla perdita di RISERVATEZZA, INTEGRITÀ *o* DISPONIBILITÀ *delle informazioni o dei sistemi informativi e che riflettono potenziali impatti negativi sulle operazioni organizzative (inclusi missione, funzioni, immagine o reputazione), sulle risorse organizzative, sugli individui e ad altre organizzazioni e alla nazione.*

Per il settore energetico, un rischio primario per OT è la mancanza di consapevolezza dei dispositivi in esecuzione sull'infrastruttura. Se le risorse OT non possono essere adeguatamente contabilizzate, non possono essere protette.

Di seguito sono riportati i rischi tattici associati alla mancanza di una soluzione di gestione delle risorse OT:

1. mancanza di conoscenza di un bene esistente, inclusa la sua configurazione e il comportamento previsto;
2. scarsa conoscenza dell'ubicazione fisica e logica del bene;
3. mancanza di un inventario completo delle risorse quasi in tempo reale;
4. mancanza di conoscenza delle vulnerabilità degli asset e delle patch disponibili;
5. mancanza di capacità di visualizzazione e analisi dei dati che aiutino i dispatcher e un analista della sicurezza a visualizzare gli eventi di sicurezza del dispositivo.

SECURITY CONTROL MAP AND TECHNOLOGIES

Per chi fosse interessato ai controlli da effettuare, la "Table 3-1 Security Characteristics and Controls Mapping—NIST Cybersecurity Framework" *del* NIST SP 1800-32 *mappa le caratteristiche di sicurezza dell'architettura di riferimento alle funzioni, categorie e sottocategorie di sicurezza del* NIST Cybersecurity Framework.

Table 3-1 Security Characteristics and Controls Mapping–NIST Cybersecurity Framework

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12	**Cisco Identity Services Engine (ISE)** provides identity and access management capabilities; determines whether users are accessing the network on an authorized, policy-compliant device, and allows access to services based on associated policy.
				TDi ConsoleWorks manages the privileged access credentials for systems. These credentials are never seen or used directly by privileged users.
				Xage Security Fabric manages identities and credentials for users, applications, and devices. .
		PR.AC-3: Remote access is managed.	AC-1, AC-17, AC-19, AC-20, SC-15	**BlackRidge Gateway** provides first-packet authentication of incoming transmission control protocol (TCP) connections and enforces network access control policy, preventing unauthorized TCP connections through the gateway to protected devices and services.
				Xage Security Fabric provides policy creation

Analogamente è necessario considerare la Table 3-1 di NIST SP 800-53.

Table 3-1 Security Control Map

Informative References								
Function	**Category**	**Subcategory**	**CIS CSC 2016**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001: 2013**	**NIST SP 800-53 Rev. 4**	**NERC CIP Standards**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	1	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8 PM-5	CIP-002-5.1a:R1, R2 CIP-010-2:R1, R2

*La "*Table 3-2 Cybersecurity Work Roles Aligned to Reference Architecture*" del* NIST SP 1800-32 *identifica i ruoli di lavoro della sicurezza informatica che più si allineano con le categorie e le sottocategorie di sicurezza del* Cybersecurity Framework *nella nostra architettura di riferimento.*

I ruoli di lavoro si basano sul quadro della forza lavoro della NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) *per la sicurezza informatica (*NICE FRAMEWORK*).*

Ulteriori informazioni su NICE *e altri ruoli lavorativi sono disponibili nel* NIST SP 800-181, WORKFORCE FRAMEWORK FOR CYBERSECURITY (NICE FRAMEWORK).

Table 3-2 Cybersecurity Work Roles Aligned to Reference Architecture

NICE Work Role ID	NICE Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
OM-ADM-001	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g., installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).	Operate and Maintain	Systems Administration	PR.AC-1, PR.AC-3, PR.AC-4
SP-SYS-001	Information Systems Security Developer	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.	Securely Provision	Systems Development	PR.AC-5, PR.DS-1, PR.DS-2, PR.DS-6, DE.AE-1
PR-CDA-001	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their	Protect and Defend	Cyber Defense Analysis	DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-4, DE.CM-7

La Tabella 4-1, ricavata dal NIST SP 1800-2B, *associa le caratteristiche di sicurezza desiderate e le capacità di esempio del caso d'uso* AL FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *noto anche come* NIST CYBERSECURITY FRAMEWORK (CSF)*; norme* NIST *pertinenti; standard di settore; e controlli e migliori pratiche.*

Table 4-1 Use-Case Security Characteristics Mapped to Relevant Standards and Controls

Example Characteristic		Sector Specific Compliance Guidance					
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 Revision 4	IEC/ISO 27001	NERC CIP Version 5
Authentication for OT	Authentication mechanisms	Protect	Access Control	AC-2, IA Family		ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-007-5 R2, CIP-007-5 R5
Access Control for OT	Access control mechanisms	Protect	Access Control and Protective Technology	PR.AC-2: Physical access to assets is managed and protected PR.AC-3: Remote access is managed PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, AC-17, AC-19, AC-20, CM-7, PE-2, PE-3, PE-4, PE5, PE-6, PE-9	ISO/IEC 27001:2013 A.6.2.2, A.9.1.2A, 11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1	CIP-003-5 R1, CIP-004-5 R2, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R1

TECHNOLOGIES

La Tabella 3-3 elenca tutte le tecnologie e il loro ruolo in questo progetto e fornisce una mappatura tra il termine generico dell'applicazione, il prodotto specifico utilizzato e i controlli di sicurezza forniti dal prodotto.

Fare riferimento alla tabella 3-1 precedentemente definita per una spiegazione dei codici della sottocategoria del framework di sicurezza informatica del NIST.

Table 3-3 Products and Technologies

Capability	Product	Project Role	Cybersecurity Framework Subcategories
Asset discovery and monitoring	Dragos Platform v1.5	Passive asset discovery, threat detection, and incident response for ICS networks	ID.AM-1, DE.AE-1, DE.AE-2
Data collection and inventory tool	ForeScout CounterACT v8.0.1	CounterACT appliance collects data from one location and reports back to the CounterACT Enterprise Manager on the enterprise network.	ID.AM-1, DE.AE-1, DE.AE-2
		Patch availability reporting is	

La Tabella 4-2, ricavata dal NIST SP 1800-2B, *fornisce informazioni sui prodotti e tecnologie implementate per soddisfare i requisiti di controllo della sicurezza.*

Questa tabella descrive solo le funzionalità del prodotto che sono state utilizzate nei test.

*La colonna "*Prodotto*" della tabella contiene collegamenti alle informazioni sui prodotti del fornitore che ne descrivono le funzionalità complete.*

Table 4-2 Products and Technologies Used to Satisfy Security Control Requirements

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Authentication for OT	Authentication mechanisms	PR.AC-1: Identities and credentials are managed for authorized devices and users	Identity Management Platform	CA	Identity Manager	R12.0 SP14 Build 9140	Implements workflows for creating digital identities and authorizing them access to physical and logical resources, including authoritative source

5. ARCHITECTURE

L'architettura del progetto si concentra sulle funzionalità chiave della gestione delle risorse:

1. *rilevamento delle risorse,*
2. *identificazione,*
3. *visibilità,*
4. *disposizione e*
5. *capacità di avviso.*

Se combinate, queste funzionalità consentono a un'organizzazione di avere una comprensione più solida, non solo dell'inventario e dell'architettura dei dispositivi, ma anche dello stato attuale dei dispositivi e delle segnalazioni automatiche per il comportamento anomalo delle risorse.

Questo capitolo presenta un'architettura di alto livello, un progetto di riferimento, topologie dettagliate e una dashboard di visualizzazione per l'implementazione di tale soluzione.

Il progetto di riferimento include un'ampia serie di funzionalità disponibili sul mercato per illustrare le funzionalità ESAM *(*ENERGY SECTOR ASSET MANAGEMENT*) che un'organizzazione può implementare.*

La dashboard di gestione delle risorse mostra la connettività di rete tra i dispositivi e un elenco di risorse note all'interno della rete.

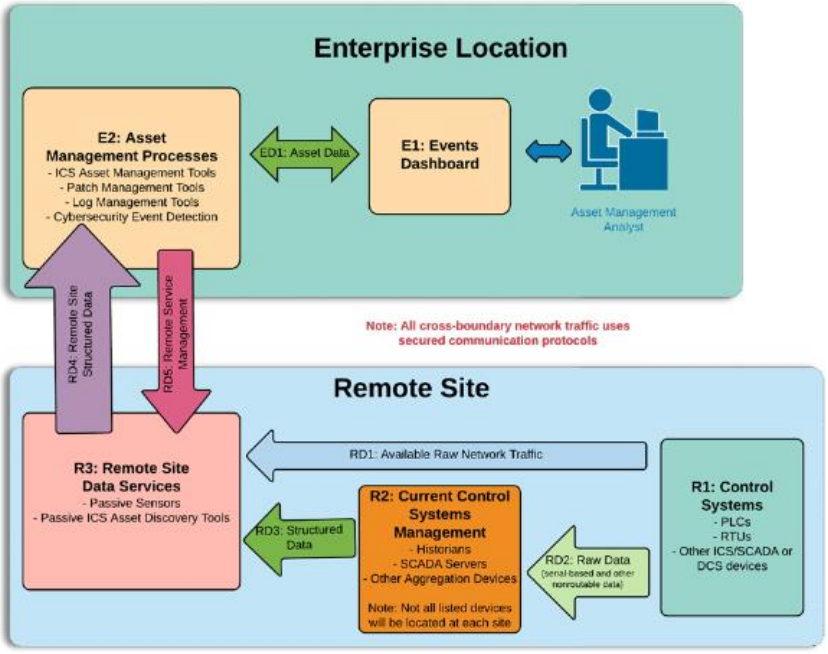
HIGH-LEVEL ARCHITECTURE

La soluzione ESAM *è progettata per affrontare le funzioni, le categorie e le sottocategorie del framework di sicurezza informatica descritte nella Tabella 3-1 (vedi precedente capitolo "*Security Control Map and Technologies*" oppure* NIST SP 1800-23B*) ed è illustrata nella Figura 3-1 (vedi capitolo Approach precedente oppure* NIST SP 1800-23B*).*

La Figura 4-1 del NIST SP 1800-23B illustra l'architettura di alto livello per il monitoraggio delle risorse ICS, comprese quelle situate in siti remoti.

Sebbene sia rappresentato un sito remoto, l'architettura consente l'inclusione di più siti remoti. Ciò consente una struttura ripetibile e standard di implementazione e strategia per più siti remoti, che può essere adattata alle esigenze dei singoli siti.

Figure 4-1 High-Level Architecture



L'architettura di alto livello (Figura 4-1) sopra è meglio descritta a partire dai sistemi di controllo del sito remoto.

Le informazioni a questo livello sono visualizzate come dati grezzi basati su ICS *(comprese le comunicazioni seriali), traffico di rete basato su* ICS *(*PROTOCOLLO DI RETE DISTRIBUITO 3, MODBUS, ETHERIP*, ecc.) o dati "raw" di rete (*TRANSMISSION CONTROL PROTOCOL [TCP]/USER DATAGRAM PROTOCOL*,* INTERNET CONTROL MESSAGE PROTOCOL *[*ICMP*],* ADDRESS RESOLUTION PROTOCOL *[*ARP*], ecc.).*

- ✓ *Le comunicazioni seriali sono incapsulate nei protocolli di rete.*
- ✓ *I dati sono raccolti e archiviati dall'oggetto server di dati del sito remoto (R3).*
- ✓ *I sensori raccolgono il traffico di rete ICS e dati "RAW" di rete IP dai sistemi di controllo (R1) e dalla gestione dei sistemi di controllo correnti (R2).*
- ✓ *I dati raccolti dai server di dati del sito remoto (R3) vengono inviati tramite un tunnel VPN ai server di ascolto nella posizione aziendale.*
- ✓ *Una volta che i dati arrivano dal sito remoto al server di raccolta dati aziendale, vengono inseriti nei processi di gestione delle risorse (E2).*
- ✓ *Questi strumenti aggregano i dati strutturati del sito remoto (RD4) da più siti, per costruire un quadro olistico dello stato di salute e della configurazione della rete.*
- ✓ *Successivamente, dagli strumenti di* ASSET MANAGEMENT PROCESSES *(E2) gli eventi e i dati degli asset vengono inviati direttamente alla dashboard degli eventi (E1).*
- ✓ *In caso di configurazione necessaria di server di dati del sito remoto (R3), è possibile stabilire connessioni di gestione del servizio remoto tra gli* ASSET MANAGEMENT PROCESSES *(E2) e i server dei dati del sito remoto (R3).*
- ✓ *Il traffico è instradato attraverso il tunnel VPN e terminato all'interno dei data server del sito remoto (R3).*
- ✓ *Ciò consente la configurazione esclusivamente nei server di dati del sito remoto (R3), utilizzando il tunnel VPN stabilito per la sicurezza, senza consentire l'accesso né ai dispositivi di gestione dei sistemi di controllo correnti (R2) né ai sistemi di controllo (R3).*

DIGITAL IDENTITY (DI) E E-AUTHENTICATION

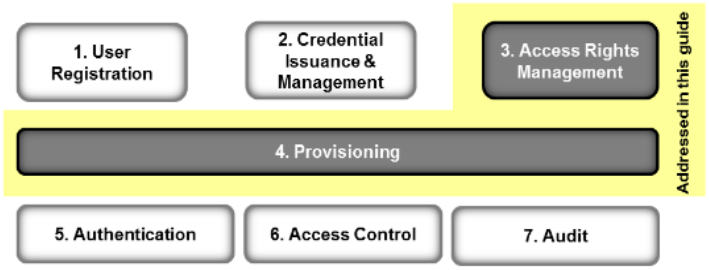
IdAM *è la disciplina di gestione della relazione tra una persona e le risorse a cui la persona deve accedere per svolgere un lavoro.*

Comprende i processi e le tecnologie con cui gli individui sono identificati, controllati, accreditati e autorizzati all'accesso alle risorse e ritenuti responsabili per il loro utilizzo di tali risorse.

Questi processi e tecnologie creano rappresentazioni dell'identità digitale delle persone, legano tali identità alle credenziali e utilizzano tali credenziali per controllare l'accesso alle risorse.

IdAM *è composto dalle funzionalità illustrate nella Figura 5-1 del* NIST SP 1800-2B *e sono di seguito dettagliate.*

Figure 5-1 IdAM Capabilities



1. *La registrazione dell'utente determina l'esistenza di un motivo per concedere a una persona l'accesso alle risorse, verifica l'identità della persona e crea una o più identità digitali per la persona.*
2. *L'emissione e la gestione delle credenziali fornisce la gestione del ciclo di vita delle credenziali, come badge dei dipendenti o certificati digitali.*
3. *La gestione dei diritti di accesso determina le risorse che un'identità digitale può utilizzare.*
4. *Il provisioning popola le informazioni su identità digitale, credenziali e diritti di accesso da utilizzare per l'autenticazione, il controllo degli accessi e il controllo.*
5. *L'autenticazione stabilisce la fiducia nell'identità digitale di una persona.*
6. *Il controllo degli accessi consente o nega a un'identità digitale l'accesso a una risorsa.* NIST IR 7316, ASSESSMENT OF ACCESS CONTROL SYSTEMS, *spiega le politiche, i modelli e i meccanismi di controllo degli accessi comunemente usati.*
7. *L'audit mantiene un registro dei tentativi di accesso alle risorse da parte di un'identità digitale.*

Le prime tre funzionalità sono di tipo amministrativo, in quanto implicano azioni umane o sono utilizzate raramente.

Le ultime tre funzionalità sono "run-time", in quanto si applicano ogni volta che una persona accede a una risorsa.

Il provisioning collega le attività amministrative alle attività di runtime.

Nel settore elettrico odierno, alcune o tutte queste funzionalità IdAM *sono spesso replicate almeno tre volte:*

1°. una volta per l'accesso di una persona a OT,

2°. di nuovo per l'accesso fisico e

3°. quindi per accedere all'IT.

Inoltre, queste funzionalità possono essere replicate in modo indipendente per ogni sistema all'interno di OT o IT.

La replica rende difficile garantire che i dipendenti abbiano accesso alle risorse di cui hanno bisogno e solo a tali risorse per svolgere il proprio lavoro.

I dipendenti appena assunti potrebbero non avere accesso a tutte le risorse di cui hanno bisogno.

I dipendenti che cambiano lavoro possono mantenere l'accesso alle risorse di cui non hanno più bisogno.

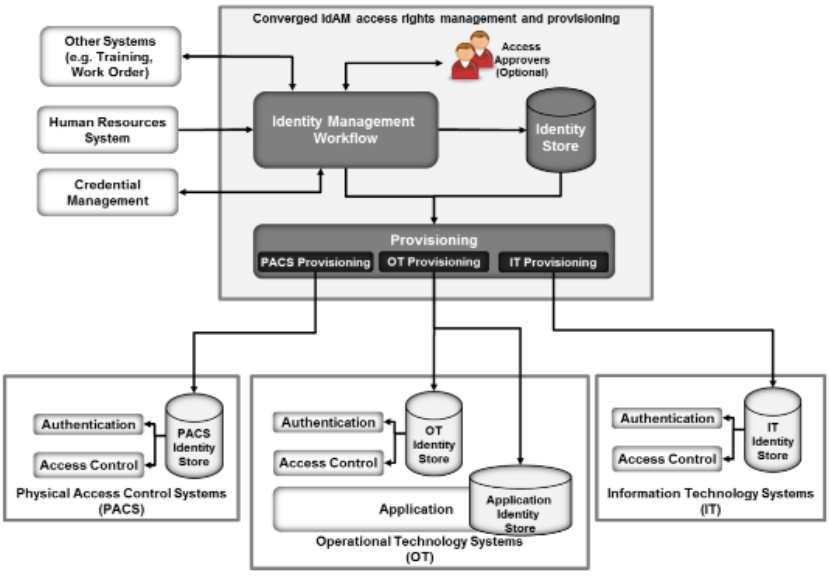
I dipendenti licenziati possono mantenere l'accesso molto tempo dopo la fuoriuscita.

La soluzione di esempio qui descritta risolve questi problemi creando un'implementazione convergente della gestione dei diritti di accesso IdAM *e delle funzionalità di provisioning utilizzate in* OT, PACS *e* IT.

Questa implementazione convergente non modifica le capacità di runtime di autenticazione, controllo degli accessi e audit, lasciandole replicate e distribuite.

L'implementazione convergente dipende dai processi esistenti di un'utilità, come l'inserimento dei dipendenti e l'emissione di badge, per fornire sia la registrazione degli utenti che l'emissione delle credenziali e le capacità di gestione.

Figure 5-2 IdAM Example Solution



La Figura 5-2 del NIST SP 1800-2B *illustra la soluzione di esempio.*

La capacità IdAM *convergente implementa i seguenti elementi:*

- *un workflow* IdAM *per gestire l'intero processo;*
- *un archivio di identità, che è la fonte autorevole delle identità digitali e dei relativi diritti di accesso alle risorse;*
- *una capacità di provisioning per popolare le informazioni dal flusso di lavoro e dall'archivio identità nelle funzionalità di runtime.*

La capacità di provisioning è ulteriormente scomposta in provisioning OT, IT *e* PACS.

Ciascuno dei tre **silo**, OT, IT *e* PACS, *può avere i propri archivi di identità che contengono identità digitali e diritti di accesso da utilizzare per controllare l'accesso ai sistemi all'interno del silo.*

Inoltre, alcune applicazioni in un silo possono avere i propri archivi di identità dell'applicazione utilizzati dall'applicazione per controllare l'accesso alle informazioni e ai servizi forniti.

La funzionalità IdAM *convergente, tramite il provisioning, gestisce le informazioni in questi altri archivi di identità.*

Le funzionalità combinate possono ridurre il tempo necessario per aggiornare l'accesso nei sistemi OT, PACS *e* IT *da giorni a minuti.*

Inoltre, migliorano l'acquisizione dell'audit trail integrando i tre registri di audit in uno.

Il provisioning può anche verificare che le autorizzazioni archiviate localmente nelle funzionalità di runtime siano coerenti con quelle nell'archivio identità.

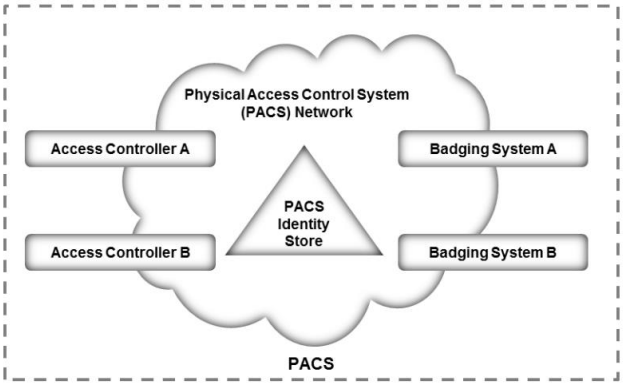
Se le autorizzazioni archiviate localmente non sono coerenti con i valori autorevoli nell'archivio identità, il provisioning può generare un allarme o modificare le autorizzazioni archiviate localmente in modo che siano coerenti con l'archivio identità.

PHYSICAL ACCESS CONTROL SYSTEM (PACS) SILO

Il silo PACS ospita sia i controller di accesso sia i sistemi badge.

- *I sistemi badge implementati emettono le credenziali per creare i badge con cui i dipendenti accederanno alle strutture e ad altre risorse fisiche.*
- *I controllori dell'accesso leggono le informazioni dai badge e verificano le informazioni per autorizzare l'accesso.*
- *Se l'accesso è consentito, il controller di accesso sblocca una porta, consentendo alla persona di entrare nella struttura.*

Figure 5-3 Notional PACS Architecture



- *L'archivio delle identità PACS contiene le identità e le informazioni di controllo degli accessi per le persone che gestiscono i sistemi sia badge sia di controllo degli accessi.*
- *Queste informazioni sul controllo dell'accesso sono fornite nell'istanza dell'archivio identità PACS dal sistema IdAM convergente.*
- *I controllori di accesso possono anche utilizzare l'archivio di identità PACS per controllare le informazioni di autorizzazione per determinare l'accesso fisico.*
- *Se i controller di accesso utilizzano l'archivio di identità PACS, il sistema IdAM fornirà le informazioni di autorizzazione all'archivio di identità PACS.*
- *Se i controller di accesso utilizzano il proprio archivio di identità interno, le informazioni di autorizzazione saranno fornite direttamente al controller di accesso.*

OPERATIONAL TECHNOLOGY (OT) SILO

Il silo OT è composto da due tipologie di impianti:

1°. *sono i sistemi di gestione operativa che operatori e tecnici utilizzano per monitorare e gestire la generazione e la consegna di energia elettrica ai clienti;*

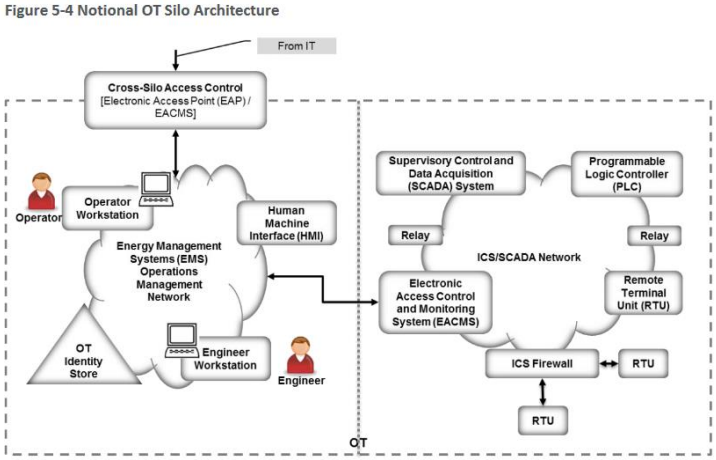
2°. *sono i sistemi di controllo industriale (*ICS*) e sistemi di supervisione e acquisizione dati (*SUPERVISORY CONTROL AND DATA ACQUISITION [SCADA]*) che forniscono il controllo in tempo reale e quasi in tempo reale delle apparecchiature che producono e forniscono energia elettrica.*

La Figura 5-4 mostra l'architettura teorica del silo OT.

La rete operativa e di gestione all'interno del silo OT dispone di un archivio di identità che contiene identità e autorizzazioni per l'accesso ai sistemi di gestione operativa.

Tali identità e autorizzazioni sono fornite dal sistema IdAM convergente.

Figure 5-4 Notional OT Silo Architecture



Una funzione di controllo degli accessi tra silo consente un accesso parziale ai sistemi di gestione operativa dal silo IT.

Il sistema IdAM convergente fornisce le autorizzazioni per accedere alle risorse OT dal silo IT all'archivio di identità OT.

Un sistema elettronico di controllo e monitoraggio degli accessi (ELECTRONIC ACCESS CONTROL AND MONITORING SYSTEM [EACMS]*) controlla l'accesso ai dispositivi* ICS/SCADA *sulla rete* ICS/SCADA*, dalla rete di gestione delle operazioni.*

L'EACMS *consente agli operatori di avere accesso tramite terminale ai controllori logici programmabili e alle unità terminali remote (*REMOTE TERMINAL UNITS [RTU]*) che forniscono il controllo in tempo reale della produzione e della consegna dell'energia.*

Le autorizzazioni che consentono l'accesso tramite EACMS possono essere fornite nell'archivio di identità OT o direttamente nell'EACMS dal sistema IdAM convergente.

Il sistema IdAM convergente può fornire autorizzazioni temporali che consentiranno l'accesso durante un periodo di tempo limitato.

Alla scadenza del periodo, viene attivato un flusso di lavoro che revoca l'autorizzazione nell'archivio identità e annulla il provisioning dell'autorizzazione dall'archivio identità OT.

ACCESS AUTHORIZATION INFORMATION FLOW AND CONTROL POINTS

*L'accesso e l'autorizzazione per ciascun utente si basano sulle regole aziendali e di sicurezza implementate nei flussi di lavoro all'interno dei prodotti del sistema IdAM centrale (*RSA IMG, CA IDENTITY MANAGER*).*

- *I flussi di lavoro includono catene di approvazione della gestione e registrazione dei dati di approvazione/rifiuto.*
- *Una volta che il sistema IdAM centrale ha elaborato la richiesta di accesso e l'autorizzazione, i dati aggiornati di accesso e autorizzazione dell'utente sono inviati all'archivio di identità centrale.*
- *L'archivio identità centrale contiene il meccanismo di distribuzione per l'aggiornamento delle varie directory downstream (sincronizzate) con l'accesso utente e i dati di autorizzazione.*

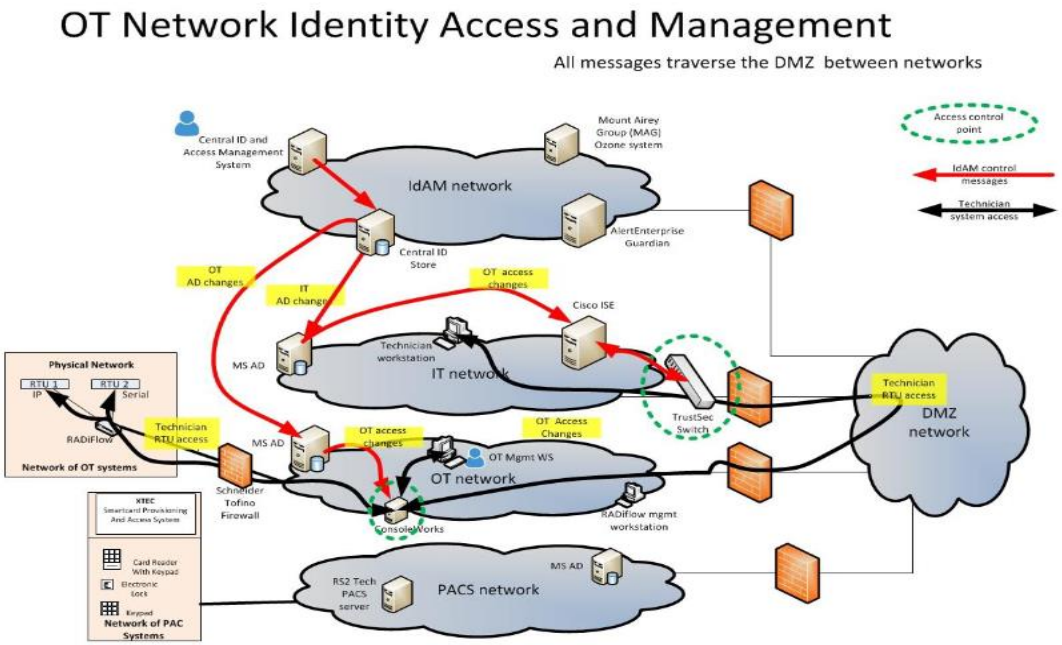
Questo processo si applica a nuovi utenti, utenti disabilitati o eliminati e a qualsiasi modifica a un profilo utente.

OT ACCESS AND AUTHORIZATION INFORMATION FLOW

Questo capitolo descrive l'accesso OT ICS/SCADA *e il flusso di informazioni sull'autorizzazione per entrambe le build.*

La Figura 5-17 del NIST SP 1800-2B *illustra il flusso d'informazioni di accesso e autorizzazione per i dispositivi OT ICS/SCADA.*

Figure 5-17 Access and Authorization Information Flow for OT ICS/SCADA Devices



- *Le linee rosse in Figura 5-17 indicano gli scambi di dati di accesso e autorizzazione.*
- *Le linee nere rappresentano i percorsi dati di due tecnici OT ICS/SCADA che accedono alle RTU nella rete SCADA (uno dalla rete IT e uno dalla rete OT).*

Si noti che tutti i dati instradati tra le reti passano attraverso la DMZ e i firewall di rete.

Nella rete OT, ConsoleWorks:

1. *controlla l'accesso ai dispositivi OT ICS/SCADA;*
2. *utilizza la directory OT per determinare quali utenti siano autorizzati ad accedere ai dispositivi OT ICS/SCADA;*
3. *punto di controllo per gli utenti che accedono ai dispositivi di rete OT;*
4. *memorizza i profili per gruppi e utenti specifici;*
5. *monitora e registra ogni sessione utente; questa funzione consente a un'organizzazione di monitorare l'attività dell'utente, bloccare attività indesiderate e generare avvisi per attività sospette o indesiderate;*
6. *autorizza inoltre gli utenti ad accedere ai dispositivi OT.*

PACS ACCESS AND AUTHORIZATION INFORMATION FLOW

BUILD #1

La rete PACS include dispositivi, come serrature e tastiere.

Nella Figura 5-18 del NIST SP 1800-2B, *le linee rosse indicano gli scambi di dati di accesso e autorizzazione.*

Si noti che tutti i dati instradati tra le reti passano attraverso la DMZ e i firewall di rete.

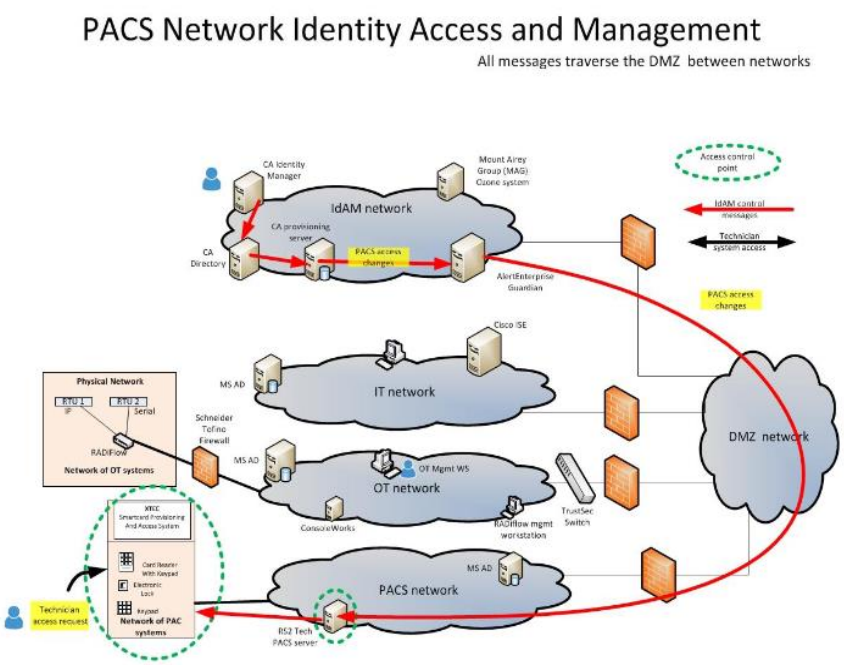
*Nella rete PACS, "*ACCESS IT!*" il server di gestione controlla l'accesso fisico a strutture, stanze, ecc. e aggiorna i dispositivi PACS secondo necessità.*

I dispositivi segnalano/registrano anche l'accesso dell'utente a questo server per scopi di registrazione/controllo.

Nella maggior parte degli ambienti, la rete PACS è separata dalle altre reti, in genere, utilizzando VLAN.

GUARDIAN *raccoglie i dati di accesso e autorizzazione dal server di provisioning di Identity Manager e li fornisce ad* ACCESS IT!.

Figure 5-18 Access and Authorization Information Flow for the PACS Network, Build #1

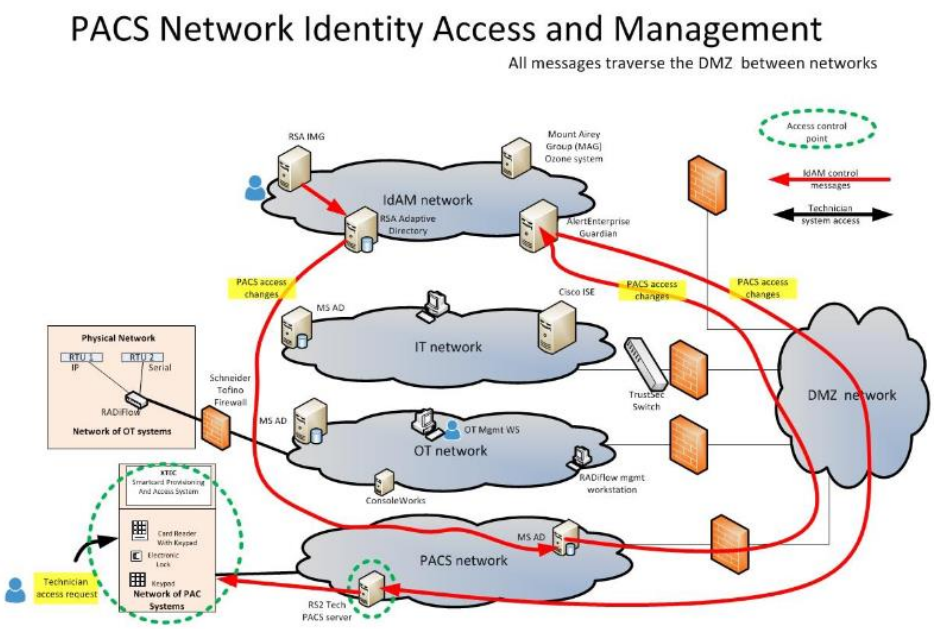


BUILD #2

Le linee rosse nella Figura 5-19 indicano gli scambi di dati di accesso e autorizzazione o l'accesso PACS in Build #2 e rappresentano i flussi di informazione logici, non fisici.

Le modifiche all'accesso PACS da RSA ADAPTIVE DIRECTORY *nella rete IdAM a* Microsoft *AD nella rete PACS passano fisicamente attraverso la rete DMZ.*

Figure 5-19 Access and Authorization Information Flow for the PACS Network, Build #2



In questa build, IMG *fornisce tutti i dati IdAM PACS alla directory PACS.*

ALERTENTERPRISE *raccoglie i dati di accesso e autorizzazione dalla directory PACS e li fornisce ad* ACCESS IT!.

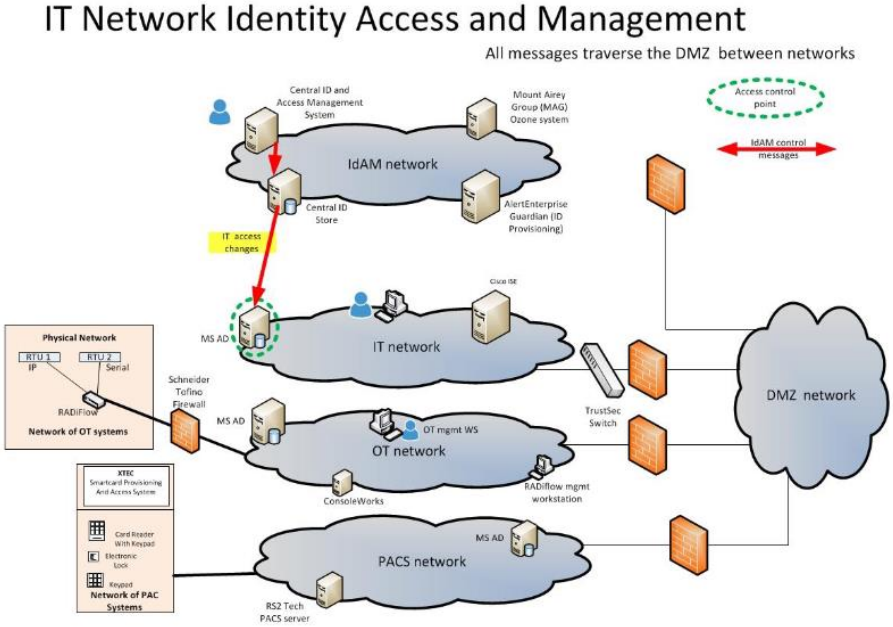
IT ACCESS AND AUTHORIZATION INFORMATION FLOW

Le linee rosse nella Figura 5-20 indicano gli scambi di dati di accesso e autorizzazione in entrambe le build.

Si noti che tutti i dati sono instradati tra le reti OT, PACS, IT e IdAM attraverso la DMZ.

Nella rete IT, gli host e altri sistemi accedono alla directory IT per determinare quali utenti sono autorizzati ad accedere ai dispositivi sulla rete IT.

Figure 5-20 Access and Authorization Information Flow for the IT Network

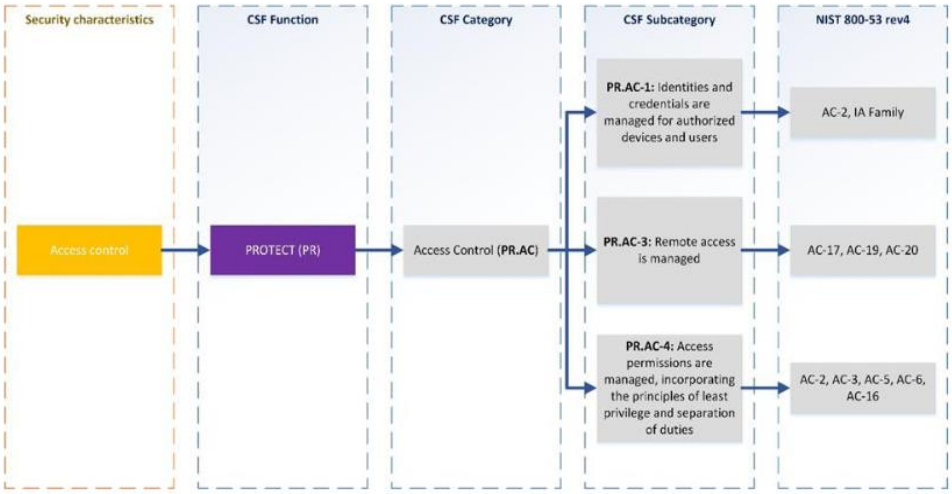


AD fornisce la tipica funzione di archiviazione delle identità per l'archiviazione delle autorizzazioni di accesso.

SECURING CHARACTERISTICS ADDRESSED

Un aspetto della nostra valutazione della sicurezza riguarda la valutazione dell'efficacia con cui la soluzione di esempio IdAM *affronta le caratteristiche di sicurezza che deve supportare.*

Figure 5-21 Example Process for Determining the Security Standards-Based Attributes for the Example Solution



Queste caratteristiche di sicurezza sono elencate in una mappa di controllo della sicurezza pubblicata nell'appendice della descrizione del caso d'uso IdAM.

Sei caratteristiche di sicurezza sono elencate nella mappa di controllo della sicurezza, ognuna delle quali è ulteriormente classificata dalle categorie e sottocategorie del CYBERSECURITY FRAMEWORK (CSF) *a cui sono mappate.*

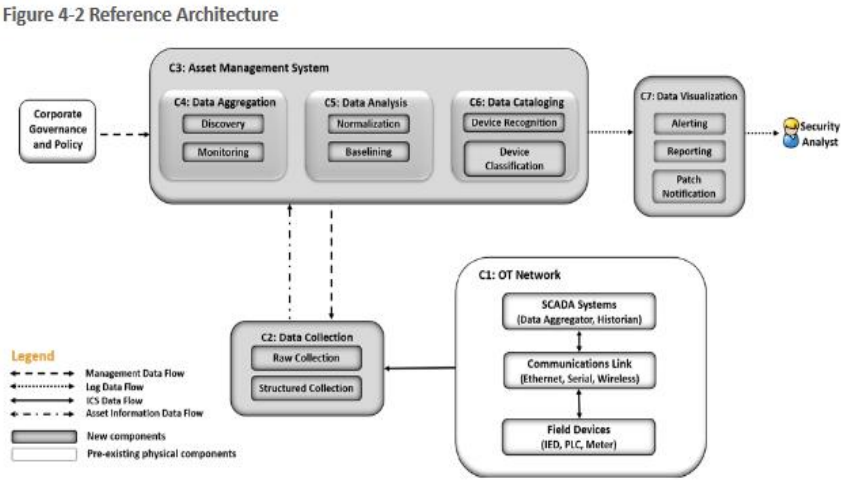
Le sottocategorie del CSF si associano ulteriormente a sezioni specifiche di ciascuna norma o best practice citate nel CSF in riferimento a quella sottocategoria.

La Figura 5-21 mostra un esempio del processo per determinare gli attributi basati sugli standard di sicurezza per la soluzione di esempio.

REFERENCE ARCHITECTURE

L'architettura di riferimento mostrata nella Figura 4-2 illustra il progetto ESAM dettagliato, comprese le relazioni tra le funzionalità incluse.

Figure 4-2 Reference Architecture



Come indicato dalla legenda, linee diverse rappresentano diversi tipi di dati che fluiscono nei vari componenti.

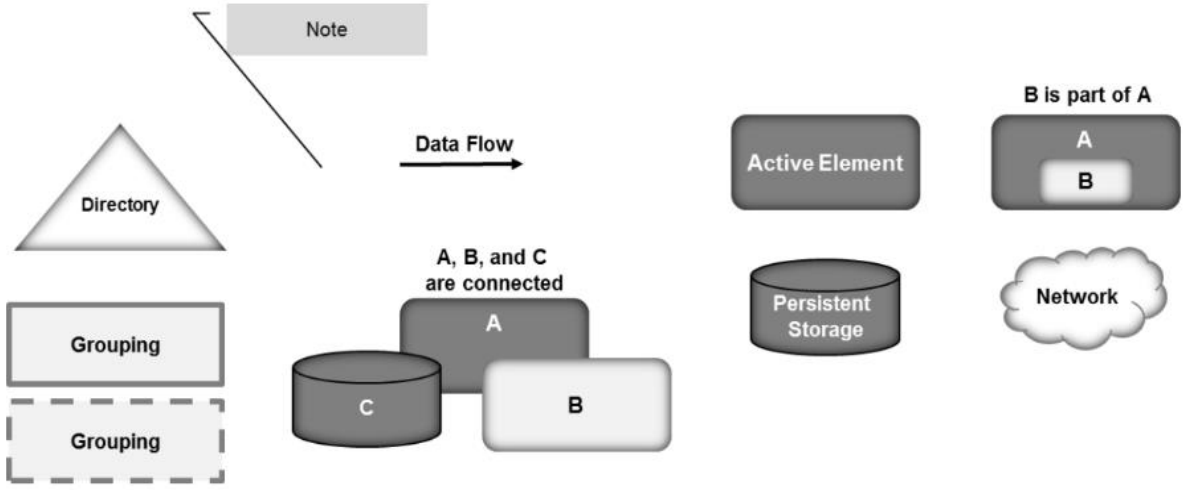
- *I dati ICS sono rappresentati con linee continue.*
- *Il flusso dei dati di gestione è rappresentato con la linea tratteggiata.*
- *Le informazioni sulle risorse sono rappresentate con una linea punto-trattino.*
- *I dati del registro sono rappresentati con una linea tratteggiata.*
- *Ciascuna delle forme chiare rappresenta un componente preesistente o opzionale.*
- *La rete OT è costituita da dispositivi composti da dati basati su ICS, traffico di rete ICS o dati di rete grezzi.*

- *L'implementazione di esempio include i dispositivi ICS sia nell'impianto di cogenerazione UMD che nel laboratorio di TD a Plano, in Texas, nel gruppo di categorizzazione Reference Design OT Network.*
- *Un altro componente che utilizza la soluzione ESAM sono la Governance e la Policy aziendale.*
- *La governance e la politica aziendale possono guidare diversi aspetti della soluzione ESAM, ad esempio per quanto tempo verranno conservati i record, come classificare i dispositivi e con quale frequenza vengono eseguiti i report.*

Le funzionalità sono descritte di seguito.

1. *La raccolta dati avviene dalla rete OT sul posto.*
   I dati possono essere raccolti in forma di acquisizione di pacchetti non elaborati, nonché in qualsiasi forma strutturata che può provenire da strumenti o dispositivi all'interno della rete OT.
2. *Il componente di aggregazione dei dati acquisisce i dati dalla funzionalità di raccolta dati e utilizza le funzionalità sia di rilevamento sia di monitoraggio.*
   La capacità di monitoraggio tiene traccia dell'attività di rete raccolta dalla rete OT.
   Dopo un periodo di formazione, la funzionalità di rilevamento identifica nuovi dispositivi quando nuovi indirizzi IP e indirizzi MAC comunicano sulla rete.
3. *La funzionalità di analisi dei dati utilizza sia una funzione di normalizzazione per portare il traffico da più siti in un'unica immagine sia una funzione di riferimento per stabilire uno standard informato di come dovrebbe comportarsi il traffico di rete di una risorsa durante le normali operazioni.*
4. *La funzionalità di catalogazione del dispositivo utilizza contemporaneamente le informazioni dal componente di raccolta dati.*
   La funzionalità di riconoscimento dei dispositivi identifica diversi tipi di dispositivi dall'indirizzo MAC per determinare il produttore o dall'ispezione approfondita del pacchetto per determinare il modello, il numero di serie o entrambi di un dispositivo se il protocollo ICS non elaborato contiene tali informazioni.
   Successivamente, la funzionalità di classificazione dei dispositivi può determinare il livello di criticità dei dispositivi sia automaticamente sia manualmente se richiesto.
5. *La funzionalità di visualizzazione dei dati mostra i dati dai componenti del sistema di* ASSET MANAGEMENT SYSTEM.
   Qui, la funzionalità di avviso di notifica agli analisti degli incidenti, incluse le deviazioni dai comportamenti normali.
   Una caratteristica chiave della funzionalità di segnalazione è la capacità di segnalare quando è disponibile una patch di sicurezza informatica.

6. LEGEND FOR DIAGRAMS



7. RIFERIMENTI

1) *NIST SP 1800-32 – Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources*
2) *NIST SP 1800-23B – Energy Sector Asset Management for Electric Utilities, Oil & Gas Industry*
3) *NIST SP 1800-2B – Identity and Access Management for Electric Utilities*