ANIE AUTOMAZIONE

ANIE FEDERAZIONE

CONFINDUSTRIA

Osservatorio dell'Industria Italiana dell'Automazione

Maggio 2017

ANIE Automazione

Osservatorio dell'Industria Italiana dell'Automazione

Maggio 2017

Cari Lettori,

inaugurare il ruolo di Presidente di ANIE Automazione è emozionante e farlo con una lettera di presentazione di una delle iniziative centrali della nostra Associazione, lo è ancora di più.
Utilizzo le pagine di questa nuova edizione dell'Osservatorio, presentata in occasione della fiera SPS IPC Drives di Parma, per confermare il positivo andamento del nostro comparto anche per il 2016. L'incremento del mercato e del fatturato delle aziende associate si è assestato intorno ad un 4,7% medio, in relazione alle tecnologie ed applicazioni rappresentate da ANIE Automazione.
Questi risultati indicano che l'automazione sta diventando l'elemento chiave nella rivoluzione industriale, dettata dai principi di Industria 4.0, che sempre più sta permeando il tessuto industriale mondiale ed italiano. Nel nostro Paese, in particolare, garantisce un impulso all'innovazione tecnologica, unico driver per le aziende manifatturiere per lo sviluppo e la sopravvivenza sui mercati globali.
L'Industrial Internet Of Things (IIoT) è il mezzo abilitante che genera una realtà di fabbrica in cui le "cose" (impianti, risorse di produzione e prodotti) acquisiscono la capacità di collegarsi e di scambiare informazioni in tempo reale per poter realizzare sistemi di produzione realmente flessibili, rapidi a riconfigurarsi, per garantire le personalizzazioni che il mercato e ed i consumatori chiedono.
L'interazione e lo scambio di informazioni, tra il mondo IT (Information Technology) ed OT (Operation Technology), consentirà di individuare ed implementare nuove strategie di business basate su inediti scenari tecnologico-produttivi, ma che genereranno anche notevoli rischi per la connettività.
Ecco perché la Cyber Security diventa un elemento chiave che ogni azienda o player nel mondo manifatturiero dovrà affrontare in modo attento e sicuro: pensate ai rischi di perdita di IP (Intellectual Property), di danni di immagine, ecc.
L'approccio dovrebbe basarsi su tre stadi: percezione del rischio (sense), misure di prevenzione (resist) e capacità di reazione (recovery). Purtroppo la visione aziendale è troppo spesso concentrata solo su alcuni di questi elementi - mentre un piano integrato cyber-sicuro dovrebbe prenderli in considerazione tutti - e, a volte, è proprio la parte di "recovery" la meno pianificata.
Ci sono moltissimi elementi di curiosità e di interesse da approfondire su un argomento, la Cyber Security, così importante per la digitalizzazione del comparto manifatturiero che si troverà a gestire una mole di dati (big data) e di informazioni che dovranno essere sicuri per garantire il futuro competitivo dei loro produttori e utilizzatori: cioè noi.
Questo Osservatorio e SPS, evento di cui ANIE Automazione è partner, avranno di certo un ruolo di approfondimento garantendo la possibilità di confronto con i maggiori operatori del comparto.

Fabrizio Scovenna
Presidente ANIE Automazione

Indice

Introduzione

Ad ANIE Automazione aderiscono le imprese, piccole medie e grandi, produttrici di beni e di servizi operanti nel campo dell'automazione dell'industria manifatturiera, di processo e delle reti di pubblica utilità. ANIE Automazione è una delle 14 Associazioni di settore di ANIE – Federazione Nazionale delle Imprese Elettrotecniche ed Elettroniche, aderente a Confindustria.

L'Associazione attraverso i suoi Gruppi rappresenta, sostiene e tutela le aziende che svolgono attività nei seguenti comparti merceologici:

- Automazione di processo
- Azionamenti Elettrici
- Componenti e Tecnologie per la Misura e il Controllo
- HMI-IPC-SCADA
- Meccatronica
- PLC-I/O
- Software Industriale
- Telecontrollo, Supervisione e Automazione delle Reti
- Telematica applicata a Traffico e Trasporti
- UPS - Gruppi Statici di Continuità

ANIE Automazione si propone di favorire lo sviluppo delle imprese e, in particolare:

- svolge un'azione di tutela e di rappresentanza delle imprese nei confronti delle Istituzioni, della Pubblica Amministrazione e della società in generale;
- risponde in maniera qualificata a quesiti legali e tecnico-normativi grazie alla competenza degli esperti dei Servizi Centrali Legale, Ambiente e Tecnico-Normativo di ANIE. Per quanto riguarda le normative internazionali, ANIE Automazione è iscritta al CEMEP *(European Committee of Manufactures of Electrical Machines and Power Electronics)*;
- fornisce ai propri Soci un servizio di raccolta ed elaborazione dei dati di mercato in collaborazione con il Servizio Centrale Studi Economici di ANIE;
- incentiva la ricerca e l'innovazione quale fattore indispensabile allo sviluppo del Sistema Paese;
- promuove la visibilità del settore nel più ampio contesto economico e fornisce un servizio di informazione e assistenza sui temi strategici di interesse del comparto anche attraverso eventi, fiere, convegni e corsi di formazione;
- supporta l'internazionalizzazione delle imprese tramite le iniziative del Servizio Centrale Internazionalizzazione di ANIE;
- realizza pubblicazioni di carattere tecnico-divulgativo e di approfondimento sui mercati di riferimento.

Automazione di processo

L'industria di processo comprende tutte le applicazioni che provvedono alla trasformazione chimico-fisica della materia prima, cioè tutto quanto attiene alla produzione di materiali e di servizi di base. Il Gruppo rappresenta le aziende specializzate nella strumentazione industriale di misura e di controllo in campo, in analizzatori di gas e liquidi, sistemi di controllo di processo, attività di consulenza e ingegneria e Service.

Azionamenti Elettrici

Presidente: Paolo Colombo

Il Gruppo Azionamenti Elettrici riunisce le principali aziende del settore dei convertitori per motori a corrente continua e alternata, dei servoazionamenti e dei motori brushless.
Tra le principali attività, si segnalano le iniziative volte alla promozione della cultura dell'efficienza energetica e dell'innovazione tecnologica; il contributo alla definizione della normativa tecnica; il costante monitoraggio del mercato sia italiano che europeo, e la partecipazione al *Working Group Variable Speed Drives* del CEMEP.

Componenti e Tecnologie per la Misura e il Controllo

Presidente: Andrea Bianchi

Il Gruppo Componenti e Tecnologie per la Misura e il Controllo è composto da aziende specializzate nel settore della sensoristica e del controllo.
Il Gruppo è suddiviso nei Sottogruppi Encoder, Networking, RFID, Safety, Sistemi di Visione e Wireless Industriale le cui attività si articolano su: l'analisi del mercato, gli aspetti tecnici connessi alla tecnologia, la promozione e la comunicazione.

HMI-IPC-SCADA

Presidente: Mauro Galano

Al Gruppo HMI-IPC-SCADA aderiscono le aziende operanti nel campo delle soluzioni che permettono all'operatore di avere il controllo del sistema attraverso la visualizzazione delle informazioni dello stato macchina, la gestione delle emergenze, l'impostazione di parametri atti a definire i cicli di lavorazione e la reportistica dei dati.
Oltre alle attività di promozione che si concretizzano nella realizzazione di documentazione tecnica e convegni, una particolare attenzione viene rivolta al monitoraggio del mercato.

Meccatronica

Presidente: Sabina Cristini

La meccatronica, area di convergenza tra le tecnologie dell'elettronica, della meccanica e dell'informatica, rappresenta un comparto trasversale di grande interesse per i Soci ANIE Automazione. Al Gruppo Meccatronica aderiscono le aziende che realizzano componenti e soluzioni meccatroniche destinate ai produttori di macchine. All'interno del Gruppo è quindi rappresentato un ampio ventaglio di prodotti, hardware e software, con particolare attenzione al mondo del motion control.
Il Gruppo organizza annualmente il Forum Meccatronica, un momento di confronto fra i fornitori di tecnologia, i costruttori di macchine e gli utilizzatori finali sulle nuove frontiere della meccatronica a fronte delle sfide poste da Industria 4.0.

PLC-I/O

Presidente: Roberto Motta

Al Gruppo PLC-I/O aderiscono le aziende del settore dei Controllori Logici Programmabili, delle reti industriali e bus di campo; dei sistemi di connessione; delle interfacce e moduli d'ingresso uscita digitali/analogici; del software di configurazione, programmazione, debug e diagnostica.
Il Gruppo monitora l'evoluzione del mercato e promuove la tecnologia attraverso la realizzazione di pubblicazioni e la partecipazione ad eventi.

Software Industriale

Presidente: Fabio Massimo Marchetti

Il Gruppo di lavoro dedicato al Software Industriale si occupa di seguire l'evoluzione dei trend di mercato e di intraprendere iniziative di alfabetizzazione del settore attraverso la redazione di articoli e manuali e la partecipazioni a manifestazioni e seminari. Al fine di delineare con chiarezza il perimetro di riferimento del WG rispetto al vasto mondo delle tecnologie software, sono state identificate le aree applicative che ne fanno parte. Si è preferito identificare le aree applicative e non le tecnologie per includere tutte le proposte software, indipendentemente dalla base tecnologica utilizzata. Le aree identificate nel perimetro di competenza sono: Area progettazione impianto e prodotto, Area produzione, Area qualità, Area manutenzione e servizi, Area safety, Manufacturing Intelligence.

Telecontrollo, Supervisione e Automazione delle Reti

Presidente: Antonio De Bellis

Al Gruppo Telecontrollo, Supervisione e Automazione delle Reti aderiscono le principali e più qualificate aziende impegnate nella realizzazione di sistemi di telecontrollo per le reti di pubblica utilità (distribuzione elettrica e del gas, ciclo completo delle acque: idropotabile, reflue-depurazione, irrigazione, monitoraggio ambientale). L'implementazione dei concetti di "smart community" e "Industria 4.0", sta trasformando lo scenario economico introducendo nuovi servizi e nuovi ambiti di applicazione delle tecnologie del Telecontrollo, quali la building automation, l'illuminazione, l'E-mobility, la filiera industriale e agricola; facendo rilevare sempre più la presenza nel comparto di aziende provenienti da sfere diverse, soprattutto del settore dell'Information Technology.
Il Gruppo organizza da oltre vent'anni il convegno nazionale biennale del Telecontrollo e opera al fine di presidiare e promuovere lo sviluppo dei temi tecnologici e di mercato propri del settore.
Il Gruppo ha un proprio marchio che attesta l'impegno delle aziende aderenti a sostegno della competitività e dell'ammodernamento sostenibile del Paese.

Telematica applicata a Traffico e Trasporti

La missione del Gruppo è orientata allo sviluppo e alla diffusione della conoscenza dei sistemi, delle tecnologie e dei dispositivi applicabili al controllo e alla sicurezza del traffico stradale e dei trasporti passeggeri e merci. Qualità dell'ambiente e gestione ottimizzata degli impianti e delle infrastrutture di traffico, anche con riferimento alle Smart City e Smart Community, sono due tra i principali obiettivi delle aziende del Gruppo.

Gruppi Statici di Continuità - UPS

Presidente: Enrico Pensini

Il Gruppo UPS di ANIE Automazione è costituito dai principali e più qualificati costruttori di sistemi di continuità. Tra le iniziative del Gruppo, per lo sviluppo del settore, si ricorda la pubblicazione di diverse guide tecniche nazionali ed europee per la scelta dell'UPS ed il monitoraggio del mercato nazionale ed europeo, quest'ultimo attuato attraverso la partecipazione al *Working Group UPS* del CEMEP.

CAPITOLO 1

I PRINCIPALI COMPARTI DELL'AUTOMAZIONE INDUSTRIALE IN ITALIA

Il punto di vista delle aziende di ANIE Automazione

Questo capitolo arricchisce l'Osservatorio con alcune considerazioni emerse nell'ambito dei gruppi di lavoro di ANIE Automazione ed è pertanto il risultato della professionalità e dell'esperienza di chi opera quotidianamente nel settore.
I temi presi in esame, poiché ritenuti di particolare interesse e attualità, sono l'andamento economico del comparto di competenza e l'impatto della digitalizzazione e delle misure previste dal "Piano nazionale Industria 4.0 2017-2020" nei mercati di riferimento.

Paolo Colombo

Presidente Gruppo Azionamenti Elettrici

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

Per il settore degli azionamenti elettrici, il 2016 si è chiuso con un crescita del 7,7%, poco sopra l'andamento complessivo generale dell'Automazione. Più in dettaglio, è il settore degli "AC Drives" a mostrare una maggiore vivacità, con un progresso del 12%, mentre i servoazionamenti seguono da lontano con un incremento del 0,8%. Occorre precisare che molti dei cosiddetti "AC Drives" in realtà possono pilotare diversi tipi di motori, brushless compresi, consolidando una presenza sul mercato di drives "universali". Il dato dei motori brushless conferma questa ipotesi, con un incremento dell'8,1%.

Anche fare previsioni puntuali su singoli paesi, per quanto importanti, sembra essere diventato un esercizio piuttosto sterile, visto che tutte le aziende del nostro settore si muovono su uno scenario globale. Siamo rassicurati dal fatto che il "macrotrend" dell'automazione industriale e della digitalizzazione su cui operano le aziende del nostro settore sono e resteranno dominanti e imprescindibili per la competitività del nostro sistema produttivo. Sarà quindi importante capire come le aziende dovranno attrezzarsi ed evolvere per un mondo sempre più incerto e flessibile.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

Dalla crisi del 2009, gli scenari industriali europeo e statunitense sono stati colpiti pesantemente.
Da allora, le strategie di riqualificazione del settore manifatturiero si sono basate su un nuovo concetto di fabbrica digitale, che ha preso nomi diversi: negli Stati Uniti "Advanced Manufacturing Partnership 2.0", in Europa "Industry 4.0", concept presentato alla fiera di Hannover nel 2011. Da allora l'industria, in particolare tedesca, non ha smesso di investire nella dotazione tecnologica delle imprese, e questa tendenza si è gradualmente allargata alle aziende clienti, con particolare riguardo alle multinazionali.
L'Italia dal 2009 ha subito una perdita della produzione manifatturiera quasi del 18%, tre volte la perdita media nell'area Euro. Nonostante questo, la produttività media delle industrie italiane ha tenuto e addirittura incrementato il suo valore, sostenuta dalle PMI fino a 250 addetti. È per questo che la presentazione del Piano Nazionale Industria 4.0, che comprende un ampio "pacchetto" di misure per la competitività (Nuova Sabatini, Patent box ecc.) sembra soprattutto indirizzato a imprese di queste dimensioni, perché ritornino a investire in beni strumentali e digitalizzazione. La formula proposta è davvero innovativa e può costituire un volano importante per gli anni a venire, generando entrate immediate per il sistema fiscale grazie ai maggiori ricavi delle imprese venditrici e dilazionando invece i benefici per le aziende compratrici secondo il loro piano di ammortamento. L'industria italiana si è mostrata da subito molto interessata e ricettiva su una prospettiva di incentivazione fiscale; i tempi ristretti per la realizzazione hanno ulteriormente accelerato le richieste di informazioni e di soluzioni tecniche alle aziende del Gruppo Azionamenti, sia per la realizzazione di nuove macchine interconnesse che di retrofit su macchine e impianti esistenti. Su questo ultimo aspetto, una recente nota del MISE chiarisce anche gli ultimi aspetti e le incertezze nell'interpretazione delle norme. Per le ragioni esposte ci aspettiamo un 2017 molto importante per il nostro mercato, con una accelerazione prevista nella seconda parte dell'anno. Sempre più prodotti delle aziende del Gruppo Azionamenti prevedono e integrano caratteristiche abilitanti per l'Industria 4.0: funzionalità "safety" integrate, funzioni per la gestione della manutenzione predittiva e del consumo energetico, interfacce uomo-macchina semplici e intuitive. I sistemi di azionamento intelligenti e interconnessi sono infatti il cuore tecnologico delle macchine "Industry 4.0".

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

In estrema sintesi: si ha coscienza dell'opportunità ma continua la difficoltà a vedere le applicazioni in azienda. E' anche per questo motivo che l'attenzione e le richieste dei nostri clienti, sia OEM che utilizzatori, sono così elevate in questa fase.
La digitalizzazione è entrata nelle nostre vite quotidiane, rivoluzionando interi settori merceologici: si pensi a come è cambiato il nostro rapporto con le banche, come organizziamo viaggi e spostamenti, come evolvono le abitudini di acquisto. Mentre tutto questo avviene, le potenzialità in ambito aziendale non sono ancora conosciute e colte appieno.
Nel corso del 2017 sarà responsabilità anche di ANIE Automazione, oltre che delle singole aziende associate, creare una "Cultura 4.0" e curare la formazione e la crescita delle persone in tal senso.
Diverse iniziative sono già in corso, dagli eventi istituzionali già programmati (ad esempio, la fiera SPS IPC Drives Italia di Parma e il Forum Meccatronica) a nuovi strumenti come "ANIE per Industria 4.0": una nuova sezione del portale anie.it dedicata a Industria 4.0 e uno sportello per richiedere chiarimenti e supporto sulla corretta applicazione del c.d. piano Calenda.

Andrea Bianchi

Presidente Gruppo Componenti e Tecnologie per la Misura e il Controllo

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

In uno scenario globale in cui i principali settori industriali stanno subendo una profonda trasformazione dettata da un sempre maggior impiego di intelligenza distribuita, digitalizzazione e interconnessione, le applicazioni di automazione industriale devono offrire soluzioni adeguate per soddisfare appieno le nuove impostazioni organizzative di fabbrica e di processo. Ciò si rivela terreno fertile per lo sviluppo del mercato della componentistica impiegata per la misura e il controllo dei processi produttivi industriali, cui fanno capo le principali tecnologie protagoniste del processo di innovazione in corso. Non a caso i risultati registrati nel 2016 dai segmenti tecnologici prevalenti del comparto mostrano un'evoluzione positiva del giro d'affari complessivo, con tassi di crescita in alcuni casi sopra l'andamento medio del mercato dell'automazione industriale. In tal senso, estremamente interessanti sono i profili del Networking industriale a base Ethernet; della sensoristica per la misura e il controllo dei processi produttivi e logistici (Encoder, Sistemi di visione, Wireless), nonostante abbia risentito in alcuni ambiti la crisi di alcuni settori applicativi trainanti (nello specifico, Rfid e Automotive); e delle soluzioni per la sicurezza della macchina e dei dati (Safety e Security). L'export risulta ancora la principale componente della crescita registrata. Il maggiore mercato di riferimento rimane l'EMEA, seguito dal Nord America che continua ad offrire importanti possibilità di sviluppo, mentre l'Asia fatica a mantenere le aspettative anche a causa della continua diminuzione dei prezzi dovuta in parte alla concorrenza di nuovi produttori a basso costo e non allineati alle certificazioni in essere.
La sensazione è che il 2017 sarà un anno di sviluppo importante per il comparto, dove il peso dell'export continuerà ad essere predominante, mentre una scossa allo stagnante mercato domestico, che finora ha mostrato solo timidi segnali di ripresa, dovrebbe arrivare dal nuovo piano nazionale di politica industriale.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

Le misure governative per agevolare gli investimenti in ottica 4.0, contenute nella Legge di Bilancio 2017, porteranno sicuramente nuovo fermento per l'implementazione di soluzioni ad alta digitalizzazione in ambito industriale, con una conseguente ricaduta benefica su tutta la filiera dell'automazione, e quindi anche sui fornitori di componenti e tecnologie.
Se da un lato non c'è dubbio che gli incentivi del Piano Calenda contribuiranno a trainare gli investimenti in innovazione, dall'altro ci si augura che le imprese che decidono di investire in soluzioni tecnologiche I4.0 siano pienamente consapevoli che solo attraverso l'innovazione si può avere lo sviluppo e la sopravvivenza sui mercati globali. Resta, infatti, da capire e valutare quanto queste misure determineranno sensibili

incrementi produttivi per le aziende italiane che, da tempo, si sono pesantemente orientate verso l'export.

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

Indipendentemente dagli incentivi statali per gli investimenti in innovazione e competitività, l'interesse del mercato per i concetti di digitalizzazione in senso lato è concreto.
L'importante sforzo di comunicazione/formazione sostenuto da tempo dai maggiori player del settore in termini di fornitura di componentistica e soluzioni industriali, affiancati in questo da Associazioni, Enti e Università, ha creato ed alimentato questo interesse. Interesse "certificato" dal successo di tutti i seminari, eventi, incontri dedicati all'argomento.
L'applicazione dei concetti non procede però di pari passo, nel senso che la risposta non è omogenea: sono infatti molte le realtà industriali, soprattutto quelle con risorse più limitate, che, pur consce dei vantaggi, non hanno ancora definito piani concreti di investimento.

Mauro Galano

Presidente Gruppo HMI-IPC-SCADA

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

L'instabilità legata al quadro geopolitico è molto diffusa: la guerra in Medio Oriente, la posizione della Turchia nei confronti dell'UE, la difficoltà di prevedere a medio lungo termine la posizione degli Stati Uniti, creano molta incertezza, in ogni settore. Al di là delle diverse situazioni contingenti, il nuovo Presidente americano potrebbe accelerare un cambiamento delle politiche economiche delle aziende multinazionali, e quindi della globalizzazione, di cui è assolutamente impossibile prevedere gli sviluppi.
Nell'immediato, nonostante questa incertezza, il mercato continua ad essere brillante, con la Cina che fa da traino soprattutto al mercato europeo.
Questo fa ben sperare per il prosieguo del 2017, che è iniziato nel migliore dei modi con un ottimo primo trimestre, ma rimane sempre arduo fare previsioni anche solo nel medio termine.
Le tecnologie di competenza del Gruppo rappresentato hanno riportato nel corso del 2016 risultati altalenanti a seconda dei settori. Il mercato del dialogo operatore, tradizionalmente legato a quello dei PLC, ha riportato un incremento di quasi l'8% rispetto all'anno precedente, attestandosi ad un valore ormai superiore a quello pre-crisi (2008). I modelli touch-colore, sempre in crescita, rappresentano oltre l'85% del mercato con una focalizzazione sui display fra 5.7" e 10.4", ma sono in continuo aumento quelli con schermi più grandi (oltre 10"). I modelli con display wide-screen (16:9) continuano la loro espansione ma quelli con schermo 4:3 tengono ancora molto bene con un 48% sul totale.
I PC industriali hanno anch'essi riportato un aumento paritetico a quello dei pannelli operatore con un incremento del'8% rispetto al 2015.
I modelli modulari, con monitor separato, rappresentano il 30% della rilevazione del mercato e sono cresciuti di circa il 20% rispetto allo scorso anno. I modelli integrati/compatti continuano ad essere le soluzioni preferite soprattutto dai costruttori di macchine: all'interno di questo gruppo c'è una buona crescita dei PC tradizionali mentre c'è stato un arresto dell'espansione dei modelli embedded, in lieve contrazione.
Ciò probabilmente è dovuto alla grande diffusione dei dispositivi di memoria SSD al posto dei tradizionali HardDisk meccanici, che insieme all'utilizzo di architetture fanless ha di fatto diminuito l'interesse dei clienti dalla piattaforma embedded: tali soluzioni, dal punto di vista dell'affidabilità della macchina, si differenziano solo dal sistema operativo, embedded appunto.
I computer con monitor grandi (oltre 18") continuano a raccogliere sempre maggiori consensi così come i touchscreen capacitivi, che si affiancano ai sempre richiesti modelli resistivi.

Il comparto SCADA ha invece riportato un risultato negativo con una contrazione di oltre il 5% rispetto al 2015, invertendo il trend positivo degli ultimi anni. Le licenze runtime con taglia sopra i 1500 tag rappresentano il 70% del fatturato complessivo ed indicano una sempre maggiore focalizzazione di questa tipologia di

prodotto verso applicazioni di medie-grandi dimensioni, per la supervisione di linee ed impianti.
Tuttavia la contrazione si registra sia sulle taglie grandi che su quelle piccole, indicando una difficoltà generale del mercato per questi prodotti su impianti e linee, ma anche presso costruttori di macchine.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

Il piano Industria 4.0 produrrà, e speriamo in modo importante, due grandi miglioramenti: il primo è il rinnovamento generale degli impianti che spesso sono obsoleti (il 70% degli impianti ha oltre 25 anni dice uno studio di Ucimu). Il secondo è l'introduzione di nuove tecnologie a livello hardware e software che contribuiscono a realizzare macchine, linee impianti e fabbriche più efficienti, flessibili e connesse. Ciò comporta un'ulteriore spinta all'utilizzo di nuove tecnologie/funzionalità anche nel campo dell'HMI, componente fondamentale che rientra come bene materiale necessario in una architettura "Industria 4.0".
La facilità d'uso e tempi di sviluppo ridotti diventano requisiti fondamentali per l'innovazione; la completezza delle informazioni e la fruibilità dei dati, attraverso l'utilizzo dell'acceso remoto, tramite cloud e dispositivi mobili, diventano indispensabili per prendere le migliori decisioni in tempo reale.
Tali funzionalità fino a ieri opzionali, diventano oggi parte indispensabile della soluzione di visualizzazione, che in questo modo integra al suo interno un sempre maggior numero di funzioni un tempo riservate a soluzioni di livello superiore.
Soprattutto consentire l'accesso di utenti occasionali da terminali portatili, quali smartphone e tablet, con il supporto del cloud per la condivisione delle informazioni, è ormai diventato un requisito indispensabile in una offerta HMI 4.0.
La diffusione di queste tecnologie nell'ambito dell'automazione, comporterà certamente una ulteriore rapida evoluzione delle soluzioni HMI che adotteranno gli ultimi ritrovati tecnologici ad oggi riservati al mondo consumer, adattandoli al mondo industriale in termini di affidabilità, stabilità e sicurezza.

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

Il piano nazionale Industria 4.0 è operativo dall'inizio del 2017, ma ancora molto spesso le aziende hanno le idee poco chiare e non sanno esattamente cosa devono fare per poter usufruire dei benefici economici previsti dal Ministero per lo Sviluppo Economico.
ANIE ha quindi voluto supportare i propri Soci, aprendo un portale web dedicato in cui vengono evidenziate le tecnologie che devono essere utilizzate in modo tale che i clienti possano sfruttare l'opportunità di modernizzare i propri impianti.
Inoltre è stato istituito anche uno sportello ad hoc (industria4.0@anie.it) per rispondere ad eventuali problematiche sollevate dai clienti.

Ma innanzitutto occorre distinguere la posizione dei costruttori di macchine e quella dei clienti finali. Tipicamente è il costruttore di macchine che è maggiormente in difficoltà perché non sa esattamente come deve essere equipaggiata la propria macchina affinché sia "conforme 4.0".
Molto spesso la macchina è già predisposta per soddisfare i criteri richiesti e possiede buona parte dei dispositivi/funzionalità necessari.
La rete Ethernet, già pronta per essere collegata alle linee ed agli impianti esistenti, è ormai sempre presente mentre la sensoristica ed i dispositivi intelligenti sono in grado di fornire informazioni dettagliate

in tempo reale ai dispositivi di visualizzazione ed ai software di livello superiore.
Nello stesso modo la presenza di un accesso remoto per monitoraggio ed assistenza sono un must da parecchio tempo, per offrire un servizio di supporto immediato a costi ridotti.
Tuttavia il costruttore di macchine OEM non sapendo come il suo macchinario verrà installato ed utilizzato dal cliente finale nel proprio stabilimento ha spesso delle perplessità, se non riceve richieste specifiche dal cliente finale.
Ed è proprio il cliente finale che deve mettere in atto il piano Industria 4.0: le nuove macchine devono essere predisposte per essere integrate nelle linee e nello stabilimento.
A questo proposito negli ultimi mesi si è creato molto interesse intorno ai software di Business Intelligence ed al MES che di fatto devono realizzare la convergenza fra Automazione e ICT.
Ad oggi questa integrazione è ancora molto parziale o manca del tutto perché i vantaggi, in funzione dei costi da sostenere, non sono ritenuti così evidenti.
Talvolta, anche gruppi multinazionali che all'estero utilizzano normalmente questi software, qui in Italia hanno deciso di non implementare queste soluzioni, convogliando tali investimenti in altri settori.
Ci auguriamo che l'opportunità di modernizzazione offerta dal Piano Industria 4.0 aiuti la diffusione di queste soluzioni software che consentono alle aziende di raggiungere obiettivi migliori in termini di maggiore flessibilità, efficienza e risposta più pronta alle esigenze di mercato, grazie ad una maggiore integrazione tra persone, processi e tecnologie.

Roberto Motta
Presidente Gruppo PLC-I/O

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

Il valore del comparto dei controllori programmabili per l'anno 2016 è rimasto praticamente stabile rispetto al 2015 (meno di un punto percentuale di crescita).
C'è da rilevare comunque, che, durante l'ultima riunione del Gruppo svoltasi all'inizio di aprile 2017, una diffusa positività è emersa per la chiusura dell'esercizio 2016 con una visibilità sull'anno in corso che lascia ben sperare sulle prospettive di chiusura almeno del primo trimestre 2017.
In generale nel 2016 si è confermato il ruolo di traino delle esportazioni, mentre le previsioni per l'anno 2017 auspicano un deciso contributo anche da parte del mercato interno grazie agli incentivi previsti dal piano Industria 4.0.
Al generale ottimismo ha probabilmente contribuito il fatto che il consuntivo del 2016 vede un mercato che si è mantenuto ad un valore superiore a quello pre-crisi del 2008. La conferma di questo trend positivo (la parità con il 2008 era stata raggiunta nel 2015) ci aiuta a vedere chiari segnali di consolidamento del settore automazione nel suo complesso volendo riporre anche una giusta aspettativa positiva per il mercato interno nel corso del secondo semestre, grazie al c.d. Piano Calenda.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

La prima delle 5 caratteristiche obbligatorie che le macchine devono avere per accedere all'iperammortamento è il controllo a mezzo di PLC (e/o CNC): pertanto è facile aspettarsi che il Piano porterà un contributo significativo al settore che rappresento.
Certo il comparto dovrà affrontare una trasformazione "epocale" per tenere il passo con l'innovazione guidata dall'Industrial Internet of Things che rappresenta una delle tecnologie abilitanti di INDUSTRIA 4.0. L'ambito applicativo tipico del PLC vede una crescita pervasiva dei dispositivi "mobile" su una rete che è sempre più "Giga ethernet", "gestita" ed in grado di offrire non solo funzioni di switching, ma anche di "routing" per il trasferimento di una mole sempre più rilevante di dati (big data) che vanno trasformati in informazioni.
Quanto sopra è supportato dal fatto che le 5 caratteristiche obbligatorie includono "l'interconnessione ai sistemi informatici di fabbrica" e "l'integrazione con il sistema logistico della fabbrica e/o altre macchine". La rete, oltre al PLC, dovrebbe rappresentare il volano più significativo per l'espansione del settore nel corso del secondo semestre 2017. I PLC sono pronti a dare il loro contributo al piano ministeriale, ma servirà che gli addetti al settore prendano sempre più padronanza anche delle tecnologie di rete IP perché, citando dalla

circolare di chiarimento ad Industria 4.0: "una macchina è definita interconnessa se scambia informazioni con i sistemi informatici interni o esterni alla fabbrica per mezzo di un collegamento su cui sia identificata univocamente mediante l'utilizzo di standard di indirizzamento internazionali (ad esempio un indirizzo IP)".

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

L'Italia rimane il secondo Paese manifatturiero d'Europa e fra i primi del mondo, oltre ad essere uno dei soli cinque ad avere un surplus commerciale positivo (dietro a Cina, Germania, Giappone e Corea). Quello che la nostra industria dovrà dimostrare di essere capace di affrontare nei prossimi mesi è proprio la sfida della così detta 4° rivoluzione industriale (da cui è stato preso il termine Industria 4.0).
La digitalizzazione della produzione avrà come denominatore comune la connettività diffusa a tutti i livelli aziendali grazie alla disponibilità di alcune tecnologie chiave quali la Mobility, la Security, il Cloud computing ed i software di Analytics. L'interesse da parte delle aziende del comparto manifatturiero che serviamo è molto elevato e alcune sono già partite a ragionare in termini I4.0, sia i costruttori per dare valore aggiunto ai propri clienti che gli utilizzatori per poter accedere alle agevolazioni. Investimenti sono già stati pianificati e a breve si prevede di iniziare la fase di effettiva implementazione.
Di pari passo sta sviluppandosi l'integrazione dell'ICT all'interno dei processi manifatturieri contribuendo in maniera significativa alla straordinaria importanza che godono oggi in ambito industriale software e networking rispetto a davvero pochi anni fa.
I software non occupano più un posto di rilievo solo per i programmi gestionali, la rete logistica e la gestione dei fornitori, ma l'integrazione fra questi livelli e le attività di progettazione, analisi, manutenzione e gestione della produzione rappresentano la vera novità dei processi di digitalizzazione. L'affermarsi di Industria 4.0 vedrà, prevedibilmente, una sempre maggiore integrazione anche a livello di catena del valore con il ricorso, per esempio, sempre più capillare al Cloud e a software di tipo Analytics.

Antonio De Bellis

Presidente Gruppo Telecontrollo,
Supervisione e Automazione delle Reti

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

Il 2016 si è chiuso con segno positivo per il mercato del Telecontrollo, con la ripresa degli investimenti nel settore Energia e una crescita degli stessi nel settore Acqua ed Industria.
Confrontando la prestazione del panel di aziende coinvolte nell'indagine statistica ANIE, la crescita rispetto al 2015 si attesta nell'intorno del 20%, con la componente di business nei servizi predominante rispetto a quella nei sistemi forniti. Tale andamento è ampiamente giustificabile con l'attuale maturità dei sistemi installati e la politica delle utility più improntata su investimenti in OPEX, piuttosto che in CAPEX, ovvero di manutenzione e aggiornamento dell'attuale, rispetto a scelte di rifacimento.
Nello specifico dei settori, da evidenziare la conferma anche nel 2016 dell'incremento di investimenti nell'Acqua. Questo risultato avvalora gli effetti positivi dovuti all'integrazione del settore idrico nell'ambito AEEGSI (Autorità per l'energia elettrica il gas ed il sistema idrico).
La trasformazione digitale guiderà gli investimenti nel mercato, con tempistiche e modalità che sono ancora da definire. Sono presenti sul mercato pochi casi in cui è stata già delineata la strategia legata alla trasformazione digitale, e in quei casi si sta assistendo a investimenti nell'infrastruttura ICT, nonché casi pilota per sperimentare e validare alcune nuove soluzioni, per esempio in ambito IA (intelligenza artificiale).

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

Il tema della trasformazione digitale è ampiamente dibattuto nel mercato del Telecontrollo, mercato che è da tempo pioniere nell'applicazione di alcuni concetti basilari, quali IOT, clouding e IA. D'altro canto, la trasformazione digitale richiede un cambio di paradigma riguardo i prodotti e servizi erogati, nonché dei processi e dell'organizzazione aziendale sottesi.
Se la trasformazione digitale è vincolante per riuscire a competere sul mercato ed è un processo al quale nessuno si può sottrarre, anche chi opera in ambiti regolamentati, la stessa richiede tempistiche e dinamiche differenti per la sua implementazione da parte dei differenti stakeholder coinvolti. Non da ultimo, la creazione di piattaforme ed ecosistemi digitali determina l'entrata in campo di nuovi stakeholder.
La trasformazione digitale è il fattore abilitante per accelerare la rivoluzione nel modo in cui lavorare e vivere, determinando un nuovo passo evolutivo per le reti di pubblica utilità, industria e città. Mondi che viaggiavano in parallelo e i cui punti di contatto e le cui regole di interazione erano ben definiti, convergono e si sovrappongono con la trasformazione digitale. L'industria e l'imprenditoria del Telecontrollo in Italia, non è impreparata a questa evoluzione, vantando esperienza quali precursori nei processi di trasformazione,

legati a fenomeni tecnologici, economici, sociali, ecc. La trasformazione e i suoi effetti sono in questo caso molto pesanti per l'intero settore, e per dare la portata di ciò si pensi a cosa comporta passare dal gestire un processo dove un utente di un sistema di telecontrollo prendeva decisioni e azioni, interagendo con il campo, per mediazione di interfacce uomo-macchina, alla realizzazione di ambienti dove macchine, basate su intelligenza artificiale, connesse in cloud ai big data, saranno in grado di fornire risposte utili per decidere ed agire, o saranno delegate a decidere ed agire da sé.
La convergenza e convivenza tra ICT e OT (Operational Technology) è un aspetto del processo di digitalizzazione che è in corso da qualche anno, nel Telecontrollo, assumendo però una valenza differente con la trasformazione digitale. Infatti tra i temi più dibattuti e sensibili ci sono la questione del clouding e della condivisione delle informazioni, driver per una trasformazione digitale che usi abilmente la convergenza tra ICT e OT.

A Verona, il 24 e 25 Ottobre 2017, il Forum Telecontrollo, organizzato da ANIE Automazione e Messe Frankfurt Italia, proporrà il tema della "Evoluzione IOT e digitalizzazione 4.0" per le reti, città, industria. Oltre a condividere quanto si sta facendo, si confronteranno le visioni sul futuro imminente e i diversi percorsi virtuosi da intraprendere, affrontando i temi di cui sopra con un dibattito aperto tra gli stakeholder. Durante il Forum Telecontrollo si è sempre data una visione prospettica di problemi, rischi ed opportunità, anticipando di qualche anno quanto poi sarebbe accaduto: anche in questa edizione, la 15°, getteremo le basi per costruire il nostro futuro, migliore.

Fabio Massimo Marchetti

Presidente Gruppo Software Industriale

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

Al momento attuale non abbiamo a disposizione dei dati certi relativi all'andamento del mercato di riferimento in quanto il Gruppo ha ripreso le sue attività operative solo di recente e quindi non dispone di trend effettivi derivanti da attività pregresse. In tal senso stiamo predisponendo un percorso di raccolta di dati tra i partecipanti al WG che sarà completato dalle analisi effettuate da altri osservatori di pari natura con cui sono in corso di definizione delle partnership di sinergia operativa. Sin da ora, però, possiamo riportare che il "sentiment" complessivo relativo al software industriale è estremamente positivo. Questa percezione deriva da dichiarazioni non contestualizzate da dati effettivi e che temporalmente possono essere riferite al secondo semestre del 2016 ed a questo inizio di 2017.
Al fine di delineare con chiarezza il perimetro di riferimento del nostro Gruppo di lavoro, e quindi del "sentiment" di cui sopra, rispetto al vasto mondo delle tecnologie software, è opportuno riportare le aree applicative che ne fanno parte. Abbiamo preferito identificare le aree applicative e non le tecnologie per includere tutte le proposte software, indipendentemente dalla base tecnologica utilizzata. Le aree identificate nel perimetro di competenza sono:

Area progettazione impianto e prodotto

- Modellazione (2d/3d)
- Disegno e progettazione (Cad/Cam/Cae - 2d/3d)
- Gestione ciclo vita prodotto (Extended Plm)
- Simulazione (2d/3d progettazione e virtual commissioning)
- Realtà aumentata
- Analytics (reporting, BI, Advanced analytics, IoT data da prodotti/impianti installati, ...)

Area produzione

- Schedulazione dinamica
- Production Management (Mom,Mes, IoT monitoring, interfaccia macchine, on prem gateways, fog computing, ...)
- Performance (Mes, KPI apps, IoT Monitoring, interfaccia macchine, on prem gateways, fog computing, ...)
- Track & Tracing (Mom, Mes, IoT tracking, interfaccia macchine, interfaccia dispositivi, tecnologie di identificazione, on prem gateways, fog computing, ...)
- Analytics (reporting, BI, Advanced analytics, ...)
- Security e Infrastrutture (security management, security agents, IoT, remote access, semplificazione cablaggi, multi protocolli, ...)

Area qualità

- Quality management (QMS, IoT predictive quality, ...)
- Tools Management
- Analytics (reporting, BI, Advanced analytics, ...)
- Security e Infrastrutture (security management, security agents, IoT, remote access, semplificazione cablaggi, multi protocolli, ...)

Area manutenzione e servizi

- Maintenance management (CMMS, ...)
- Predicitive maintenance (CMMS, IoT, ...)
- Remote maintenance (Open VPN, IoT platform, on prem gateways, fog computing, ...)
- Remote maintenance support (Wearable devices, condivisione vista, realtà aumentata, ...)
- Analytics (reporting, BI, Advanced analytics, ...)
- Security e Infrastrutture (security management, security agents, IoT, remote access, semplificazione cablaggi, multi protocolli, ...)

Area safety

- Monitoraggio persone (RTLS, verifica DPI, uomo a terra, ...)
- Gestione emergenza
- Analytics (reporting, BI, Advanced analytics, ...)
- Security e Infrastrutture (security management, security agents, IoT, remote access, semplificazione cablaggi, multi protocolli, ...)

Manufacturing Intelligence

- Analytics di aggregazione, pianificazione, gestione, predizione, prescrizione e cognitive.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

Alcuni dei requisiti fondamentali alla base del paradigma Industria 4.0 sono relativi alla connessione dei sistemi di produzione nelle infrastrutture ICT ai fini di rendere disponibili dati e ricevere parametri ed informazioni. Come ben descritto nel Piano Nazionale Industria 4.0, i benefici attesi dall'adozione del paradigma (e delle relative tecnologie) sono individuabili nella flessibilità dei processi produttivi, il miglioramento delle performance, una sempre più elevata qualità, una riduzione dei costi per le attività manutentive ed un utilizzo ottimizzato dei vettori energetici. E' proprio l'adozione di software industriali avanzati che permette di raggiungere questi obiettivi. In questo contesto stiamo assistendo ad un elevato incremento della domanda che si convertirà in un'espansione significativa del mercato relativo al software industriale. Naturalmente esistono delle criticità che potranno limitare questa crescita. Tra queste possiamo sottolineare: la conoscenza delle possibilità rese disponibili da queste tecnologie soprattutto nel segmento della piccola-media industria manifatturiera, la definizione di modelli di calcolo del ritorno degli investimenti che includano i fattori di accelerazione resi disponibili dagli incentivi del PNI4.0, la velocità di riconversione dei modelli di business al fine di sfruttare al massimo l'opportunità generata dai nuovi paradigmi.

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

La percezione sul tema della digitalizzazione è abbastanza marcata nelle aziende di grande dimensione, mentre nelle piccole e medie imprese risulta ancora un po' disomogenea con punte di eccellenza e situazioni di estrema non comprensione. Possiamo segnalare che il PNI4.0 ha creato un fenomeno di interesse generato dalla disponibilità automatica di incentivi e ha incuriosito gli imprenditori, generando un innalzamento del livello di percezione che, essendo necessariamente un percorso di crescita culturale (sia di comprensione che di utilizzo), non può essere estremamente rapido. Da un punto di vista tecnologico la digitalizzazione sta diffondendo una percezione di semplificazione delle architetture e del livello di investimento necessario per la loro adozione.
La convergenza tra automazione ed ICT sta creando però anche un fenomeno di "conflitto" di competenza sul tema della digitalizzazione tra le figure aziendali di riferimento delle aree tecnologiche, che dovrebbe portare al decadimento dei confini di dipartimento tradizionalmente in uso nelle aziende manifatturiere.
La crescita culturale da una parte, ed un approccio multidisciplinare dall'altra, sono i nuovi fattori in corso di definizione all'interno delle aziende.
Quanto sia impattante la convergenza tra automazione e ICT, e quindi percepita o meglio percepibile, lo riscontriamo anche nel nostro Gruppo di lavoro dove abbiamo rappresentate aziende che si sono evolute arrivando dal mondo dell'automazione ed altre che, operando da sempre nel settore ICT, hanno completato la loro offerta a copertura dell'area industriale.

Enrico Pensini

Gruppi statici di Continuità - UPS

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

Gli UPS sono ormai dei prodotti maturi, con un prezzo in fase calante che fa si che la potenza istallata si sia mantenuta leggermente superiore, ma a prezzi inferiori. Le aziende, sia pubbliche che private, hanno tagliato i costi relativi alla qualità dell'energia e, di conseguenza, ai gruppi di continuità. A questo dobbiamo aggiungere che è molto difficile quantificare quale sia il ritorno positivo di un investimento in UPS, con la conseguenza che le aziende preferiscono risparmiare, assumendosi il rischio per eventuali interruzioni di energia. Tutte queste componenti hanno influito sulla stagnazione del mercato.
Fortunatamente, l'invecchiamento dei gruppi esistenti e i relativi investimenti per la loro sostituzione hanno permesso una crescita del mercato. Va rilevato altresì che le imprese attente all'analisi dei consumi hanno provveduto alla sostituzione delle macchine con UPS di recente costruzione che presentano rendimenti molto più elevati consentendo notevoli risparmi nei costi imputabili al consumo di energia.
Un altro fattore critico registrato nel 2016 è stato l'incremento delle importazioni dai Paesi dell'Estremo Oriente che, con una politica dei prezzi molto aggressiva, hanno acquisito quote di mercato a scapito della produzione di aziende italiane leader del settore.
In conclusione, si prevede per l'anno in corso una situazione pressoché invariata rispetto al 2016 mancando le premesse di investimenti significativi nel breve periodo. In questo contesto stazionario saranno avvantaggiate le aziende affidabili in grado di assicurare prodotti di altissima qualità e un servizio di assistenza presente e capillare.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

Il "Piano nazionale Industria 4.0 2017-2020" offre senz'altro ottime opportunità a chi vuole sfruttare le possibilità che stanno emergendo. Per ciò che concerne il nostro settore purtroppo quest'ultimo è solo sfiorato dalle agevolazioni previste dal Piano se non per il fatto che chi investe nelle industrie manifatturiere ha bisogno che la qualità dell'energia elettrica sia maggiore dello standard (che fra l'altro è buona in Italia) e quindi l'applicazione dei gruppi di continuità diventa indispensabile per alimentare tutti i processi produttivi. Una prova di ciò è rappresentata dai grandi data-center che assumono sempre più importanza anche in Italia e che sono indispensabili per le Telecomunicazioni e i settori finanziari che devono operare 24 ore al giorno, 365 giorni all'anno.
Una gestione e applicazione intelligente delle misure previste dal c.d. Piano Calenda potrà quindi portare un beneficio indiretto anche al nostro settore.

Da un punto di vista tecnologico qual è il grado di percezione dei vostri clienti sul tema della digitalizzazione? E quindi della convergenza tra automazione e ICT?

Questo è un punto molto importante che penso non sia completamente percepito dalla maggioranza dei nostri clienti. Non dimentichiamo che in Italia oltre il 50% delle aziende sono di piccole dimensioni e non sono in grado quindi di percepire i benefici della digitalizzazione se non dopo che la stessa si è affermata nella società. Ma ritengo che sia solo questione di tempo e arriveremo poi molto rapidamente ad una convergenza completa.

Sabina Cristini

Meccatronica

Il 2016 è stato un anno positivo anche se con dati di crescita inferiori all'anno precedente. Qual è stato l'andamento del mercato per le tecnologie di competenza del Gruppo?
Dalla scorsa estate è in atto nei mercati avanzati e in alcuni dei maggiori emergenti (Cina in testa) una marcata accelerazione delle attività produttive, sia nel manifatturiero sia nel terziario. La progressione dovrebbe proseguire nel 2017 nonostante l'instabilità legata sia all'alta volatilità dei mercati finanziari sia al quadro geopolitico. Cosa prevede per il settore da lei rappresentato? Ci sono segnali in tal senso?

Nel 2016 in generale si è evidenziato un rafforzamento delle principali economie emergenti.
Stati Uniti e Giappone hanno registrato un andamento dinamico, grazie alla tenuta della domanda interna e agli effetti previsti di politiche di bilancio espansive di sostegno alla produttività. Nel 2016 le esportazioni verso gli USA hanno registrato un rallentamento in attesa delle elezioni presidenziali e, di fatto, sull'andamento dell'economia pesa l'incognita delle future scelte USA, che potrebbe condizionare pesantemente gli sviluppi dei prossimi mesi.
La Cina d'altro canto ha dimostrato di essere in grado di mantenere gli obiettivi di crescita predisposti dal governo, portando a un aumento del Pil tra il 6,5 e il 7% nel 2016. L'industria cinese rimane quindi forte, il suo indice manifatturiero è salito ben oltre le attese degli economisti e il 2016 è stato confermato come anno di consolidamento dell'economia cinese, allontanando le preoccupazioni di inizio 2016, quando l'indice era sceso e si paventava una contrazione dell'economia.
A livello europeo si sono registrati ritmi diversi in termini di ripresa, più trainante la Germania, Spagna in exploit, Francia e Italia più in difficoltà nel trovare forti stimoli per il rilancio.
In Italia il 2016 si è concluso con risultati in positivo, con una crescita della produzione industriale buona nel primo semestre e con un'accelerazione verso la fine dell'anno, sia per quanto riguarda il valore della produzione, sia per le forniture sul mercato interno. È risultato in ripresa, infatti, anche il consumo domestico.
La quasi totalità delle declinazioni dell'industria meccanica italiana ha chiuso quindi il 2016 in positivo, sia sul fronte produzione sia in esportazione.
Questo andamento si è riflesso nel dato positivo per l'automazione in generale nei diversi settori tecnologici e in modo specifico sugli aspetti legati alla meccatronica.
Di conseguenza i trend registrati anche per quanto riguarda la comunicazione e la digitalizzazione sono risultati particolarmente significativi.
Il 2017 inizia a dimostrare un andamento ancora più stimolante e le previsioni sono particolarmente favorevoli con una stima di crescita interessante.
Soprattutto previsioni favorevoli per i prossimi mesi si possono fare per coloro che puntano sull'alta tecnologia e sulla produzione di impianti ad alto valore aggiunto.
Orientando l'attenzione anche sugli sviluppi della robotica e del suo impiego più allargato in ambito manifatturiero, già si registra e ci si attende in futuro un aumento significativo della produzione di robot industriali: sono attesi circa 2,6 mln di unità entro il 2019, circa il 60% in più rispetto al 2015.
I campi applicativi risultano oggi per il 70% in ambito automotive, elettrico/elettronico, lavorazione metallo, asservimento macchina.
La distribuzione degli utilizzi varierà e si diversificherà in futuro, segnando già oggi la crescita dei robot

antropomorfi venduti nella General Industry.
Pertanto, la maggior parte dei costruttori di robot europei sono orientati ad acquisire nuove posizioni nei mercati che saranno maggiormente caratterizzati da grandi vendite, come Cina e Stati Uniti.
Nella corsa all'automatizzazione del settore manifatturiero, l'UE è una delle apripista a livello mondiale: ospita infatti il 65% dei Paesi con numero maggiore della media di robot industriali ogni 10.000 dipendenti. I driver di crescita più forti però sono in Cina, dove si prevede che nel 2019 sarà venduto il 40% del volume del mercato mondiale.

L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete a favore della manifattura digitale. In che modo questo piano industriale può o potrà incidere sul settore di riferimento in termini di crescita ed espansione del mercato?

L'Italia ha riconosciuto l'urgenza di mettere la manifattura al centro di un piano organico di rilancio, partendo dall'esigenza di migliorare le performance che sono variegate e concentrate, in un sistema che performa bene nella competizione globale, con bilancia commerciale positiva nell'esportazione del sistema manifatturiero, ma che dimostra sofferenza sul piano interno. Il Ministero dello Sviluppo ha stanziato fondi per stimolare la realizzazione di investimenti in innovazione, considerando beni abilitanti la trasformazione in Industria 4.0, tra cui la meccatronica e la robotica, e pensando al supporto sia per aziende di grandi dimensioni, sia e soprattutto per la realtà delle piccole e medie imprese.
La meccatronica risulta la modalità sinergica necessaria per affrontare le sfide di questa evoluzione. Parte dai presupposti necessari per approcciare l'engineering di prodotto, la simulazione del processo produttivo, la progettazione flessibile e la capacità di interazione di macchine al fine di ridurre il time to market.
In questa trasformazione non ci si aspettano salti tecnologici estremamente significativi - infatti molte tecnologie abilitanti sono disponibili anche se in rapida evoluzione - ci si attende però un loro utilizzo migliore, più efficiente e con migliori performance energetiche.
La connettività e il collegamento del mondo virtuale con il mondo fisico sono il fattore minimo e gli elementi qualificanti per le macchine del futuro, per poter utilizzare i dati in maniera evoluta, per renderli a fattor comune di progettisti, tecnici, clienti.
La meccatronica interpretata così anche a livello di operatività richiede però investimenti significativi in organizzazione, sfruttando l'ingresso prorompente delle tecnologie digitali nel modo di produrre e fare industria.
La metodologia progettuale del concurrent engineering alla base dell'approccio meccatronico potrà venire adottata non solo all'interno della singola azienda, ma sarà possibile anche tra aziende della filiera sullo stesso progetto.
Pertanto, un'impresa, se vuole attivare o accelerare questa trasformazione, deve di fatto aprirsi a un processo di riorganizzazione aziendale, dove le macchine sono un elemento fondamentale, ma l'evoluzione tecnologica deve essere accompagnata da una reale verifica e trasformazione organizzativa, senza concentrarsi solo sui vantaggi fiscali. Questo perché le scelte strategiche hanno impatto su più anni con estensione temporale molto più lunga rispetto ai tempi, ad esempio, dell'iperammortamento.
È necessario che le aziende colgano quindi l'opportunità per migliorare la propria competitività e produttività e la sfida sarà quella di riuscire a passare da logiche competitive conflittuali a logiche di collaborazione, spingendo di più modelli di interazione collaborativa all'interno delle filiere.

CAPITOLO 2

L'INDUSTRIA ITALIANA DELL'AUTOMAZIONE INDUSTRIALE MANIFATTURIERA E DI PROCESSO[1]

Principali tendenze nel 2016

- Nel 2016 nuove incognite sono emerse nello scenario macroeconomico internazionale.
  Il commercio mondiale ha visto un rallentamento evidenziando un tasso di sviluppo inferiore alla media dell'ultimo decennio. I Paesi emergenti, che avevano fornito un contributo importante alla crescita negli anni precedenti, hanno mantenuto un andamento meno dinamico.
  Su queste tendenze si è riflesso negativamente soprattutto l'indebolimento dell'economia cinese, che mantiene il primato di maggiore produttore manifatturiero globale e rappresenta al contempo il secondo mercato mondiale per importazioni di beni. In controtendenza, i principali Paesi Avanzati hanno mostrato una maggiore capacità di tenuta. Gli Stati Uniti hanno registrato un rafforzamento della ripresa, mentre nell'area europea è proseguito il graduale percorso di uscita dalla crisi.
  Al moderato incremento di consumi e investimenti, nell'UE-28 si è associato anche un recupero nei livelli di attività industriale (vicina al 2,0 per cento la crescita su base annua della produzione industriale per il manifatturiero europeo nel 2016).
  Queste dinamiche sono intercettate anche dai dati relativi alle importazioni di beni e servizi che nella media del 2016 hanno visto un maggiore dinamismo per l'aggregato dei Paesi Avanzati rispetto a quelli Emergenti. Il miglioramento del profilo macroeconomico nelle Economie di antica industrializzazione svolge un ruolo importante come attivatore di domanda per i settori tecnologicamente più avanzati. Nonostante la profonda trasformazione evidenziata negli ultimi anni nelle catene di fornitura globale, questo gruppo di Paesi mantiene una quota importante e vicina alla metà sul totale delle importazioni globali di beni strumentali. In dettaglio, nell'ultimo quinquennio negli Stati Uniti la domanda di beni strumentali è cresciuta a un tasso medio annuo vicino al 5,0 per cento.

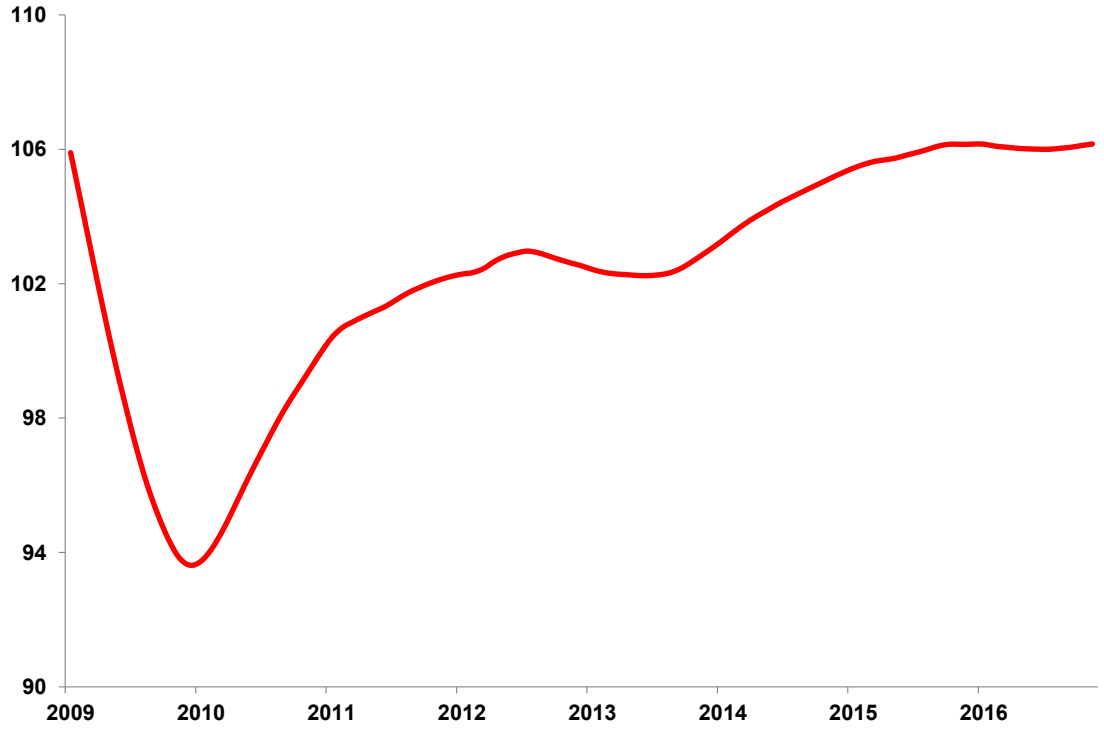
- Nel 2016 l'economia italiana ha confermato un lento percorso di ripresa, comune alla quasi totalità delle componenti, ma non tale da consentire un pieno ritorno ai livelli pre-crisi.
  In dettaglio, in corso d'anno il rallentamento dello scenario globale si è riflesso negativamente sull'evoluzione delle esportazioni italiane di beni e servizi che hanno mostrato un andamento meno dinamico rispetto all'anno precedente.
  In un quadro ancora complesso, alcuni segnali di riattivazione hanno interessato la domanda interna. L'evoluzione degli investimenti totali ha mantenuto un profilo positivo, proseguendo il trend di recupero intrapreso nel 2015. Anche nel 2016 si è confermata trainante la componente relativa ai Mezzi di Trasporto, che ha svolto un ruolo importante a sostegno della crescita nell'ultimo biennio.
  Pur in un quadro di miglioramento restano più contrastanti le indicazioni relative agli investimenti in Costruzioni. Nella media annua un andamento di segno positivo ha caratterizzato anche gli investimenti in Macchinari e Attrezzature, componente che nei diversi trimestri del 2016 ha mostrato tendenze altalenanti e che svolge un ruolo importante come propulsore della crescita.

1. A cura del Servizio Centrale Studi Economici di ANIE

Il miglioramento del profilo macroeconomico, unitamente all'avvio di nuovi strumenti di incentivazione per l'acquisto di beni strumentali, potrebbero favorire nel 2017 un effettivo consolidamento di questa componente. In un contesto di luci e ombre nel 2016 l'industria manifatturiera italiana ha proseguito il percorso di uscita dalla crisi, ma a un ritmo più lento rispetto a quanto evidenziato l'anno precedente. Fra i settori più dinamici si confermano Farmaceutica e Automotive che hanno beneficiato della prima riattivazione della domanda interna, mentre tradizionali comparti del Made in Italy come Tessile e Abbigliamento e Meccanica hanno maggiormente risentito del rallentamento del canale estero. Il ritorno degli scambi esteri in un sentiero in espansione potrebbe fornire nuova linfa alla crescita del manifatturiero italiano nell'anno in corso.

Evoluzione della produzione industriale nelle Economie Avanzate

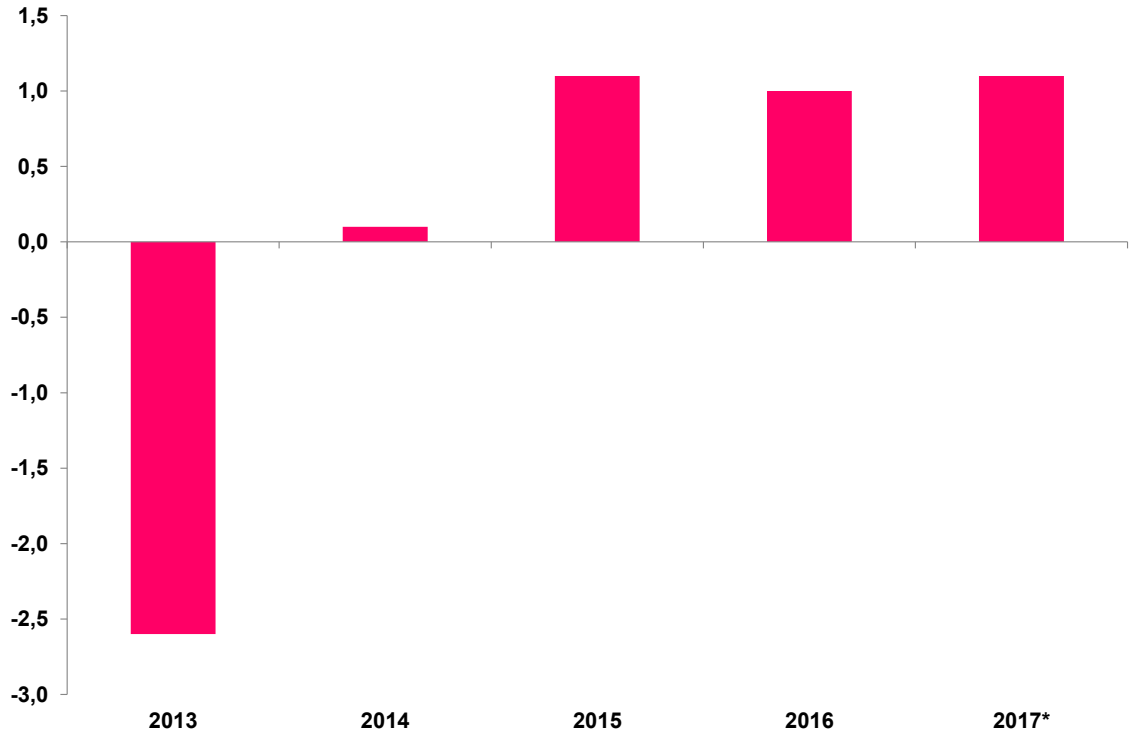
indice 2010=100, ciclo trend da dati in volume



Fonte: elaborazioni ANIE su dati CPB

Evoluzione della domanda interna in Italia

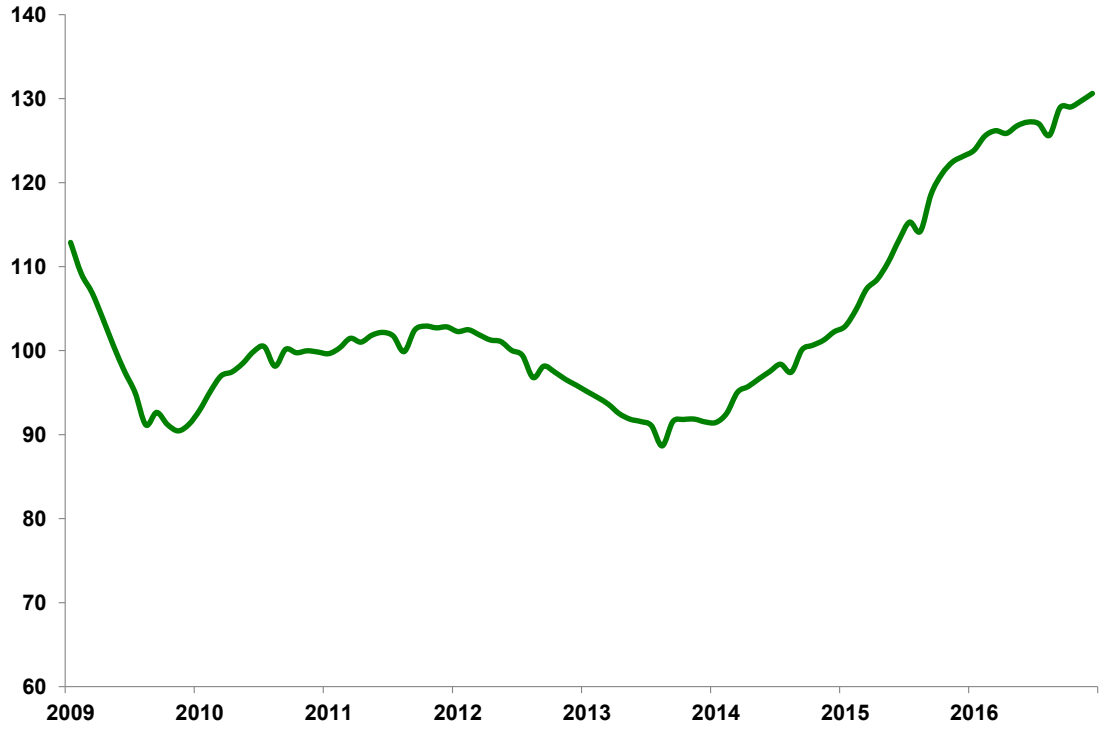
variazioni % annue



*dato previsionale
Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

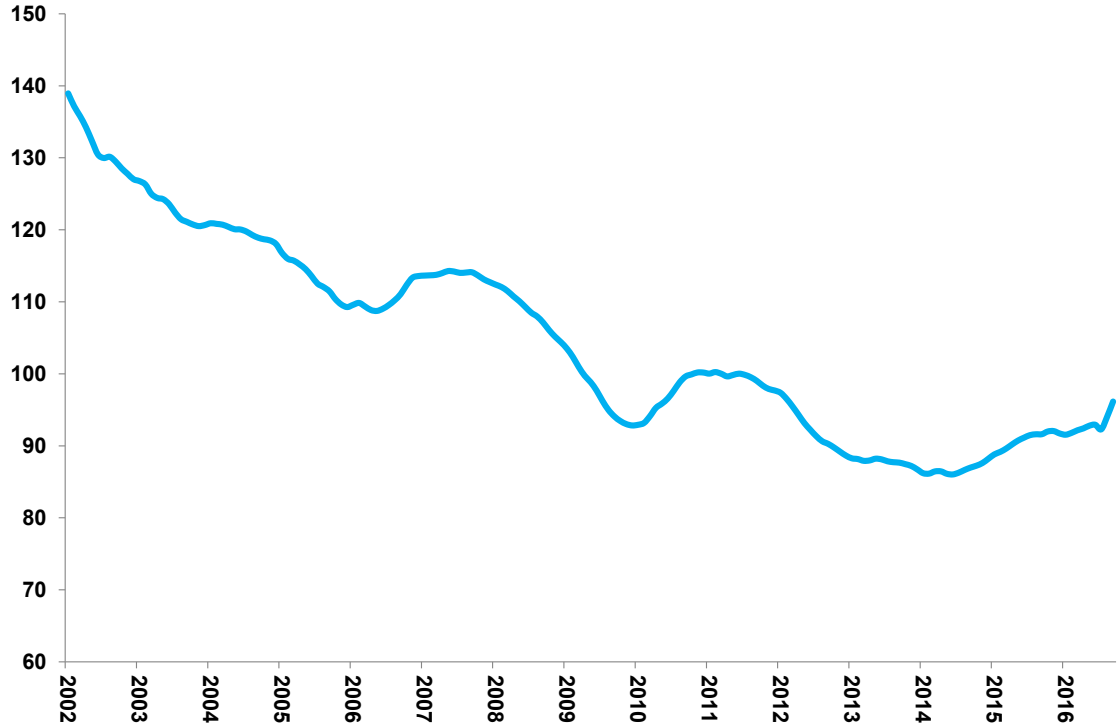
Evoluzione del fatturato totale nell'industria Automotive italiana

indice 2010=100, ciclo trend da dati in valore



Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

Andamento della produzione industriale nell'industria Elettronica italiana*
indice 2010=100, ciclo trend



**incluse le tecnologie ICT*
Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

- In un contesto incerto, in corso d'anno l'industria Elettronica italiana, comprensiva delle tecnologie per l'ICT, ha evidenziato un andamento eterogeneo tra i diversi segmenti che compongono il settore. Fra i comparti più dinamici si conferma l'Automazione industriale manifatturiera e di processo, espressione nel 2016 di un volume d'affari aggregato di 4,3 miliardi di euro. Nel 2016 il comparto ha registrato una crescita del fatturato totale del 4,0 per cento a valori correnti (+7,1 per cento la corrispondente variazione nel 2015), in linea con le tendenze al rialzo evidenziate nel triennio precedente. L'industria italiana fornitrice di tecnologie per l'automazione non solo ha da tempo pienamente recuperato, ma anche superato - di oltre dieci punti percentuali - i livelli del volume d'affari espressi nel periodo pre-crisi. L'andamento registrato nel 2016 ha beneficiato del positivo contributo sia del canale estero sia della domanda interna. In corso d'anno la quasi totalità dei segmenti merceologici che compongono il comparto ha evidenziato un andamento di segno positivo, seppur con tassi di crescita differenziati. In dettaglio, hanno registrato un maggiore dinamismo i segmenti Wireless, Telecontrollo, Motori brushless e Azionamenti. Nonostante un contesto più incerto, la tenuta evidenziata dal comparto ha continuato a beneficiare della domanda espressa dai principali settori a valle, in particolare dai costruttori di macchine. Nel 2016 secondo dati UCIMU gli ordini totali di macchine utensili hanno registrato nella media annua un incremento vicino all'1,5 per cento. Questo risultato complessivo ingloba al contempo il calo mostrato dalla componente estera in conseguenza del peggioramento dello scenario internazionale e il vivace andamento del portafoglio ordini interno. A differenza delle tendenze evidenziate negli anni precedenti, nel 2016 la domanda interna ha fornito un contributo alla crescita del settore determinante rispetto a quello offerto dai mercati esteri. Su questo andamento si è riflessa positivamente anche la presenza di mirati strumenti agevolanti per gli acquisti di beni strumentali. Più in generale, la domanda lungo la filiera

di tecnologie per l'automazione industriale si conferma trainata dalla crescente attenzione del mercato verso soluzioni innovative. In questo contesto svolge un ruolo centrale il percorso di rinnovamento dei processi manifatturieri sostenuto dallo sviluppo del nuovo paradigma Industria 4.0.

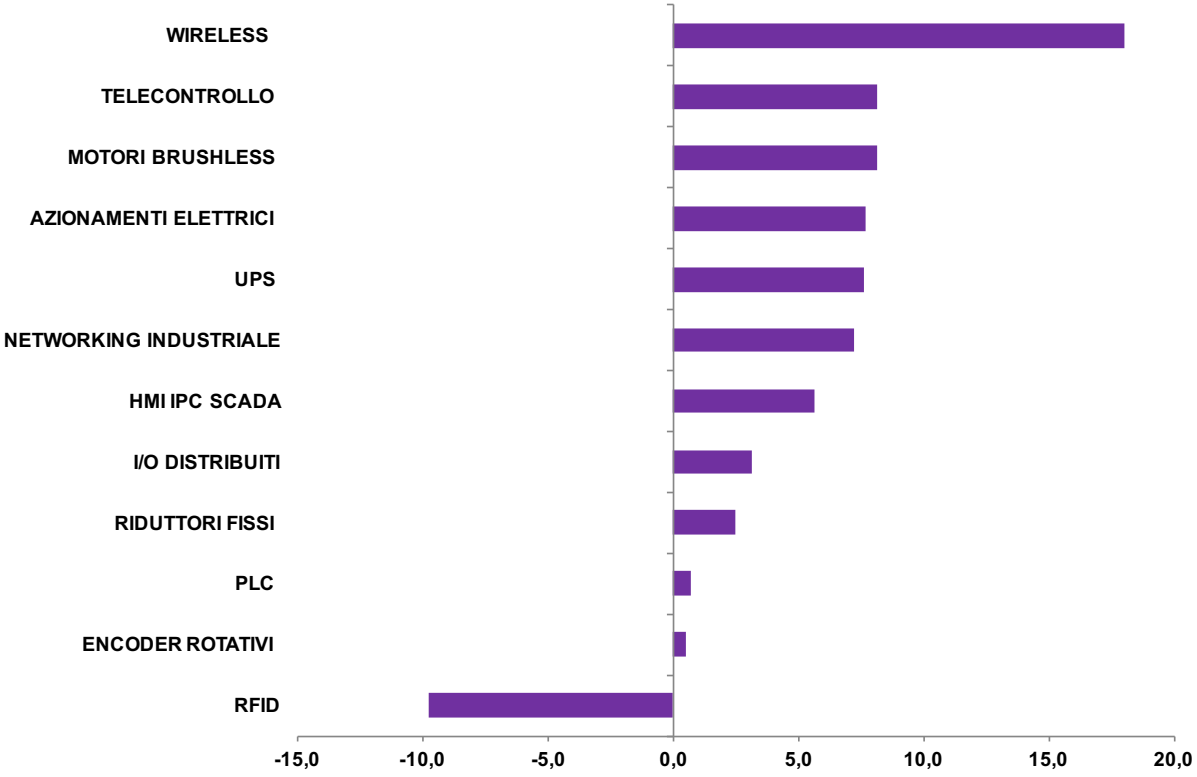
L'industria dell'Automazione industriale manifatturiera e di processo in Italia

	2014	2015	2016	2015/2014	2016/2015
	milioni di euro a prezzi correnti			variazioni %	
MERCATO INTERNO	3.901	4.226	4.389	8,3	3,9
FATTURATO TOTALE	3.853	4.126	4.290	7,1	4,0
ESPORTAZIONI	1.100	1.172	1.198	6,5	2,2
IMPORTAZIONI	1.148	1.273	1.297	10,8	1,9
BILANCIA COMMERCIALE	-48	-101	-99		

Fonte: ANIE

Andamento del fatturato Italia dell'Automazione industriale manifatturiera e di processo per principali segmenti

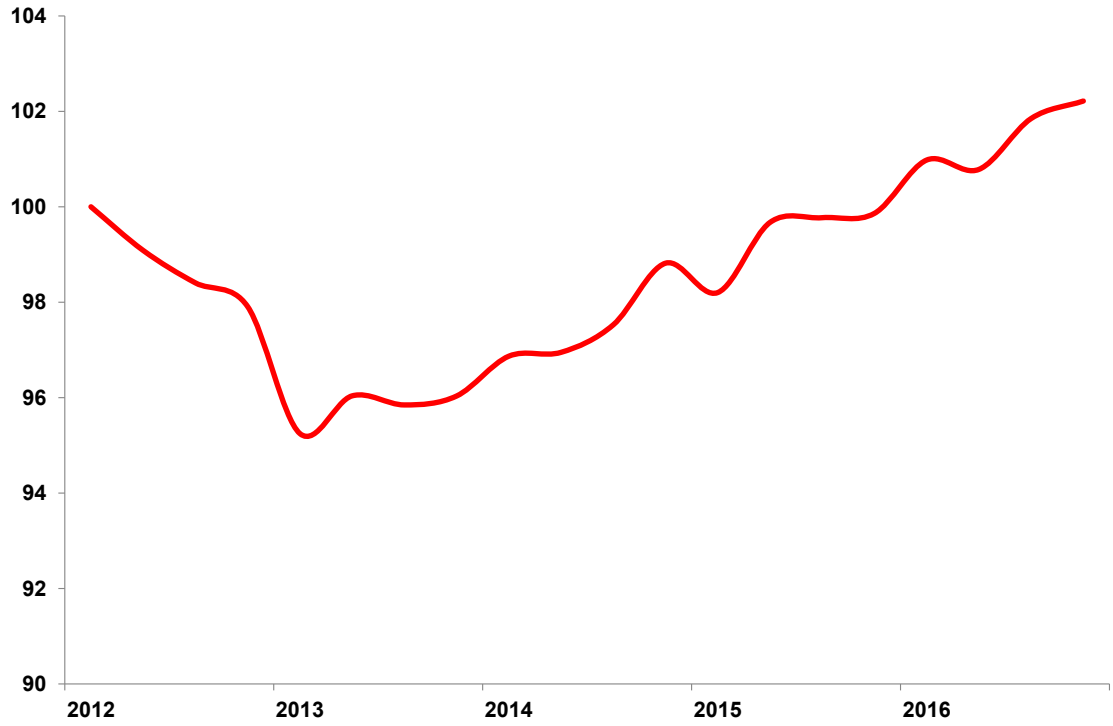
variazioni %, anno 2016



Fonte: ANIE Automazione

Evoluzione degli investimenti in Macchinari e Attrezzature in Italia

indice I trimestre 2012=100, valori concatenati



Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

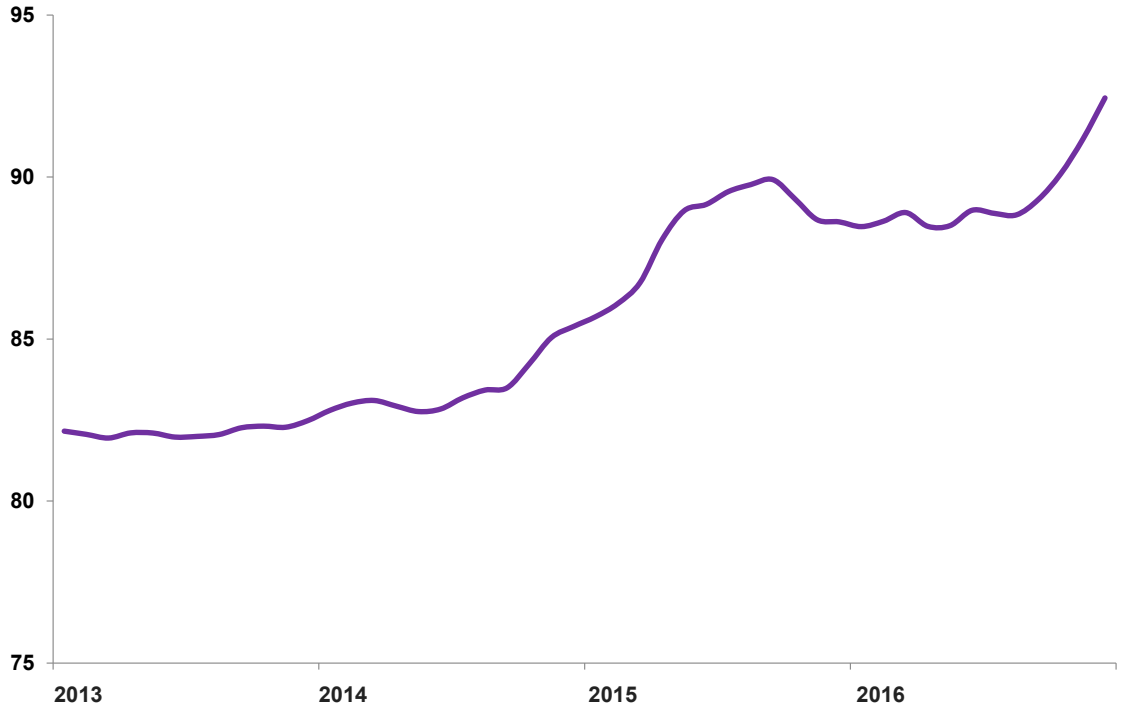
Evoluzione del fatturato totale nell'Automazione industriale manifatturiera e di processo

milioni di euro (2007-2016)

Fonte: ANIE

Evoluzione degli ordini totali nell'Industria Meccanica italiana

indice 2010=100, ciclo trend

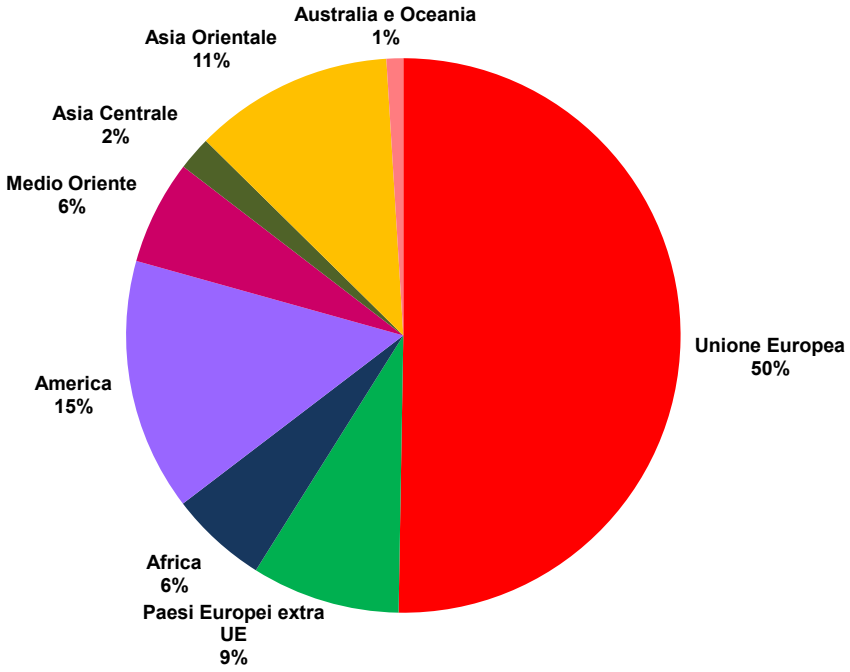


Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

- In linea con le tendenze registrate negli ultimi anni, il canale estero mantiene un ruolo importante per la crescita del comparto. Guardando alle esportazioni dirette, nel 2016 le vendite estere di tecnologie per l'automazione industriale hanno mostrato un incremento su base annua del 2,2 per cento. Su questo andamento si è riflessa positivamente la tenuta della domanda europea, area che assorbe in aggregato quasi il 60 per cento delle esportazioni del comparto. Secondo dati Eurostat, nel 2016 gli investimenti totali hanno mantenuto nella media europea un profilo positivo, beneficiando soprattutto della crescita ascrivibile alla componente in Macchinari e Attrezzature che ha evidenziato una variazione annua vicina al 4,0 per cento. In questo contesto favorevole, fra i mercati europei che hanno espresso una maggiore ricettività all'offerta tecnologica del Made in Italy si annoverano Germania e Spagna. In particolare, nel 2016 la Germania - che si conferma con una quota pari al 13 per cento sul totale esportato primo mercato di destinazione delle tecnologie italiane per l'automazione industriale - si è caratterizzata per una domanda vivace e superiore al 5,0 per cento annuo. Guardando invece ai mercati extra europei, in corso d'anno sono emersi andamenti differenziati fra le diverse aree geografiche, risentendo dell'elevata instabilità dello scenario.

I principali mercati di sbocco dell'industria italiana dell'Automazione industriale manifatturiera e di processo nel 2016

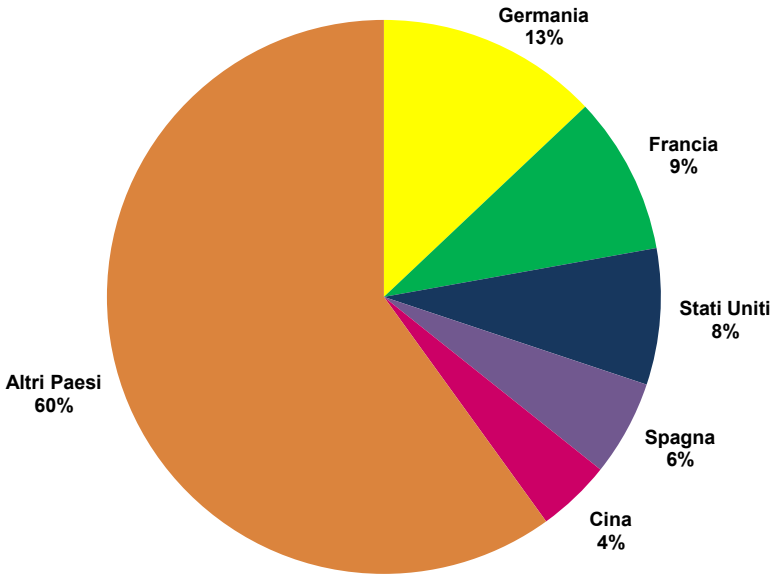
distribuzione %



Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

I principali Paesi di sbocco dell'industria italiana dell'Automazione industriale manifatturiera e di processo nel 2016

distribuzione %

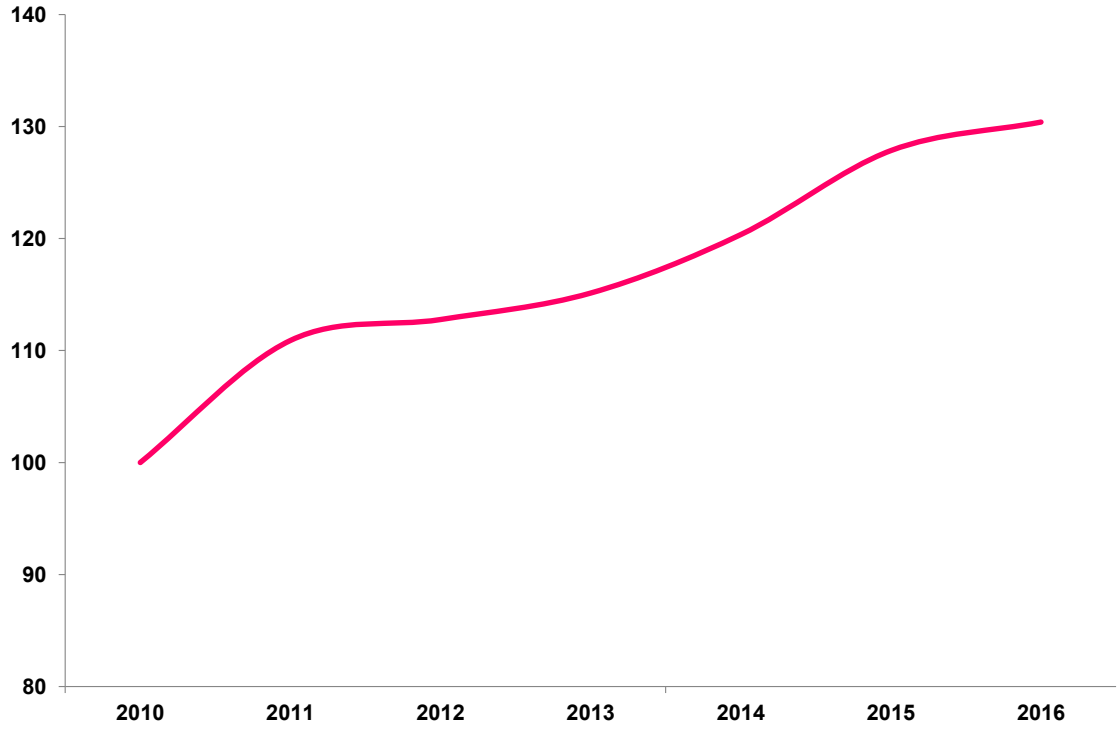


Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

- Dopo una fase di debolezza, fra la fine del 2016 e la prima metà del 2017 sono emersi nello scenario internazionale segnali di miglioramento, intercettati dalla riattivazione degli scambi globali e dalla crescita dei livelli produttivi. In particolare, negli ultimi mesi indicazioni di recupero hanno interessato importanti mercati Emergenti che l'anno precedente avevano mostrato un rallentamento. In un contesto che mantiene elevate incognite, questo elemento potrebbe riflettersi in misura rilevante sulla domanda rivolta all'industria manifatturiera italiana, fornendo nuova linfa alle esportazioni delle principali filiere del Made In Italy fra cui quella metalmeccanica. L'avvio di un nuovo ciclo internazionale di acquisti di macchinari e impianti potrebbe svolgere un ruolo centrale in questo percorso. Guardando ai più recenti dati ISTAT disponibili, fra la fine del 2016 e l'inizio del 2017 le esportazioni di beni strumentali hanno acquisito nuovo slancio. L'accelerazione della ripresa nel mercato interno e, in particolare il consolidamento del ciclo degli investimenti, gioca altresì un ruolo rilevante per lo sviluppo dei settori manifatturieri più avanzati. Ampie attese sono legate soprattutto all'implementazione del Piano Industria 4.0 che potrebbe offrire un importante sostegno alla domanda di tecnologie innovative. Attese di tenuta caratterizzano anche la componente degli investimenti in Mezzi di Trasporto che nell'ultimo biennio aveva fornito un contributo trainante alla crescita. Inglobando queste aspettative, nelle più recenti previsioni pubblicate dal Centro Studi Confindustria gli investimenti in Macchinari e Attrezzature e in Mezzi di Trasporto in Italia potrebbero evidenziare nel biennio 2017-2018 un incremento medio annuo vicino al 3,0 per cento. Queste tendenze potranno riflettersi positivamente sull'andamento dell'industria italiana dell'Automazione industriale manifatturiera e di processo nel consolidato ruolo di portatrice di innovazione nei processi e nelle reti.

Evoluzione delle esportazioni italiane di beni strumentali

indice 2010=100



Fonte: elaborazioni Servizio Centrale Studi Economici ANIE su dati ISTAT

CAPITOLO 3

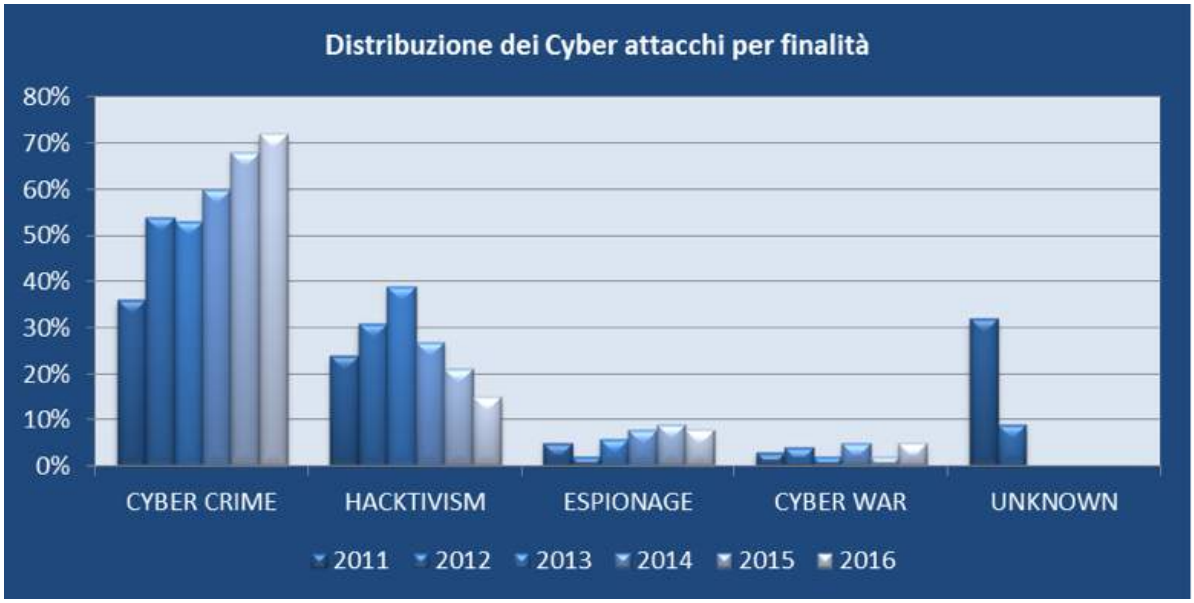
NOTE DI APPROFONDIMENTO
La Cyber Security nell'industria digitale

Indice

1. Quadro di riferimento

Internet ha rivoluzionato la società e l'economia, favorendo l'interazione, lo scambio di idee, la condivisione delle informazioni. Il termine Cyberspace si riferisce all'ambiente all'interno del quale avvengono le operazioni che fanno uso di Internet. La riduzione dei costi di accesso alla rete e lo sviluppo della banda larga portano ad un'ulteriore espansione del Cyberspace, che diviene un fattore cruciale per la crescita economica e sociale. Tuttavia, il suo utilizzo comporta problemi di vulnerabilità delle applicazioni e dei sistemi informatici, dovute anche al fatto che la stragrande maggioranza delle reti e dei sistemi che lo formano sono stati progettati e realizzati pensando a criteri di usabilità e di resilienza, senza tenere in debito conto fin dall'inizio gli aspetti legati alla sicurezza. Queste vulnerabilità sono sempre più utilizzate da singoli e da gruppi a fini illeciti.

La differenza tra il Cyber Crime e la criminalità tradizionale non risiede tanto nella tipologia di aggressioni che li caratterizza, quanto nella circostanza che le violazioni perpetrate tramite il Cyberspace sono prive di confini fisici e di limiti geografici. Non può quindi stupire il progressivo incremento, quantitativo e qualitativo, di attacchi informatici con le finalità più disparate, in quella "terra di mezzo" che è oramai diventato il Cyberspace: dalle frodi e dalle estorsioni informatiche ai furti di identità e di dati sensibili, fino ad arrivare allo spionaggio e al sabotaggio.



Fonte: Clusit - Rapporto 2017 sulla sicurezza ICT in Italia

Sotto il profilo delle vittime potenziali, un rilievo particolare hanno le istituzioni pubbliche e le imprese multinazionali. Tuttavia, anche le imprese di piccole e medie dimensioni, che costituiscono il fulcro del tessuto economico italiano, sono un potenziale bersaglio di attacchi informatici. Le PMI appaiono anzi le più vulnerabili e per loro le conseguenze negative sono in proporzione ancora maggiori, a causa delle ridotte risorse organizzative ed economiche di cui dispongono. È quindi indispensabile che gli interventi di regolamentazione volti a tutelare le vittime degli attacchi informatici tengano conto delle diverse caratteristiche dei destinatari. Altrettanto importante è che le imprese minori siano concretamente incoraggiate a incrementare la cultura della sicurezza, che stentano ancora a fare propria. La Cyber Security costituisce, del resto, una componente essenziale del "valore" che l'impresa è istituzionalmente chiamata a generare per i propri stakeholder, nei confronti dei quali ha precisi obblighi di protezione.

Il tema della Cyber Security diviene centrale in relazione alla diffusione dell'IoT (Internet of Thing) dal momento che consente di interconnettere miliardi di dispositivi in tutto il mondo che, a fronte della loro capacità di generare dati ed informazioni, devono essere gestiti e protetti dalle aziende e dalle organizzazioni che li abilitano e li portano sul mercato. L'estensione della tecnologia e dei sistemi informativi ad oggetti fisici differenti per natura e ambito applicativo amplia le possibilità e le modalità di intrusione e di attacco, coinvolgendo potenzialmente infrastrutture critiche (come ad esempio le Smart Grid) o oggetti che possono influenzare il benessere e la sicurezza delle persone (si pensi ai dispositivi nell'ambito dell'eHealth, alla Connected Car o ai sistemi di controllo nella Smart Home).

I nuovi trend dell'innovazione digitale come Cloud, Big data, Internet of Thing, Mobile e Social richiedono dunque risposte non più rimandabili. Il nuovo Regolamento europeo sulla Protezione dei Dati Personali crea alcuni dei presupposti necessari per giungere a un quadro di riferimento, che deve essere compreso ed attuato. Il percorso di gestione dell'Information Security & Privacy chiede alle aziende di mettere in campo adeguati modelli di governance, progettualità e soluzioni per affrontare la trasformazione.

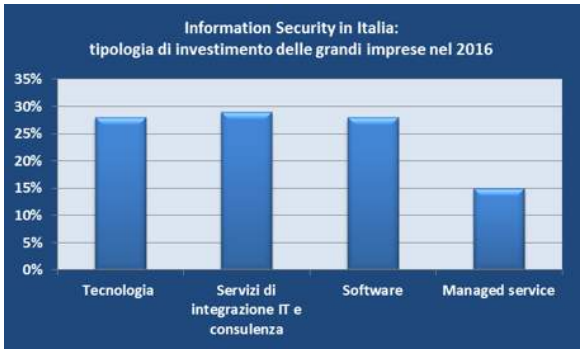
L'assenza di una politica digitale in un Paese può produrre danni gravissimi nel breve e nel medio periodo, esponendolo al rischio di perdere rilevante opportunità di crescita, quali posti di lavoro qualificati in tutti i settori industriali e nei servizi, ricerca universitaria e privata, produzione di know-how, imprese innovative e start-up. La sicurezza informatica non va quindi considerata un costo superfluo o un freno all'attività, ma una precondizione indispensabile per il suo esercizio, che per le imprese si traduce in un vantaggio in termini di competitività. Il diffondersi di una cultura della sicurezza informatica è un fattore decisivo per il Paese, in chiave non solo difensiva ma soprattutto di crescita economica.

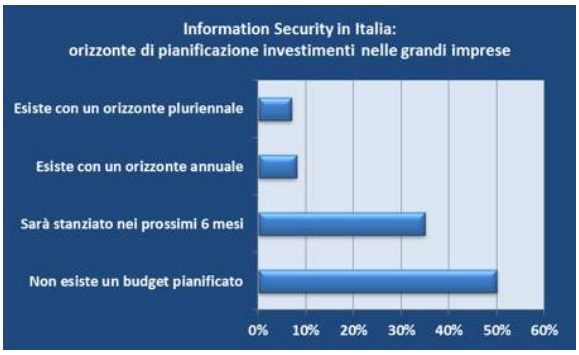
Del resto i governi di tutto il mondo hanno posto la Cyber Security come tema prioritario nella propria agenda politica e dall'analisi comparata delle Cyber Strategy pubbliche risulta che uno dei pilasti strategici condivisi a livello internazionale è proprio quello di incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici. Per ciò riguarda nello specifico l'Italia, il 13 aprile 2017 è stato pubblicato sulla Gazzetta Ufficiale il nuovo decreto del Presidente del Consiglio in tema di protezione cibernetica e sicurezza informatica nazionali.
La direttiva rappresenta una fase importante del programma nazionale per la Cyber Security approvato lo scorso 17 febbraio dal CISR (Comitato interministeriale per la sicurezza della Repubblica). Il nuovo provvedimento rafforza il ruolo del CISR che emanerà direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese, e si avvarrà in questa attività del supporto del coordinamento interministeriale delle amministrazioni CISR (il cosiddetto CISR tecnico) e del Dipartimento delle informazioni per la sicurezza (DIS). Tra le novità il Nucleo sicurezza cibernetica (NSC) viene ricondotto all'interno del DIS e assicurerà la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei Ministeri competenti in materia. È inoltre prevista una forte interazione con l'Agenzia per l'Italia Digitale (AgID) del Dipartimento della funzione pubblica, con il Ministero dello sviluppo economico, con il Ministero dell'interno, con il Ministero della difesa e, infine, con il Ministero dell'economia e finanze. Il nuovo decreto attribuisce poi al Direttore generale del DIS il compito di definire linee di azione che dovranno portare ad assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati, verificandone ed eliminandone le vulnerabilità.
Per la realizzazione di tali iniziative è previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore.

2. Il mercato della sicurezza informatica

Il settore della Cyber Security rappresenta un mercato strategico e in forte crescita. A livello mondiale, l'industria della sicurezza informatica vale oltre 75 miliardi di dollari e per il 2020 se ne prevede il raddoppio. La domanda mondiale di posti di lavoro in questo campo sarà di 6 milioni di unità entro il 2019, con un deficit previsto di 1,5 milioni di posti. Lloyd's Assicurazioni ha stimato i danni causati da attacchi informatici in circa 450 miliardi di dollari all'anno, somma che include sia i crash di sistema che i costi di ripristino. La Juniper Networks valuta che entro il 2019 il costo mondiale per la perdita di dati sensibili di aziende e cittadini si attesterà su una cifra pari a 1,2 trilioni di dollari.

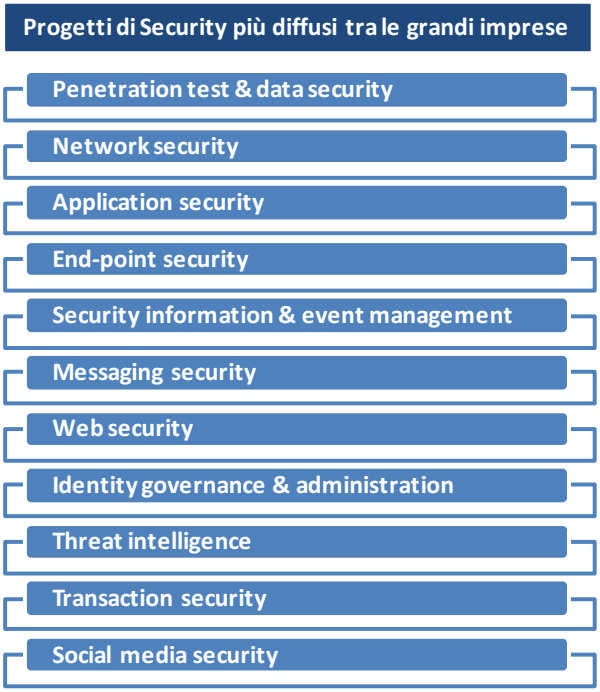
In Italia, secondo i risultati della ricerca condotta dall'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano, il mercato delle soluzioni di Information Security nel 2016 ha raggiunto i 972 milioni di euro (+5% rispetto al 2015), con una spesa pressoché concentrata tra le imprese di grandi dimensioni.





Fonte: Report 2017 - Osservatorio Information Security & Privacy

Sebbene sia cresciuta la consapevolezza, di fronte alle nuove sfide poste dallo sviluppo di tecnologie come Cloud, Big data, IoT, Mobile e Social, non è ancora diffuso un approccio di lungo periodo alla gestione della sicurezza e della privacy. Oltre la metà delle grandi organizzazioni italiane non ha ancora una figura manageriale codificata per la gestione della sicurezza informatica, evidenziando un gap importante rispetto a quanto avviene in altri Paesi.
Sempre secondo lo studio del Politecnico, i progetti di sicurezza delle aziende italiane sono orientati principalmente all'identificazione dei rischi e alla protezione dagli attacchi, mentre sono ancora immaturi il supporto alla rilevazione degli eventi, la risposta e il ripristino.



Fonte: Report 2017 - Osservatorio Information Security & Privacy

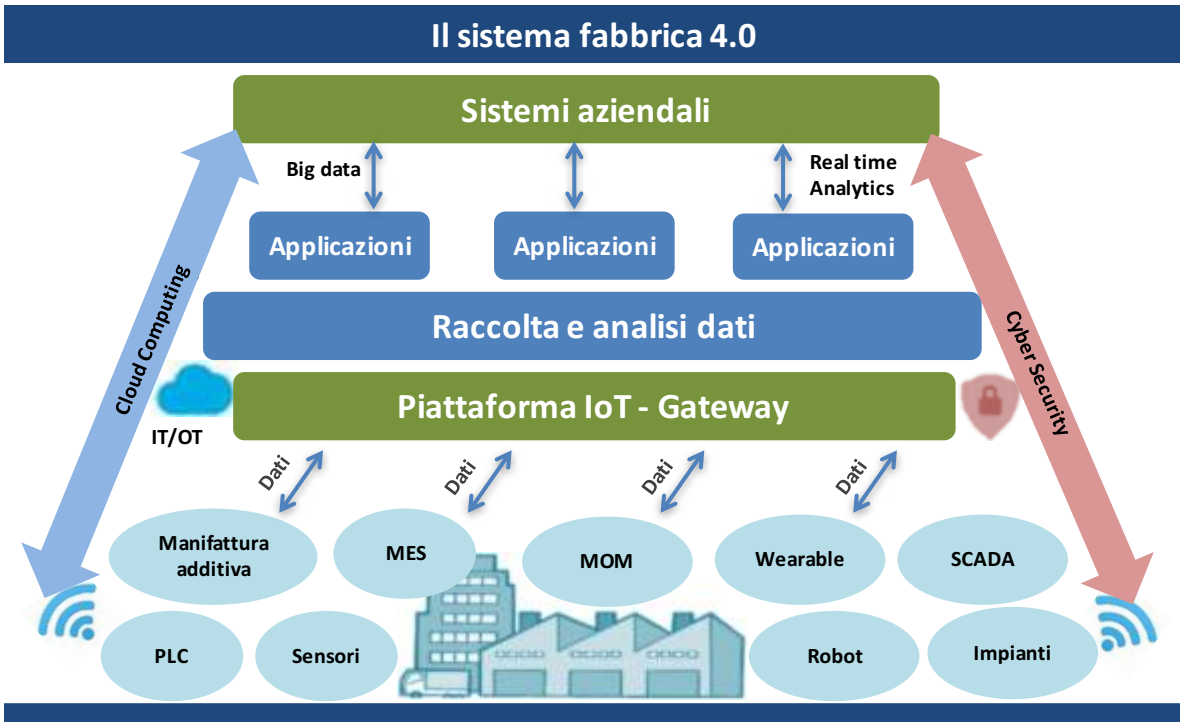
Le PMI italiane, evidenzia ancora lo studio, iniziano a spendere per la Cyber Security ma spesso sottovalutano la crescita della consapevolezza dei rischi tra i propri dipendenti e pochissime hanno specifici programmi di formazione.
L'analisi sulla diffusione delle soluzioni di Information Security tra circa 800 piccole e medie imprese italiane rivela, infatti, che il 93% delle PMI ha dedicato un budget nel 2016. Le principali motivazioni agli investimenti sono l'adeguamento normativo e gli attacchi subiti in passato, ma a volte seguono la necessità di rispondere a nuove esigenze tecnologiche o di business. Un'organizzazione su quattro si fa guidare dal buon senso, senza un approccio tecnologico definito. L'approccio alla sicurezza nelle PMI è orientato prevalentemente all'identificazione e alla protezione, molto meno alla rilevazione e alla risposta. L'attenzione alla rilevazione cresce all'aumentare della dimensione di impresa.

3. La protezione di reti e sistemi di automazione e controllo industriale

3.1 Il contesto industriale

Il processo irreversibile di digitalizzazione del settore manifatturiero espone gli asset industriali a vulnerabilità e minacce che minano la sicurezza e l'integrità dei sistemi e la privacy delle informazioni. La convergenza tra i sistemi produttivi (OT, Operational Technology) e il mondo virtuale delle informazioni (IT, Information Technology) solleva molti problemi legati alla sicurezza informatica dei sistemi di automazione e controllo industriale (IACS, Industrial Automation Control System).

Prima della diffusione delle tecnologie Internet in ambito industriale, quello dei sistemi IACS - in cui rientrano i sistemi di controllo (ICS), i sistemi di controllo distribuiti (DCS), i sistemi di acquisizione dati (SCADA) e i PLC - era un mondo ideale in cui si aveva a che fare con sistemi "chiusi" operanti su reti separate prive di collegamento con infrastrutture di comunicazione pubbliche. La diffusione delle tecnologie Internet e il conseguente aumento di connettività hanno sottratto i sistemi di controllo dalla condizione di isolamento, aprendo le porte a possibili vulnerabilità informatiche.



L'evoluzione del mercato industriale e la nascita di nuovi servizi legati alle tecnologie digitali hanno reso necessario aprire all'esterno l'accesso ai sistemi di controllo. Questo è sempre più vero se caliamo il discorso nel contesto della fabbrica 4.0 in cui tutti gli oggetti e le macchine sono componenti intelligenti integrati in un'infrastruttura totalmente interconnessa e distribuita, intrinsecamente aperta all'esterno, che espone gli apparati critici a problemi di Cyber Security.

La sempre maggiore diffusione del concetto di fabbrica digitalizzata rende più diffuso lo sviluppo di infrastrutture Ethernet anche all'interno degli ambienti industriali. Questo con i dovuti accorgimenti: la natura gravosa dell'ambiente industriale in termini di temperature di utilizzo, di vibrazioni e di perturbazioni EMC impone l'uso di componentistica adeguata, così come la necessità del rispetto di isocronia e determinismo delle applicazioni tipiche dell'automazione di fabbrica ha condotto allo sviluppo di reti di automazione con protocolli a base Industrial Ethernet. Quella che in precedenza era quindi una preoccupazione tipica del mondo IT, vale a dire la Cyber Security, trova sempre più cittadinanza anche nel mondo dell'industria manifatturiera, fin al livello puramente produttivo (macchine o linee di produzione).

Come è possibile declinare il concetto generale di Cyber Security (prevenzione di accessi fraudolenti a reti o dispositivi) nella realtà di reti industriali di produzione?

Attingendo alla definizione inclusa all'interno della specifica tecnica internazionale IEC/TS 62443-1-1, in questo caso, la Cyber Security si occuperà della prevenzione di accessi illegali, quindi non autorizzati, o di interferenze nello specifico e previsto funzionamento di un sistema di comando e controllo per l'automazione industriale.

Fino a quando le reti di automazione di macchine e impianti erano costituite da fieldbus a base seriale, le macchine non erano interconnesse in modo complesso e l'accesso da remoto era un'eccezione, le preoccupazioni dei progettisti di automazione nei confronti della Security si limitavano al predisporre opportune misure e/o modalità operative tali da evitare accessi al progetto installato sul sistema di controllo. Questo al fine di evitare modifiche dello stesso, con possibili conseguenze che avrebbero potuto coinvolgere la responsabilità dell'installatore o del produttore del macchinario. La diffusione di protocolli a base Industrial Ethernet ha ancor più favorito l'integrazione della rete di macchina nella piramide di comunicazione con scambi da/verso sistemi ERP/MES e con l'accesso alla rete anche da remoto: la Security diventa un'esigenza imprescindibile anche per i progettisti di automazione industriale.

3.2 I rischi

La protezione dei sistemi è divenuta un elemento critico di ogni attività industriale e delle infrastrutture. I danni di un possibile attacco possono, infatti, provocare incidenti anche gravi. Si pensi, ad esempio, a una centrale nucleare, a un aeroporto o a un veicolo con sistema di controllo via rete: un possibile attacco potrebbe provocare danni enormi sia alle persone sia alle cose.

Le conseguenze di una sottovalutazione della Cyber Security sono, dunque, molteplici e possono avere ripercussioni gravi non solo su un'applicazione specifica ma anche sulla solidità dell'azienda che ospita la rete violata. Questo perché, come già accennato, sempre più spesso, la rete di macchina è interconnessa all'infrastruttura IT aziendale: oltre ai dati che di per sé possono comunque essere vitali per la produzione aziendale (quali, ad esempio, ricette o procedure lavorative) attraverso la rete di macchina, in assenza di adeguata protezione, si potrebbe accedere anche ad altri comparti sensibili di azienda (come ad esempio R&S, Financial, Legal). Senza contare i possibili atti di sabotaggio o l'uso delle risorse aziendali come strumenti per triangolazione di attacchi Cyber, tutti aspetti che possono condurre a perdite irreversibili di

reputazione sul mercato dell'azienda coinvolta.

Anche gli aspetti associati alla sicurezza di macchine e impianti potrebbero subire modifiche non volute e questo potrebbe comportare incidenti con tutte le conseguenze, civili e penali, del caso ma anche con possibili danni ambientali, di maggiore o minore rilevanza, in funzione della tipologia produttiva del sito violato. Quindi non solo danno economico per fermi di produzione.

Una recente analisi di SANS (SANS 2016, State of ICS Security Survey) sullo stato della Security dei sistemi di controllo industriale indica che il 42% delle minacce ai sistemi arrivano dall'interno delle organizzazioni. In questa cifra rientrano quelle intenzionali (i sabotaggi) che rappresentano oltre il 10% del totale; quelle non volute (errori degli operatori dovuti a scarsa competenza oppure a sistemi di interfacciamento non chiari) che pesano per oltre il 15%; i problemi derivanti da malfunzionamenti o da non accurata integrazione IT/OT (circa il 10%).

Security: stima dei costi	
1	**Perdita dei dati** Improvvisamente tutti i vostri dati vengono persi. Quale potrebbe essere il costo della ricostruzione di tali dati?
2	**Perdita di know-how** Un vostro competitor riesce ad accedere ai vostri dati sensibili (progettazione, ingegnerizzazione, ...). Quanto può economicamente valere il danno?
3	**Fermi di produzione** A causa di problemi legati alla security, la produzione deve arrestarsi per alcune ore. Quanto può essere il costo di una tale mancata produzione?
4	**Ore lavoro dei vostri dipendenti** Quante ore lavoro dei vostri dipendenti sarebbe necessario impiegare per risolvere i danni generati da una falla nelle vostre misure di security?
5	**Hijacking dai vostri computer** Quanto potrebbe costare una campagna di comunicazione per spiegare che una terza parte ha usato i vostri sistemi per spiare o attaccare un'altra società?
6	**Reputazione** Quanto potrebbe essere importante un danno alla vostra reputazione se i vostri clienti non riponessero in voi la giusta fiducia circa la protezione da Cyber attacchi?

Un recente caso di Cyber attacco

Il Ransomware (una delle molteplici e sempre più raffinate versioni di Cryptolocker) è stata una delle minacce informatiche più diffuse nel 2016. Il pensiero comune è che le vittime siano solo consumatori inesperti, facile preda delle numerose trappole di cui è popolata la rete. La realtà è ben diversa: Cryptolocker e le sue varianti hanno funestato anche le aziende.

È capitato, per esempio, ad un'impresa del settore alimentare che si è vista bloccare l'applicazione di supervisione e monitoraggio dei macchinari di un impianto di produzione. Che cosa era successo?

La rete di stabilimento era piatta, con scarsa segmentazione e senza segregazione degli asset critici (PC/Server di fabbrica). Sulla stessa rete erano collegati anche i PC per la posta ed altri applicativi, con accesso a

internet. E così è bastato che un impiegato dell'amministrazione aprisse un allegato denominato "fattura" per scatenare la violenza del Ransomware che ha criptato i file di tutti i dischi dei PC con risorse condivise. Tra questi dischi c'era anche quello del server SCADA, che era collegato alla rete office al fine di poter produrre e scaricare reportistica sull'andamento dell'impianto. Il server SCADA, che lavora con routine contenute nella RAM, ha continuato a funzionare, ma su questo computer non era più possibile cambiare schermate: il sistema era bloccato. È stato così necessario provvedere allo spegnimento dei sistemi per la bonifica dei computer. Siccome l'ultimo back-up degli applicativi e della configurazione installata era datata, una parte delle ultime variazioni applicative è andata persa. Sono risultati inutilizzabili anche i file delle licenze dei software installati e sono andati persi gli ultimi dati storici e gli allarmi raccolti dopo l'ultimo back-up. Il danno è difficilmente calcolabile, tra tempo di fermo macchina, costi diretti per consulenti e componenti da sostituire, costi indiretti dovuti alla mancata produzione, alla cancellazione dei lotti, all'impossibilità di produrre e alla lesa reputazione.

Morale: la base di ogni sistema "sicuro" (anche se nessuna architettura può ritenersi al sicuro al 100%) sono le policy, bisogna essere pronti e avere sempre un piano di riserva, ovvero sapere come ripartire in fretta e senza perdere dati.

3.3 Concetti generali di protezione

Siamo abituati a sentir parlare di IT, Information Technology. Ma quando si parla di industria la parola chiave è OT, Operational Technology, che rappresenta l'insieme di tutti i "sistemi intelligenti" che gestiscono informazioni dell'impianto. Pensare di affrontare la questione della Security dei sistemi industriali con lo stesso approccio impiegato nelle soluzioni business sarebbe un errore. Se in ambito IT i principi base della Cyber Security definiscono un dato sicuro quando sono rispettati i criteri di Riservatezza, Integrità e Disponibilità, in ambiente OT l'ordine di questi tre fattori va letto al contrario: le caratteristiche irrinunciabili sono Disponibilità ed Integrità, mentre la Riservatezza è quasi un parametro accessorio. Un sistema infatti deve essere innanzitutto essere "always-on" e, a seconda dell'utilizzo più o meno critico, la disponibilità del sistema deve prevedere anche la Fault Tolerance: questo significa avere sistemi ridondati a caldo e tempi di ripartenza ridotti al minimo.

L'Integrità del dato, invece, si può ottenere adottando soluzioni software pensate e sviluppate per garantire affidabilità nella catena di gestione del dato (dal sensore allo schermo del computer), una completa tracciabilità degli accessi e una precisa registrazione in caso di variazioni o correzione di dati o valori.

Una logica conseguenza di questi principi è che in ambito industriale vanno utilizzate soluzioni espressamente pensate per questo scopo. L'approccio ad una corretta progettazione della rete dovrebbe implicare una gestione globale della Security aziendale, tenendo conto delle esigenze IT e OT in maniera olistica.

In un sistema di Security olistico della rete, vanno considerati in primo luogo diversi livelli di accesso per differenti classi di utilizzatori. Esiste un'ampia disponibilità sul mercato di sistemi software per l'identificazione degli accessi che sono operativi in modo trasparente agli utenti e senza utilizzare se non una minima parte delle risorse di rete disponibili per non ridurre in nessun modo le prestazioni dei processi in corso. Ogni richiesta di accesso alla rete avvia un processo di identificazione che dovrebbe valutare anche aspetti quali il mezzo di connessione usato (rame, fibra, wireless), la posizione e la velocità della porta di accesso sullo switch o router usata dal dispositivo che sta accedendo, oltre ad identificare il tipo dello stesso (netebook, tablet, smartphone, ...) e successivamente applicare la policy definita per quello specifico utente su quella rete.

I moderni sistemi di identificazione sono in grado di validare l'accesso da uno specifico sistema operativo, oppure ad un determinato applicativo. Solo dopo aver verificato la congruità di ognuna delle precedenti discriminanti poste come condizioni, l'accesso dovrebbe essere consentito alla subnet di una specifica zona.

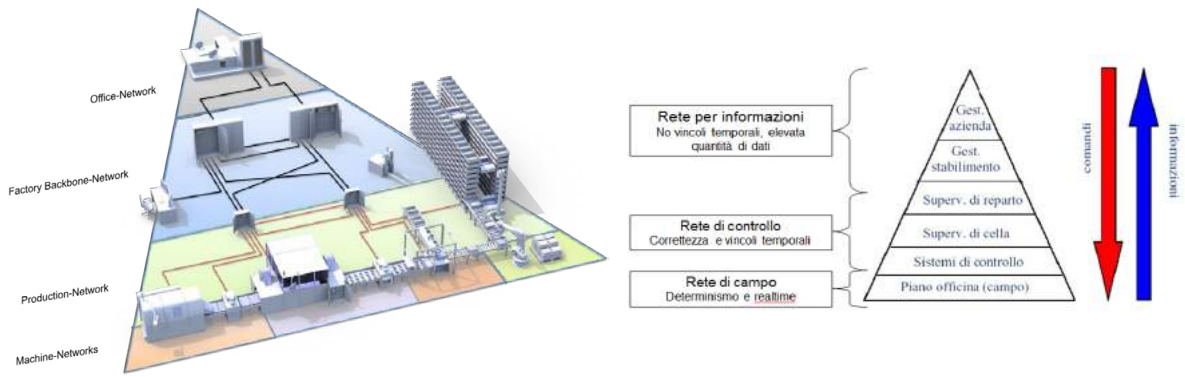
Sono oggi disponibili dispositivi intelligenti con funzioni IPS/IDS, Firewall, Antimalware e soprattutto dotate di avanzate funzioni di filtraggio, application/protocol/datapackage White-Listing ed Anomaly detection: tecniche che si sono dimostrate efficaci nel contrastare problemi di Security su reti e sistemi di controllo e telecontrollo in molti settori industriali. Si è invece rivelato inefficace il semplice utilizzo di Firewall pensati per le applicazioni web ed IT tradizionali, in quanto non è agevole definire regole per le connessioni ed il filtraggio dei dati che possano essere valide anche per il mondo dell'OT: porte, protocolli e regole sono diverse e tipiche dei dispositivi collegati alla rete di impianto e dei sistemi di controllo e telecontrollo. Come diverse sono le competenze richieste per capire e quindi proteggere in modo adeguato le applicazioni OT in reti di automazione, controllo e telecontrollo dai rischi informatici nell'industria e nelle infrastrutture critiche.

Di grande aiuto poi risultano tecnologie come la virtualizzazione, il Cloud, i Virtual desktop e i thin client che hanno mostrato come lavorare su credenziali e controllo accessi, sul traffico dati in entrata e in uscita, sulla possibilità di eseguire backup temporizzati e ravvicinati sia strada assai più sicura di quella di creare un "perimetro invalicabile" come si tendeva a fare negli anni passati. Inoltre, la possibilità di creare un elevato numero di immagini dei server online permette di programmare i backup del sistema anche a distanza molto ravvicinata, consentendo di recuperare dati e rimettere in piedi il sistema in tempi molto rapidi, tenendo conto della resilienza. Le architetture con l'utilizzo di macchine virtuali aumentano la disponibilità e le prestazioni in caso di Disaster Recovery: una macchina sempre attiva o dormiente si riavvierà più in fretta di un server tradizionale.

In modo schematico, un'adeguata protezione contro intrusioni non volute in una rete Ethernet è basata su pochi concetti fondamentali:

- il primo è relativo a una corretta protezione delle porte di accesso alla rete, siano esse accessibili localmente (porte fisiche di switch, PC, PLC o altri dispositivi) o che possano prevedere accesso da remoto per operazioni di teleassistenza;
- un secondo concetto fondamentale è quello basato sulla segmentazione della rete in più zone, separate tra loro, che comunicano tra loro solo attraverso percorsi ben definiti e ben protetti (firewall, VPN, ...) secondo i principi inclusi all'interno della serie di norme internazionali IEC 62443 "Industrial communication networks - Network and system security";
- da ultima, ma non ultima per importanza, la presenza di soluzioni di controllo continuo della rete permette di poter accorgersi in tempo reale di anomalie indicative di accessi e modifiche già intervenute.

Il Networking e la Smart Factory



3.4 Gli standard di Security digitale industriale

Mentre le minacce informatiche attuali diventano sempre più pericolose per i sistemi di automazione, la continua evoluzione dei rischi suggerisce che un elevato livello di sicurezza può essere raggiunto con l'approccio di tecniche di security digitali o di sicurezza funzionale.

Gli Industrial Automation Control System (IACS) hanno bisogno di implementare alti livelli di Security per la sicurezza funzionale: senza Security il raggiungimento delle funzioni di sicurezza può essere compromesso.

Esempi di IACS sono di seguito elencati:

- Industrial Control System (ICS) e Distributed Control System (DCS);
- Programmable Logic Controller (PLC);
- Remote Terminal Unit (RTU);
- Intelligent Electronic Device (IED);
- Supervisory Control and Data Acquisition (SCADA);
- Networked Electronic Sensing & Control and Monitoring & Diagnostic System (inclusi i Safety-Instrumented System - SIS).

Se uno IACS esegue una funzione di sicurezza e l'attacco Cyber è classificato come potenzialmente pericoloso, il sistema di controllo deve essere sviluppato e validato in accordo agli standard IEC 62443, al fine di:

- garantire un adeguato livello di security contro le minacce esterne;
- aumentare il livello di protezione dei dati;
- aumentare l'affidabilità dei sistemi.

La serie di standard IEC 62443 definisce le line guida per incrementare la sicurezza digitale degli Industrial Automation and Control System. Questi standard si applicano agli utilizzatori finali (es. proprietari della rete), system integrator, operatori di security e costruttori di sistemi di controllo.

Gli standard di Security digitale industriale sono organizzati su quattro livelli:

1. Generale - La prima categoria include informazioni e concetti generali, modelli e la terminologia. Sono descritti anche i parametri di sicurezza digitali e il ciclo di vita della sicurezza digitale per IACS.
2. Politica e Procedure - La seconda categoria è destinata ai gestori della rete.
3. Sistemi - La terza categoria descrive il modello di sviluppo di sistemi attraverso l'integrazione di componenti.
4. Componenti - La quarta categoria descrive i requisiti dei prodotti che implementano tecniche di protezione da attacchi Cyber.

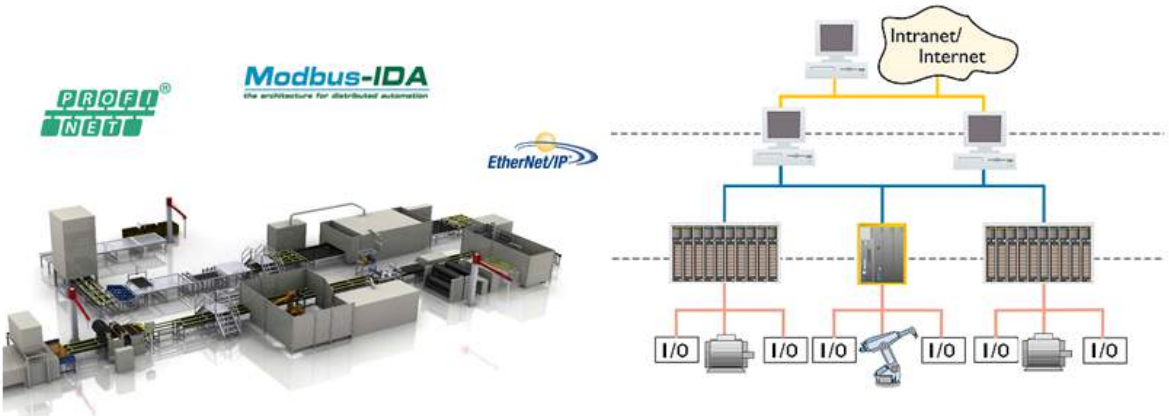
General	Policy & Procedure	System Integrator	Component Provider
IEC TS 62443-1-1 Terminology concepts and models	**IEC 62443-2-1** Requirements for an IACS security management system	**IEC TR 62443-3-1** Security technologies for IACS	**ISA 62443-4-1** Product development requirements
IEC 62443-1-2 Master glossary of terms and abbreviations	**IEC 62443-2-2** Implementation guidance for an IACS security management system	**IEC 62443-3-2** Security levels for zones and conduits	**ISA 62443-4-2** Technical security requirements for IACS components
IEC 62443-1-3 System security compliance metrics	**IEC TR 62443-2-3** Patch management in the IACS environment	**IEC 62443-3-3** System security requirements and security levels	
IEC TS 62443-1-4 IACS security lifecycle and use-case	**IEC 62443-2-4** Installation and maintenance requirements for IACS suppliers		

3.5 I sistemi di protezione delle reti

Per quel che riguarda gli strumenti da prevedere per un'adeguata Cyber Security, semplicemente riferendosi a prodotti o soluzioni tecnologiche dedicate, esistono sul mercato molteplici offerte, scalabili in funzione delle reali necessità e che risultano più o meno complesse, quindi costose, in funzione degli obiettivi specifici di protezione necessari. Difficile quindi sintetizzare ma diciamo che le regole tecniche di base per una corretta protezione di una rete industriale sono relative a un'opportuna segmentazione della rete, a un'adeguata protezione (routing/firewall) dei punti di segmentazione, a una corretta gestione delle prerogative di accesso locale alla rete e a un'efficace protezione degli accessi da remoto (VPN, firewall, security cloud).

Diverse sono le strategie che consentono la protezione nella comunicazione dati, cominciando dai livelli più bassi di protezione fisica dei cavi e apparati, fino ad arrivare a meccanismi di protezione a livello di protocollo di comunicazione. Di seguito vengono illustrate sinteticamente alcune delle possibili soluzioni tecnologiche atte alla creazione di un adeguato sistema di difesa contro accessi non voluti a reti Industrial Ethernet.

Industrial Ethernet nella Fabbrica 4.0



Port Security

Uno degli approcci più comuni per mettere al sicuro la propria rete dati si basa sulla sicurezza fisica degli apparati. L'obiettivo alla base di quest'approccio è di impedire l'accesso fisico non autorizzato alle porte di rete degli apparati.

Se un malintenzionato ha accesso fisico a una porta di rete dell'impianto, potrebbe collegare un proprio dispositivo per cercare di rubare informazioni o dare disservizio. Per operare tale protezione è necessario utilizzare dei dispositivi che supportano questa funzionalità, come i "Managed Switch", cioè switch che possiedono un'interfaccia amministrativa che consente di variarne la configurazione. Una protezione di facile implementazione consiste nel disabilitare tutte le porte di rete che non sono utilizzate. Tuttavia la protezione non risulta efficace nel caso in cui il malintenzionato abbia la possibilità di scollegare uno dei cavi delle porte funzionanti e collegarsi alla rete attraverso questa porta attiva. Pertanto occorre configurare le singole porte in modo che solo i dispositivi autorizzati possano accedervi. Ciò si può realizzare impostando sull'apparato l'indirizzo fisico (MAC address) delle macchine autorizzate oppure utilizzando un sistema di autenticazione che viene descritto nello standard IEEE 802.1x.

VLAN - Virtual Local Area Network

Una delle metodologie più utilizzate per proteggere una rete industriale è la sua suddivisione in zone isolate tra loro, tipicamente classificate per area funzionale e/o criticità. Operando in questo modo s'impedisce che l'accesso non autorizzato a una di queste zone possa essere utilizzato per accedere ad altre zone più critiche o vulnerabili. Ad esempio, l'accesso a una zona di controllo qualità può essere mantenuta separata dalla produzione vera e propria. Nella zona qualità, caratterizzata da un maggior passaggio di persone, un disservizio può essere tollerato, mentre in produzione no. Le VLAN sono dunque delle reti logicamente separate ma situate sugli stessi supporti fisici. Possono essere considerate in senso lato una componente della Security perché la segmentazione realizza reti più strutturate e robuste. Una catena di apparati di rete può propagare selettivamente più di una VLAN, rendendole disponibili anche a distanze molto elevate. La trasmissione nelle reti che implementano le VLAN avviene secondo lo standard IEEE 802.1q, cioè aggiungendo un TAG al pacchetto dati che contiene il numero di VLAN sulla quale si vuole trasmettere. Ciascun apparato di rete può definire, porta per porta, a quali VLAN appartengono, e quindi quali TAG possono essere accettati o meno.

SNMP - Simple Network Management Protocol

E' un protocollo di comunicazione definito dall'IETF (Internet Engineering Task Force) che consente la configurazione, la gestione e la supervisione degli apparati collegati a una rete. Attraverso opportuni cruscotti di supervisione è possibile monitorare lo stato della rete, il verificarsi di alcuni eventi, come l'inserimento di un nuovo dispositivo nella rete, l'aumento improvviso del traffico e del carico di lavoro degli apparati, può offrire utili indicazioni per prevenire le intrusioni. Il protocollo SNMP consente anche la configurazione a distanza degli apparati che può essere sfruttata per contrastare il verificarsi di un attacco. Ad esempio, è possibile disabilitare la porta di rete alla quale il malintenzionato si è collegato.

HTTPS - HyperText Transfer Protocol over Secure socket layer

Si tratta di un protocollo di comunicazione che rende sicura la trasmissione HTTP, comunemente utilizzata dai dispositivi, attraverso l'utilizzo di algoritmi di cifratura e autenticazione dei dati trasmessi. L'utilizzo di questo protocollo assicura la protezione da un attacco di tipo "Man In The Middle", cioè da parte di un terzo soggetto che s'interpone tra i due dispositivi per intercettare o modificare i valori scambiati. HTTPS garantisce: l'autenticità di chi trasmette - impedisce a una terza parte di falsificare i dati e spacciarsi per il

mittente; protezione del dato - impedisce a un malintenzionato di poter leggere i dati che i due dispositivi si stanno scambiando; integrità del dato - impedisce a un malintenzionato di modificare i dati trasmessi tra i due dispositivi.

VPN - Virtual Private Network

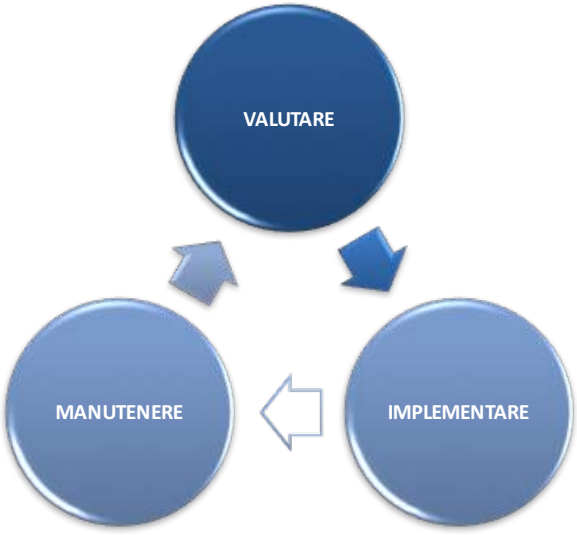
Una grossa percentuale della comunicazione dati in un impianto industriale avviene "in chiaro", cioè senza alcun meccanismo di protezione del dato. Questo scenario ha sia origini storiche, dove chi ha implementato i sistemi di comunicazione non si è posto il problema della sicurezza, ma anche una logica di comunicazione in una zona intrinsecamente considerata sicura. Basti pensare a una zona di produzione dove l'accesso all'edificio (e dunque alla rete) è consentito al solo personale autorizzato. Con l'avvento di Industry 4.0 e dell'IoT i sistemi vengono spesso collegati alla rete globale di Internet per trarre vantaggi dalle più recenti tecnologie, come i servizi di Amministrazione Remota e Cloud. Questo impone l'adozione di meccanismi di protezione del dato che viene veicolato su una rete considerata "non sicura". Le VPN vengono incontro a questa esigenza: implementano un meccanismo di protezione, basato su sistemi di cifratura e firma digitale, che impediscono l'intercettazione e contraffazione dei dati da parte di malintenzionati. Le reti VPN offrono alle aziende, a un costo relativamente contenuto, la possibilità di effettuare teleassistenza sicura dei propri apparati e la possibilità di estendere la rete locale, nel caso l'azienda operi su un ampio territorio.

Firewall

E' un elemento di rete perimetrale necessario per la protezione in ambito industriale qualora essa venga esposta a una rete non sicura, tipicamente Internet. Il firewall regola gli accessi dalla zona non sicura verso la zona sicura, impedendo accessi indesiderati e che potrebbero danneggiare l'impianto. La zona non sicura viene tipicamente indicata come WAN (Wide Area Network) mentre la rete sicura è indicata con l'acronimo LAN (Local Area Network): in questa concezione il firewall regola gli accessi tra WAN e LAN. A volte è presente una terza zona di rete chiamata DMZ (DeMilitarized Zone) atta a ospitare i sistemi che per loro natura devono rimanere isolati dalla LAN ma che necessitano comunque una protezione da attacchi provenienti dalla WAN. Un firewall, per poter essere efficace, deve essere configurato da personale specializzato che inserisce le regole di accesso. Tali regole operano dei filtri sul traffico in ingresso/uscita in base ai dispositivi che generano i dati, ai protocolli e alla direzione del traffico. I sistemi firewall più evoluti implementano anche dei filtri selettivi di protocollo industriale come OPC o MODBUS che possono consentire solo certe operazioni, ad esempio la sola lettura delle variabili MODBUS e non la loro scrittura.

3.6 Ciclo di gestione della Cyber Security

Ciclo di gestione della Cyber Security



Gli strumenti da prevedere per un'adeguata Cyber Security sono un aspetto tecnico e rappresentano solo una delle sfaccettature della Cyber Security, una fase di un ciclo di gestione della problematica, spesso di tipo iterativo.

Un ciclo di gestione che deve partire da una prima fase di analisi e identificazione dei potenziali rischi presenti in una rete, deve proseguire con una loro valutazione per definire le necessarie modalità di riduzione per poi arrivare alla definizione tecnologica atta al raggiungimento degli obiettivi fissati.

Previste le adeguate protezioni tecniche il compito non è comunque concluso.

Bisogna prevedere gli opportuni "corollari" organizzativi: definizione di responsabilità e attribuzione di opportune qualifiche operative ai vari operatori chiamati a interagire con la rete per le normali operazioni produttive o anche per aspetti di configurazione o manutenzione.

La stessa politica di Cyber Security necessita, infine, di una sua "manutenzione": l'efficacia delle misure adottate deve essere monitorata nel tempo, anche alla luce delle evoluzioni tecnologiche e delle eventualmente mutate modalità operative di potenziali intrusi malintenzionati.

A questo scopo è utile prevedere anche sistemi di monitoraggio continuo di rete in modo da poter cogliere in tempo reale modifiche non previste, indice di un processo in atto di tentativo di intrusione. Sistemi di questo tipo più evoluti possono definire in modo personalizzato i parametri di riferimento la cui modifica non prevista deve generare allerta con anche la possibilità di attivare in automatico opportune misure di reazione volte ad escludere o limitare al massimo i rischi di questi tentativi di accesso.

4. La Cyber Security nel Piano Nazionale I4.0

Nell'Industria 4.0 l'integrazione dei sistemi di automazione con quelli IT segna un profondo cambiamento che richiede innovazioni nelle infrastrutture di connettività, nei dispositivi intelligenti collegati via IP e nelle differenti applicazioni software in grado di elaborare e creare valore dai dati. Il tutto con nuovi requisiti a livello di Safety e di Security.

Sensori di nuova generazione che consentono di misurare, monitorare, identificare e localizzare qualsiasi cosa, unitamente a Intelligent Transport System applicati a ogni mezzo di trasporto, dentro e fuori alle fabbriche, aiutano l'Industria 4.0 a ridurre i rischi legati agli errori umani, garantendo massima visibilità rispetto al funzionamento degli impianti, ottimizzando la produzione e la gestione del magazzino a beneficio di tutta la supply chain. Si parla non a caso di Smart Manufacturing che, tra i suoi obiettivi, porta anche a un miglioramento della sicurezza fisica per il personale e di quella IT per impianti, dispositivi e prodotti connessi e comunicanti.

Attorno al concetto di Industria 4.0, infatti, non c'è solo un nuovo orientamento alla gestione del ciclo di vita del prodotto e alla logistica. La trasformazione digitale che sta travolgendo l'industria ruota attorno ai temi della business continuity, del disaster recovery e della protezione dei dati, ma anche una nuova consapevolezza legata al fatto che la sicurezza informatica non riguarda solo la protezione dell'hardware o del software. L'informatizzazione della società, culminata nel digitale, allarga le maglie della sicurezza ICT, includendo persone e cose.

Analizzando in dettaglio le tecnologie abilitanti Industria 4.0 descritte nel Piano Calenda emerge chiaramente come la Cyber Security sia parte integrante di qualsiasi scelta, sistema o soluzione. Nell'elenco dei cluster tecnologici che abilitano Industria 4.0 riassunti dal Ministero per lo Sviluppo Economico, la Cyber Security si posiziona al punto 8 ma, in realtà, ognuno dei singoli cluster la porta con sé come fattore abilitante:

Fonte: Piano Nazionale Industria 4.0 - MiSE

1. **Advanced Manufacturing Solution:** garantire la continuità operativa dei robot collaborativi, interconessi, autoapprendenti e/o rapidamente programmabili significa presidiare il livello di automazione con una serie di soluzioni di monitoraggio e di controllo che possono andare dal logging delle macchine alla protezione di tutta l'intelligenza software, inclusa la garanzia di una rete ad alta affidabilità.

2. **Additive Manufacturing:** le stampanti 3D connesse a software per lo sviluppo digitale sono sistemi complessi, che implicano non solo un controllo dei progetti CAD custoditi in uno o più database on site o in Cloud, ma anche la definizione di nuove modalità di accesso e di condivisione delle informazioni finalizzate a proteggere la proprietà intellettuale ma anche il controllo qualità della produzione. Il tutto con le massime garanzie di banda, per assicurare i workflow.

3. **Augmented Reality:** utilizzare la realtà aumentata a supporto dei processi produttivi significa inserire un nuovo livello informativo rispetto all'operatività delle risorse, che deve essere sempre puntuale e precisa per assolvere la sua funzione. Anche in questo caso si tratta di garantire la continuità operativa dei sistemi di accesso e di recupero delle informazioni, ma anche la qualità della connessione che garantisce quel servizio informativo a valore aggiunto.

4. **Simulation:** utilizzare le simulazioni aiuta le aziende ad essere più proattive e produttive a minor costo e con un livello di efficienza superiore. I programmi di simulazione devono tener conto di una gestione delle informazioni capace di elaborare un grandissimo numero di dati provenienti da fonti diverse, con una scalabilità e una flessibilità che impone agli sviluppatori aggiornamenti continui e patch. Anche in questo caso, tra protezione dei dati, testing, gestione degli accessi, messa in sicurezza dei database e controllo della qualità del software, la Cyber Security ha una rilevanza strategica.

5. **Horizontal/Vertical Integration:** dal fornitore al consumatore integrare lungo la catena del valore le informazioni significa tutelare ogni singolo anello della supply chain. Le tecnologie coinvolte sono tantissime. Tecnologie auto-ID (Identificazione Univoca) che mettono a sistema la tracciabilità e la rintracciabilità delle informazioni, dalle materie prime ai prodotti, dagli asset a ogni singola componente e utili anche per la geolocalizzazione, supportano la logistica ma anche l'anticontraffazione e i furti. I sistemi di fatturazione elettronica e conservazione sostitutiva, invece, ottimizzano il ciclo dell'ordine nel B2B e nel B2C. Il digital asset management più spinto aiuta le imprese a capitalizzare anagrafiche prodotti e velocizzare logistica e distribuzione, unitamente a un CRM evoluto, che riesce a orchestrare le informazioni provenienti da qualsiasi touch point, dai call center ai social media, dalle app alle mail. L'integrazione è fondamentale ma rende i confini aziendali sempre più liquidi, imponendo nuovi criteri di sicurezza per proteggere l'azienda e i clienti in un'unica soluzione di continuità.

6. **Industrial Internet:** la comunicazione multidirezionale tra processi produttivi e prodotti, innestata su un'omnicanalità sempre più pervasiva e una ibridizzazione dei processi on line e off line, necessita di una capacità di gestione dei rischi molto più ampia e olistica, che va ben oltre la scelta addizionale di soluzioni di sicurezza dedicate.

7. **Cloud:** gestire un'elevata quantità di dati su sistemi aperti non è banale. La nuvola funziona molto bene, ma i regimi di sicurezza devono essere definiti da SLA (Service Level Agreement) contrattuate insieme ai fornitori secondo precise direttive.

8. **Cyber Security:** il Piano I4.0 definisce questa voce come "sicurezza durante le operazioni in rete e su sistemi aperti". Il tema dell'Industria 4.0 è proprio una nuova intelligenza che rende potenzialmente ogni cosa connessa e comunicante attraverso un uso evoluto di Internet e di un software sempre meno proprietario, ma fruito in chiave "as a service". L'obiettivo di Industria 4.0 deve essere quello di coniugare la Cyber Security con il concetto di Cyber Resilience. Il Cyber Crime lavora con le tecnologie ed evolve spesso giocando in anticipo: le aziende sanno che è impossibile garantire una sicurezza totale. Proteggere i dati, le macchine, i programmi, i prodotti, le persone deve rientrare in una strategia allargata, in cui convergono sensori di monitoraggio, sistemi di videosorveglianza, telecontrollo, antintrusione, antieffrazione ma anche di protezione da tutte le derive del Cyber Crime che colpisce gli utenti in azienda oppure in mobilità. Non a caso con la sicurezza vengono coinvolti i legali e gli enti certificatori, il garante della Privacy e le autorità preposte, le risorse umane e gli addetti al facility management. Bisogna lavorare in modalità trifasica, attuando una strategia capace di ragionare prima, durante e dopo un attacco. Cyber Security significa, infatti, progettare sistemi predittivi e reattivi che da un lato riescono ad anticipare le minacce e, dall'altro, sono in grado di attuare piani di intervento quanto più tempestivi ed efficaci.

9. **Big Data e Analytics:** analizzare un'ampia base dati per ottimizzare prodotti e processi produttivi è un aspetto fondamentale di Industria 4.0. Anche in questo caso proteggere i database e i flussi delle informazioni è basilare, quanto definire algoritmi puntuali e funzionali al business. Una buona gestione dei dati (qualsiasi tipo di dato) aiuta la sicurezza a capire, analizzare e reagire: capire in che modo tenere traccia delle informazioni e, al momento opportuno, utilizzarle invece di farsi sopraffare dagli alert è altrettanto fondamentale per la Cyber Security.

La Cyber Security, ottavo punto di Industria 4.0

Semplificando le direttive del Governo, per il mondo dell'industria il 4.0 riassume il modello delle 4I: Informazione, Innovazione, Integrazione, Interazione. Industria 4.0, infatti, significa gestire la digitalizzazione progressiva delle informazioni, scegliere e adottare le tecnologie più innovative e adattare a supportare il business, lavorare di integrazione secondo un approccio che elimina le logiche a silos e punta alla massima condivisione e cooperazione tra le filiere, favorire la collaborazione impostando il lavoro attraverso la costruzione di piattaforme capaci di mettere a fattor comune le risorse, sfruttando Internet e la banda larga, in maniera quanto più semplice e intuitiva per velocizzare le operation e i servizi.

Figlia dell'IoT, Industria 4.0 è una rivoluzione industriale innestata su un mix tecnologico fatto di automazione, informazione, connessione e programmazione. Le soluzioni coinvolte sono tantissime, organizzarle in maniera armonica e coordinata è una sfida che ha bisogno di competenze diversificate e di vision ampie e lungimiranti, che ha come denominatore comune la Cyber Security. Proteggere e controllare i sistemi produttivi, la gestione dei flussi di informazioni e di merci, l'automatizzazione delle catene di produzione e la sicurezza di ogni operatore va di pari passo col progresso delle tecnologie, e la ricerca da parte delle aziende di nuove soluzioni. Come sottolineano gli esperti, non è un tema solo da addetti ai lavori.

Chi si occuperà di offrire chiare linee guida e un coordinamento a tutti gli aspetti della Cyber Security, dovrà puntare a una ricerca e uno sviluppo di tipo collaborativo, finalizzato a contrastare le minacce alle infrastrutture critiche. La possibilità per il settore privato di investire, co-sviluppare e integrare tecnologie innovative nel mercato della sicurezza informatica in cooperazione con le istituzioni governative avrà un impatto significativo rispetto ai progressi contro il Cyber Crime. L'integrazione e la cooperazione, infatti, saranno fondamentali nell'era digitale.

È necessario che le aziende colgano rapidamente l'impatto della trasformazione digitale sulla gestione di infrastrutture, dati e applicazioni, impostando una sicurezza bimodale che, tra tecnologia e compliance, riesca a gestire una configurazione sempre più complessa per la governance, armonizzando le soluzioni tattiche con sistemi fondanti strategici.

Internet of Thing, Smart City, Industria 4.0 non potranno essere realizzati senza un sufficiente livello di Cyber Security. Si tratta di una sfida che va indirizzata e gestita, con il coinvolgimento e la collaborazione di tutti, e soprattutto con la consapevolezza che la sicurezza delle informazioni non deve essere vista come un costo o un ostacolo alle attività, ma piuttosto come una opportunità che produrrà vantaggio competitivo, rappresentando un fattore decisivo per la crescita economica delle imprese e dell'intero Paese.

5. Bibliografia

2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity, CIS Sapienza

Atti Forum Meccatronica di ANIE Automazione, Edizioni 2015 e 2016

Cyber security e Industria 4.0, E. M. Tieghi, ICT Security Magazine, febbraio 2017, ictsecuritymagazine.com

Cyber Security e investimenti quali scenari?, A. Teti, maggio 2016, sicurezzanazionale.gov.it

Cyber security: entra in vigore il nuovo decreto, aprile 2017, sicurezzanazionale.gov.it

Cybersecurity nel piano Calenda: perché Industria 4.0 significa anche più sicurezza, L. Zanotti, digital4.biz

Cybersecurity, le startup italiane della nuova corsa all'oro, G. Moccia, dicembre 2016, Linkiesta.it

Cybersecurity, una nuova architettura industriale per un problema di salute pubblica, A. Bairaghi, C. Verdecchia, forumpa.it

Cybersicurezza: 2016 da incubo. È stato l'anno peggiore di sempre, B. Simonetta, febbraio 2017, ilsole24ore.com

Digital Factories & Cyber Security: due facce della stessa medaglia, crit-research.it

Guida per il Networking industriale, WG Networking di ANIE Automazione, maggio 2017

IEC TC65/WG10 Committee, iec.ch

Il Futuro della Cyber Security in Italia, E. Baldoni, R. De Nicola, CINI, ottobre 2015, consorzio-cini.it Cyber Security standards, en.wikipedia.org

Introduzione alla protezione di reti e sistemi di controllo e Automazione, E. M. Tieghi, Quaderni Clusit 2007, clusit.it

La Cyber Security in applicazioni di automazione industriale, Gruppo Meccatronica di ANIE Automazione, InMotion, maggio 2017

La cybersecurity: un business da 74 miliardi e il caso Italia, L. Tremolada, dicembre 2016, ilsole24ore.com

La security digitale nelle reti di comunicazione industriali, DNV GL - Business Assurance, dnvgl.it

Maggiori capacità e nuove funzioni al servizio dei PLC destinati a Industria 4.0, Gruppo PLC I/O di ANIE Automazione, Automazione Oggi, marzo 2017

Report 2017, Osservatorio Information Security & Privacy, Politecnico di Milano

Sicurezza informatica, it.wikipedia.org

Un Security Framework per l'IIoT, A. Cavalcoli, Industrie 4.0, marzo 2017

Wireless e Cyber Security industriale: opportunità e rischi, WG Wireless di ANIE Automazione, Automazione e Strumentazione, gennaio-febbraio 2014

CAPITOLO 4

AZIENDE ASSOCIATE ANIE AUTOMAZIONE

- 3W POWER SPA
- A.T.I. SRL ACMO TECNOLOGIE INTEGRATE
- ABB SPA - ELECTRIFICATION PRODUCT DIVISION
- ABB SPA - INDUSTRIAL AUTOMATION DIVISION - POWER GENERATION LBU
- ADVANTECH EUROPE BV
- ALLEANTIA SRL
- ANSALDO ENERGIA SPA
- AUTEC SRL
- B&R AUTOMAZIONE INDUSTRIALE SRL
- BALLUFF AUTOMATION SRL
- BECKHOFF AUTOMATION SRL
- BONFIGLIOLI RIDUTTORI SPA
- BORRI SPA
- BOSCH REXROTH SPA
- C.E.A.I. ELETTRONICA SRL
- CALVI SISTEMI SNC
- DANFOSS SRL
- DELTA ENERGY SYSTEMS ITALY SRL
- DKC EUROPE SRL
- DUCATI ENERGIA SPA
- E.T.A. SPA
- EATON INDUSTRIES (ITALY) SRL
- ELETTRONICA SANTERNO SPA
- ELETTROPIEMME SRL
- ENDRESS + HAUSER ITALIA SPA
- EPLAN SOFTWARE & SERVICE SRL
- ESA ELETTRONICA SPA
- ETG SRL
- FAMAS SYSTEM SPA
- FANDIS SPA
- FESTO SPA
- FINCANTIERI SI SPA
- FRABA GMBH
- FRIEM SPA
- GEFRAN SPA
- GEOCART SPA
- GEWISS SPA
- GTEC EUROPE SRL
- HEIDENHAIN ITALIANA SRL
- HONEYWELL SRL
- ID&A SRL
- IDEA SPA
- INTESIS SRL
- KEB ITALIA SRL
- LACROIX SOFREL SRL
- LAPP ITALIA SPA
- LENZE ITALIA SRL
- LEVER SRL
- LOGIKA CONTROL SRL
- M.D. MICRO DETECTORS SPA
- META SYSTEM SPA
- MICROTEC SRL
- MITSUBISHI ELECTRIC EUROPE B.V.
- MOTOVARIO SPA
- NATIONAL INSTRUMENTS ITALY SRL
- NIDEC ASI SPA
- NIDEC INDUSTRIAL AUTOMATION ITALY SPA
- ODE SRL
- OLTREBASE SRL
- OMNICON SRL
- OMRON ELECTRONICS SPA
- PANASONIC ELECTRIC WORKS ITALIA SRL
- PARKER HANNIFIN ITALY SRL
- PCVUE SRL
- PHOENIX CONTACT SPA
- PHOENIX MECANO SRL
- PILZ ITALIA SRL
- PNEUMAX SPA
- POWERTRONIX SRL
- PRISMA IMPIANTI SPA
- REEL SRL
- REER SPA
- RITTAL SPA
- ROCKWELL AUTOMATION SRL
- RPS SPA - RIELLO UPS
- SAIA BURGESS CONTROLS ITALIA SRL
- SAIRA ELECTRONICS SRL
- SCHNEIDER ELECTRIC SPA
- SCHUNK INTEC SRL
- SDI AUTOMAZIONE INDUSTRIALE SPA
- SDPROGET INDUSTRIAL SOFTWARE SRL
- SELTA SPA
- SEW EURODRIVE SAS
- SICK SPA
- SICON SRL
- SIECAB SRL
- SIEL SPA
- SIEMENS SPA
- SODI SCIENTIFICA SPA
- SP ELECTRIC SRL
- TDE MACNO SPA
- TECNOWARE SRL
- TELESTAR SRL
- TELETECNICA SRL
- TEX COMPUTER SRL
- TURCK BANNER SRL
- VAR SIRIO INDUSTRIA SRL
- VERTIV SRL
- VIPA ITALIA SRL
- WEIDMÜLLER SRL
- WIT ITALIA SRL
- WITTENSTEIN SPA
- WONDERWARE ITALIA SPA
- YOKOGAWA ITALIA SRL

Federazione ANIE
ANIE Automazione
Viale Lancetti, 43 - 20158 Milano - Tel. 02 3264.252 - Fax 02 3264.327
anieautomazione@anie.it - www.anieautomazione.it - www.anie.it
www.forumtelecontrollo.it - www.forumeccatronica.it - @ANIEAutomazione