Var Group Advisory, l'approccio integrato per la cybersecurity delle infrastrutture

di Davide Grassano, CEO Var4Advisory

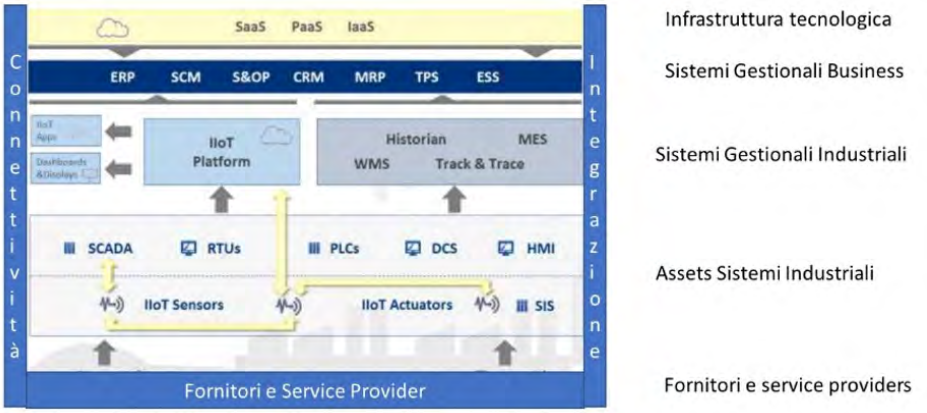
Var4Advisory S.p.A. è la società di Var Group per i servizi di Advisory focalizzata sui servizi di digital advisory e di sostenibilità e resilienza ed è partner aderente al global success program di IFS.

In ambito cybersecurity, supporta i clienti con un approccio Risk based Integrato che coniuga le molteplici esigenze di sicurezza dal rispetto delle normative attraverso l'integrazione e la razionalizzazione dei controlli in essere alla gestione dei rischi finalizzata ad indirizzare, a valle di un'attività di assesment preliminare, gli investimenti in modo mirato e puntuale. Supportiamo i clienti nell'adozione di standard di sicurezza informatica con attenzione alla convergenza di ambienti IT, IoT e OT che richiedono ormai un approccio integrato e tecnologie innovative per garantire sicurezza e continuità dei processi di business.

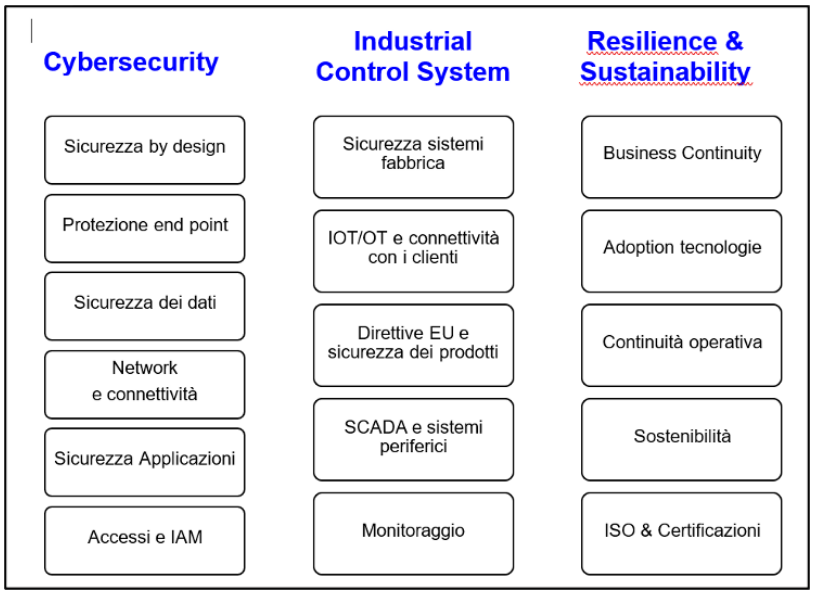
La gestione della convergenza IT, IoT/OT

Nell'attuale contesto, l'integrazione tra OT (Operation Technology) e IT (Information Technology) è diventata sempre più necessaria. Il processo di digitalizzazione, accelerato anche dal COVID in diversi settori e in particolare nel settore industriale, sta accelerando la progettazione di sistemi integrati e interconnessi IoT/OT e IT che si scambiano informazioni e dati. Come risultato vi è sempre più dipendenza tra infrastruttura tecnologica e sistemi gestionali dai sistemi industriali e dagli asset sottostanti IoT/OT.

La conseguenza è che un attacco informatico, un sabotaggio fisico o un default di asset è oggi in grado di avere gravi ripercussioni sulla continuità produttiva, sui sistemi gestionali e logistici e su tutte quelle componenti che oggi rappresentano dei veri fattori abilitanti per l'attività di produzione.



L'Interconnessione di sistemi vulnerabili, come ad esempio i sistemi Scada o altri dispositivi non sicuri, amplifica le debolezze e le vulnerabilità di quei sistemi, che in passato rimanevano segregati nel proprio perimetro, ma che ora sono interconnessi comportando rischi molto più elevati.
Per questo motivo, è necessario approcciare la sicurezza dell'intera infrastruttura, oggi evoluta in eco-sistema, non limitandosi ad analizzarla nelle singole componenti ma con un approccio olistico in grado di gestire in maniera integrata i processi aziendali.
Pertanto, quando i sistemi e i dispositivi OT IoT sono connessi in ambienti IT, la sicurezza informatica si declina nella protezione della disponibilità, dell'integrità, dell'affidabilità, della produttività e della sicurezza dei dispositivi fisici stessi.
Nell'ottica di fornire un'efficace sicurezza informatica con protezione end-to-end, **Var Group** ha sviluppato un framework di cybersecurity finalizzato ad indirizzare i piani evolutivi dei processi e delle tecnologie aziendali per ridurre al minimo l'esposizione ai rischi e contenere le minacce e le vulnerabilità a cui sono soggette oggi le Aziende.
Il Framework Var Group analizza le seguenti aree:



Gli industrial control system (ICS) sono sistemi che consentono di monitorare la salvaguardia dei sistemi di controllo industriale. L'hardware e il software integrati sono progettati per monitorare e controllare il funzionamento dei macchinari e dei dispositivi associati negli ambienti industriali, nonché le reti, i controlli utilizzati per azionare e/o automatizzare i processi industriali o servizi gestiti sul territorio con il supporto di dispositivi interconnessi. A seconda del settore, ogni ICS funziona in modo diverso e sono progettati per gestire digitalmente i processi di business. Oggi i dispositivi e i protocolli utilizzati in un ICS sono utilizzati in quasi tutti i settori industriali e infrastrutture critiche dalle industrie manifatturiere, dei trasporti, dell'energia e utilities.

Esistono diversi tipi di IACS, i più comuni dei quali utilizzano i sistemi SCADA (Supervisory Control and Data Acquisition) e i sistemi di controllo distribuito (DCS). Le operazioni locali sono spesso controllate da Field Device che ricevono comandi di supervisione da stazioni remote e gestiscono eventi sulla base di dati acquisiti con dispositivi sul campo.

La roadmap per i sistemi IACS

Var Group supporta i clienti nel definire la road map nell'adozione di sistemi IACS, coprendo tutte le aree in ambito: dalla gestione degli asset alla continuità operativa individuando con i nostri clienti strategie, modelli operativi, soluzioni e servizi necessari a rendere sicuri e resilienti i processi aziendali.

Sicurezza e gestione IACS e adozione standard IEC 62443

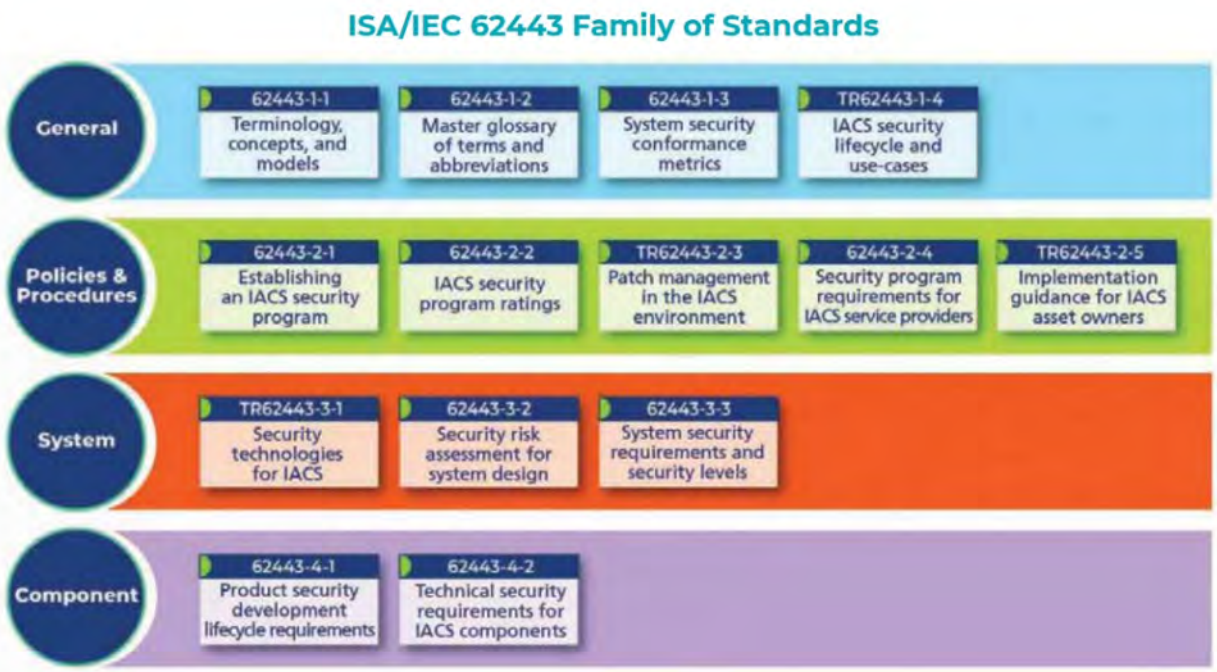
L'adozione dello Standard IEC 62443, lo standard internazionale specifico per la sicurezza dei sistemi di controllo industriale orientata al mondo dell'automazione dei sistemi IoT e OT e dispositivi correlati, risulta fondamentale per quelle organizzazioni caratterizzate da una struttura organizzativa complessa o che gestiscono infrastrutture distribuite o processi produttivi multi site.

Lo standard IEC 62443 è un insieme di 12 norme che coprono e definiscono diversi requisiti di sicurezza di un sistema ICS e si riferiscono a: COMPONENTI, SISTEMI, NORME E GESTIONE DEL SISTEMA, MISURE GENERALI di prevenzione e protezione.

Queste norme sono orientate alla necessità di progettare i sistemi di controllo industriali con buone pratiche di cybersecurity, in modo da rendere questi sistemi robusti e resilienti.

La norma adotta un approccio basato sul rischio per prevenire e gestire i rischi per la sicurezza nelle proprie attività.

- Generale: tratta argomenti comuni all'intera serie.
- Politiche e procedure: tratta i metodi e i processi associati alla sicurezza IACS.
- Sistemi: tratta i requisiti a livello di sistema.
- Componenti: tratta e definisce i requisiti dettagliati per i prodotti IACS.



L'adozione della norma IEC 62443 aiuta a proteggere i sistemi di controllo industriale durante tutto il loro ciclo di vita dalle minacce, quali blocco degli impianti, attacchi informatici e fisici che causano l'interruzione della operatività con l'obiettivo di garantire la "safety" dell'impianto, insieme alla confidenzialità, disponibilità ed integrità dei dati che vengono utilizzati nello stesso.

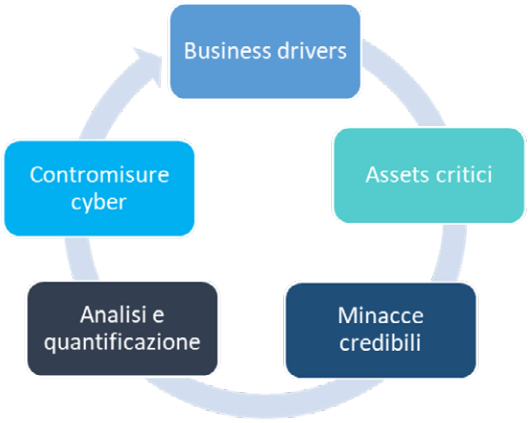
Analisi dei rischi e il livello di sicurezza in ambito IACS

L'analisi dei rischi identifica le vulnerabilità presenti nei device dell"infrastruttura di rete e consente la definizione di specifiche contromisure in funzione del livello di rischio di business adottando livelli di sicurezza differenziati per categorie di asset.

I livelli di sicurezza previsti in funzione dei rischi rilevati si catalogano nei seguenti:

- Livello di sicurezza 0: nessun requisito o protezione speciale richiesta.
- Livello di sicurezza 1: protezione contro l'uso improprio non intenzionale o accidentale.

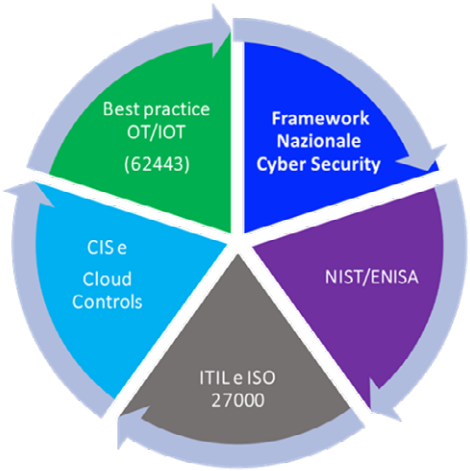
• Livello di sicurezza 2: protezione contro l'abuso intenzionale con mezzi semplici con poche risorse, competenze generali e scarsa motivazione.
• Livello di sicurezza 3: protezione contro l'uso improprio intenzionale con mezzi sofisticati con risorse moderate, conoscenza specifica dell'IACS e motivazione moderata.
• Livello di sicurezza 4: protezione contro l'uso improprio intenzionale utilizzando mezzi sofisticati con ampie risorse, conoscenze specifiche IACS e alta motivazione.



Gli elementi analizzati in questa fase di analisi puntano all'adozione di modelli di zone e conduit per segregare e ridurre i rischi di attacco di asset critici, adottando misure di sicurezza che si possono sintetizzare come segue:
• Definizione di zone e sub-zone
• Definizione di conduit per la comunicazione tra zone
• Attribuzione del target security level alle zone/conduit
• Definizione di policy sicurezza specifiche per le diverse zone
• L'analisi dei rischi dei dispositivi e individuazione GAP
• Tecniche di mutua autenticazione
• Definizione di policy per gli asset non controllati direttamente
• Cifratura selettiva
• Identity Management Asset
• Monitoraggio traffico dei sistemi IoT/OT

L'analisi dei rischi IT

Il framework Var Group include anche l'analisi della componente IT recependo gli standard e le linee guida del NIST (National Institute of Standards and Technology) ed utilizzando Framework Nazionale Cyber Security dell'ENISA (Agenzia dell'Unione europea per la cybersicurezza), introdotto dalla recente normativa nazionale sulle infrastrutture critiche.
Il framework utilizza un sistema di Business Intelligence che può essere opzionalmente integrato anche con i framework ITIL, ISO 27000 e con il Cloud Controls Matrix e il framework CIS (Center for Internet Security) Control CIS (Center for Internet Security) Control.



Road map per adeguamento di entità nel perimetro di sicurezza nazionale

Per le infrastrutture critiche definite alla luce della recente normativa, **Var Group** renderà disponibile una road map in grado di rispondere ai nuovi requisiti derivanti dalla normativa EU e relativa normativa di attuazione.