Industrie 4.0 – sicura e smart

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Esclusione di responsabilità

Abbiamo redatto il nostro whitepaper con estrema accuratezza. Esso contiene informazioni relative alla nostra azienda e ai nostri prodotti. Tutte le indicazioni si rifanno all'attuale stato dell'arte e alle tecnologie più avanzate del momento. Tuttavia non possiamo fornire alcuna garanzia sull'esattezza e la completezza delle indicazioni, eccetto i casi di colpa grave, in quanto non è possibile, nonostante tutta l'accuratezza, escludere totalmente la presenza di errori. In particolare, le informazioni non possiedono qualità di garanzie giuridiche o caratteristiche assicurative. Vi saremo grati se vorrete segnalarci eventuali errori.

Diritti d'autore

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern

2ª edizione

Indice

1. Informazioni su Industrie 4.0

Industrie 4.0 è molto più di una visione futuristica. La combinazione intelligente rappresenta una grande opportunità per l'industria. Grazie ad una produzione flessibile si ottiene lo sfruttamento ottimale degli impianti. La possibilità di realizzare prodotti personalizzati alle stesse condizioni della produzione di serie fa aumentare la produttività degli impianti. Tuttavia, molte aziende continuano ad esitare nell'implementazione di Industrie 4.0 nei propri processi produttivi. Secondo lo studio "Industry 4.0 – How to navigate digitization of the manufacturing sector, 2015"1 condotto dall'Istituto McKinsey, soltanto sei aziende su dieci in Germania si sentono pronte per Industrie 4.0, nonostante nel 91 percento dei casi esse riconoscano che la digitalizzazione della produzione industriale sia un'opportunità. Noi vogliamo andare controcorrente offrendo alle aziende di tutto il mondo soluzioni e prodotti da Industrie 4.0. Infatti, anche a livello internazionale si pone sempre maggiore accento sul tema Industrie 4.0: è proprio la progressiva globalizzazione che richiede di creare i presupposti per consentire i collegamenti in rete tramite la digitalizzazione dei processi di produzione lungo la catena del valore.

1.1. Storia e retroscena: dalla macchina a vapore alla fabbrica intelligente

Nella prima rivoluzione industriale la protagonista fu la meccanizzazione grazie all'energia prodotta da acqua e vapore, seguì la seconda rivoluzione industriale: la produzione in massa a cottimo con l'ausilio delle catene di montaggio e dell'energia elettrica. Dopodiché fu la volta della rivoluzione digitale, conosciuta anche come "Industrie 3.0". Lavorare al computer divenne la normalità e fece il suo ingresso anche il primo dispositivo di comando PLC.
"Industrie 4.0" è sinonimo di quarta rivoluzione industriale, quella dei sistemi cyberfisici (CPS), dell'"Internet delle cose" e della smart factory. Per Pilz, Industrie 4.0 rappresenta piuttosto un'evoluzione, in quanto il progetto Industrie 4.0 non è realizzabile senza la disponibilità verso il cambiamento da parte di tutti gli attori coinvolti .

L'espressione Industrie 4.0 è stata usata per la prima volta in pubblico nel 2011 in occasione della fiera di Hannover. A ottobre del 2012 un gruppo di lavoro composto dai promotori della comunicazione dell'unione per la ricerca dedicato al progetto Industrie 4.0 ha consegnato al governo federale tedesco una serie di raccomandazioni per la sua implementazione. Sempre lo stesso gruppo di lavoro Industrie 4.0 nell'aprile del 2013 in occasione della fiera di Hannover ha consegnato il proprio rapporto conclusivo ad alcuni importanti rappresentanti del governo federale tedesco. Allo stesso tempo, si è messa all'opera la piattaforma Industrie 4.0 che vede la collaborazione delle tre associazioni settoriali Bitkom[2], VDMA[3]e ZVEI[4] . Il suo scopo è di coordinare in futuro le attività di questo settore futuristico. Sin dall'inizio Pilz ha partecipato attivamente sostenendo i progetti con la propria lunga esperienza nella tecnica di automazione.

[1] https://www.mckinsey.de/sites/mck_files/files/mck_industry_40_report.pdf
[2] Bitkom (Digitalverband Deutschlands / Germany's digital association), https://www.bitkom.org/EN/index-EN.html
[3] VDMA (Verband Deutscher Maschinen- und Anlagenbau, Mechanical Engineering Industry Association), http://www.vdma.org/ueber-uns
[4] ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e. V.), http://www.zvei.org/en/Pages/default.aspx

1.2. La fabbrica intelligente - smart factory

La smart factory è la fabbrica intelligente di domani. Il termine è stato coniato nell'ambito della ricerca nelle tecnologie di produzione. La smart factory è l'obiettivo che la strategia high-tech del governo federale tedesco intende raggiungere nell'ambito del proprio progetto futuristico Industrie 4.0.5 All'interno dell'ambiente di produzione della smart factory, gli impianti di produzione e i sistemi logistici sono ampiamente in grado di organizzarsi e ottimizzarsi autonomamente. I prodotti realizzati nella smart factory sanno in ogni momento dove si trovano, conoscono la propria storia, il proprio stato attuale e le proprie fasi di produzione mancanti prima di arrivare al prodotto finito. Ma come si realizza tutto questo?
Tecnicamente questo progetto si basa sui sistemi cyberfisici[6], che comunicano tra loro attraverso l'Internet delle cose[7]. Questo scenario futuristico implica l'esistenza di una comunicazione tra il prodotto o il portapezzi e l'impianto di produzione: il prodotto porta con sé le proprie informazioni di produzione in un formato leggibile meccanicamente, ad esempio su un chip RFID. Questi dati consentono di controllare sia il percorso del prodotto attraverso l'impianto di produzione, sia i singoli passaggi di produzione. Nelle scuole superiori e nelle sedi di ricerca la smart factory è oggetto di studio nell'ambito delle cosiddette fabbriche modello.

1.2.1. SmartFactory^{KL}

La SmartFactory^{KL} come centro di competenze e piattaforma di ricerca e dimostrazione indipendente anticipa quella che sarà la fabbrica intelligente di domani. In questa sede vengono sviluppati quei sistemi produttivi innovativi dove la visione Industrie 4.0 sta già diventando una realtà.[8] L'obiettivo è di operare nell'ambito di una rete con partner rinomati dell'industria e della ricerca per elaborare nuovi concetti, standard e soluzioni che divengano il fondamento per una tecnica di automazione altamente flessibile.
In qualità di membro ordinario, Pilz persegue gli obiettivi di questa iniziativa da tutti i punti di vista. Pilz tiene monitorate le conoscenze acquisite da questo lavoro comune sulla piattaforma di sviluppo, traendone vantaggio per la propria offerta.
La SmartFactory^{KL} dispone già oggi del primo impianto al mondo multimarca per il progetto Industrie 4.0.[9] In questo contesto, sicurezza e modularizzazione sono temi importanti. Da un lato Pilz, grazie alla pluriennale esperienza nel settore della sicurezza delle macchine, apporta un notevole contributo alla standardizzazione e alla realizzazione di una procedura comune per la sicurezza, in entrambe le sue accezioni di "safety" (sicurezza delle macchine) e "security" (sicurezza IT). Dall'altro, Pilz contribuisce concretamente al tema della modularizzazione: la realizzazione di impianti secondo i principi della meccatronica permette di ottenere una totale modularizzazione sotto forma di elementi macchina. E' possibile standardizzare e riutilizzare le funzioni per mezzo di appositi moduli. Alla base ci sono sistemi di automazione come PSS 4000 di Pilz, in grado di distribuire le funzioni di controllo. Nella smart factory è possibile collaudare tutte queste soluzioni di automazione. Da diversi anni la SmartFactory^{KL} presenta un impianto di produzione modulare, multimarca, nei quale i singoli moduli di diverse produttori interagiscono con diverse architetture di controllo. Pilz contribuisce a questo impianto dimostrativo di SmartFactory^{KL} con un modulo di stoccaggio intelligente e automatizzato.

[5] http://www.hightech-strategie.de/de/Industrie-4-0-59.php
[6] Definizione nel glossario a pagina 20 e seg.
[7] Definizione nel glossario a pagina 20 e seg.
[8] http://www.smartfactory.de/
[9] http://www.smartfactory.de/

Figura 1: SmartFactory^{KL} alla Fiera di Hannover 2015

1.2.2. Il modulo dimostrativo per la smart factory di Pilz

Il nostro modulo dimostrativo per la smart factory serve a dare prova di come sia possibile realizzare prodotti personalizzati in maniera rapida, flessibile ed economica. La linea di produzione basata sul concetto modulare pone l'accento sulla comunicazione tra sistemi di automazione ottenuta dall'interazione tra attuatori e sensori. Il sistema di automazione PSS 4000, adeguato ai principi di Industrie 4.0 coordina il funzionamento di tutti i componenti per le funzioni di sicurezza e automazione collegati in rete: dalla progettazione alla visualizzazione. La nostra linea di produzione intelligente produce contenitori personalizzati per biglietti da visita e penne a sfera. In questo contesto è importante rendere i processi di produzione trasparenti. Con le nostre soluzioni è possibile rappresentare in maniera semplice anche macchinari e impianti complessi con funzioni avanzate, per fare comprendere come nascono in Industrie 4.0, grazie ai sistemi collegati in rete in modalità digitale.

L'impianto dimostrativo è composto da tre diversi moduli funzionali:
- un magazzino per i portapezzi
- un robot con magazzino pezzi/stazione di erogazione del prodotto
- una stazione laser

In un terminale clienti vengono registrati tramite un PC i dati dei clienti (contatto, indirizzo, ...). Inoltre il cliente può scegliere tra un contenitore per biglietti da visita e una penna a sfera, da personalizzare con il proprio nome (nel caso della penna a sfera) o con il proprio biglietto da visita digitale e il proprio nome scritto (nel caso del contenitore per biglietti da visita).
I dati inseriti vengono salvati in formato digitale su un chip RFID previsto sul portapezzi. In questo modo si è certi che tutte le informazioni siano disponibili in ogni singolo modulo. Le informazioni necessarie vengono quindi lette dal chip per eseguire le operazioni necessarie. Una volta eseguite le operazioni correttamente, nel momento in cui il prodotto viene erogato, il contenuto del chip RFID viene cancellato. Si potrà quindi procedere con la descrizione del record di dati successivo. Una volta cancellati i dati, il portapezzi con il chip RFID viene riportato

in magazzino, se non ci sono altri record di dati da salvare, o altrimenti inviato di nuovo nel circuito di produzione.

Figura 2: Il modulo dimostrativo smart factory di Pilz alla fiera di Hannover 2016

1.3. Sicurezza – Safety & Security

Il costante sviluppo del panorama dell'automazione verso il mondo Industrie 4.0 comporta sempre nuove sfide aziendali relative alla sicurezza: così il mondo dell'automazione si fonde con il mondo dell'IT. I rispettivi punti di vista riguardo alla sicurezza sono nettamente contrastanti: i concetti - utilizzati a livello internazionale - di "safety" per la sicurezza delle macchine e "security" per la sicurezza dei dati e informatica aiutano a comprendere le differenze fondamentali.

Il concetto di "safety" prevede che i rischi residui correlati a una macchina o a un impianto non superino i valori accettabili. Questo include sia i pericoli in prossimità dell'impianto (ad es. danni ambientali), sia i pericoli all'interno dell'impianto stesso (ad es. per le persone che si trovano nell'impianto).
Il concetto di "security" concerne la protezione di una macchina o di un impianto da accessi non autorizzati dall'esterno e la protezione dei dati sensibili dalla falsificazione, dalla perdita e dall'accesso non autorizzato a livello interno. Questo include attacchi espliciti e incidenti involontari relativi alla sicurezza.

La protezione globale dei dati di controllo per la produzione e la sicurezza durante la trasmissione, elaborazione e conservazione dei dati deve contemplare i seguenti aspetti di security:

- sicurezza fisica e disponibilità dei sistemi IT
- sicurezza della rete
- sicurezza delle applicazioni software

- sicurezza dei dati
- sicurezza aziendale

1.4. Le macchine modulari e la decentralizzazione

La chiave per una maggior flessibilità produttiva da molti anni è rappresentata dalla struttura modulare di impianti e macchine. Un impianto completo è composto da più moduli indipendenti. Un modulo assolve una o più fasi produttive standardizzate e può essere abbinato ad altri moduli per ottenere un processo completo. A tale scopo, tutti i moduli vengono collegati ad un backbone che alimenta il moduli sia dal punto di vista energetico (corrente trifase a 400 VAC, aria compressa, ...) sia a livello di dati di processo e controllo. Se le esigenze produttive vengono modificate oppure la produttività aumenta, è possibile sostituire uno o più moduli oppure aggiungere moduli dello stesso tipo.

Per l'automazione del futuro pertanto la modularizzazione e la decentralizzazione sono due dei principali fattori di successo. A tale scopo sono imprescindibili dei sistemi di automazione che siano in grado di controllare in maniera user-friendly l'intelligenza distribuita nei moduli macchina. Tutte le macchine e gli impianti pertanto possono essere suddivise in unità ben visibili ed autonome.

La struttura modulare di macchine e impianti è in linea con i principi della meccatronica. Questo approccio segue la filosofia di riunire tutti gli aspetti coinvolti nel processo produttivo di una macchina: meccanica,elettricità e automazione. In questo caso viene costantemente definita la sinergia tra i vari componenti singoli legati alla tecnica dell'automazione e i rispettivi tool software per realizzare una soluzione di automazione. Questa continuità coinvolge tutti i quattro livelli della piramide dell'automazione (livello di direzione aziendale, livello di direzione della produzione, livello di comando e livello di campo). In base all'approccio meccatronico è necessario che anche le funzionalità di comando possano essere "trasferite" ai singoli moduli meccatronici.
E' qui che fino ad oggi i sistemi incontravano i propri limiti. Infatti pur potendo produrre dei moduli gestionali, quando questi devono essere realizzati tramite potenti sistemi di controllo centralizzati e, a causa della loro complessità, la loro messa in funzione diventa rapidamente laboriosa. Allo stesso modo anche eventuali modifiche successive necessarie a livello di configurazione e programmazione dei singoli moduli funzionali possono aumentare il carico di lavoro.
I sistemi decentralizzati consentono di mettere in funzione i moduli in modo semplice. Altrettanto semplice risulta anche la configurazione per l'utente, in quanto per i diversi moduli è possibile utilizzare programmi e funzioni secondarie di controllo identici.

L'automazione del futuro richiede quindi soluzioni che da una parte siano in grado di distribuire le logiche di controllo e dall'altra garantiscano il necessario collegamento in rete di diversi comandi comunque semplici da gestire per l'utente. Una soluzione di questo tipo è quella offerta da Pilz con il sistema di automazione PSS 4000.

2. Industrie 4.0 e Pilz

2.1. Il contributo di Pilz

Susanne Kunschert, membro amministrativo di Pilz, è stata personalmente nominata nel 2010 dal governo federale tedesco a rappresentante delle Pmi all'interno del comitato di ricerca. Il comitato di ricerca era il principale ente di consulenza per le politiche innovative del governo federale tedesco per l'implementazione e lo sviluppo di strategie high-tech. A Susanne Kunschert è stato chiesto espressamente di portare la propria esperienza di azienda innovativa selezionata tra quelle di media dimensione.

L'Amministratore Delegato e Socio di Pilz è anche membro del gruppo di promotori della sicurezza informatica, che si occupa attivamente della protezione delle reti di comunicazione e dello sviluppo della Germania come mercato leader nella sicurezza informatica. Il comitato di ricerca ha operato secondo distinti gruppi di lavoro per lanciare progetti in settori specifici che ne hanno dimostrato necessità. Uno dei progetti più importanti è "Industrie 4.0".

Pilz ha supportato attivamente in diversi progetti il lavoro del nuovo ente "Industrie 4.0", nato sotto l'egida delle associazioni di categoria BITKOM, ZVEI e VDMA, ed ha partecipato alla definizione delle linee guida che sono state presentate al Governo Federale in occasione della fiera di Hannover del 2013.

Attualmente Pilz è attiva nei seguenti comitati e iniziative:
- collaborazione alla piattaforma Industrie 4.0
- collaborazione al gruppo direttivo Industrie 4.0 dell'associazione di elettrotecnica ed elettronica ZVEI
- collaborazione con la rete regionale meccatronica “Landesnetzwerk Mechatronik BW”
- membro del Gruppo Direttivo della rete Allianz Industrie 4.0 del Land Baden-Württemberg
- partecipazione alla piattaforma indipendente di ricerca e dimostrazione SmartFactory^{KL}
- membro di ARENA2036 – Il futuro del settore auto

2.2. Industrie 4.0 e i prodotti Pilz

Con la partecipazione al gruppo di ricerca e alla piattaforma di ricerca SmartFactory^{KL} Industrie 4.0 per Pilz non rappresenta solo un progetto futuro ma è già parte integrante del processo produttivo**.**
Grazie al crescente collegamento in rete di macchine e infrastrutture con l'impiego di tecnologie IT nella produzione, Pilz sosterrà il proprio ruolo di leader a livello tecnologico anche nella propria area produttiva. Nell'ambito di Industrie 4.0 è stata creata l'infrastruttura necessaria per attuare la produzione intelligente e gli elementi di Industrie 4.0 hanno già trovato impiego. Per il trasporto pezzi viene implementato un sistema intelligente, sviluppato internamente. Questo sistema velocizza e semplifica il caricamento di circuiti stampati e le operazioni di saldatura. I portapezzi individuano autonomamente il percorso grazie a un chip RFID integrato, spostandosi dall’impianto di saldatura fino all'unità di montaggio.
Pilz proseguirà l'implementazione graduale della produzione intelligente: per il controllo della produzione i dati macchina vengono raccolti ed elaborati in modo mirato, consentendo di acquisire importanti informazioni sui cambiamenti delle situazioni e sull'usura delle macchine.

Tutto ciò permette di eseguire attività di manutenzione in modo preventivo. La "manutenzione predittiva" evita guasti e tempi di fermo macchina. Inoltre è previsto il salvataggio dei documenti operativi aggiornati in un cloud Pilz. In questo modo, tutti i dati e i documenti saranno sempre disponibili in tempo reale e nella versione più aggiornata e potranno essere consultati mediante dispositivi mobili da qualsiasi punto della produzione.

2.2.1. IT nella produzione collegata in rete

Pilz è consapevole delle sfide poste a livello di IT Security da una produzione completamente collegata in rete e, di conseguenza, investe in un'ampia infrastruttura IT per il controllo di tutto il traffico dati. L'investimento include un nuovo sistema computerizzato autonomo che soddisfi gli standard più moderni. L'analisi e protocollizzazione costante dei dati di processo e di tutti gli altri dati consente di individuare tempestivamente le anomalie. Inoltre, per le singole aree di produzione sono stati installati diversi sistemi firewall che permettono di definire il livello richiesto di "security" per ogni singola area. Vengono ridotti guasti, rischi di sicurezza e il know-how è al sicuro.

2.2.2. "Pilz Denkfabrik 4.0"

Pilz conferisce la massima priorità anche all'importante collaborazione tra i reparti di IT e ingegnerizzazione della produzione nell'ambito del progetto Industrie 4.0. "Pilz Denkfabrik 4.0" riunisce dipendenti dei reparti di produzione e IT che ricevono le risorse necessarie per progettare e implementare progetti comuni sull'argomento Industrie 4.0.

2.3. Campi di implementazione di Industrie 4.0

Alla base di un'accettazione costante da parte del mercato c'è la realizzazione di meccanismi standardizzati per la comunicazione tra macchine e all'interno di una stessa macchina. Soltanto tenendo conto dei requisiti di entrambi i mondi (automazione e IT) è possibile realizzare soluzioni praticabili, accolte dagli utenti.
In sintesi questo significa che Pilz si impegna nella realizzazione di architetture di controllo moderne nell'ambito del concetto di Industrie 4.0.

A tale proposito i seguenti argomenti rappresentano i nostri punti chiave:

- Safety & Security:
  - Hanno punti in comune evidenti nell'ambito della standardizzazione e del metodo del processo di engineering. Pilz intende portare avanti questo importante compito sulla base dell'esperienza maturata nei settori dell'automazione e della sicurezza delle macchine.
  - Tutti i dispositivi e componenti di automazione necessari alle funzioni di controllo hanno un accesso diretto a Internet che consente lo scambio dei dati di processo e di parametrizzazione a scopo di diagnostica e manutenzione (a distanza). In questo modo per tutti i dispositivi di automazione coinvolti aumentano i requisiti di "security" e per un collegamento e rappresentazione diagnostica uniforme.
- Il principio di modularità:
  - Le nostre moderne funzioni di comando e controllo sono sviluppate per supportare i concetti di distribuzione e orientamento agli oggetti. I sensori e gli attuatori diventano intelligenti. Così facendo, riproponiamo l'orientamento verso il controllo meccatronico degli oggetti (componenti per l'automazione) nei nostri prodotti e nei rispettivi strumenti di engineering.

3. Area di azione sicurezza – Safety & Security

Safety & Security sono due presupposti importanti per il funzionamento degli impianti Industrie 4.0, che a differenza dei tradizionali impianti produttivi dispongono di interfacce di collegamento con il proprio ambiente.

Gli impianti Industrie 4.0 in futuro saranno in grado riconfigurarsi e ottimizzarsi autonomamente, un aspetto che richiederà una nuova valutazione della sicurezza (Safety & Security) rispetto al runtime, ovvero durante il regolare funzionamento dell'impianto. Inoltre si dovrà garantire che eventuali lacune a livello di “security” non causino alti rischi inaccettabili in termini di “safety”.

Infine rispetto a questo argomento si dovrà sostenere la fidelizzazione delle piccole e medie aziende, un aspetto fondamentale per la produzione nelle reti ad-hoc. A tale scopo, trasparenza, partecipazione e comunicazione aperta sono presupposti importanti.

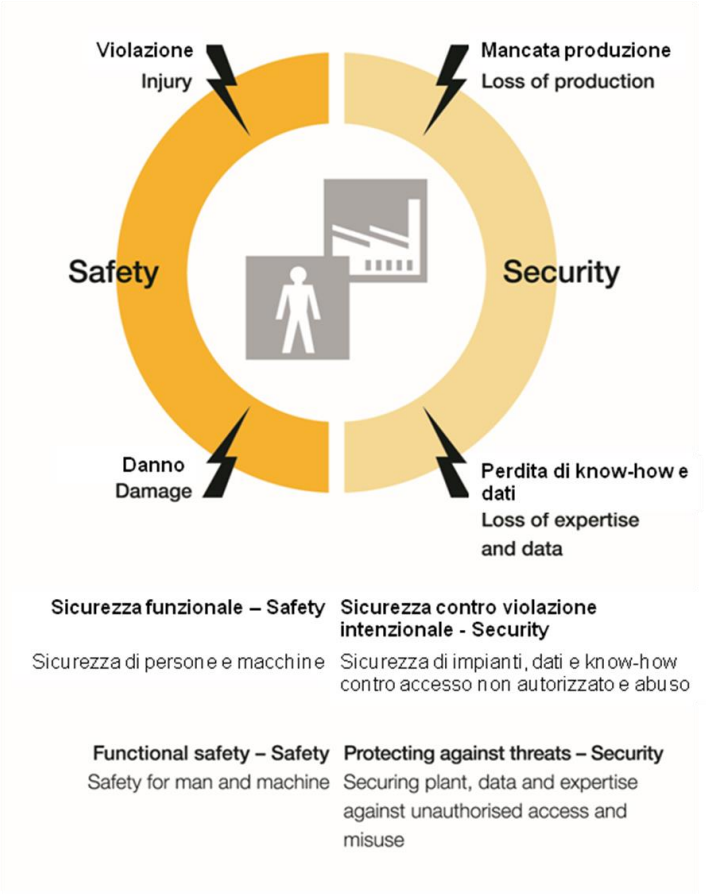

Figura 3: l'interazione tra "safety" e "security"

3.1. Safety

Il settore "safety" è già caratterizzato da una grande sicurezza a livello di investimenti e giuridico. Questo anche grazie alle norme e alle disposizioni in vigore. Tutti i processi per l'analisi e valutazione del rischio e per l'esecuzione delle analisi sono chiaramente definiti dalle

classificazioni internazionali standardizzate Safety Integrity Levels (SIL) e questo consente una valida comparabilità delle soluzioni.

3.1.1. Safety - dalla sicurezza statica a dinamica

Il termine safety fa riferimento alla sicurezza funzionale delle macchine, in altre parole: la protezione delle persone e dell'ambiente dalle minacce provenienti dalle macchine. Il concetto di "safety" prevede che i rischi residui correlati a una macchina o a un impianto non superino i valori accettabili. Questo comprende sia i pericoli per l'ambiente provocati dall'impianto (ad es. danni ecologici), sia i pericoli interni all'impianto (ad es. per le persone che si trattengono all'interno dell'impianto).
Una possibilità nella peggiore delle ipotesi è di interrompere l'alimentazione elettrica e bloccare immediatamente la macchina. Normalmente questo avviene tramite uno speciale cablaggio e componenti di sicurezza, come possono essere i relè di sicurezza. Essendo questo intervento è molto legato all'hardware e quindi molto statico, si rivela poco adatto per i processi di produzione intelligenti dove la configurazione degli impianti deve essere costantemente modificata. Uno spegnimento brusco generalmente comporta diversi svantaggi aggiuntivi, come ad esempio una perdita di produttività, prolungati tempi di fermo macchina dovuti a procedure laboriose per la rimessa in funzione o una limitazione del controllo e della manutenzione della macchina.

I concetti di sicurezza dinamica offrono un'alternativa basata su un'osservazione globale dei processi di automazione mutevoli e dei requisiti di sicurezza funzionale. Questo cambia anche la percezione della sicurezza in sé: essa non è più considerata una caratteristica dell'hardware, bensì una funzione che interessa i dispositivi nel complesso. Con questo approccio, sviluppato ancora prima dell'avvento di Industrie 4.0, i processi si possono gestire in maniera più sicura e controllata, senza doverli interrompere immediatamente ogni volta che si verifica un'anomalia. L'approccio dinamico tuttavia può essere implementato con efficacia soltanto se la sicurezza funzionale viene tenuta in considerazione sin dall'inizio della pianificazione dei progetti di automazione. Diversamente può accadere di dover modificare l'andamento delle singole fasi di produzione o di un intero processo in un secondo momento, il che impedisce di adottare soluzioni ottimali e comporta costi notevoli.
Mentre la sicurezza statica spesso prevede soltanto la trasmissione di segnali binari, ad esempio per interrompere il movimento della macchina dopo l'apertura di un riparo mobile, la “safety” dinamica richiede molte più informazioni. Infatti in questo caso esistono diverse modalità operative sicure che consentono ad esempio il "funzionamento con il riparo mobile". L'informazione di tali modalità operative sicure deve tuttavia essere disponibile in tutti i componenti coinvolti. Facendo riferimento all'esempio del riparo mobile, a seconda del livello di autorizzazione dell'utente, l'apertura di tale riparo, non comporta più automaticamente lo spegnimento immediato della macchina, piuttosto i meccanismi di sicurezza in questo caso verificano che venga mantenuto un numero di giri limite ridotto oppure essi stessi producono e monitorano in maniera sicura l'assegnazione del valore nominale di sicurezza dell'asse di rotazione.

3.1.2. Safety 4.0 - dalle strutture monolitiche alle soluzioni modulari

Nella smart factory gli impianti a struttura modulare devono poter essere riconfigurati in modo rapido e flessibile oppure spostati come corpo unico. La validazione di una soluzione sicurezza deve quindi prevedere la possibilità di estendere questa flessibilità (a posteriori). Questo perché

tutte le configurazioni non contemplate nella certificazione CE non sono facilmente definibili neanche dal gestore dell'impianto stesso. Non vale la semplice equazione: $CE_{Modulo1}$ + $CE_{Modulo2}$ = $CE_{Macchina\ intera}$!
Il vantaggio funzionale dei concetti di macchine modulari è evidente: fanno aumentare la flessibilità nel processo di produzione e al tempo stesso incrementano la possibilità di standardizzazione a livello di funzionamento. Il massimo potenziale di standardizzazione si raggiunge quando si possono configurare moduli con spazi di progettazione identici, indipendentemente dal fatto che si tratti di un modulo con funzione meccanica, elettrica, di controllo o visualizzazione. L'approccio meccatronico si pone l'obiettivo di creare elementi di automazione dalla struttura standardizzata.
I vantaggi della modularizzazione vengono spesso annullati da un concetto di sicurezza rigido, e possibilmente basato su un cablaggio eccessivo. Anche i comandi di sicurezza elettronici sono quasi sempre una copia della sicurezza basata sull'hardware, sotto forma di circuiti di sicurezza fissi, anche se i prodotti vengono proposti in una logica di collegamento per così dire liberamente programmabile.
Le architetture di controllo moderne si fondano invece sulla capacità di funzionare senza strutture di regolazione controllate dal sistema. Lo scopo è di mettere l'utente in condizione di poter ottimizzare i propri impianti liberamente secondo i propri gradi di modularizzazione. Riuscendo ad abbattere le barriere delle diverse interpretazioni rispetto alle funzioni dell'automazione e della sicurezza delle macchine, si conferisce all'utente un grado molto maggiore di libertà.
Il PSS 4000 è un sistema di automazione che ha come due funzioni base la modularizzazione e la maggiore flessibilità. Per la prima volta è possibile gestire tutte le variabili di processo, comprese le funzioni di sicurezza in maniera completamente simbolica e senza alcun coinvolgimento dell'hardware nel sistema. Questo viene dimostrato dal fatto che tutte le variabili di processo sono disponibili nell'intero sistema e che grazie all'architettura multi-master esse sono rese disponibili automaticamente per tutti i comandi all'interno del sistema di automazione distribuito.

3.1.3. La certificazione modulare

Più sono le macchine create dai moduli e più sono i componenti che devono essere collegati a livello decentralizzato. La modularità delle macchine o delle parti di macchine ha numerosi grandi vantaggi: i moduli delle macchine si possono combinare in maniera diversa e scambiare, le macchine si possono ampliare oppure, per es. si può sostituire un attrezzo a produzione in corso. Le macchine diventano più flessibili. A parità di numero di macchine, il gestore dell'impianto può ottenere più prodotti. Partendo dal presupposto che questo possa essere utile per il gestore dell'impianto, i concetti di controllo vengono decentralizzati. Il tema Safety & Security assume quindi una grande importanza. La parola chiave è certificazione modulare degli impianti. Attualmente le macchine vengono collaudate dagli enti di certificazione nel loro complesso. Una minima modifica, come può essere la sostituzione di due moduli, richiede un nuovo collaudo. Sono in esame diverse proposte di soluzione, ma attualmente non esiste una procedura standardizzata. Una proposta di soluzione è: la macchina è sicura quando i suoi singoli moduli sono sicuri. A questo punto si tratta di sensibilizzare le aziende e gli organi decisionali politici attraverso le associazioni, perché in questo caso non è pensabile poter fare dei progressi se non esiste un quadro legislativo adeguato.

3.2. Security

La sfida per la “security”, a differenza della sicurezza funzionale, consiste nel dover adattare costantemente i meccanismi di “security” alle condizioni di rischio imminenti. Le cause possono essere gli aggiornamenti occasionali, in quanto virus, bachi, cavalli di Troia e via dicendo sono in costante evoluzione e delle lacune nella “security” possono compromettere la produzione con tutti i rispettivi elementi funzionali.
Per reagire con flessibilità a qualsiasi possibile minaccia, anche la protezione delle applicazioni “safety” deve essere supportata da una strategia di “security” globale, suddivisa in diversi strati: i componenti di automazione sono il cuore. Poi segue la rete, attraverso la quale questi componenti comunicano con altri o con un sistema ERP (Enterprise Resource Planning). Lo strato più esterno è lo stabilimento stesso, che tramite uno speciale concetto di firewall, la cosiddetta zona demilitarizzata, viene schermata verso l'esterno.

I requisiti del mondo IT e del mondo dell'automazione sono profondamente diversi. Mentre all'interno degli uffici la riservatezza delle informazioni ha la massima priorità, nel contesto produttivo al primo posto c'è la disponibilità dei dati, in quanto si tratta di un presupposto fondamentale per consentire processi di produzione senza difficoltà. Attualmente è in fase di studio una norma internazionale (IEC 62443) che dovrebbe unificare questi due diversi mondi della “security”. Poiché il cybermondo è caratterizzato da minacce dinamiche, “safety” e “security” rimarranno due argomenti separati anche in futuro, seppur strettamente correlati tra loro.

In questo senso è importante sviluppare metodi e strumenti che siano di ausilio per analizzare gli effetti delle lacune nella “security” su altri rischi residui a livello di “safety”. Possibilmente, questi metodi e strumenti dovrebbero essere applicati già a livello di sviluppo dei prodotti legato ai sistemi cyberfisici (CPS): Security by Design.

Gli aspetti da tenere in considerazione sono:
- protezione delle interfacce (PLC) verso l'esterno (Internet, rete aziendale, ...)
- protezione dei sistemi di comunicazione interni alle macchine e agli impianti in base alle tipologie di utilizzo (funzionamento costante, manutenzione a distanza, diagnostica a distanza, collegamenti ad-hoc)
- la “security” può essere definita un "moving target", ovvero non esiste una soluzione di sicurezza costante

3.2.1. Proposte di soluzione nell'ambito della “security”

Come proteggere le applicazioni “safety” dalle minacce del cybermondo? Per anticipare subito la risposta: soltanto combinando diversi provvedimenti e disposizioni di “security” che tutte le parti coinvolte dovranno rispettare con coerenza.
A livello di rete, la ricetta per il successo si chiama "defense in depth", ovvero una difesa radicata in profondità. Un elemento centrale, adottato anche nella costruzione delle fortezze del medioevo, è quello costituito dal modello di Security "zones and conduits" (zone e passaggi), già definito nella norma IEC 62443. Esso prevede la suddivisione di una rete di automazione in diverse zone all'interno delle quali gli apparecchi possono comunicare tra loro. Lo scambio di dati con apparecchi in altre zone è possibile soltanto attraverso un unico passaggio che viene monitorato da un router sicuro o da una firewall che filtrano il flusso di dati attraverso precise regole e bloccano gli attacchi non autorizzati. Anche se un attacco dovesse riuscire a penetrare

in una zona, sarebbero in pericolo soltanto gli apparecchi in essa presenti, mentre gli altri continuerebbero ad essere al sicuro.

3.2.2. Soluzioni di automazione

Per proteggere le soluzioni di automazione, nelle indicazioni IEC 62443 della serie di norme sulla sicurezza informatica nei sistemi di automazione industriale, sono definiti i cosiddetti sette "foundational requirements" per la sicurezza delle soluzioni di automazione di questo genere:

- Identification and authentication control (IAC)
- Use control (UC)
- Data integrity (DI)
- Data confidentiality (DC)
- Restricted data flow (RDF)
- Timely response to events (TRE)
- Resource availability (RA)

Ciascun requisito fondamentale è suddiviso nei seguenti elementi:

- Identification & authentication
- Human user identification
- Multifactor authentication for untrusted networks
- Software process and device identification
- Unique identification and authentication
- Strength of password-based authentication
- Password generation and lifetime restrictions for human users

Ogni elemento prevede quattro livelli di “security”, raggiungibili in base all'impegno dedicato allo sviluppo delle soluzioni di automazione. In questo caso sono chiamati in causa l'integratore di sistemi e il gestore dell'impianto, che definiscono i rispettivi livelli di protezione per l'applicazione e dal conseguente modello di zone. Il livello di protezione massimo "level 4" non sarà sicuramente sempre applicabile, in quanto potrebbe comportare un'enorme mole di lavoro.

Anche il migliore tra i provvedimenti tecnici di Security tuttavia non serve a nulla se non viene attuato o, peggio ancora viene deliberatamente bypassato, perché richiede troppo tempo o lavoro o perché esistono incomprensioni e incertezze. I provvedimenti tecnici devono essere affiancati da disposizioni e provvedimenti organizzativi. A cosa servono le migliori impostazioni firewall, se la password predefinita indicata nel manuale non viene modificata oppure se è facile stabilire un collegamento tra la password e l'apparecchio. Soltanto dalla sinergia tra i provvedimenti tecnici e organizzativi si può ottenere un livello di protezione per una parte di impianto.

3.3. L'interazione tra Safety & Security

La realizzazione di concetti di sicurezza globali non richiede soltanto la sinergia tra Safety & Security. Sono necessarie anche architetture di sistema speciali basati su standard aperti e che includano valutazioni adatte a tutti i costruttori. Considerando l'aspetto “safety” va verificato fino a che punto le problematiche di “security” influiscono sulla sicurezza funzionale.

In questo caso sono temi centrali le prove di identità univoche e sicure per prodotti, processi e macchine, oltre allo scambio sicuro di informazioni lungo l'intero processo di produzione.

Inoltre sono richieste soluzioni user-friendly: Safety & Security devono essere gestibili e riflettere le esigenze dell'utente. Dal punto di vista microeconomico, la sicurezza è anche un fattore trainante dell'innovazione: essa comprende la valutazione delle strutture dei costi rispetto alla produttività. In questo caso sono imprescindibili l'assicurabilità del danno e i metodi di calcolo necessari a questo scopo.
Per quanto riguarda il fattore uomo, la questione è incentrata sulla "usable security and privacy". L'obiettivo è mantenere l'impegno a livello di tempo e comprensione per i necessari provvedimenti di “security” il più contenuto possibile.

In questo caso esistono delle analogie con la sicurezza funzionale: la disponibilità non deve essere compromessa dai provvedimenti di “safety”. I principi del mondo “safety” sono trasferibili uno ad uno al mondo “security”. La sicurezza richiede un approccio globale.

4. Area di azione - l'approccio modulare

Considerate le sfide, nel medio e lungo termine, soltanto un "approccio modulare" coerente e interdisciplinare porterà al successo. In questo senso giocano un ruolo centrale i sistemi di controllo che devono supportare questo principio.

4.1. Sistemi intelligenti distribuiti - il sistema di automazione PSS 4000

Con il sistema di automazione PSS 4000 Pilz persegue un approccio meccatronico. Il PSS 4000 è in grado di coniugare l'automazione con la sicurezza. I dati di processo o di controllo, i dati fail-safe e le informazioni di diagnostica vengono scambiati e sincronizzati tramite il sistema di comunicazione multi master SafetyNET p. Di conseguenza, per la funzione di controllo il punto di elaborazione della rispettiva parte di programma risulta irrilevante. Al posto di un dispositivo di controllo centralizzato l'utente ha a disposizione un programma applicativo, distribuito rispetto al runtime, nell'ambito di una vista progetti centralizzata. Questa progettazione centralizzata consente di configurare, programmare e diagnosticare tutti i dispositivi della rete. Al termine della progettazione, le singole parti di programma vengono assegnate ai singoli dispositivi di controllo. Questo avviene sulla base di chiare indicazioni da parte dell'utente per il clustering delle unità funzionali. In questo modo è possibile ottenere una gestione semplice e omogenea dell'intero progetto. Oltre alla creazione di moduli e alla possibilità di standardizzazione, esistono altri vantaggi dati da una reazione più flessibile alle anomalie, una maggiore disponibilità, così come una maggiore produttività grazie ai tempi di reazione più brevi dell'intero sistema.

Mentre nel caso dell'automazione classica, un sistema di controllo singolo, centralizzato monitora la macchina o l'impianto ed elabora tutti i segnali, lPSS 4000 consente una distribuzione conforme delle funzioni di controllo. Nello specifico, il sistema di automazione PSS 4000 è composto da componenti hardware e software, dal sistema Ethernet real time SafetyNET p e da numerosi editor di programmi con relativi blocchi funzionali applicativi per diversi settori. L'hardware comprende diverse classi di prestazione dei sistemi. I dati di

processo e di controllo, i dati fail-safe e le informazioni di diagnostica vengono scambiati e sincronizzati tramite Ethernet. L'unione coerente delle funzioni di sicurezza e automazione riduce la complessità nell'ambito della comunicazione e comporta inoltre un'ottimizzazione dei costi.

4.2. Engineering-Tool PAS4000

Il compito del sistema di automazione PSS 4000 è quello di semplificare la decentralizzazione delle funzionalità di controllo garantendo una gestione chiara e precisa. In questo caso la piattaforma software PAS4000 gioca un ruolo centrale. Essa include diversi editor per la programmazione e la configurazione del dispositivo PLC e di moduli software. In PAS4000 gli strumenti per la progettazione, la programmazione, la messa in servizio e il funzionamento sono tutti strettamente compatibili fra loro.

Il PAS4000 supporta la scomposizione di una funzione della macchina/dell'impianto in moduli funzionali sempre più piccoli che seguono allo stesso modo i limiti di suddivisione delle unità meccatroniche. La modularizzazione è un aspetto chiave: dalle funzioni base derivano gli elementi, dagli elementi i moduli, dai moduli le macchine e gli impianti: semplicemente tramite un confezionamento gerarchico dei moduli. Le funzioni base, gli elementi e i moduli compongono la spina dorsale della creazione software e si possono riutilizzare in modo eccellente come componenti software in quanto incapsulabili e orientabili all'oggetto.

Il PAS4000 mette a disposizione delle biblioteche software che contengono le funzioni base, gli elementi e i moduli più comuni. La possibilità di scegliere i componenti finiti dalle biblioteche sicuramente non è una novità. La particolarità del PAS4000 sta nel fatto che questi componenti sono corredati di diverse caratteristiche, le cosiddette "properties". Esse consentono di impostare facilmente i parametri delle funzioni desiderate. Questo si rivela particolarmente vantaggioso per una standardizzazione delle funzioni.

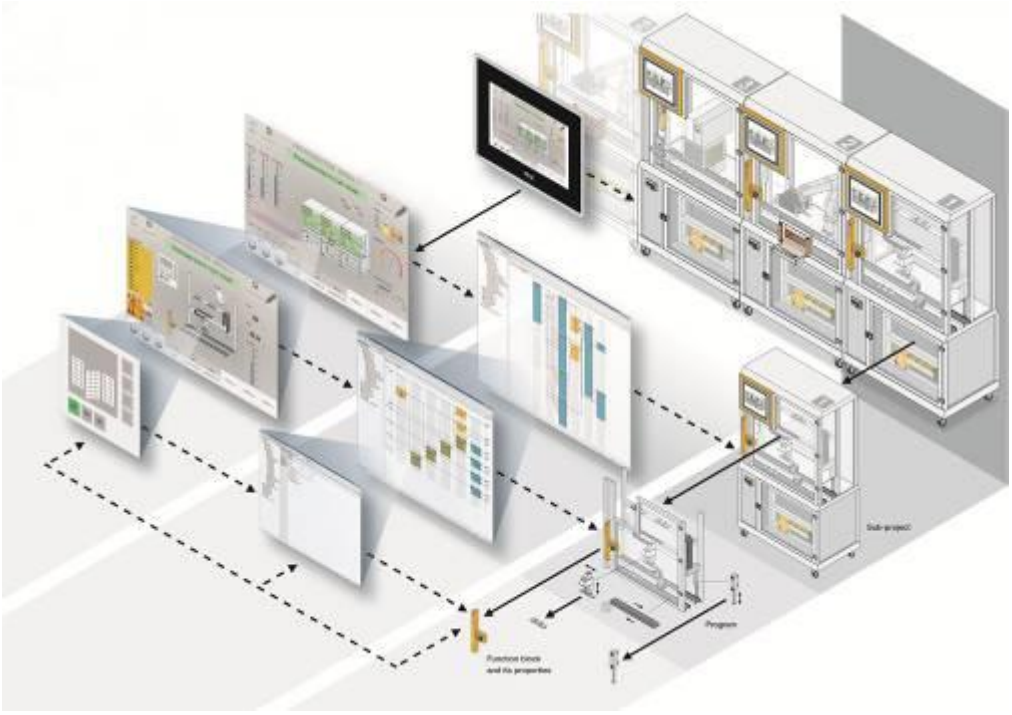

Figura 4: Le linee automatiche possono essere suddivise in unità monitorabili ed autonome.

4.3. Visualizzazione con PASvisu

Secondo lo stesso principio, si possono suddividere fino alla più piccola unità anche i comandi di visualizzazione e controllo. Una base dati comune dei singoli moduli consente ai moduli di comunicare tra loro. Grazie a questa struttura uniforme è possibile riutilizzare facilmente i dati di progettazione.

Il software di visualizzazione consente di creare e configurare i progetti di visualizzazione semplicemente tramite PASvisu Builder.
L'accesso a tutti i dati del progetto di automazione, incluse tutte le variabili di processo e i namespace OPC, rende superflue le operazioni manuali di inserimento e assegnazione delle variabili che potrebbero comportare eventuali errori. E' così possibile, ad esempio, richiamare informazioni come il checksum del progetto o la versione firmware del modulo principale di controllo.

Con il progetto Industrie 4.0 si prende in considerazione il "valore dei dati", in questo caso i dati di progettazione. Una base dati comune riduce le possibili cause di errore estrapolando automaticamente i dati "giusti"; mentre il controllo automatico della consistency consente una riduzione dei tempi di engineering: La conformazione omogenea dei moduli di controllo e visualizzazione facilita il riutilizzo degli elementi e moduli delle macchine.

Glossario

Smart Product
Il prodotto intelligente è corredato di una ID o direttamente di informazioni importanti per la sua produzione e può quindi controllare autonomamente il proprio processo di produzione. Come oggetto intelligente pone le basi per l'"Internet delle cose".

Internet delle cose
Nell'Internet delle cose (Internet of Things, IoT), le "cose", elementi o oggetti intelligenti comunicano tra loro tramite una rete digitale universale. I computer tendono a scomparire sempre più come dispositivi singoli e vengono sostituiti dagli "oggetti intelligenti". Questi oggetti si collegano in rete con Internet in modo da poter comunicare autonomamente attraverso Internet e poter svolgere alcune mansioni per il proprietario.
Si deve soprattutto alla Radio Frequency identification (RFID) come tecnica intelligente di localizzazione se già oggi gli oggetti si sanno identificare da soli e in certa misura anche controllare. Su questi oggetti sono salvate determinate informazioni che indicano cosa devono fare. In questo modo i prodotti stessi comunicano al proprio impianto di flusso del materiale o di produzione quale sia il passaggio successivo. L'intervento umano non è più necessario.

Sistemi cyberfisici (CPS)
Ne fanno parte i dispositivi, gli apparecchi e le macchine (tra questi anche i robot) mobili e movibili, i sistemi integrati e gli oggetti collegati in Internet (Internet delle cose). Il trasferimento e lo scambio dati, così come i controlli e i comandi, avvengono tramite un'infrastruttura, come può essere Internet, in tempo reale.
Si possono controllare e leggere senza alcun contatto diretto e, con l'ausilio dell'intelligenza ad essi assegnata, sono in grado di prendere delle decisioni. Un sistema cyberfisico è caratterizzato da un livello di complessità molto elevato. I sistemi cyberfisici si creano integrando i sistemi intrinsechi attraverso reti di comunicazione collegate via cavo o wireless.

Modello di riferimento per l'architettura (RAMI)
In passato l'automazione era caratterizzata da una struttura basata sull'hardware (piramide dell'automazione). Oggi questa struttura è obsoleta, in quanto l'automazione non è più soltanto una questione di collegamento via cavo tra apparecchi hardware, bensì prevede collegamenti tra cloud e dati. Inoltre, oltre ad avere a disposizione nel processo i dati di produzione, è anche possibile accedere ai dati di comando dall'esterno. Per questo motivo il modello di riferimento per l'architettura (RAMI) è strutturato come una piramide dell'automazione modernizzata. Il ZVEI ha sviluppato le idee e i concetti del settore dell'automazione insieme a VDI/VDE-GMA, DKE e i partner della piattaforma delle associazioni Industrie 4.0 Bitkom e VDMA.[10] Questo modello raduna per la prima volta gli elementi essenziali per Industrie 4.0 in un modello a strati tridimensionale.[11] Sulla base di questa struttura, il progetto Industrie 4.0 può essere ulteriormente classificato e sviluppato in maniera sistematica. Il modello stabilisce anche gli standard Industrie 4.0. Tale standardizzazione è necessaria in quanto il progetto Industrie 4.0 implica che i componenti di aziende diverse possano comunicare tra loro.

[10] http://www.zvei.org/Themen/Industrie40/Seiten/Das-Referenzarchitekturmodell-RAMI-40-und-die-Industrie-40-Komponente.aspx
[11] http://www.zvei.org/Downloads/Automation/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf

Siamo rappresentati a livello internazionale. Per maggiori informazioni visitate
la nostra homepage www.pilz.com o contattate direttamente la nostra casa madre.

Casa madre: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germania
Telefono: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY