Progettare Sicurezza - Un Caso Aziendale

Date : 29 novembre 2016

PROGETTARE SICUREZZA

L’argomento sicurezza è abbondantemente trattato sotto molteplici punti di vista da quello normativo a quello della consulenza. E’ consolidata una definizione di Security Management in cui si indicano le attività manageriali relative alla gestione di un generico rischio riguardante un generico asset, dalla individuazione, alla valorizzazione, alla definizione di azioni di mitigazione o di riduzione degli impatti. Come esempi della vastissima letteratura esistente possono essere citate le norme ISO 27001 e seguenti [1], scritti che traducono riflessioni normative in modelli applicativi come [2], raccolte di osservazioni specifiche sugli impianti e di interessanti spunti per la costruzione di best practices [3], scritti sull’Enterprise Risk Management [4], [5] o sul Project Risk Management [6].

Sono state altresì proposte diverse articolazioni del concetto di sicurezza al fine di ridurre il campo di analisi dei rischi e il set di tecniche e strumenti per fronteggiarli adeguatamente. Questa suddivisione dei rischi inerenti la sicurezza, unitamente ad una riduzione del campo di indagine, per settori industriali piuttosto che per tipi di attività svolte, consente di trattare in modo approfondito i rischi e i relativi parametri di valutazione. La strada della riduzione dell’ambito di applicazione del concetto di sicurezza appare indubbiamente quella che consente di “maneggiare” meglio le azioni da svolgere, le tecniche e le tecnologie da adottare.

Partire da un contesto aziendale circoscritto appare utile e produttivo di risultati che non siano la mera elencazione di concetti già talmente consolidati da apparire ovvi. In specifico verrà preso in considerazione il caso di Tecnica Elettronica S.p.A. azienda localizzata in Veneto che da oltre 30 anni:

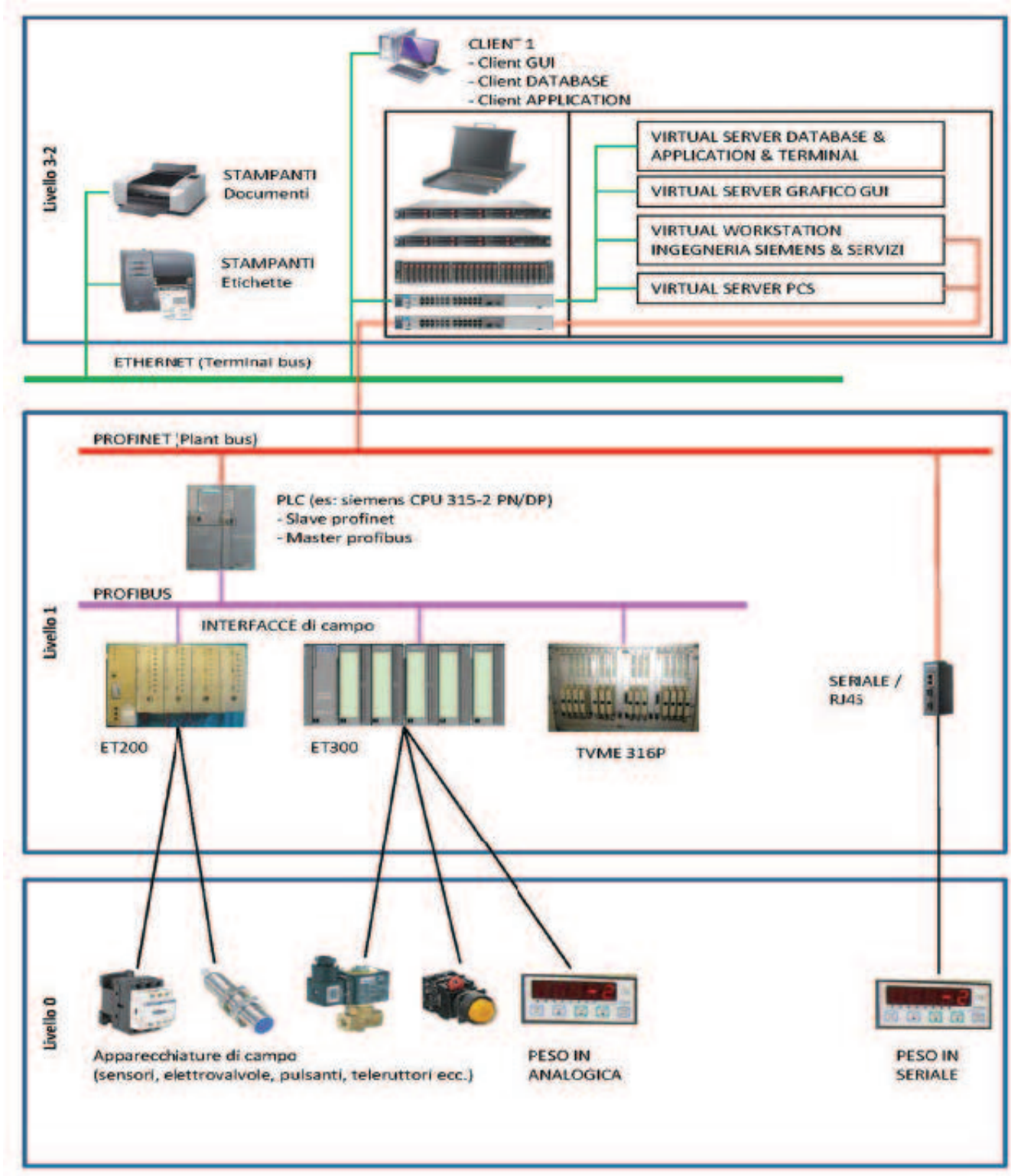
- progetta, realizza, manutiene, dismette sistemi automatici di produzione in differenti settori industriali. E’ leader nell’agroalimentare e, in particolare, nei mangimifici;
- progetta, realizza, manutiene sistemi automatici di programmazione e controllo di impianti di Power Generation, dalle biomasse alla cogenerazione al geotermico;
- collabora con i propri clienti lungo tutto il ciclo di vita degli impianti: dalla valutazione preliminare di fattibilità tecnica ed economica, alla progettazione di massima e di dettaglio, all’acquisto di beni e servizi, alla supervisione all’installazione e al collaudo,

alla manutenzione ordinaria, straordinaria ed evolutiva, al revamping, al decommissioning.

Nel corso della sua attività l’azienda ha sviluppato propri metodi e tecnologie proprietarie sia hardware che software, ma è in grado, su richiesta del cliente e sulla base delle caratteristiche dell’impianto, di integrare i propri metodi e le proprie tecnologie con quelle di terzi. I sistemi, progettati e realizzati su specifiche dei clienti, si concentrano prevalentemente in tre settori: Agroindusriale, Power Generation, Process & Factory.

Per quanto riguarda il Security Management, l’ambito di interesse dell’azienda è, in genere, la sicurezza dei sistemi di programmazione e controllo di impianti di produzione automatizzati. Spesso la progettazione del sistema di programmazione e controllo e la progettazione dell’impianto produttivo procedono di pari passo e i problemi relativi alla sicurezza possono essere allocati all’uno o all’altro dei due sistemi.

Un esempio tipico è la situazione “green field” o impianti in cui l’azienda ha maturato un’esperienza tale da proporsi come partner del cliente e, quindi, a risolvere gran parte dei problemi dell’impianto inclusi quelli relativi alla sicurezza. La struttura logico-fisica di un sistema di programmazione e controllo (SP&C) di impianti automatizzati di produzione è riportata in Figura 1 sino al confine con le macchine e le apparecchiature che eseguono il processo produttivo. Il sistema di programmazione e controllo è inserito all’interno di un impianto produttivo e svolge un ruolo di “comando” che richiede un elevato livello di interfacciamento con le operazioni svolte dall’impianto.



Il sistema di programmazione e controllo è costituito da un insieme di moduli, software e/o hardware tra loro interconnessi in un’architettura complessa. Una parte rilevante dei moduli software che realizzano le funzioni più critiche dell’impianto è stata sviluppata dall’azienda. Alcuni moduli sono connessi, tramite interfacce, ai sistemi informativi dell’azienda cliente da cui

sono importate ed in cui vengono esportate informazioni relative al piano di produzione e al suo avanzamento, al prodotto e alla sua composizione, nonché ai principali KPI (Key Performance Indicator) dell'impianto produttivo.

Progettare la sicurezza di un sistema di programmazione e controllo vuol dire disporre di un metodo del tipo Design For X (DFX), nel caso specifico di un metodo di Design For Security che:

- precisi il concetto di sicurezza articolandolo in temi coerenti con la struttura logico fisica del sistema di programmazione e controllo e della sua interazione con il sistema produttivo;
- consenta di suddividere le responsabilità in relazione alla sicurezza tra il progettista del sistema di programmazione e controllo e il progettista dell'impianto produttivo;
- si articoli in procedure, regole tecniche e tecnologie applicabili da parte del progettista del SP&C per definire e garantire la sicurezza dello stesso durante l'intero ciclo di vita dell'impianto produttivo;
- supporti la manutenzione e lo sviluppo degli strumenti operativi per la gestione della sicurezza;
- faciliti i processi di approfondimento in tutte quelle situazioni in cui le competenze disponibili sono insufficienti.

RESPONSABILITÀ

Il confine delle responsabilità è uno degli argomenti nella definizione del progetto in quanto determina quali funzioni relative alla sicurezza fanno parte dello scope of work del progetto affidato all'azienda, quali sono da interfacciare e quali quelle su cui non si deve intervenire.

Il confine delle responsabilità è, nella gran parte dei casi concreti, definito con riferimento a tre elementi di base:

1) gli item (o componenti) che costituiscono il concetto di sicurezza. Come si vedrà successivamente le componenti della sicurezza prese in considerazione sono: funzionale, fisica, informativa.

2) oggetto della sicurezza costituito dall'insieme degli asset fisici o intangibili residenti nell'impianto la cui sicurezza è garantita dall'azienda. In genere sono gli asset che costituiscono il sistema di programmazione e controllo specificati a livello contrattuale. L'elenco degli asset può essere desunto, nelle prime fasi del progetto dal contratto o dall'offerta e, successivamente modificato in funzione delle esigenze.

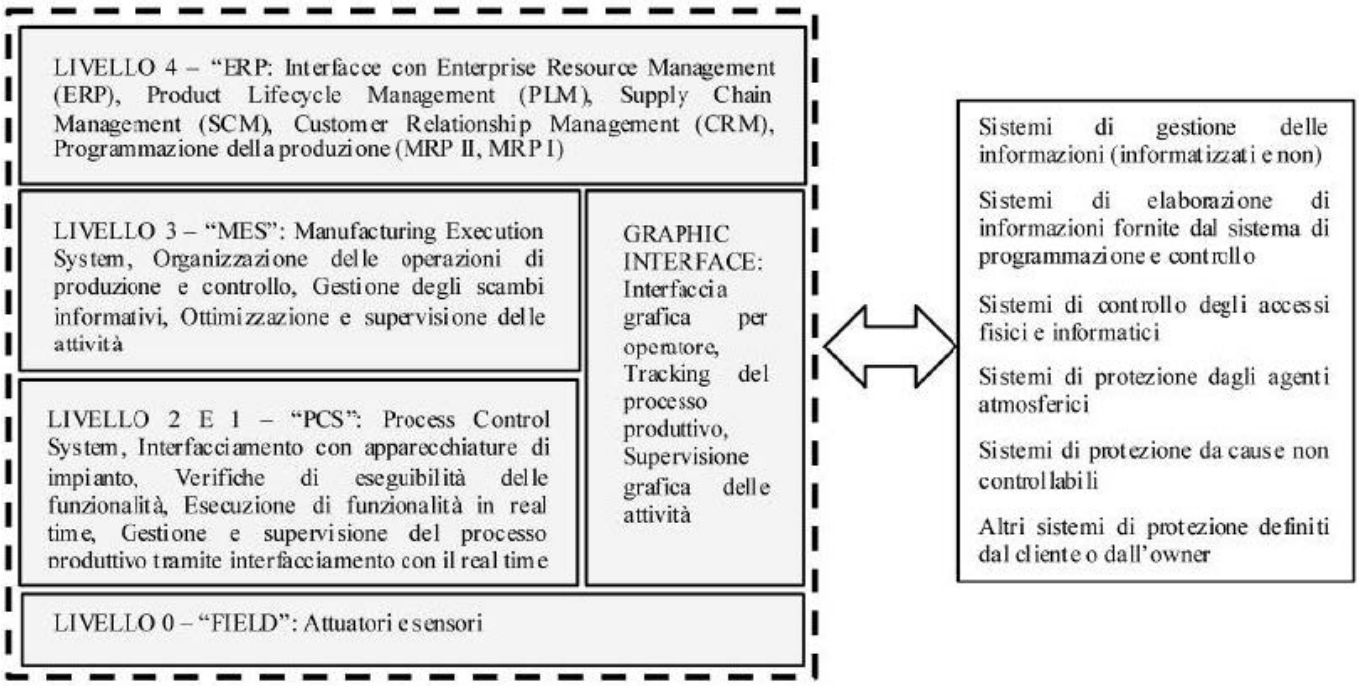
3) il ciclo di vita del sistema di programmazione e controllo o dell'impianto nel caso coincidessero.

Le responsabilità aziendali si esercitano durante:

a) il progetto (fase EPCC – Engineering, Procurement, Construction, Commissioning) [7] su tutti gli asset di cui al punto 2 precedente;

b) la fase di Produzione su tutti gli asset di cui al punto 2 precedente:

c) l'erogazione dei servizi di assistenza e manutenzione limitatamente alle informazioni del cliente residenti presso l'azienda.



La struttura funzionale di più alto livello del sistema di programmazione e controllo è presentata in Figura 2. E' qui definito tramite un bordo tratteggiato l'ambito in cui l'azienda esercita in genere le proprie responsabilità in merito alla sicurezza. La freccia indica eventuali collegamenti tra il sistema di programmazione e controllo e altri sistemi ad esso esterni che presidiano il tema sicurezza. La freccia è in genere costituita da interfacce che gestiscono flussi di informazioni. Tra i servizi relativi alla sicurezza che l'azienda è in grado di progettare e gestire è presente l'acquisizione e la conservazione delle informazioni trasmesse dai sistemi di sicurezza esterni al sistema di programmazione e controllo. Queste informazioni sono inserite tra i KPI in quanto la sicurezza è una delle funzionalità dell'impianto e quindi va prevista un'adeguata e continuativa documentazione [8].

Anche se il confine va definito caso per caso, l'azienda dispone o deve disporre di tutti gli strumenti organizzativi e tecnologici che le permettano di garantire la sicurezza del sistema di programmazione e controllo indipendentemente da quanto è disponibile presso il cliente e nello specifico impianto produttivo.

ARTICOLAZIONE DEL CONCETTO DI SICUREZZA

La scomposizione del concetto di sicurezza adottato all'interno dell'azienda è: sicurezza funzionale, sicurezza fisica, sicurezza informativa. Ciò deriva dalla compresenza di strumenti hardware e software (cfr. Figura 1) e dal peso che le informazioni hanno all'interno del sistema (cfr. Figura 2) e determina le aree disciplinari da esplorare per identificare gli elementi rilevanti per la sicurezza quali minacce, tecnologie, procedure.

Sono rilevanti, in questo caso, due aree disciplinari. La prima è la sicurezza informativa in quanto il sistema di programmazione e controllo è un sistema di gestione delle informazioni, la seconda è la sicurezza degli impianti industriali controllati tramite DCS (Distributed Control System) [8]. Sicurezza funzionale La sicurezza funzionale ha lo scopo di garantire al cliente (o al gestore dell'impianto di produzione) il corretto funzionamento del sistema di programmazione e controllo come una delle condizioni del funzionamento dell'intero impianto di produzione.

L'azienda articola la verifica della sicurezza funzionale in tre fasi:

1) Avvio (o riavvio) dell'impianto di produzione. In questo caso la verifica è del tipo ready to use. Tramite opportune procedure vengono interrogati i componenti hardware e software del sistema di programmazione e controllo e vengono analizzate le risposte. Lo stato del sistema può essere archiviato;

2) Funzionamento della produzione. Questo è uno dei compiti del sistema di controllo della produzione. Le informazioni sullo stato del processo produttivo e sull'impianto vengono comunicate ad un supervisore che può o correggere il comportamento dell'impianto o allarmare nel caso che uno o più parametri siano al di fuori di un range previsto. In molti casi si adopera un supervisore grafico basato su un sinottico dell'impianto;

3) Fermata, in questo caso vengono registrati tutti i dati che, al successivo riavvio, consentiranno di procedere alla verifica che il sistema di programmazione e controllo non è stato modificato durante la fermata sia per errate operazioni sia per eventuale dolo.

Tramite l'inserimento di opportune funzioni è possibile estendere la verifica funzionale a parti dell'impianto esterne al sistema di programmazione e controllo predisponendo, in fase di progettazione, appositi moduli software, le necessarie connessioni e i sensori. A titolo di esempio potrebbe essere verificato il funzionamento di uno strumento di analisi delle emissioni gassose o liquide che, normalmente, non è connesso al sistema di programmazione e controllo.

Sicurezza fisica

Ha l'obiettivo di salvaguardare gli asset materiali che costituiscono il sistema di programmazione e controllo e, quindi, di proteggere le diverse aree "geografiche", impedendo accessi non autorizzati, danni e interferenze agli ambienti, e di proteggere gli apparati mediante la prevenzione di perdite, danni, manomissione degli investimenti.

Per molti beni, la sicurezza fisica coincide con la sicurezza patrimoniale ossia la certezza di mantenimento del valore del bene nel tempo. Esiste una sovrapposizione tra sicurezza fisica e

funzionale, ma in un impianto quale quello di Figura 1 esistono delle differenze. Il caso delle reti di comunicazione è emblematico, alla integrità fisica della rete potrebbe non corrispondere un corretto funzionamento della stessa. Nel caso degli impianti la sicurezza fisica è demandata alle procedure di progettazione che debbono prevedere, in funzione del contesto in cui l'impianto opera, apposite soluzioni per fare fronte ai rischi. Rispetto a questo caso, i sistemi di programmazione e controllo non presentano differenze significative rispetto ad altri tipi di impianto.

Sicurezza informativa

Riguarda la sicurezza delle informazioni che entrano ed escono dal sistema di programmazione e controllo e che circolano al suo interno tra i componenti che lo costituiscono.

Esiste un'ampia letteratura in merito da cui in estrema sintesi si possono estrarre tre concetti:

- salvaguardare integrità, riservatezza e disponibilità delle informazioni;
- identificare le minacce specifiche rilevanti nel contesto siano esse interne o esterne, volontarie o involontarie;
- ridurre o eliminare le vulnerabilità del sistema.

La sicurezza informativa, secondo l'azienda, è al momento attuale quella di maggiore criticità e di interesse per vari motivi:

- la sicurezza funzionale e la sicurezza fisica sono già ampiamente "assorbite" nell'ambito delle procedure di progettazione;
- l'interconnessione delle reti informatiche e l'integrazione tra elaborazione e comunicazione consentono un accesso a punti rilevanti del sistema di programmazione e controllo che, per sua natura può contenere informazioni riservate, per tutti valga l'esempio della ricetta di produzione o della distinta base di un prodotto;
- la possibilità, attraverso una violazione del sistema di programmazione e controllo di accedere ad un set di "comandi eseguibili" con possibilità di produrre danni anche con una limitata conoscenza dell'impianto produttivo;
- il mantenimento delle informazioni per lunghi periodi di tempo che risulta talvolta poco compatibile con l'uso di tecnologie di gestione in rapido sviluppo.

Uscendo dal contesto aziendale, il caso Stuxnet, ampiamente trattato in letteratura, ha fornito un quadro drammatico delle caratteristiche e delle capacità di aggressione agli impianti tramite le infrastrutture di elaborazione e comunicazione [9], [3].

Di particolare interesse, inoltre, sono le informazioni di proprietà del cliente che, per esigenze legate alla progettazione, all'assistenza e alla manutenzione, sono residenti nei sistemi informativi di Tecnica Elettronica.

APPROCCIO ALLA SICUREZZA: DESIGN FOR SECURITY

La definizione delle procedure, delle regole e degli strumenti tecnici e tecnologici per inverare il Design For Security richiede di dare uno sguardo a come il tema della sicurezza viene affrontato nella letteratura e nella pratica manageriale.

Le metodologie che affrontano il tema della sicurezza, come dimostra anche l'analisi delle norme e delle linee guida presentata successivamente, fanno riferimento alla disciplina del Risk Management che, in estrema sintesi, prevede:

- la disponibilità di una descrizione accurata del comportamento atteso del sistema in termini di funzionalità e di performance. Alcuni autori definiscono questa descrizione come un attributo di qualità dell'output denominata "qualità teorica" [10]. Nel caso del Risk Management non viene di solito usato un termine così forte e sintetico e la "qualità teorica" è costituita da mappe di rischio o da database descrittivi dei rischi o da elenchi di rischi da tenere sotto controllo, dai relativi modelli di valutazione dei rischi e dalle modalità con cui affrontarli;
- la possibilità di rilevare il comportamento effettivo del sistema. Ciò può essere fatto o tramite audit specifici o verifiche cadenzate dei processi o tramite misure continue come nel caso dello Statistical Process Control. Questo metodo è utilizzato ampiamente per i sistemi "certificati". Il Risk Management prevede, in generale, un aggiornamento dei parametri che descrivono il rischio. Ad esempio, nel caso dei progetti, si possono aggiornare le mappe dei rischi in funzione dell'avanzamento del processo o a fronte di determinati eventi [11];
- correzione dei modelli di progettazione o dei modelli di funzionamento dei processi. Ciò è fatto a seguito delle segnalazioni di cui al punto precedente. I modelli dei rischi, comunque costruiti, vanno aggiornati sulla base delle misure effettuate o degli eventi registrati. Ad esempio, nel caso che i parametri descrittivi di un rischio siano la probabilità di accadimento e l'impatto sulle attività o sul prodotto, la probabilità può essere modificata sulla base del numero di volte che un evento accade. Il modello di previsione del comportamento atteso può essere modificato di conseguenza.

Il comportamento atteso di un prodotto o di un impianto è definito durante la sua progettazione. E' in questa fase infatti che si definiscono le funzioni che il prodotto o il sistema devono realizzare (funzionalità), le performance che il prodotto o il sistema deve garantire, i rischi che queste performance non siano garantite nel ciclo di vita del prodotto o del sistema e le attività che devono essere svolte per ridurre i rischi.

La gestione dei rischi comincia durante la progettazione e accompagna il prodotto o il sistema lungo tutto il suo ciclo di vita. Molti di questi concetti legati alla qualità del prodotto o dei sistemi, alla esplorazione del comportamento lungo l'intero ciclo di vita, alla "anticipazione" in fase di progettazione attraverso attività di simulazione o di calcolo dei rischi sono elementi costituenti dei metodi di anticipazione e sono stati "raccolti", formalizzati e sviluppati nell'ambito del Concurrent Engineering [12], [13].

Molti di questi metodi sono stati definiti con il termine Design For X dove la X sta per una funzione o una caratteristica o una performance del prodotto o del sistema. Esempi molto citati sono il DFM (Design for Manufacturing), DFA (Design for Assembly), DFR (Design for

Reliability), DFC (Design for Recycling).

Nel caso della sicurezza in azienda è stato sviluppato un Design For Security supportato da uno strumento informatico, al momento in forma prototipale, che ha lo scopo di rendere più agevole e strutturata l'individuazione, la raccolta, la classificazione, la definizione dei controlli o, in generale, delle azioni atte a mitigare i rischi relativi alla sicurezza.

Il metodo:

- si basa sul Risk Management e, in particolare, adotta un modello di rischio elementare ampiamente usato nella letteratura specialistica;
- è focalizzato su una particolare e specifica "prestazione" del sistema: la sicurezza così come definita in precedenza;
- consente di individuare i rischi legati ad uno specifico impianto/sistema tramite la sua traduzione in funzioni e in asset e quindi sulla base di un modello gerarchico espandibile secondo le esigenze;
- consente di associare a ciascun rischio identificato le cause che lo possono determinare, in particolare le minacce che inficiano la sicurezza e gli effetti sul sistema tramite l'esplicitazione delle vulnerabilità;
- obbliga alla definizione di azioni di controllo che possono ridurre o eliminare le cause o gli effetti del rischio;
- si adopera nella fase di progettazione del sistema e, tramite l'interlocuzione con il cliente, definisce i rischi osservando il ciclo di vita del sistema.

Il Design For Security messo a punto è un complesso di cultura, conoscenze, procedure, ruoli, tecniche e tecnologie per garantire la sicurezza nel ciclo di vita del sistema di programmazione e controllo e, in molti casi, dell'impianto. Ciò ha richiesto uno sforzo considerevole di analisi in cui il contributo proveniente dall'interno dell'azienda è, per sua natura, limitato dalla cultura aziendale sui rischi, dal tipo di progetti e di clienti con cui si è interagito e, spesso, dalle dimensioni e dalla possibilità di investire [14]. L'ampiezza dell'analisi effettuata è però foriera di risultati "robusti" in grado cioè di resistere nel tempo alle mutazioni dello scenario dei progetti aziendali se supportati da idonei processi di aggiornamento.

La manutenzione e l'evoluzione dei metodi di Design For Security d'altra parte richiede che essi siano parte integrante delle piattaforme aziendali in modo da poter essere al centro dei processi di innovazione.

RISULTATI DI UNA RICERCA

L'azienda ha definito politiche, procedure, ruoli, strumenti e tecnologie per progettare la sicurezza nei sistemi di programmazione e controllo rilasciati al cliente e, spesso, interfacciati con sistemi di terzi, nel corso di un progetto finanziato dalla Regione Veneto, dal titolo "Ricerca e sperimentazione di innovativo sistema integrato di automazione industriale ad ampia accessibilità ed alto grado di sicurezza".

La prima fase del progetto è consistita in una ricerca sulle norme, linee guida, best practices esistenti e raggiungibili sulla sicurezza di cui vengono riportati i risultati principali suddivisi in tre argomenti:

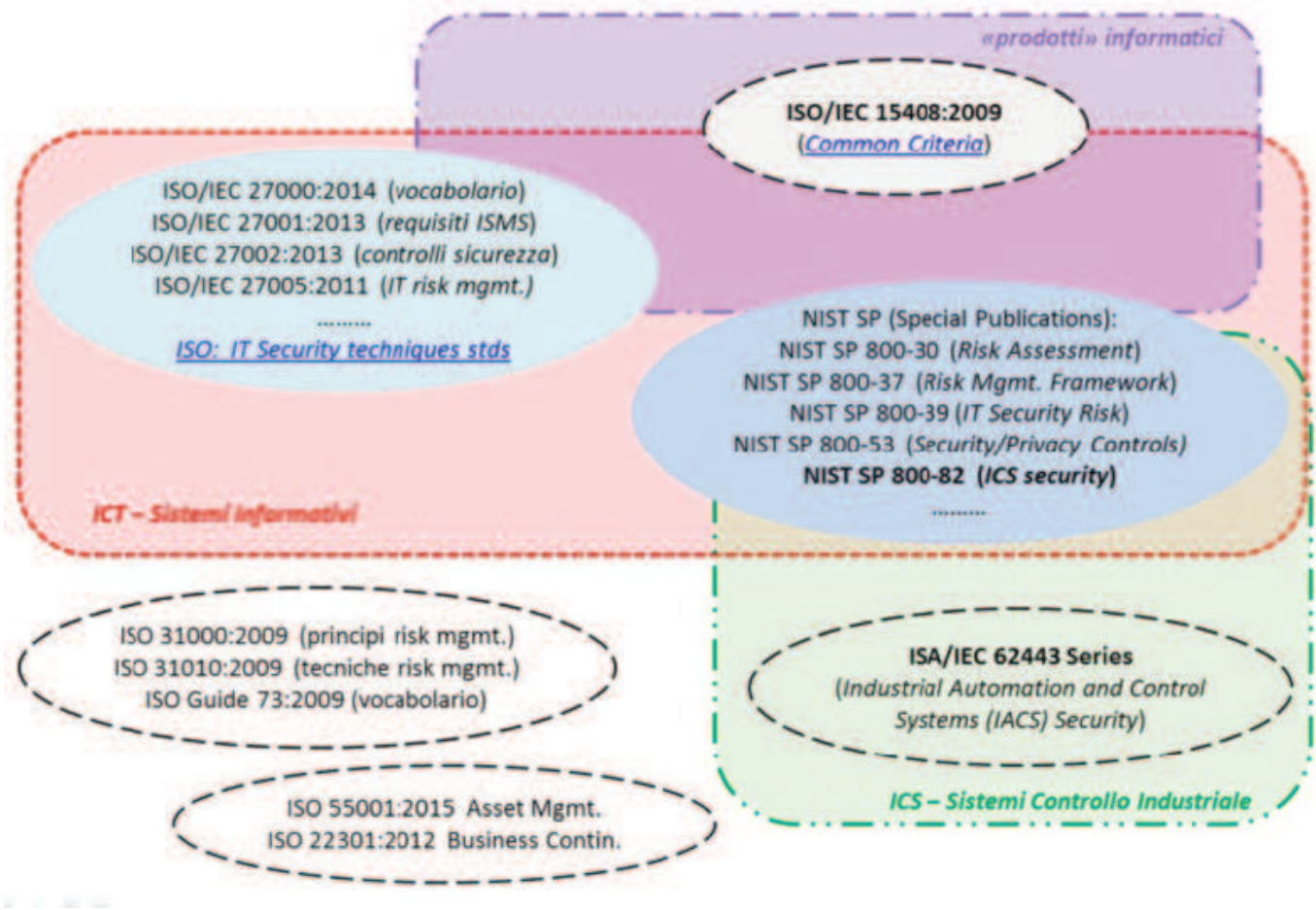
- il campo di esplorazione della ricerca ossia l'insieme delle norme, linee guida e best practices analizzate;
- il modello di analisi e intervento per il Risk Management suggerito da quanto trovato nel "campo di esplorazione";
- il modello di valutazione qualitativo e quantitativo dei rischi.

IL CAMPO DI ESPLORAZIONE

Per qualunque ambito disciplinare, il campo delle norme, linee guida e best practices applicabili è spaventosamente esteso ed è già un'attività onerosa tenersi aggiornati [8].

L'esplorazione ha identificato quattro ambiti applicativi di interesse aziendale:

- la sicurezza dell'informazione (ICT – Sistemi Informativi in Figura 3) considerabile una base di partenza in quanto focalizzata sulla difesa dell'oggetto "informazione" durante tutti i processi ed entro qualunque sistema che ne effettui la trasmissione, l'elaborazione e la conservazione;
- la sicurezza del software inteso come "prodotto" (prodotti informatici in Figura 3) ossia le caratteristiche che un software deve possedere per garantire la sicurezza dell'informazione;
- la cyber-security nei sistemi di controllo industriale (ICS – Sistemi Controllo Industriale in Figura 3) che adegua principi e tecniche della sicurezza dell'informazione alle specificità dei sistemi di controllo industriale (dagli SCADA, ai DCS, ai PLC);
- le norme e le linee guida di carattere generale che descrivono sistemi di gestione "trasversali", orientati al Risk Management, alla Business Continuity, alla gestione degli asset.



La Figura 3 riporta le famiglie di norme e pubblicazioni tecniche riconosciute come fondamentali in letteratura e dai professionisti del settore; permette inoltre di intuire le forti interrelazioni e sovrapposizioni fra gli ambiti identificati.

Per quanto riguarda la sicurezza dell'informazione, la maggiore notorietà riguarda la "famiglia ISO 27000", composta da oltre 30 norme fra cui spiccano per diffusione i titoli legati al sistema di gestione della sicurezza dell'informazione:

- ISO/IEC 27000:2014, che introduce i concetti basilari e ne formalizza le definizioni. Questo è al momento l'unico standard della famiglia disponibile gratuitamente;
- ISO/IEC 27001:2013, che esplicita i requisiti obbligatori per impostare un Sistema di Gestione per la Sicurezza dell'Informazione certificabile;
- ISO/IEC 27002:2013, che guida l'applicazione delle contromisure (controlli di sicurezza) elencate nell'Annex A di ISO/IEC 27001:2013.

Tali controlli di sicurezza devono obbligatoriamente essere presi in esame. In base al contesto specifico si può motivare l'aggiunta di ulteriori contromisure o la non applicabilità di alcuni dei controlli richiesti. Per ogni controllo di sicurezza è fornita una guida per l'implementazione. Il sistema definito da ISO/IEC 27001 è un'applicazione del Risk Management alla sicurezza delle informazioni. Il percorso proposto consiste, in estrema sintesi nell'impostazione di un Risk

Assessment da ripetere ad intervalli pianificati e nell'attuazione del conseguente piano necessario per trattare i rischi individuati.

Analizzando i controlli di ISO/IEC 27002:2013 risulta chiaro che essi non si limitano alla sicurezza dei soli sistemi ICT (la cosiddetta cyber security), ma si preoccupano di proteggere tutte le possibili forme assunte dall'informazione affiancando alle contromisure tecniche e tecnologiche anche opportune regole organizzative. I controlli, inoltre, non riguardano solo l'utilizzo di sistemi ICT, ma anche le attività di progettazione e realizzazione e toccano argomenti quali la conformità alla legislazione in tema di protezione dei dati personali, la gestione degli incidenti e la continuità operativa.

La sicurezza del "prodotto" software, (prodotti informatici in Figura 3) è oggetto del framework noto come Common Criteria (CC), descritto sul portale ufficiale www.commoncriteriaportal.org. Le pubblicazioni contenenti i requisiti sono reperibili liberamente sia sul portale sia entro il set ISO/IEC 15408. La certificazione secondo i Common Criteria non garantisce di per sé la sicurezza del prodotto, ma si limita a documentare formalmente i dettagli dell'iter di implementazione e valutazione del prodotto. L'onerosità di tale approccio ne ha di fatto frenato l'adozione diffusa [15], [16], pertanto anche l'azienda non ha ulteriormente approfondito la ricerca in quanto, per garantire la qualità del software da lei prodotto, fa riferimento a standard interni ampiamente consolidati e validati.

La cyber-security nei sistemi di controllo industriale (ICS – Sistemi Controllo Industriale in Figura 3), è autorevolmente affrontata da specifiche pubblicazioni del NIST (National Institute for Standard and Technologies) e dagli standard ISA/IEC-62443, sviluppati congiuntamente dal comitato ISA99 dell'International Society of Automation (ISA) e dal comitato TC65/WG10 di IEC. Le ISA/IEC 62443 si propongono di guidare le attività che garantiscono la security dei sistemi di automazione e controllo industriale nell'intero ciclo di vita [17]. Il relativo stato di aggiornamento è consultabile su http://isa99.isa.org/ISA99%20Wiki. La ricerca ha inoltre rilevato il crescente interesse degli enti normatori verso temi trasversali toccati anche all'interno delle norme e pubblicazioni sinora citate. Il Risk Management, ad esempio, è l'approccio con cui viene usualmente affrontata la sicurezza non solo informativa ed è oggetto del "tool" ISO composto dai requisiti generali ISO 31000:2009, dal vocabolario ISO Guide 73:2009 e dai riferimenti applicativi ISO 31010:2009.

La gestione degli asset, strettamente legata anche alla sicurezza fisica degli impianti, è trattata entro la famiglia "ISO 55000", mentre la business continuity, che completa la gestione del rischio indicando come reagire ad un evento distruttivo in modo da garantire un accettabile livello di produzione, è trattata in ISO 22301 e standard collegati. Come segnalato dalla Figura 3, fra gli ambiti identificati nell'esplorazione sono presenti sia sovrapposizioni che interrelazioni.

Le sovrapposizioni sono riscontrabili in uno stesso testo come nel caso della ISO/IEC 27001 che cita anche controlli utili a progettare e realizzare "prodotti" hardware e software nonché controlli per la gestione degli incidenti e la business continuity. L'esame delle pubblicazioni del NIST (National Institute for Standard and Technologies), e, in particolare la serie NIST SP-800 di "Special Publications" dedicate alla Computer Security, mostra come le sovrapposizioni tra ambiti applicativi siano state risolte attraverso la complementarietà dei contenuti e le

interrelazioni fra le varie pubblicazioni della serie stessa.

L’azienda ha reputato particolarmente interessanti le seguenti pubblicazioni NIST:

- SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations” che offre un catalogo di controlli di sicurezza assimilabile a quello contenuto in ISO/IEC 27002, da scegliere nell’ambito di un processo di risk assessment (ad es. come descritto da SP 800- 37);
- SP 800-82 “Guide to Industrial Control Systems (ICS) Security”, che applica agli ICS (Industrial Control Systems) i medesimi controlli di SP 800-53, indicando le sole modifiche, integrazioni o esclusioni derivanti dalle peculiarità dei sistemi di controllo industriale.

L’esplorazione di norme e letteratura svolta ha aumentato la consapevolezza aziendale sul cambiamento di prospettiva in atto per la sicurezza dell’informazione e per la sicurezza degli apparati di ICT inclusi nei sistemi di controllo industriale:

- la scelta del modello di sicurezza da adottare non può prescindere dalla consapevolezza delle differenze fra sistemi di ICT e sistemi di controllo industriale (ICS) esposte nella Tabella 2-1 di NIST SP 800-82 e proposte in modo incisivo da [3];
- l’integrazione fra le cosiddette reti di business e le reti industriali visibili in Figura 1, è via via crescente e ciò avvicina le “minacce” tipiche del mondo ICT al cuore del mondo dei sistemi di controllo industriale (ICS);
- il mito del “air gap” che separa gli ICS da ogni possibile cyber-attacco è crollato, basti pensare al wireless o ai dispositivi portatili (removibili/inseribili manualmente);
- gli attacchi nascono nelle risorse computazionali comuni, generalmente presenti ai livelli alti dell’architettura (cfr. Figura 1);
- alcune contromisure usuali dell’ICT security, ad esempio applicazioni antivirus “invadenti” o cicli di aggiornamento/patch frequenti/ automatici, non possono essere adottate senza alcuna avvertenza nei sistemi di controllo industriale;
- anche in presenza di risorse dello stesso tipo, ad esempio reti Ethernet, gli obiettivi dei sistemi ICT e dei sistemi industriali sono assai diversi.

L’azienda ha pertanto deciso di focalizzare l’attenzione sulla coppia di linee guida NIST, SP 800-53 e SP 800-82, in quanto:

- SP 800-82 adegua agli ICS i medesimi controlli di SP 800-53;
- SP 800-53 mette in relazione diretta i propri requisiti, e quindi anche quelli di SP 800-82, con i controlli previsti da ISO/IEC 27001 e 27002.

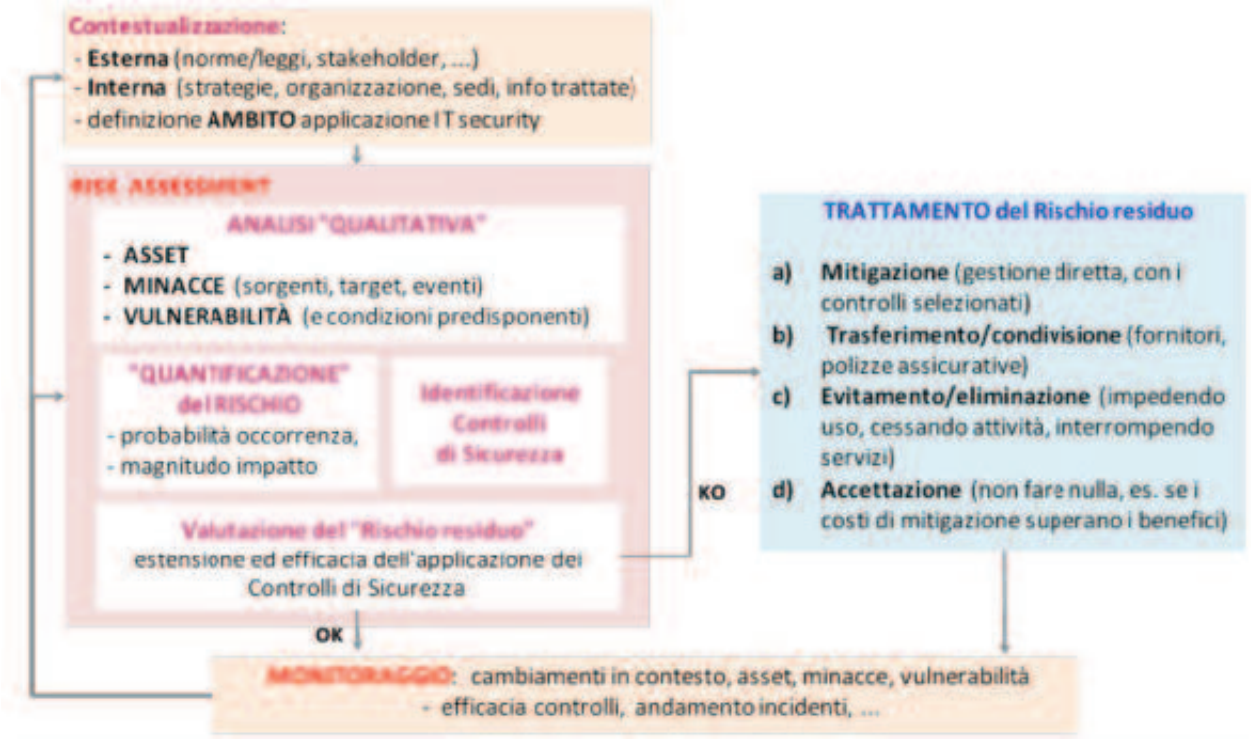
IL MODELLO DI ANALISI#INTERVENTO

Il processo di individuazione, qualificazione, monitoraggio dei rischi è stato definito sia per quanto riguarda il caso dei progetti sia per quanto riguarda il caso delle attività e dei processi routinari.

Durante l’esplorazione si sono incontrati diversi modelli di Risk Management:

- il RMF (Risk Management Framework) suggerito da NIST SP 800-37, NIST SP 800- 30 e adottato da NIST SP 800-53 / da NIST SP 800-82;
- il modello ISO 31000:2009 raccomandato da ISO/IEC 27001:2013;
- esemplificazioni di adozione o adattamento presenti in letteratura, ad esempio [3] e [2].

I modelli citati sono sostanzialmente compatibili tra loro. Gli elementi comuni sono stati estratti per comporre il modello adottato in azienda che viene esplicitato in Figura 4.



Una prima contestualizzazione ha permesso di riconoscere la presenza di due ambiti applicativi distinti:

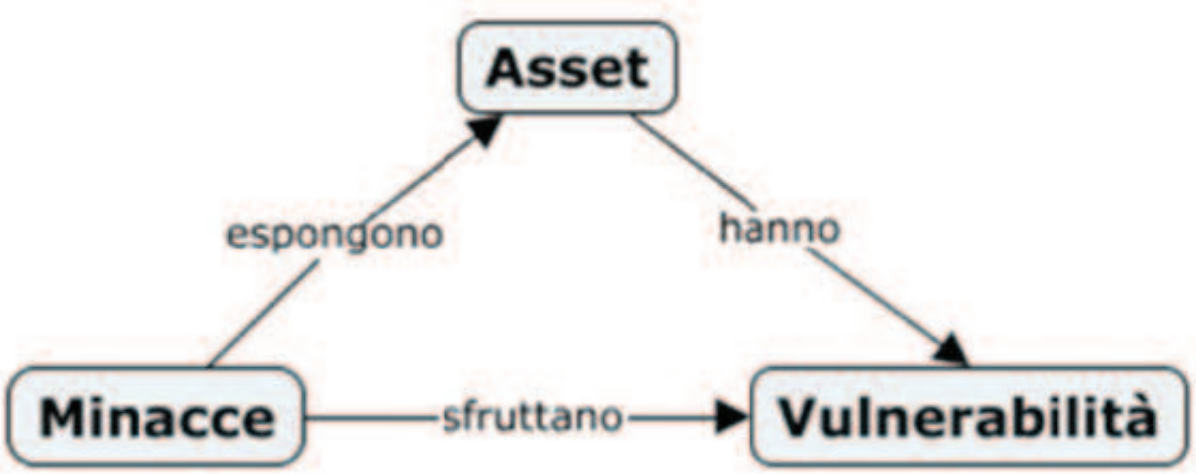
- i processi di tipo amministrativo e i relativi sistemi IT, con cui l’azienda tratta, presso la propria sede, le informazioni di interesse del cliente, sulle quali il cliente stesso può vantare specifiche esigenze di sicurezza. Di particolare interesse sono le attività di progettazione, manutenzione e assistenza;
- i sistemi di controllo degli impianti installati presso i clienti. Si tratta dell’ambito in cui è rilevante l’integrazione della IT security con la ICS security. Ad ogni sistema di controllo corrisponde uno specifico progetto.

Per quanto riguarda la fase di risk assessment sono state, al momento, implementate le attività di analisi qualitativa e di identificazione dei controlli di sicurezza. Qualche passo ulteriore verrà fatto per la valutazione quantitativa. Tutta la parte restante del processo è, di fatto, svolta all’interno del progetto di un impianto specifico, in collaborazione con il cliente.

All’inizio di ogni progetto viene eseguita una specifica fase di contestualizzazione il cui output è la definizione dei confini fra le responsabilità del cliente e dell’azienda. Per la realizzazione di questa fase l’azienda si avvarrà delle proprie procedure, delle conoscenze e delle tecniche e tecnologie di cui dispone.

LA VALUTAZIONE DEI RISCHI

La valutazione dei rischi, come mostrato dal modello presentato in Figura 4, inizia “qualificando” i rischi attraverso i fattori da cui dipendono: asset, minacce e vulnerabilità, che sono in relazione come indicato nello schema concettuale di Figura 5, ossia gli asset sono esposti a rischi a causa delle minacce che agiscono sfruttando le vulnerabilità presenti negli asset stessi.



Per quantificare i rischi si può ricorrere ad una “formula” del tipo [2]: (1) R(m, a, v) á p(m) * i(m, a) * g(v) in cui il rischio R(m, a, v), funzione della minaccia m, dell’asseta e del controllo c, è proporzionale alla probabilità di accadimento della minaccia p(m), all’impatto i(m, a) della minaccia sull’asset e alla gravità g(v) della vulnerabilità.

Prendendo in considerazione i controlli di sicurezza, siano essi organizzativi/procedurali, tecnici o tecnologici, e interpretandoli come “il reciproco” delle vulnerabilità, nel senso che un controllo di buon livello riduce una o più vulnerabilità del sistema, si può dare una formulazione alternativa della (1): (2) R(m, a, c) á p(m) * i(m, a) / r(c) dove r(c) è il rigore del controllo che può porre rimedio alla vulnerabilità.

Modellizzazioni dei rischi di questo tipo sono abbastanza comuni nel caso di Project Risk Management applicati all’impiantistica [18].

Asset

Durante l’analisi qualitativa sono stati individuati gli asset di interesse per i sistemi di programmazione e controllo progettati dall’azienda, ascritti alle seguenti categorie:

- Information Asset (informazioni), riferiti a processi e attività aziendali, quali, a titolo esemplificativo, offerta, progettazione e commissioning impianto del cliente, fasi successive del ciclo di vita dell'impianto del cliente, gestione di fornitori e forniture, gestione del personale interno, altri adempimenti da norme/leggi (fiscali, sicurezza luoghi lavoro, ambiente, …);
- Asset fisici e tecnologici, utilizzati per trattare le informazioni quali, ad esempio, sistemi e/o servizi informatici (CRM, gestionale, …), relativi archivi informatici, archivi cartacei aziendali, archivi cartacei/informatici presso esterni (commercialista, Medico Competente, …), infrastrutture e locali aziendali;
- Asset legati ai «prodotti TE»: sistemi/servizi informatici installati presso il cliente, che molto spesso coincidono con moduli software sviluppati ad hoc per un progetto.

Per quanto riguarda gli Information Asset è stato effettuato un primo censimento delle informazioni interne all'azienda, dal quale è emerso che la maggioranza delle informazioni appartiene all'ambito IT security, mentre una parte dei dati codificata come DCC (Dati Confidenziali Clienti) è in ambito ICS security.

Minacce

Le minacce possono provenire da ambienti esterni a quello considerato o da ambienti interni e possono essere determinate da dolo o da imperizia.

Partendo da quanto suggerito da NIST SP 800-82 e da testi quali [2] e [3] è stato realizzato un elenco di minacce adattato alle specifiche esigenze dei progetti aziendali. L'elenco presenta una struttura gerarchica i cui primi livelli sono:

- Azioni dolose, quali furto di informazioni, alterazioni/inserimento di informazioni, trattamenti scorretti;
- Azioni non autorizzate (non necessariamente malevole), ad esempio uso o accesso non autorizzato a strumentazioni, servizi e sistemi;
- Azioni accidentali, ossia attività errate, effettuate individualmente durante il normale lavoro;
- Strutturali, ad es. guasti a strumentazioni, controlli o software, causa invecchiamento, saturazione o altre condizioni inattese/anomale;
- Ambiente/infrastrutture (naturale/cause umane), ad es. disastri naturali o danni alle infrastrutture critiche da cui dipende l'organizzazione, ossia eventi fuori dal controllo dell'organizzazione.

In definitiva si è ottenuto un elenco di circa 70 minacce, che costituisce una robusta base di confronto con i clienti per identificare le minacce specifiche del progetto.

Vulnerabilità e controlli di sicurezza

Col termine vulnerabilità si intendono i punti deboli di un sistema o di un prodotto che permettono l'insinuarsi di una minaccia. È stata costruita una serie di elenchi / check list di

vulnerabilità, partendo da NIST SP 800-82 che appaiono particolarmente utili nell'analisi congiunta da sviluppare col cliente.

Le check list sono strutturate come segue:

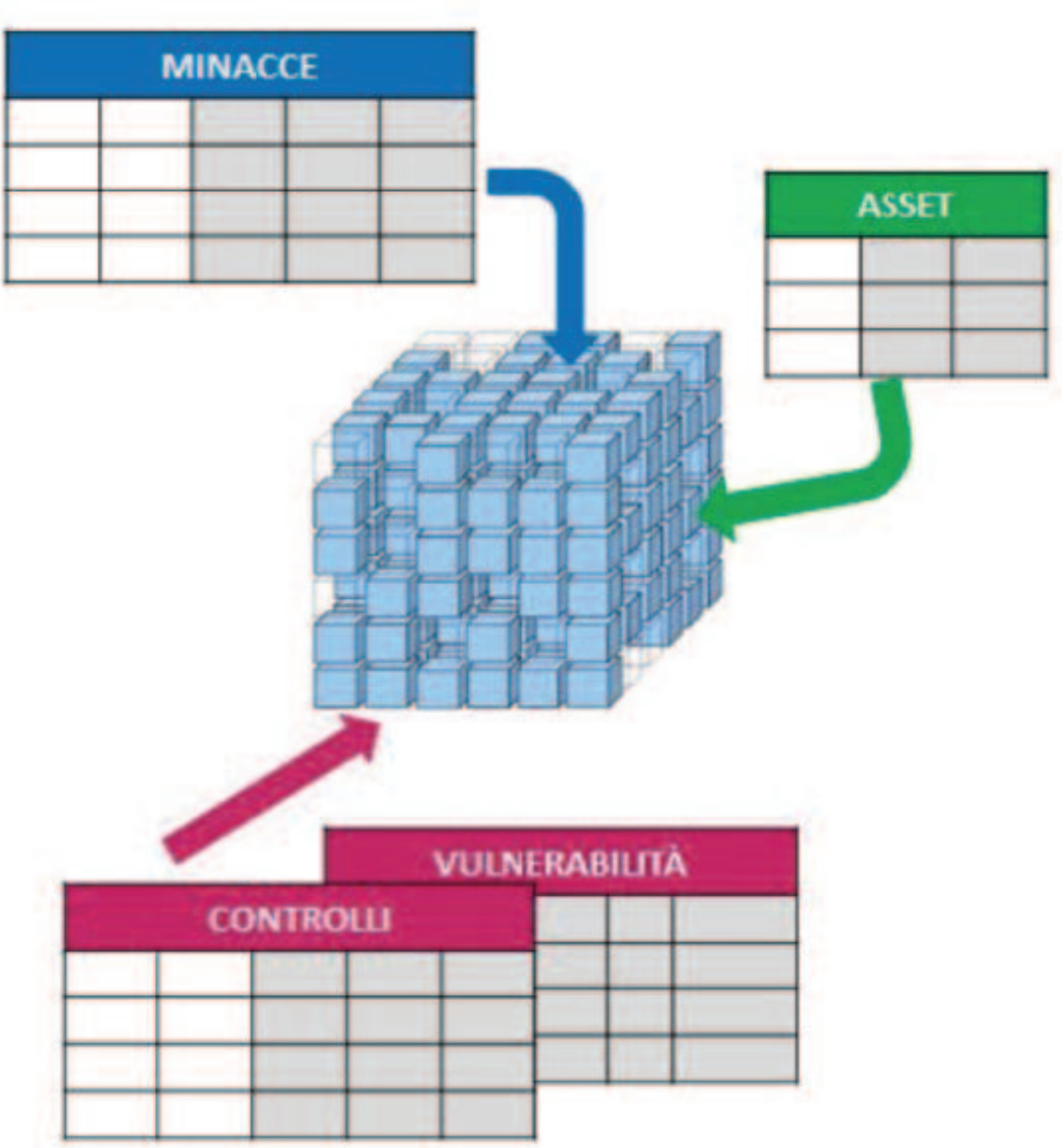
- Vulnerabilità di tipo organizzativo: Politiche e procedure;
- Vulnerabilità a livello di sistema ICS, relative a: Architettura e design, Configurazione e manutenzione, Vulnerabilità fisiche, Legate allo sviluppo del software, Legate alle comunicazioni e alle configurazione di rete.

Per supportare la necessaria attività di monitoraggio, riportata in Figura 4, legata all'evoluzione temporale delle vulnerabilità ed anche delle minacce, sono stati identificati i siti più autorevoli e pertinenti all'attività aziendale.

D'altro canto la protezione dei sistemi e delle informazioni si attua applicando opportuni controlli di sicurezza: per facilitarne l'individuazione è prassi consolidata ricorrere agli elenchi offerti da norme e/o linee guida. Come già citato in precedenza, l'azienda ha deciso di fare riferimento alla coppia di linee guida NIST SP 800-53 e SP 800-82. È stato inoltre avviato un processo di linking fra le check list di vulnerabilità e l'elenco dei controlli, assicurando il necessario legame fra una vulnerabilità ed i controlli necessari a sanarla.

Verso l'analisi quantitativa

Nel corso della ricerca, l'analisi quantitativa è stata realizzata solo parzialmente. È stato però progettato il modello concettuale per mettere in relazione asset, minacce, vulnerabilità e/o controlli. Come citato in precedenza, ogni rischio è funzione di una terna (asset, minaccia, vulnerabilità e/o controllo); può pertanto essere considerato alla stregua di un piccolo cubo. L'insieme dei possibili rischi riguardanti un sistema/impianto ossia delle possibili terne è in astratto rappresentabile con una costruzione complessa di cubi elementari, come visualizzato in Figura 6.



Per semplificare l’analisi e la gestione, data la numerosità dei componenti, è necessario attuare processi di semplificazione e/o riduzione, che possono essere:

- contestualizzazione a progetto: comporta la riduzione degli item lungo le 3 dimensioni (asset, minacce, vulnerabilità), che è rappresentabile come un’operazione di “dicing”;
- fissare uno degli item (ad esempio una famiglia di asset) e porre in relazione minacce e controlli, che è rappresentabile come un’operazione di “slicing”.

Il completamento dell’analisi quantitativa implica una “valorizzazione” del legame fra gli elementi, che può partire, a titolo esemplificativo, dal valore economico/patrimoniale degli asset, dalla probabilità di occorrenza di una minaccia e dalla disponibilità di un controllo. Al termine della ricerca è stato realizzato un prototipo e sono stati lanciati alcuni progetti organizzativi e

tecnologici con l’obiettivo di consolidare quanto appreso.

CONCLUSIONI

Il tema della sicurezza degli impianti è attualmente all’ordine del giorno in quanto alle “minacce tradizionali” si sono aggiunte quelle che possono essere portate appoggiandosi alle tecnologie di comunicazione che rendono gli impianti sempre più connessi al mondo esterno. Ciò è particolarmente vero nel caso in cui sistemi di programmazione e controllo “comandino” impianti automatizzati di produzione.

La struttura logico funzionale di un sistema di programmazione e controllo è infatti ampiamente basata su tecnologie informatiche che, come hanno dimostrato eventi recenti, sono per loro natura vulnerabili. Il sistema di programmazione e controllo può diventare pertanto un veicolo attraverso il quale si può danneggiare in modo volontario o involontario un impianto con conseguenze economiche e di mercato.

Le aziende che operano nel settore delle progettazione e realizzazione questi sistemi devono dotarsi di metodi per il Design For Security intesi come complesso di cultura, conoscenze, procedure, ruoli, tecniche e tecnologie per garantire la sicurezza nel ciclo di vita del sistema di programmazione e controllo e, in molti casi, dell’impianto.

Mettere a punto metodi per il Design For Security richiede però uno sforzo considerevole di analisi in cui il contributo proveniente dall’interno delle aziende è, per sua natura, limitato dalla cultura aziendale sui rischi, dal tipo di progetti e di clienti con cui si è interagito e, spesso, dalle dimensioni e dalla possibilità di investire. L’ampiezza dell’analisi è però foriera di risultati “robusti” in grado cioè di resistere nel tempo alle mutazioni dello scenario dei progetti aziendali.

La manutenzione e l’evoluzione dei metodi di Design For Security d’altra parte richiede che essi siano parte integrante delle piattaforme aziendali in modo da poter essere al centro dei processi di innovazione.

SUGGERIMENTI BIBLIOGRAFICI

[1] ISO/IEC 27001 - Information security management, pagina introduttiva alla famiglia di standard ISO 27000, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[2] Gallotti C., Sicurezza delle informazioni – Valutazione del rischio – I sistemi di gestione – La norma ISO/IEC 27001:2013, Narcissus ebook, 2014

[3] Knapp E.D., Langill J.T., Industrial Network Security, 2° ed., Syngress – Elsevier, 2015

[4] CoSo, La Gestione del rischio aziendale, Edizioni ilSole24ore, 2001

[5] AAVV, Guide to Enterprise Risk Management. Frequently asked questions, Protiviti –

Indipendent risk consultant, 2006

[6] A Guide to the Project Management Body of Knowledge (PMBOK® Guide) 5th edition, Project Management Institute Inc., USA, 2013, chap. about Project Risk Management

[7] Bellucci A., Plant Lifecycle Management – Opportunità per la costruzione di nuovi prodotti e servizi, Impiantistica Italiana, Gennaio – Febbraio 2014

[8] Bellucci A., Rossi M., Tunesi U., Plant Lifecycle Management – Autocertificazione dal mito alla realtà, Impiantistica Italiana, Gennaio - Febbraio 2015

[9] https://it.wikipedia.org/wiki/Stuxnet

[10] Garvin, D. A., Competing on the eigth dimension of Quality, Harvard Business Review 65, n°. 6 (November – December 1987)

[11] Bellucci A., Colombo R., Opere pubbliche e Risk Management negli Enti Locali, Sviluppo & Organizzazione, n° 224, Novembre – Dicembre 2007

[12] Winner R.I., Pennel P.J., Bertrand E.H., Slusurczuck M.G., The role of Concurrent Engineering in weapons system acquisition, IDA Report, Dicember 1988

[13] Nevins J.L., Whitney D.E. (editors), Concurrent Design of Products & Processes, McGraw-Hill, 1989

[14] Hillson D., Murray-Webster R., Understanding and managing risk attitude, Gower Publishing Ltd, 2007

[15] Sinibaldi A., Risk Management, Hoepli Informatica, Milano, 2007

[16] https://en.wikipedia.org/wiki/Common_Criteria

[17] https://en.wikipedia.org/wiki/Cyber_security_standards

[18] Cagno E., Caron F., Colombini F., Corner G., Mancini M.; Modello multidimensionale multilivello per l'analisi dei grandi rischi nelle società di Engineering e Contracting, Impiantistica Italiana, 2004

A cura di:

Arturo Bellucci: Laurea in Ingegneria Elettronica. Docente a contratto di Metodi per la gestione dei progetti complessi presso l'Università di Bologna, Scuola di Ingegneria e Architettura, Corso di Laurea Magistrale in Ingegneria Gestionale. Consulente Free lance. Dal 1972 al 1988 manager presso Telettra SpA. Dal 1988 consulente e formatore sui temi del Project Management, dell'Innovazione di prodotto, della Progettazione organizzativa e della Reingegnerizzazione di processi. Autore di articoli e libri sui temi del Project Management e

dell’Innovazione di prodotto.

Fabio Beghelli: Laurea Quinquennale in Ingegneria Elettronica presso l’Università di Padova. Si occupa di Analisi e Progettazione di Sistemi di Automazione e della loro integrazione con i Sistemi Informativi aziendali. Membro del consiglio di amministrazione della Tecnica Elettronica S.p.A. con delega alla gestione e allo sviluppo dei rapporti con enti e laboratori di ricerca e dei progetti di formazione del personale interno.

Manuela Rossi: Laurea Magistrale in Ingegneria Gestionale e Laurea Triennale in Ingegneria Informatica conseguita presso l’Università di Bologna. Si occupa di consulenza e formazione su temi organizzativi, sicurezza, miglioramento dei processi, sviluppo e mantenimento di Sistemi di Gestione Qualità.