



ASSOLOMBARDA
Confindustria Milano Monza e Brianza

Approfondimento sulle tecnologie abilitanti Industria 4.0

RICERCA

08/2016

A cura dell'Area

Industria e Innovazione

Approfondimento sulle tecnologie abilitanti Industria 4.0

La presente ricerca è stata sviluppata dall'Area Industria e Innovazione di Assolombarda Confindustria Milano Monza e Brianza, in coordinamento con il team di esperti costituito da Alessandro Brusaferrì, Giacomo Copani, Fabio Martinelli, Lorenzo Molinari Tosatti, Andrea Passarella e Walter Terkaj, coordinati dal prof. Tullio A. M. Tolio, Direttore dell'Istituto ITIA – CNR.

Indice

INTRODUZIONE	9
1. LA ROBOTICA IN OTTICA INDUSTRY 4.0	11
1.1. Scopi e vantaggi della Robotica nel paradigma Industry 4.0	12
1.2. A che punto siamo	13
1.3. Verso la robotica di Industry 4.0	15
2. LA FABBRICA DIGITALE	17
2.1 Scopi e vantaggi della Fabbrica Digitale	18
2.2. A che punto siamo	20
2.3. La strada verso la Fabbrica Digitale	22
3. CONTROLLO E SUPERVISIONE AVANZATI DEL PROCESSO PRODUTTIVO	24
3.1. Scopi e vantaggi dei sistemi di controllo e supervisione avanzata nel paradigma Industry 4.0	25
3.2. A che punto siamo	28
3.3. La strada verso i sistemi di controllo e supervisione avanzati in ottica Industry 4.0	28
4. IOT E BIG DATA	30
4.1. Scopi e vantaggi di IoT e Big Data	32
4.2. A che punto siamo	33
4.3. La strada verso IoT e Big Data	35
5. CYBER SECURITY	37
5.1. Scopi e vantaggi delle tecnologie di cyber security	39
5.2. A che punto siamo	41
5.3. La strada verso la cyber security in Industry 4.0	44

Introduzione

L'Industria 4.0 è la teorizzazione di un paradigma manifatturiero basato sul concetto di "Cyber Physical System" (CPS), cioè sistemi informatici in grado di interagire con i sistemi fisici in cui operano, che sono dotati di capacità computazionale, di comunicazione e di controllo.

La diffusione del concetto di Industry 4.0 è stata tale e talmente diversificata nei diversi Paesi, ambienti industriali e della ricerca che non esiste una definizione univoca del fenomeno. Industry 4.0 è spesso identificato con l'insieme di una serie di tecnologie abilitanti: "Internet of Things" (IoT), Big Data Analytics, Robotica collaborativa, Additive Manufacturing, Digital Factory, ecc. Attraverso tali tecnologie abilitanti, le imprese hanno la possibilità di innovare radicalmente il loro modello di business.

Guardando all'innovazione manifatturiera degli ultimi anni, si può affermare che Industry 4.0 è più un'evoluzione già in corso da decenni, che una vera e propria rivoluzione improvvisamente abilitata dalla disponibilità di nuove tecnologie. Nei campi della robotica, sensoristica, additive manufacturing, "Digital Factory", sistemi di automazione e controllo, ecc., infatti, il trend verso la digitalizzazione, l'aumento delle performance e l'integrazione delle risorse produttive è in corso da tempo. Di conseguenza, già oggi è possibile implementare, almeno parzialmente, soluzioni innovative "in ottica 4.0" con tecnologie commerciali. Anche in termini di business model e di "paradigm shift" che Industry 4.0 rende possibile, il trend verso la "personalizzazione" e la "servitizzazione" dell'offerta resi possibili da nuove modalità di gestione e dall'accresciuta intelligenza dei sistemi produttivi è dibattuto già da diversi anni. Indubbiamente, la recente disponibilità e la sempre maggior diffusione di alcune tecnologie abilitanti per la realizzazione del concetto di Industry 4.0 nella sua interezza, quali ad esempio i sensori miniaturizzati a basso costo, forniscono nuovi strumenti tecnologici e di interconnessione delle risorse manifatturiere che danno nuova linfa e maggiore potenzialità al trend di adozione delle tecnologie informatiche e di rinnovamento dei modelli di business che è già in corso.

Nel contesto di innovazione manifatturiera italiana l'Industria 4.0 abbraccia un'importante parte delle tematiche di ricerca e innovazione indicate come prioritarie per il futuro del manifatturiero nazionale e indirizza un numero significativo di "Linee di Intervento" prioritarie, in particolare: strategie per la produzione personalizzata; strategie, metodi e strumenti per la sostenibilità industriale; sistemi per la valorizzazione delle persone nelle fabbriche; sistemi di produzione ad alta efficienza; sistemi di produzione evolutivi e adattativi; strategie e management per i sistemi produttivi di prossima generazione.

Occorre chiedersi quali siano i problemi delle nostre imprese che l'implementazione di Industria 4.0 può contribuire a risolvere e, di conseguenza, quali le opportunità per il sistema Paese. Tale strada deve essere disegnata identificando puntualmente ciò che oggi manca nei vari ambiti tecnologici rispetto allo stato dell'arte per arrivare alla realizzazione del paradigma nel suo complesso e per cogliere conseguentemente i vantaggi traguardati. Per questo è necessario addentrarsi nell'analisi dei sotto-ambiti tecnologici che concorrono alla realizzazione di Industria 4.0.

Nella presente ricerca si approfondiscono cinque ambiti tecnologici che risultano di particolare importanza per l'implementazione di Industria 4.0. Per ciascuno di questi si identificano le principali sfide che le imprese si trovano ad affrontare oggi, si indicano le risposte per affrontare tali sfide che le soluzioni in ottica Industria 4.0 possono già fornire, si segnalano le risposte che la tecnologia potrà fornire nel medio-lungo periodo in seguito alla loro evoluzione, nonché i fattori che abiliteranno l'evoluzione delle tecnologie.

Si considerano nella presente Ricerca cinque aree tecnologiche ritenute strategiche per l'implementazione di Industria 4.0:

- Robotica collaborativa
- “Fabbrica Digitale”
- Controllo e supervisione avanzati del processo produttivo
- Internet of Things e Big Data
- Cyber Security

Con lo scopo di introdurre una visione applicativa delle tecnologie abilitanti di tali aree tecnologiche, si identificano per ciascuna di queste le sfide che le imprese manifatturiere devono affrontare, per le quali le tecnologie abilitanti possono fornire risposte. In tal modo, si introduce il legame tra tecnologia abilitante di Industria 4.0 e la sua concreta utilità per le imprese. I vantaggi sono indicati sia nel breve periodo (derivanti dall'applicazione delle tecnologie già a disposizione oggi) che nel lungo periodo (ottenibili cioè quando le tecnologie Industria 4.0 saranno mature). Infine, si indicano i fattori che abiliteranno lo sviluppo delle tecnologie Industria 4.0 nel lungo periodo.

1. La Robotica in ottica Industry 4.0

Nel paradigma di Industria 4.0, i robot che collaborano con operatori umani per l'esecuzione dei processi produttivi già possono essere e saranno una risorsa fondamentale delle fabbriche. Le tecnologie di cooperazione uomo-robot offriranno agli operatori modalità di fruizione naturali (usabilità) e un elevato livello di fiducia nelle funzionalità delle macchine (affidabilità, manutenibilità, disponibilità e sicurezza). La fruizione risulterà semplice e intuitiva, rendendo quindi non necessariamente visibili o percepibili le tecniche e le tecnologie impiegate nella realizzazione delle funzioni dei dispositivi robotici. Tali tecnologie consentiranno di ottenere agenti robotici non isolati dall'ambiente produttivo occupato da operatori umani, bensì attivamente partecipi di processi cooperativi in ambienti condivisi. L'agente robotico (spesso indicato come "co-worker"), immerso in un contesto di fabbrica 4.0, pur rimanendo una macchina automatica si caratterizzerà per capacità di interazione quasi-umane: nelle interazioni da contatto l'esperienza sensoriale e percettiva sarà molto simile a quella naturale, così come i movimenti e i comportamenti dei robot seguiranno pattern "cognitivamente accettabili" (basse velocità, traiettorie morbide, forme non ostili, operazioni prevedibili, contatti con cedevolezza). Oltre all'interazione fisica, che per definizione annulla le distanze e le separazioni tra operatori e robot, le tecnologie per la condivisione dello spazio di lavoro saranno rivolte a trasformare la fabbrica tradizionale in un ambiente più fluido e dinamico, aperto e interattivo (misura e monitoraggio dell'ambiente e degli operatori, allocazione dinamica dei programmi, navigazione piattaforme mobili, spazi virtuali sicuri, tecnologie multirobot). Alla base delle tecnologie di interazione si collocano tutte le tecnologie e gli aspetti relativi alla sicurezza (safety) dell'interazione fisica e della condivisione degli spazi. Nello specifico, la cooperazione si caratterizza diversamente (o può essere definita) a vari livelli come:

- Fisica (physical Human-Robot Interaction, pHRI): laddove avviene scambio diretto di energia tra operatori umani e agenti robotici, ad esempio nella manipolazione congiunta e nel contatto (intenzionale o accidentale). Esempi di tale modalità comprendono la programmazione intuitiva (lead-through programming) in cui un manipolatore viene addestrato accompagnando il movimento, fisicamente guidando il manipolatore lungo traiettorie, da ripetere in autonomia successivamente; la manipolazione concorrente di stesse parti (material handling) per grossi carichi o posizionamenti particolari; la possibilità di limitare/fermare il moto o l'esecuzione di task automatici ostacolando direttamente il manipolatore per motivi intenzionali o per interventi di emergenza; ecc.
- Funzionale: laddove l'organizzazione dello spazio produttivo prevede una concorrenza di attività tra operatore umano e robotico. La collaborazione può assumere modalità seriali (passi di workflow produttivo alternati tra robot/operatore) o parallele (operazioni indipendenti congiunte a determinati passi). Nel caso di compiti condivisi, questi devono essere necessariamente svolti in collaborazione al solo scopo di raggiungere la massima efficacia ovvero nei casi in cui la semplice sostituzione dell'operatore non dia valore aggiunto o il processo non sia conseguibile altrimenti. Esempi includono casi specifici di assemblaggio, in cui il robot co-manipola parti di dimensioni ampie o predispone guide/ausili al montaggio. Nel caso di processi paralleli, l'organizzazione dello spazio di lavoro condiviso (workspace sharing) si avvale invece di tecnologie di ripianificazione del

moto (collision avoidance, riduzione velocità, riallocazione target) e del task (rescheduling adattativo) in modo da garantire la presenza sicura dell'operatore nello spazio condiviso.

- Cognitiva: complementare alle precedenti, laddove l'organizzazione dei processi condivisi prevede un certo grado di interpretazione del contesto (context awareness). La trasparenza di interazione tra uomo e robot è tanto maggiore quanto più è estesa l'entità del trasferimento di attività, comandi, informazioni espliciti dall'operatore al robot. Ovvero, quanto più l'agente robotico si fa carico di interpretare e gestire localmente informazioni (es. task specifici in relazione ad uno specifico passo di lavorazione, parti di programma in relazione ad una specifica configurazione di cella, configurazioni specifiche in relazione a particolari contesti di rischio), tanto minore è il sovraccarico di trasferimento esplicito (ridondante) di nozioni dall'operatore alla macchina con conseguente riduzione di tempi di esecuzione, miglioramento dell'esperienza d'uso, maggiore flessibilità e velocità di riorganizzazione dei task. Questa componente agisce non solo a livello di dispositivi (robot) attraverso una serie di tecnologie di behavior e gesture recognition (tipicamente includendo sensori di visione tridimensionale, ricostruzione degli ambienti e della controparte umana, model-based matching, machine learning, deep learning etc); ma anche a livello di sistema dal momento che le singole informazioni generate localmente sono distribuite e condivise con altri agenti coinvolti (pianificazione di processo, supervisione di sistema, allocazione risorse, etc). Per rendere possibile tale sistematizzazione delle informazioni sono necessarie tecnologie di livello architetturale comprendenti sia le infrastrutture (control system architectures, knowledge-base control) sia le componenti modellistiche (environment modeling, behavior modeling, sensor data modeling, object modeling).

I vari livelli di cooperazione concorreranno a costruire un sistema di capacità sensoriali, motorie e cognitivo-funzionali tali da creare, nel contesto della Fabbrica 4.0, una collettività di agenti misti (umani e robotici) la cui flessibilità di allocazione di attività, comportamenti e compiti sarà molto elevata.

1.1. Scopi e vantaggi della Robotica nel paradigma Industry 4.0

Le nuove soluzioni robotiche permetteranno di rendere flessibili e più efficaci i sistemi di produzione, aumentando la competitività delle imprese manifatturiere che ne faranno uso. La flessibilità nella gestione di cella/sistema verrà perseguita grazie alla partecipazione diretta dell'uomo nel ciclo di lavorazione e controllo nei passi a più elevato valore aggiunto, eliminando i vincoli strutturali/tecnologici che erano soliti imporre un'alternativa tra sistemi automatici e sistemi manuali.

L'efficacia nella gestione di produzione sarà determinata da un accorciamento della filiera di programmazione attraverso soluzioni di intuitive programming, context recognition e dalla possibilità di rispondere in modo dinamico alle variazioni di condizioni.

La trasformazione da robot tradizionali (robot industriali) e di servizio in smart manufacturing robots permetterà anche di espandere le possibilità di ingresso in nuovi

mercati, grazie alla opportunità di automatizzare nuovi processi e sistemi di produzione o di incrementare la produttività del team uomo-robot.

La robotica all'interno del paradigma Industria 4.0 genererà anche impatti positivi in termini di valorizzazione dell'uomo all'interno delle fabbriche e di adeguatezza e accettabilità ergonomica – sia fisica che cognitiva - dell'ambiente di lavoro, andando incontro anche ad esigenze sociali emergenti. I “robot assistants” potranno infatti sgravare gli operatori dai compiti onerosi, rendendo le fabbriche più inclusive per i lavoratori di età avanzata e per le donne. Potranno inoltre valorizzare le capacità delle persone consentendo l'esecuzione di task a più alto valore aggiunto complessivo che combinano la precisione e performance dei robot con la capacità di azioni complesse e di adattamento a contesti variabili, tipiche degli operatori umani. Il tutto, in condizioni di sicurezza per le persone.

I vantaggi offerti dai sistemi robotici collaborativi saranno particolarmente rilevanti per l'industria italiana. Essa infatti è costituita per la maggior parte da piccole e medie imprese la cui capacità competitiva è basata sulla flessibilità e capacità di customizzazione, che consente loro di fornire soluzioni personalizzate sulla base delle esigenze dei clienti. Tali imprese necessitano di sistemi in grado di supportare in maniera efficiente produzioni su commessa, ad alto valore aggiunto e caratterizzate da notevole variabilità. Questi sistemi dovranno inoltre essere utilizzati in maniera semplice e intuitiva, per essere immediatamente alla portata del personale.

1.2. A che punto siamo

Le attività di ricerca e innovazione per lo sviluppo di soluzioni robotiche collaborative sono in corso da circa quindici anni in Europa e a livello globale. Esse hanno già portato alla disponibilità di alcune soluzioni di mercato fruibili dalle imprese, così come ampiamente mostrato durante AUTOMATICA1, la più grande fiera della robotica e dell'automatica svoltasi come ogni anno a fine Giugno a Monaco di Baviera in Germania.

I nuovi sistemi robotici in ottica 4.0 non rappresentano quindi una novità assoluta in termini di concezione. Tuttavia, le soluzioni attualmente a disposizione per le imprese presentano ancora dei limiti significativi rispetto alle potenzialità sopra illustrate.

Le attività di sviluppo si sono infatti principalmente focalizzate sugli aspetti di sicurezza degli operatori umani al fine di consentire ai lavoratori e ai robot di condividere lo spazio operativo senza che siano necessarie barriere. Questo molto spesso ha portato come risultato – sia in termini di ricerca che in termini di soluzioni commerciali effettivamente implementate a livello di shopfloor – a sistemi robotici indubbiamente sicuri nella collaborazione, ma non necessariamente collaborativi. Inoltre gli aspetti di produttività sono stati spesso trascurati e la collaborazione e la sicurezza sono rimasti aspetti abbastanza puntuali in grado di supportare la cooperazione con gli operatori solo in pochi

¹ <http://sparc-robotics.eu/automaticas-exhibitors-were-trumpeting-industry-4-0-is-this-the-turning-point-for-robotics/>; http://www.automatica-munich.com/en/Home/cn/about_the_fair/umcn/videos/overview; <https://www.youtube.com/user/AUTOMATICAmunich>

specifici task o in celle robotizzate confinate in spazi molto definiti e limitati a livello di shopfloor.

Questo approccio di fatto abbastanza limitante e rigido non è compatibile con la necessità di riorganizzare gli spazi produttivi e di rispondere ai cambiamenti della richiesta di capacità produttiva e della logistica all'interno della fabbrica. Infine, molti degli sviluppi nella interazione uomo-robot hanno mantenuto il focus sull'adattamento di robot industriali dalla struttura classica (bracci antropomorfi o altre configurazioni convenzionali dell'ambito industriale), mentre poca attenzione è stata dedicata allo sviluppo di nuovi concetti e nuove architetture robotiche che siano inerentemente sicure e collaborative (quali soluzioni caratterizzate da diverse configurazioni cinematiche – per esempio cinematica parallela, soluzioni “tendon driven”, esoscheletri indossabili, ecc.).

Attualmente i robot collaborativi sono inoltre stati principalmente pensati per l'esecuzione di task leggeri. I robot industriali ad oggi adattati all'esecuzione di task collaborativi “pesanti” rappresentano soluzioni sub-ottimali perché non sono altro che adattamenti esposti di robot industriali pensati per il massimo trasferimento della potenza e l'alloggiamento di un certo ammontare di equipaggiamenti ausiliari. Allo stesso tempo, però, i miglioramenti conseguiti a livello di strategie di controllo di forza/impedenza/ammettenza hanno dimostrato come sia possibile costruire un ampio spettro di dispositivi con i quali sia possibile per l'operatore co-manipolare carichi pesanti accrescendo la produttività ed espandendo così gli ambiti di penetrazione dell'automazione anche ad ambiti applicativi manifatturieri che ancora oggi si basano pesantemente sul lavoro umano.

Tali limiti tecnologici (focalizzazione su aspetti di sicurezza trascurando la produttività e su applicazioni “leggere”) sono particolarmente rilevanti nel contesto dell'industria manifatturiera italiana. Alla luce dei principali settori della manifattura nazionale, fortemente caratterizzata da processi “pesanti” quali ad esempio quelli della meccanica, nonché della prevalenza delle piccole e medie imprese che non possono prescindere dall'efficienza produttiva, infatti, le soluzioni attualmente a presentano significativi limiti da superare.

Dal punto di vista non strettamente tecnologico, le attività volte allo sviluppo di sistemi robotizzati collaborativi hanno portato negli ultimi anni ad evoluzioni anche in ambito normativo e regolamentativo. Malgrado tuttavia i robot collaborativi e le loro applicazioni industriali siano una delle frontiere più promettenti e interessanti in molti settori produttivi ad elevata manualità in cui destrezza, versatilità e limitatezza degli spazi disponibili sono fattori chiave per il conseguimento di elevati indici di prestazione, molta incertezza regna tutt'ora circa gli aspetti normativi inerenti la sicurezza. La cultura della sicurezza dei sistemi robotizzati gravita attorno alla norma di prodotto UNI EN ISO 10218-2:2012 (sistemi robotizzati) e alla norma di metodo UNI EN ISO 12100:2010 (risk assessment). Le modalità collaborative, sinteticamente valutate nella prima delle due norme citate, trovano un approfondimento nei requisiti di applicazione della specifica tecnica ISO/TS 15066, relativamente alle possibili combinazioni d'uso dei sistemi robotizzati. Un passaggio molto importante è stato recentemente segnato dalla nuova specifica tecnica ISO/TS 15066 sulla sicurezza dei robot collaborativi. Tale specifica consente di superare l'incertezza sull'utilizzo sicuro dei robot collaborativi in quanto precisa gli aspetti tecnici da tenere in considerazione durante la progettazione di una soluzione collaborativa e evidenzia le caratteristiche dei sistemi di comando da utilizzare nelle celle robotizzate (sicurezza funzionale). Tuttavia, solo l'ulteriore sviluppo di un corpus normativo adeguato consentirà ai robot di oggi di assistere da vicino l'uomo nelle sue operazioni determinando benefici

concreti, in termini di produttività e comfort.

Infine, occorre sottolineare che esistono a livello nazionale ottime competenze tecnologiche per la concezione, produzione e servizio di nuove piattaforme robotiche customizzate in ottica di Industria 4.0, sebbene alcune tra le più forti realtà del settore siano state acquisite da aziende asiatiche.

1.3. Verso la robotica di Industry 4.0

La concezione di sistemi ibridi robot-operatori dovrà nei prossimi anni estendersi oltre ai concetti di safety. Aspetti di ergonomia, produttività, adattabilità, accettabilità e simbiosi con l'utente dovranno essere considerati come un tutto nella concezione di nuove soluzioni per la collaborazione uomo-robot. Il focus deve pertanto essere esteso dal singolo utilizzatore e dalla collaborazione con il singolo robot alla pianificazione ed implementazione di ambienti robotizzati dove i robot e gli operatori lavorino effettivamente come componenti di uno stesso team all'interno di tutta la fabbrica. I robot devono accrescere in modo continuo le proprie capacità cognitive e quindi evolvere per dimostrare livelli crescenti di percezione, ragionamento e adattabilità. Solo in questo modo i robot potranno lavorare all'interno delle fabbriche in totale simbiosi con gli operatori, garantendo flussi di conoscenza bidirezionali e soprattutto operando come organismi completamente armonizzati con una base cognitiva olistica e condivisa.

Le attività di ricerca e sviluppo da implementare nel prossimo futuro devono pertanto affrontare i seguenti aspetti:

- Incrementare le capacità di carico dei robot collaborativi (oggi i pochi prodotti commerciali esistenti sufficientemente robusti da un punto di vista industriale hanno payload che va dai 300 gr ai 7-10 kg massimo) assicurando i livelli di sicurezza, ergonomia dei task e scalabilità della soluzione finale. Ciò impone lo sviluppo di nuovi gripper più avanzati e adattativi e ha come obiettivo il superamento di alcuni approcci convenzionali alla progettazione dei robot industriali. Molto importante sarà l'ibridazione con altri domini applicativi al fine di consentire l'efficace industrializzazione delle soluzioni più recenti sviluppate nell'ambito della mecatronica e della robotica di servizio (per esempio soluzioni di wearable robotics pensate per ambito medicale o militare o più in generale security).
- Rendere possibile l'effettiva mobilità dei robot a livello di shop floor pensando a soluzioni robotizzate montate su piattaforme mobili capaci non solo di navigare all'interno dei siti produttivi ma anche di posizionarsi in modo molto accurato per consentire l'esecuzione finale del task.

- Sviluppare nuove tecnologie di intelligenza artificiale e machine/deep learning che rendano i robot capaci di processare big-data (massive moli di dati e informazioni) durante l'interazione con gli operatori e di reagire in tempo reale. L'interazione durante l'esecuzione di un processo richiede infatti nuovi livelli di autonomia, navigazione, percezione cognitiva e manipolazione (per esempio predizione dei movimenti dell'operatore, caratterizzazione dinamica dei processi e delle capacità dell'operatore, apprendimento dall'operatore).
- Sviluppare o utilizzare standard relativi agli strumenti di programmazione, modellazione e simulazione, ai protocolli di comunicazione e alle interfacce. Non è infatti immaginabile che l'obiettivo di produttività e configurabilità non sia raggiunto tramite lo sviluppo di elementi in grado di rendere trasparenti e intuitive le capacità dei sistemi robotizzati, soprattutto se questi ultimi dovranno operare in ottica service-oriented.
- Introdurre innovazioni a livello di componente, sensore, robot e sistema di produzione in grado di incrementare le capacità cognitive, elaborative e di attuazione autonoma ed indipendente, in modo da implementare in maniera semplice ed economicamente sostenibile comportamenti evolutivi e adattativi garantendo la compatibilità con il parco robot installato. E quindi: sviluppo di nuovi metodi di progettazione per sensori embedded; sviluppo e integrazione di sensori in grado di operare come sistemi autonomi distribuiti per l'acquisizione di dati inerenti il contesto, il robot e il processo produttivo; sviluppo di gateway universali intelligenti – basati per esempio su paradigmi open source e vendor neutral – per l'interfacciamento a reti di sensori sia a livello di robot che a livello di sistema di produzione; sviluppo di metodi e strumenti basati su logiche di “Data Fusion”, “Machine Learning” “Deep Learning” e Intelligenza Artificiale per la raccolta ed elaborazione anche centralizzata dei dati; sviluppo di metodologie e attuatori per l'implementazione di comportamenti adattativi ed evolutivi a livello di componente/robot; integrazione a livello di robot e processo di tecniche di monitoraggio “in-process” per il controllo in anello chiuso della qualità del semilavorato/prodotto finito e per l'implementazione di logiche di autodiagnostica e manutenzione predittiva; sviluppo di strumenti basati su HMI innovative e realtà aumentata in grado di semplificare l'intervento correttivo da parte dell'operatore.

Il sistema italiano possiede competenze e risorse eccellenti per affrontare tali sfide, essendo presente nel nostro paese un validissimo comparto di fornitori di tecnologie, integratori di sistema e istituti di ricerca e innovazione. Sarà fondamentale orientare tale eco-sistema di innovazione verso lo sviluppo coerente di soluzioni orientate alle necessità delle PMI italiane.

2. La Fabbrica Digitale

Il concetto di Fabbrica Digitale (o Fabbrica Virtuale o Manifattura Digitale) consiste nella mappatura dei processi tecnici e di business nel mondo digitale per fornire un supporto avanzato alle decisioni relative alla progettazione di prodotto, processo e sistema, programmazione e controllo della produzione nel mondo reale, sfruttando tecnologie ICT quali ad esempio la realtà virtuale o aumentata, la simulazione, l'ottimizzazione, ecc.

La Fabbrica Digitale sarà disponibile agli utenti (manager, progettisti e operatori) attraverso un insieme eterogeneo di strumenti software che spaziano dal CAD/CAM al PLM (Product Life-cycle Management), dalla simulazione a eventi discreti alla simulazione cinematica, dalla realtà virtuale alla realtà aumentata, da sistemi ERP (Enterprise Resource Planning) a strumenti di schedulazione e supervisione. Pur essendo eterogenei fra di loro, gli strumenti software della Fabbrica Digitale potranno interagire fra di loro grazie alla presenza sottostante di un modello di fabbrica complessivo e coerente, che guiderà gli utenti nella fruizione delle funzionalità della Fabbrica Digitale. Ogni strumento software potrà interagire con il modello di fabbrica operando su una particolare vista del modello stesso (ad esempio, una vista logica nel caso di simulazione a eventi discreti, una vista fisica e geometrica per applicazioni di realtà virtuale, una vista chimica/fisica/cinematica per simulazioni di processo, ecc.). L'interoperabilità fra gli strumenti sarà abilitata dall'uso di standard sia per la modellazione dell'informazione che per quanto riguarda i protocolli di comunicazione e le modalità di scambio dati.

La Fabbrica Digitale potrà sfruttare la connettività avanzata ai bassi livelli di fabbrica per l'acquisizione di dati su macchine, stati dell'ordine, garanzie, tempi personali, guasti e così via. I sistemi di acquisizione dei dati della fabbrica (che attualmente fanno parte dei sistemi MES - Manufacturing Execution Systems) saranno messi direttamente a disposizione dei più alti livelli aziendali e renderanno possibile la gestione intelligente dei dati e funzionalità analitiche e computazionali mediante il costante aggiornamento e manutenzione della rappresentazione digitale della fabbrica. Per raggiungere queste funzionalità, i nuovi sistemi di produzione basati su Industria 4.0 andranno a rivedere la tradizionale struttura della piramide di automazione (sensori/attuatori, PLC, SCADA, MES, ERP).

Il Modello di Fabbrica sarà sfruttato non solo in fase di progettazione, ma anche nella fase operativa della fabbrica. Ciò richiederà di garantire la continuità digitale fra la fabbrica reale e la sua rappresentazione virtuale, mantenendo la coerenza fra dati di varia origine (es. piani di produzione, monitoraggio, previsioni di domanda, ecc.) che concorrono a definire l'evoluzione nel tempo del sistema produttivo.

La fruibilità e riusabilità degli strumenti software della Fabbrica Digitale potrà essere incrementato mediante l'introduzione di architetture orientate ai servizi (SOA - Service Oriented Architecture), cioè architetture tipicamente basate sul web in cui gli applicativi sono messi a disposizione degli utenti come servizi/funzioni all'interno di una piattaforma con accesso remoto. Le recenti potenzialità offerte dalle tecnologie di Cloud Computing potranno ulteriormente enfatizzare i benefici derivanti da un approccio SOA, consentendo di allocare su cloud le operazioni che richiedono alti carichi computazionali facendo uso di computer ad alte prestazioni (HPC - High Performance Computing).

2.1 Scopi e vantaggi della Fabbrica Digitale

La possibilità di sincronizzare la fabbrica reale e la fabbrica digitale permetterà di sfruttare maggiormente le funzionalità di strumenti software, in parte già esistenti, per realizzare attività aziendali come:

- validazione fuori linea, analisi di sensitività della programmazione della produzione rispetto a possibili incertezze;
- identificazione di anomalie in linea, scostamenti dai piani di produzione eseguendo simulazioni a breve termine;
- gestione della manutenzione programmando i servizi, gestendo gli ordini e le richieste, tracciando le spese di manutenzione, controllando l'inventario, gestendo i flussi di lavoro, prevedendo la possibile manutenzione. Effetti positivi saranno anche la riduzione del numero di parti di ricambio a magazzino e del tempo di risposta per le attività di manutenzione;
- monitoraggio dei processi di miglioramento attraverso il confronto nominale-effettivo;
- valutazione in linea di quali possono essere le migliori azioni di gestione della produzione e della manutenzione al sopraggiungere di eventi esterni.

In ambito di progettazione di prodotto e processi di lavorazione, l'integrazione di diversi strumenti software già esistenti consentirà di effettuare in modo congiunto la progettazione di un processo e la validazione virtuale della sua esecuzione in macchina considerando il percorso degli utensili, gli ingombri delle attrezzature e dei componenti delle macchine utensili, identificando anche eventuali collisioni. Infatti, se la progettazione di prodotto e dei processi di lavorazione si basa sempre più sul supporto di strumenti software CAD (computer-aided design) e CAM (computer-aided manufacturing), il collegamento fra la fase di progettazione di prodotto e la pianificazione di processo è ancora debole a causa della difficoltà nel confrontare i requisiti di processo con le capacità messe a disposizione dalle risorse produttive e dai sistemi di gestione della produzione. Per questo motivo è ancora scarsa la disponibilità di soluzioni software per la generazione automatica di piani di processo (CAPP - Computer Aided Process Planning). Nel caso di risorse produttive a controllo numerico (NC), il collegamento fra CAD, CAM e questioni relative a NC dovrà mirare all'integrazione delle informazioni di prodotto e processo con informazioni cinematiche e funzionali delle risorse produttive. La possibilità di svolgere velocemente la fase di validazione renderà possibile la valutazione di un numero maggiore di opzioni di processo, ottimizzando i vari obiettivi fissati dall'utente (ad esempio la minimizzazione del consumo energetico).

La progettazione di prodotti e sistemi, ma anche la gestione e la valorizzazione delle persone che operano in fabbrica, potranno sfruttare le nuove potenzialità offerte dalle tecnologie di Realtà Virtuale (VR) e Realtà Aumentata (AR). Tali tecnologie potranno essere tanto più efficaci quanto più le relative applicazioni saranno in grado di basarsi su un modello di fabbrica condiviso.

Nel caso della VR, si possono identificare le seguenti applicazioni:

- progettazione del layout di impianti/sistemi di produzione in ambiente 3D immersivo e collaborativo. Se il modello di fabbrica usato per la visualizzazione viene costantemente aggiornato e arricchito, allora diventa anche possibile integrare la progettazione di layout con la valutazione delle prestazioni del sistema produttivo (es. volumi produttivi, qualità della produzione, costi, utilizzazione delle risorse, livello medio dei magazzini, ecc.). La valutazione delle prestazioni può essere eseguita ad esempio mediante simulazione ad eventi discreti o metodi analitici (figura 1);

Figura 1. La valutazione delle prestazioni eseguita mediante simulazione



- addestramento degli operatori in un ambiente realistico per velocizzarne l'apprendimento e migliorarne l'efficacia, senza che sia necessario impiegare sistemi reali che potrebbero porre problemi di sicurezza, di costo, o di disponibilità per la produzione;
- riduzione dei tempi di produzione e consumo di materiale grazie ad analisi basate su virtual mock-up svolte durante la progettazione di prodotto.

Le tecnologie AR possono invece essere impiegate, ad esempio, per:

- fornire informazioni utili all'assemblaggio di prodotto in una linea. In questi casi si possono usare dispositivi video portatili che aiutano l'operatore identificando le zone e i componenti coinvolti nell'operazione. Tali funzionalità diventano ancor più rilevanti nel caso di prodotti estremamente complessi oppure in presenza di una alta varietà di prodotti che vengono realizzati nello stesso sistema di produzione;
- guidare le operazioni di manutenzione di componenti o risorse produttive senza che sia necessario l'intervento fisico di operatori altamente specializzati,

eventualmente fornendo assistenza remota;

- identificare codici prodotto all'interno di magazzini di grandi dimensioni.

Grazie all'integrazione multi-livello delle informazioni relative al ciclo di vita dei prodotti e della fabbrica, delle risorse fisiche, software e umane e all'allineamento tra il modello reale e quello virtuale, le tecnologie per la Fabbrica Digitale consentiranno di migliorare l'efficienza e l'efficacia complessiva delle fabbriche, riducendo i costi complessivi di progettazione e gestione, nonché i lead time associati. Esse contribuiranno inoltre a incrementare la flessibilità delle fabbriche rispetto all'evoluzione del contesto e alla riduzione del ciclo di vita dei prodotti, grazie alla maggiore integrazione dei sistemi di progettazione e gestione, nonché alla possibilità di anticipare i cambiamenti e di simulare in anticipo le migliori strategie di adattamento.

Infine, la Fabbrica Digitale consentirà una maggiore valorizzazione delle persone, che potranno dedicarsi alle attività a più alto valore aggiunto e che avranno a disposizione una maggior quantità di informazioni e di strumenti di supporto per svolgere con maggiore efficacia i propri compiti in un ambiente più inclusivo e motivante.

2.2. A che punto siamo

Le imprese hanno già a disposizione da diversi anni soluzioni di mercato volte a supportare i processi di progettazione e gestione delle fabbriche in ottica 4.0, tra cui:

- soluzioni di simulazione a eventi discreti e simulazione continua/di processo. Esse abilitano la generazione di modelli digitali consentono la sperimentazione e l'esame di possibili scenari senza creare disturbi ai sistemi di produzione reali o, quando utilizzati in fase di progettazione, molto prima che i sistemi di produzione reali siano installati. Alcuni linguaggi di modellazione consentono anche di definire diverse regole per il flusso di materiali e di controllare il loro effetto sulle prestazioni;
- soluzioni digitali per la progettazione e rappresentazione 3D del processo manifatturiero che, basandosi su librerie di processi, permettono la collaborazione in gruppi di lavoro per confrontare alternative al fine di sviluppare e selezionare le strategie ideali di processo che incontrano i requisiti aziendali. L'obiettivo è di ridurre gli sforzi e la durata della creazione del progetto ideale, migliorandone la qualità e la standardizzazione, riducendo anche i costi relativi alle riconfigurazioni. Oltre che per la progettazione, tali soluzioni possono essere sfruttate anche per validare i processi manifatturieri. In questo modo si può simulare il comportamento di robot singoli e linee complete per mostrare eventuali problemi prima di costruire la linea. Inoltre è possibile caricare e scaricare dei programmi reali per la programmazione off-line.

- Soluzioni di “Product Life-cycle Management” (PLM), pacchetti software eterogenei il cui obiettivo è gestire tutte le informazioni del ciclo di vita dei prodotti e processi, dalla progettazione, alla produzione, fino all’End-Of-Life.

A causa della complessità del contesto manifatturiero, tuttavia, tali strumenti software sono tradizionalmente progettati per affrontare specifiche attività, spesso legate a limitate aree di prodotto, processo e sistemi di produzioni. Inoltre, essi risultano spesso di difficile integrazione a causa della mancanza di un'intesa comune tra attori e strumenti software che si occupano del rapporto tra prodotto e processo all'interno del sistema di produzione e durante la fase di progettazione. Questa mancanza colpisce, quindi sia la fase di progettazione che la fase di monitoraggio. Un ostacolo rilevante è rappresentato dalla difficoltà nel mappare le strutture dati di sistemi MES e sistemi ERP (Enterprise Resource Planning). Il supporto alle decisioni manifatturiere non può quindi essere ottimale, in quanto chi deve attuare una strategia non può accedere alle informazioni necessarie in modo strutturato e integrato, principalmente a causa di mancanza di interoperabilità tra i diversi strumenti. Infatti, anche i pacchetti software PLM integrati difficilmente sono in grado di soddisfare i requisiti di catturare, rappresentare e scambiare una ampia varietà di dati lungo tutte le fasi del ciclo di vita di prodotti/fabbriche, non garantendo il riuso della conoscenza con sufficiente facilità ed efficacia. Inoltre, i grandi pacchetti software PLM commerciali sono caratterizzati da eccessive funzionalità e complessità rispetto ai fabbisogni e richiedono ingenti costi di acquisto, formazione e gestione.

A supporto dell’interoperabilità dei sistemi e dell’integrazione di dati provenienti dai diversi domini di conoscenza, una importante attività di standardizzazione è già stata avviata ed ha recentemente portato allo sviluppo di nuovi standard (si citano qui “AutomationML - Automation Markup Language”, “OPC-UA - OPC Unified Architecture”, “STEP - ISO 10303 Standard for the Exchange of Product Model Data”, “PSL - ISO 18629 Process Specification Language”, “ISA-95” PER lo sviluppo di una interfaccia automatizzata tra i sistemi aziendali e i sistemi di controllo, “STEP-NC ISO 14649 Data model for computerized Numerical Controllers”, “STEP ISO 10303” per la geometria del prodotto, le dimensioni geometriche, le tolleranze e l’informazione sulla gestione dei dati relativi al prodotto, “IFC - Industry Foundation Classes”). Sono inoltre attivi per lo sviluppo di nuovi standard i comitati tecnici “IEC/TC 65 Industrial process, measurement, control and automation” (in cui è presente un gruppo di lavoro incentrato proprio sul tema della Fabbrica Digitale con lo scopo di contribuire alla famiglia di norme IEC 62832) e “ISO/TC 184 “Automation Systems and Integration”. Tuttavia, la partecipazione italiana in tali comitati tecnici è limitata e si riduce soprattutto ad iniziative personali con uno scasso supporto istituzionale. Ciò preclude il coinvolgimento di esperti con qualifica adeguata e possibilità di incidere.

Tali limiti costituiscono una barriera per l’implementazione della Fabbrica Digitale soprattutto per le PMI, che non sono in grado di acquisire soluzioni così onerose. Esse, oltre a richiedere ingenti investimenti, rischiano di ingessare le imprese all’interno di logiche rigide e lente che mal si coniugano con la necessità di dinamicità e flessibilità tipica delle produzioni customizzate delle imprese italiane cui il concetto di Fabbrica Digitale potrebbe andare incontro.

2.3. La strada verso la Fabbrica Digitale

La principale sfida per l'implementazione della Fabbrica Digitale consiste nell'innovativa integrazione di strumenti e metodologie all'interno di una piattaforma software comune che garantisca la modellazione della fabbrica nella sua interezza e complessità e che consenta lo scambio di informazioni tra attori e applicazioni coinvolte in compiti diversi durante le varie fasi del ciclo di vita della fabbrica. Le tecnologie della Fabbrica Digitale dovrebbero andare verso la democratizzazione degli approcci di analisi e simulazione, riducendo il costo totale per la realizzazione e aggiornamento della rappresentazione virtuale della fabbrica. In particolare sarà necessario sviluppare soluzioni ai seguenti problemi:

- gestione di informazioni eterogenee relative alla produzione, gestione e alla fase esecutiva di prodotti, processi e sistemi di produzione all'interno di un modello concettuale coerente ed aggiornato;
- integrazione ed armonizzazione della conoscenza ed informazione proveniente da vari strumenti e tecniche che fanno riferimento a diverse discipline e diversi livelli di dettaglio;
- riduzione dei costi di investimento ed operativi rispetto ai costi attuali dei grandi pacchetti commerciali;
- manutenzione della rappresentazione digitale/virtuale dei sistemi di produzione in modo che siano costantemente sincronizzati con i corrispettivi reali;
- estensione delle funzionalità degli strumenti software per permettere ai tecnici e agli ingegneri di sfruttare la simulazione e virtualizzazione dei processi senza che sia necessario affidarsi a specialisti con competenze dedicate, problema che diventa ancor più rilevante nel caso di PMI, di cui è ricco il contesto italiano. Ad esempio, la possibilità di generare/aggiornare modelli di simulazione in modo automatico (o semi-automatico) rappresenta ancora una delle principali sfide nell'ambito della simulazione dei sistemi di produzione.

Una efficace piattaforma per la Fabbrica Digitale che supporti l'interoperabilità fra gli strumenti software deve fornire soluzioni tecnologiche che garantiscano:

- un modello di dati comune che formalizzi le informazioni in un modo che possa essere compreso dai diversi attori e strumenti coinvolti nel processo descritto. Il modello di dati richiede l'organizzazione e l'armonizzazione delle proprietà geometriche, fisiche e tecnologiche della fabbrica. Il modello di dati dovrebbe essere olistico, flessibile, estendibile, scalabile, in modo da integrare

diversi domini di conoscenza e le norme relative alla costruzione, prodotto, processo, risorse e al sistema di produzione. Alcuni requisiti di base che devono essere soddisfatti: (1) rappresentazione dei concetti di fabbrica relativi a sistemi di produzione, risorse, processi, prodotti, edifici, servizi d'impianto, ecc.; (2) uso di standard esistenti; (3) rappresentazione semantica dei dati; (4) il modello di dati dovrà essere il più completo possibile, ma anche facilmente estendibile.

- un sistema di gestione dei dati che sia condiviso e accessibile dai vari strumenti digitali per procurare dati di input e contribuire con i dati di output generati. Il sistema di gestione dati dovrebbe garantire accesso remoto e garantire la consistenza dei dati grazie a meccanismi di versionamento e locking. Si può prevedere l'uso di tecnologie tradizionali come database relazionali, oppure soluzioni più recenti come database NoSQL, database a oggetti, database basati su grafi, soluzioni miste.
- Un middleware software che permetta di accedere ai dati condivisi in modo sicuro e consenta la conversione input/output dei dati nel rispetto del modello di dati condiviso. Un middleware appropriato può essere impiegato dai vari strumenti software se questi offrono la possibilità di accesso e modifica delle strutture dati interne (ad esempio attraverso API, application programming interface) e se risulta possibile mappare le classi e proprietà fra il modello di dati comune e le strutture dati interne.

Sul fronte della standardizzazione, occorre maggiore collaborazione fra i vari attori coinvolti, cioè aziende di ogni dimensione, comitati tecnici, università ed istituti di ricerca, ministeri. Senza azioni di coordinamento che portano a soluzioni basate sul consenso, si potranno sviluppare solo delle soluzioni Industria 4.0 isolate. Ad esempio, in Germania è stato costituito il gruppo di lavoro "Standardization Roadmap" partendo da una iniziativa congiunta di DIN e DKE per sviluppare una prima versione della roadmap di standardizzazione per Industry 4.0. Questo gruppo ha fra i principali obiettivi quello di creare canali di comunicazione fra i comitati di standardizzazione, l'industria, le associazioni, gli istituti di ricerca e i ministeri. Si può auspicare che iniziative simili vengano fatte partire anche a livello nazionale e regionale in Italia in modo da poter giocare un ruolo attivo e rilevante per la standardizzazione internazionale, tenendo in considerazione anche le peculiarità del mondo manifatturiero italiano e permettendo anche a piccole e medie aziende di accedere e partecipare alle decisioni, almeno per via indiretta.

Infine, è di importanza strategica garantire la presenza e il mantenimento di opportune competenze tecnico-scientifiche nel territorio italiano, con conseguenti benefici anche in termini di bilancia commerciale. Infatti non va dimenticato che gran parte degli strumenti hardware e software che attualmente concorrono alla realizzazione di Industria 4.0 sono attualmente di importazione estera. In Italia non sono infatti presenti grandi operatori nel mercato di software a supporto della fabbrica digitale, ma esistono realtà medio-piccole che potrebbero accompagnare nella transizione le aziende manifatturiere medio-piccole, che non sarebbero quindi costrette ad acquistare intere suite software caratterizzate da alti costi di investimento e gestione. Si può pertanto prevedere il potenziale sviluppo del settore di fornitori di soluzioni I4.0 per le PMI, andando a coprire una fetta di mercato che le grandi aziende software non sono in grado di penetrare.

3. Controllo e supervisione avanzati del processo produttivo

La visione di lungo termine promossa da Industria 4.0 prevede sistemi di automazione “auto-organizzati”, composti da prodotti e risorse produttive intelligenti ed autonomi che interagiscono all’interno di architetture decentralizzate. Lo scenario odierno di automazione, basato tradizionalmente su logiche di controllo precostituite implementate dal programmatore all’interno delle singole unità di esecuzione (e.g.: PLC- controllori a logica programmabile), lascerà quindi il passo a quello in cui sistemi autonomi sono in grado di identificare dinamicamente la strategia ottimale di controllo del sistema produttivo, massimizzandone le performance in ciascuna condizione operativa.

A tale scopo, si utilizzeranno architetture basate sul paradigma di auto-orchestrazione dei servizi. Ciò significa che, ad esempio, ciascuna risorsa (macchinario, tool, ecc.) offrirà servizi (quali fresatura, foratura, assemblaggio, ecc.) che il singolo prodotto customizzato potrà “acquistare” nello shop-floor secondo uno schema cooperativo ad agenti indipendenti. Di conseguenza, prodotti e macchine intelligenti saranno in grado di collaborare e decidere autonomamente quali azioni intraprendere al fine di raggiungere gli obiettivi produttivi, ad esempio allocando dinamicamente i prodotti sui macchinari in base alla capacità utilizzabile, alla disponibilità o al costo delle macchine, identificando quale risorsa utilizzare e quando procedere con la fase produttiva successiva, definendo in tempo reale le attività.

Decentralizzazione, autonomia e negoziazione automatizzata dei servizi costituiranno quindi pilastri fondamentali dei sistemi di automazione e controllo per garantire flessibilità, robustezza, efficienza produttiva ed ottimizzazione dei consumi energetici. Per superare i limiti delle odierne tecniche di controllo, basate su regole predeterminate e codificate dal progettista del sistema di automazione, che si dimostrano inefficaci nella gestione di processi industriali caratterizzati da variabilità o articolati su molteplici unità produttive, si impiegheranno tecniche di controllo avanzato di tipo “model-based”. Grazie alla modellazione del sistema produttivo, che caratterizza in termini digitali dinamiche e vincoli dello stesso, tali tecniche sono in grado di simulare il comportamento del sistema e di calcolare in ciascun istante il comando “ottimale” da impartire ad ogni dispositivo controllato, secondo una strategia intesa a minimizzare globalmente una funzione obiettivo (massimizzazione della produzione, minimizzazione dei costi o dei tempi, ecc.). A tale scopo, verranno utilizzati specifici strumenti di calcolo, in grado di trovare la soluzione del complesso problema di ottimizzazione mediante tecniche sviluppate in contesti come la programmazione matematica o l’intelligenza artificiale. Inoltre, al fine di compensare disturbi o deviazioni dovute a fattori contingenti o comunque non sufficientemente predicibili, l’azione di controllo ed ottimizzazione verrà applicata iterativamente e con continuità nel tempo, ricalcolando automaticamente la migliore re-azione di compensazione.

Tali approcci consentiranno di coniugare obiettivi di ottimizzazione che considerano da un lato il raggiungimento e mantenimento del set-point produttivo (ad esempio il tempo ciclo), dall'altro la minimizzazione del consumo di risorse produttive del processo. Essi consentiranno di inoltre di variare dinamicamente l'azione di controllo desiderata a seconda delle mutate esigenze di produzione.

3.1. Scopi e vantaggi dei sistemi di controllo e supervisione avanzata nel paradigma Industry 4.0

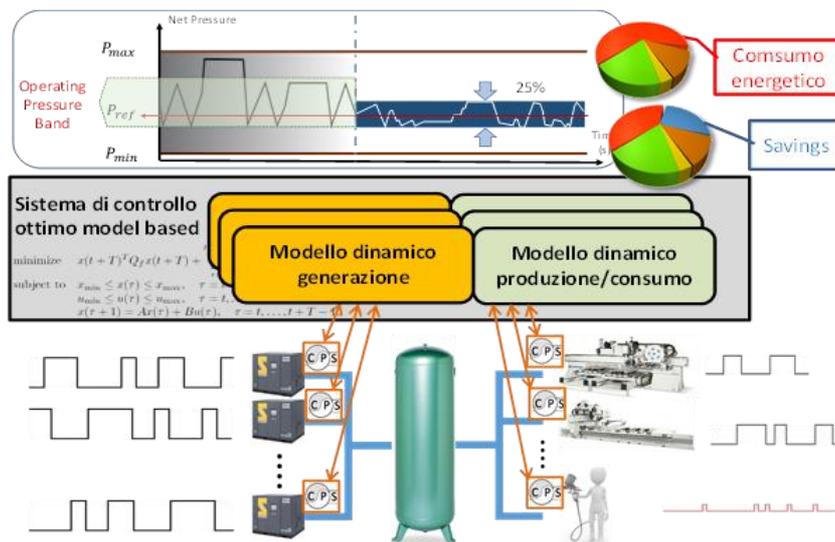
Tecniche di controllo avanzato model-based hanno trovato in passato diffusione primariamente negli ambiti dell'industria di processo (in particolare Oil&Gas), sia per la natura specifica di tali sistemi caratterizzati da comportamento continuo e dinamiche lente, sia per la dimensione economica del settore, in grado di supportare la complessa attività di ingegnerizzazione del modello.

Grazie alle opportunità offerte dalle tecnologie Industria 4.0 che permettono di coniugare modelli dinamici del processo in grado di auto-aggiornarsi (secondo paradigmi CPS -based) con una maggiore potenza di calcolo distribuita a basso costo, risulta oggi possibile l'adozione di tali tecniche di controllo avanzato anche negli ambiti tipici dell'industria manifatturiera, ancor più complessi e sfidanti in quanto caratterizzati da sistemi produttivi ibridi ove processi di natura continua e discreta, coesistono.

Le possibili applicazioni sono molteplici e possono indirizzare le soluzioni di automazione ed ottimizzazione avanzate dal livello macchina/cella, linea/impianto, fino al livello dell'intero sistema produttivo, beneficiando in tutti i casi dei vantaggi derivati dall'uso avanzato dell'informazione digitale in tempo reale del processo.

A titolo esemplificativo, si riporta un primo esempio di possibile applicazione che coniuga aspetti di controllo della produzione e di minimizzazione del consumo di risorse, basato su tecniche model-based e sul bilanciamento automatico della domanda ed offerta.

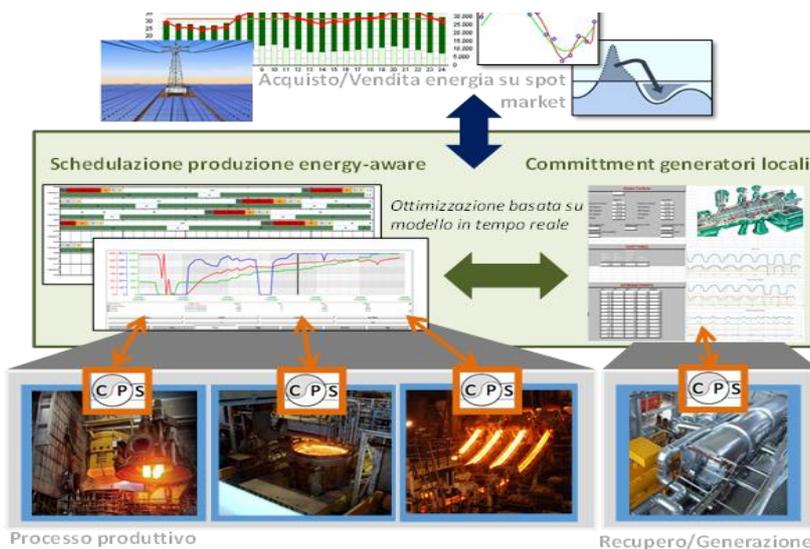
Figura 2. Applicazione di controllo ed automazione innovativa



Si consideri un processo produttivo costituito da macchinari che, a seconda della specifica condizione operativa, consumano una certa quantità di risorse produttive (quali ad esempio l'aria compressa, l'energia termica sotto forma di vapore, elettricità, ecc.). Disponendo del modello dinamico di ciascun macchinario e del modello del sistema di generazione (ad esempio dei compressori e mappatura impianto di distribuzione), risulterebbe possibile sviluppare nuove soluzioni di controllo che ad oggi non sono disponibili. Il sistema di controllo model-based sarebbe infatti in grado a calcolare la strategia di allocazione ottimale dell'impianto di generazione per soddisfare puntualmente la domanda effettiva, considerando nel contempo le specifiche condizioni di ciascuna unità, sia in termini di stato che di efficienza. In questo modo sarebbe possibile ridurre notevolmente le tipiche oscillazioni di prestazioni ottenute mediante i sistemi di controllo tradizionali, basati su regole predeterminate in risposta alla domanda misurata sui punti di utilizzo, determinando inoltre una sostanziale riduzione del consumo energetico e dei relativi costi (in ragione del 30-35% per sistemi medio grandi).

L'approccio di ottimizzazione model-based può essere identicamente scalato ed adottato per la gestione di processi caratterizzati da elevati consumi di energia (ad esempio, processi chimici, metallurgici, produzione di cemento, Consumer Packaged Goods-CPG, etc.) anche in relazione alle recenti evoluzioni della fornitura elettrica in chiave smart grid e di mercato libero dell'energia (spot market).

Figura 3. Applicazione di controllo ed automazione innovativa



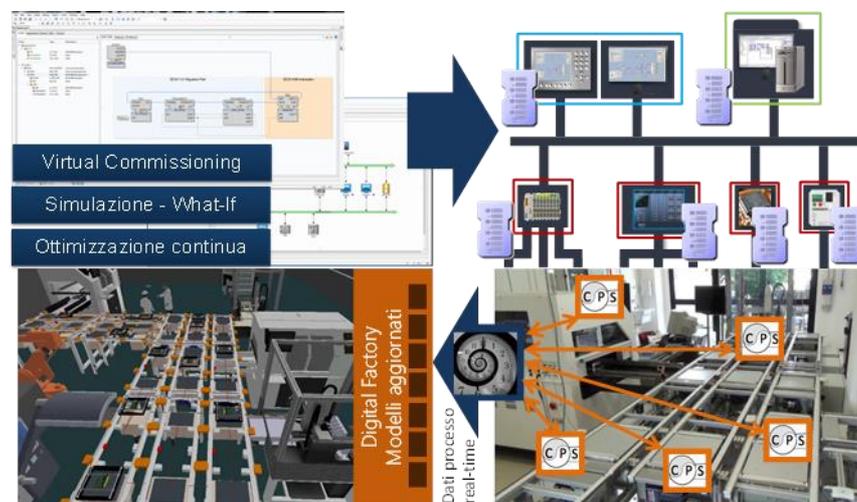
Sarebbe ad esempio possibile realizzare sistemi di schedulazione della produzione in tempo reale -a livello di sistema MES (Manufacturing Execution System)- in grado di considerare il profilo di costo dell'energia e le capacità di generazione locali basate ad esempio su cogenerazione e recupero energetico. L'obiettivo da raggiungere può comprendere l'inseguimento del prezzo su mercato energetico, il controllo dei picchi di potenza su contratti di fornitura di tipo base-load o misti, il tutto considerando vincoli di demand/response nonché l'opportunità di vendita dell'energia in condizioni di riduzione della domanda interna. Tale opportunità può essere colta sfruttando la flessibilità del sistema dovuta alle caratteristiche del processo o alla fluttuazione della domanda da parte dei clienti, grazie alla adozione delle tecnologie abilitanti Industry 4.0.

Un'altra esemplificazione delle potenzialità dei sistemi di supervisione e controllo in ottica Industry 4.0 riguarda l'estensione delle piattaforme di virtual commissioning all'interno di

sistemi a supporto della ottimizzazione continua. Le piattaforme di virtual commissioning vengono utilizzate ad oggi per lo sviluppo e validazione del sistema di automazione in fase di progetto, collegando il sistema di automazione con un ambiente di simulazione del macchinario/processo. Grazie all'integrazione degli ambienti di simulazione con il processo fisico, all'incremento di sensorizzazione di ciascun macchinario ed alla capacità di elaborazione locale dei dati, è possibile costruire un modello dinamico aggiornato in tempo reale allo stato del sistema fisico, oltrepassando la barriera della discrepanza tra il comportamento del processo reale e di quello virtuale.

Il modello di simulazione sarà quindi in grado di rappresentare fedelmente il processo fisico in tempo-reale durante tutto il suo ciclo di vita. Grazie a tale piattaforma di nuova generazione, risulterebbe possibile effettuare simulazioni ed analisi altamente affidabili dell'impatto di strategie e layout produttivi diversi sull'intero sistema reale controllato, connettendo il sistema di automazione distribuito in anello chiuso con il processo modellato nell'ambiente digitale aggiornato.

Figura 4. Applicazione di controllo ed automazione innovativa



Riconfigurazioni di sistema o variazioni di strategia produttiva possono quindi essere valutate ed ottimizzate confortevolmente ed in tutta sicurezza nell'ambiente digitale prima della implementazione nello shop-floor. I conseguenti adattamenti del sistema di automazione possono essere validati prima del download della soluzione di controllo sui target distribuiti nell'impianto, minimizzando in tal modo i fermi macchina/impianto in fase di ramp-up ed i successivi blocchi/inefficienze post commissioning dovuti a flussi operativi non correttamente identificati e gestiti. In aggiunta a ciò, grazie alla possibilità di velocizzare il tempo simulato, è possibile analizzare scenari di lungo termine in pochi secondi in risposta ad evoluzioni di processo o prodotto.

Gli esempi riportati nelle figure 2, 3 e 4 rappresentano solo alcune tra le molteplici possibili applicazioni di controllo ed automazione innovative indirizzabili nel contesto Industria 4.0, mostrano come i vantaggi di tali soluzioni consistono nell'aumento dell'efficienza produttiva, nella riduzione del lead time, del consumo di materiali e di energia, nonché nell'aumento della flessibilità produttiva nel caso di necessità di adattamento ad una domanda variabile. Tali vantaggi saranno particolarmente importanti per l'industria italiana, per la maggior parte composta da PMI, che necessita di soluzioni di automazione dinamiche e flessibili per produrre efficientemente manufatti customizzati ad lato valore aggiunto.

3.2. A che punto siamo

L'evoluzione verso i sistemi di automazione e controllo sopra descritti è già in corso da diversi anni e non rappresenta una novità assoluta nel settore manifatturiero e tra gli attori di ricerca e innovazione industriale. Le logiche di automazione rigide, gerarchiche e centralizzate, basate su algoritmi di controllo pre-determinati, stanno infatti già lasciando il passo a sistemi modulari distribuiti, in grado di supportare dinamicamente la rapida integrazione di nuove funzionalità e l'adattamento del sistema alla variazione dei requisiti. Si sta in particolare già osservando una forte tendenza verso la sempre maggiore sensorizzazione dei processi che, in alcuni casi, abbraccia anche l'adozione di architetture distribuite e l'implementazione di sistemi di controllo basati su modelli elaborati a partire dalle informazioni raccolte in tempo-reale dai sensori. Un consistente numero di nuove tecnologie di automazione abilitanti il paradigma Industria 4.0 è infatti apparso recentemente sul mercato e nei prossimi anni è prevista un'ulteriore forte diffusione degli stessi, supportata dalla disponibilità di sistemi industriali basati su Internet of Things (IoT) e da soluzioni "embedded" con crescente potenza di calcolo a basso costo.

Ciononostante, a causa dell'attuale assenza sul mercato di sistemi di automazione in grado di supportare gli utenti con appropriate funzionalità di implementazione e gestione di controlli distribuiti model-based in chiave Industria 4.0, tali applicazioni risultano attualmente fortemente verticalizzate su applicazioni specifiche in progetti dedicati. Infatti, stante l'assenza di tali strumenti all'interno delle soluzioni di mercato, la realizzazione di sistemi di automazione di questo tipo richiede oggi lo sviluppo di strumenti software ad-hoc, con conseguente sforzo elevato di codificazione, implementazione e validazione, nonché scarsa trasferibilità ed interoperabilità. Esse sono quindi difficilmente estendibili ad altri applicazioni, processi e settori industriali rispetto a quelli per cui sono concepite, soprattutto considerando le capacità e le risorse a disposizione delle PMI. Si può dunque affermare che le imprese si trovano attualmente nella possibilità tecnologica di raccogliere un numero di dati ed informazioni dei propri processi molto più vasto di quello che hanno gestito nel passato, ma che non hanno dall'altra parte a disposizione su larga scala i modelli e le tecnologie per trarre vantaggio da tale mole di informazioni al fine di cogliere effettivamente i vantaggi di cui sopra. Ovviamente, la sensorizzazione dei processi è una condizione necessaria e preliminare all'implementazione dei sistemi di automazione e controllo di nuova generazione che tutte le imprese dovrebbero attuare nell'attesa di avere a disposizione "l'intelligenza e la tecnologia di controllo" necessaria a processare i dati provenienti dai sensori.

3.3. La strada verso i sistemi di controllo e supervisione avanzati in ottica Industry 4.0

Al fine di supportare opportunamente la nuova rivoluzione garantendone il massimo impatto positivo, numerose sfide dovranno quindi essere affrontate e risolte. Un primo aspetto riguarda la definizione di modelli evoluti di processo e l'estensione ed il potenziamento delle tecnologie di ottimizzazione, la cui potenzialità di calcolo dovrà essere aumentata al fine di garantire la necessaria scalabilità su processi altamente complessi e con elevati requisiti di performance in real-time. Tecniche di decomposizione e

parallelizzazione del calcolo potranno fornire un ulteriore supporto fondamentale per raggiungere questo obiettivo.

Dovranno essere sviluppati sistemi di automazione in grado di supportare in modo nativo lo sviluppo di soluzioni di controllo distribuito model-based, che possano abilitare l'adozione della tecnologia su larga scala nell'ambito di applicazioni complesse ed eterogenee. In questo contesto, sarà necessario che le soluzioni di automazione, sia a livello di singola unità operativa che di sistema, siano sviluppate secondo elevati requisiti di affidabilità, robustezza, semplicità di adattamento e riconfigurazione, mantenendo allo stesso tempo caratteristiche di scalabilità e facilità di implementazione.

Tecnologie avanzate di data mining e di machine learning (necessarie alla costruzione automatica dei modelli utilizzati per le ottimizzazioni, sulla base delle misure effettuate dai sensori) dovranno essere ulteriormente sviluppate per supportare l'aggiornamento in tempo reale del modello sulla base delle evoluzioni in tempo reale del sistema fisico, con particolare riferimento ad approcci in grado di supportare elevati volumi di dati in rapida fluttuazione, rispettando i vincoli di elaborazione connessi alla dinamica del processo produttivo.

Le linee di sviluppo suddette sono tra le portanti indirizzate dalle progettualità e dalle call Horizon2020 in ambito Factory of the Future.

Infine, nuovi standard e protocolli di comunicazione dovranno essere definiti per supportare l'interoperabilità tra i sistemi di automazione degli impianti reali e gli ambienti digitali. Tale condizione risulta fortemente abilitante per la diffusione delle nuove tecnologie presso le imprese italiane, vista la loro specificità. I nuovi standard e protocolli dovranno essere in grado di supportare la gestione di elevati volumi di dati su architetture fortemente distribuite, garantendo il rispetto dei vincoli temporali di esecuzione. A tale scopo, si può considerare come punto di partenza l'estensione degli standard disponibili e maggiormente considerati a livello industriale per comunicazione "machine to machine" (M2M), come l' IEC 62541 OPC-UA.

Oltre agli sviluppi tecnologici, la realizzazione completa dei sistemi di automazione in chiave Industria 4.0 necessita di attori di nuova generazione lungo la value chain, dai technology providers ai system integrator, in grado di complementare le competenze di controllo ed automazione tradizionale con tecniche di controllo avanzato, ottimizzazione nonché capacità di integrazione con le piattaforme digitali. Tali competenze dovranno essere sostanziate in ambito formativo avanzato mediante corsi e indirizzi di studio specifici, con particolare riferimento alle competenze di controllo avanzato, ottimizzazione, interoperabilità automazione/digital factory e machine learning.

4. IoT e Big Data

IoT e BigData sono considerate, spesso in modo accoppiato, due delle tecnologie abilitanti per Industria 4.0, ed in particolare per il suo elemento fondamentale, cioè la “Cyber-Physical Convergence”. Seguendo un approccio logico “bottom-up”, è possibile illustrare gli elementi essenziali di queste tecnologie come segue.

Partendo dall’Internet of Things, si evidenziano i seguenti elementi:

- la miniaturizzazione delle tecnologie di sensing e di comunicazione wireless consente di includere ormai in quasi ogni oggetto fisico dispositivi (sistemi embedded) per la raccolta di informazioni sull’ambiente fisico e la loro comunicazione in rete. Per oggetti che nascono privi di tali dispositivi è ormai possibile aggiungerli in un secondo tempo; pertanto, praticamente ogni oggetto fisico ha (o può avere) la capacità di generare dati sul suo stato e lo stato dell’ambiente fisico che lo circonda.
- la disponibilità di reti wireless pervasive ad alta capacità (es., lte, wifi, zigbee, bluetooth) permette di raccogliere questi dati e di connettere praticamente qualunque oggetto fisico in internet. Questo permette, da un lato, la raccolta e condivisione dei dati generati dai dispositivi embedded negli oggetti fisici, e dall’altro di configurarli, e quindi agire anche da remoto sugli oggetti fisici ed il loro ambiente circostante.
- i dispositivi personali degli utenti (smartphones, tablets, oggetti wearable come gli smart watches) possono anch’essi generare dati, comunicarli su internet e ricevere comandi da remoto, esattamente secondo lo stesso paradigma.
- l’insieme di questi tre elementi (pervasività di sistemi embedded, pervasività delle reti, pervasività di dispositivi personali collegati alla rete) costituisce la base tecnologica dell’internet of things.

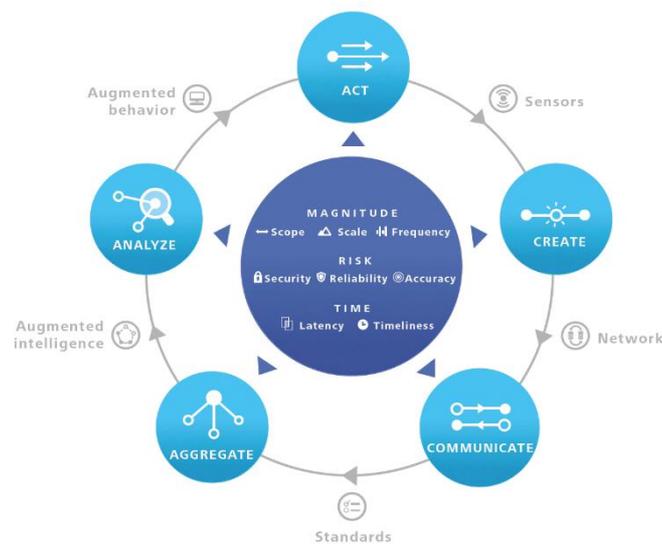
Da un punto di vista tecnologico, l’Internet of Things è quindi l’estensione dell’Internet tradizionale - pensato per far comunicare oggetti specifici, i computer, senza un particolare legame con il mondo fisico circostante - ad una rete che permette agli oggetti fisici di comunicare direttamente tra loro e alle persone di interagire con gli oggetti fisici sia vicini che remoti.

Con la grande diffusione dei dispositivi IoT si assiste di pari passo al cosiddetto “data deluge”, cioè la disponibilità di una quantità enorme di dati “grezzi” generati dai dispositivi nell’ambiente fisico. Stime di istituti di ricerca ed aziende IT internazionali prevedono che nei prossimi anni si arriverà ad un numero di dispositivi IoT connessi di centinaia di miliardi (IDC e CISCO) fino a trilioni (McKinsey), equivalenti cioè a centinaia (se non migliaia) di

dispositivi IoT connessi per persona. Se da un lato la presenza di una tale mole di dati fornisce opportunità eccezionali, dall'altro diventa più che mai necessario accoppiare a tecnologie IoT tecnologie specifiche per la gestione, integrazione dei dati, ed estrazione di conoscenza dai dati grezzi generati dai dispositivi IoT, chiamate comunemente BigData Analytics (che, a loro volta, tipicamente richiedono infrastrutture di calcolo ad alta capacità per poter immagazzinare ed analizzare tali quantità di dati, attualmente fornite tramite piattaforme di cloud storage and computing).

La sinergia tra tecnologie IoT e Big Data è una delle basi della Cyber-Physical Convergence (e dei corrispondenti Cyber-Physical Production Systems – CPPS), che un recente report di Deloitte vede come una delle fondamentali basi tecnologiche di Industry 4.0 (si veda la sezione successiva). La Cyber Physical Convergence è caratterizzata da un processo circolare (Information Value Loop, nella terminologia usata da Deloitte) tra il mondo fisico ed il mondo cyber (Internet). Grazie a tecnologie IoT, gli oggetti e le persone generano costantemente dati che passano dal mondo fisico al mondo cyber tramite reti pervasive. Nel mondo cyber, le tecnologie Big Data permettono di analizzare i dati raccolti estraendone conoscenza. Sulla base di tale conoscenza diventa possibile “chiudere il cerchio”, individuando azioni da compiere sugli oggetti stessi per configurarli e, in alcuni casi, agire sul mondo fisico che sta loro attorno.

Figura 5. Deloitte: l'Information Value Loop creato da IoT e BigData technologies



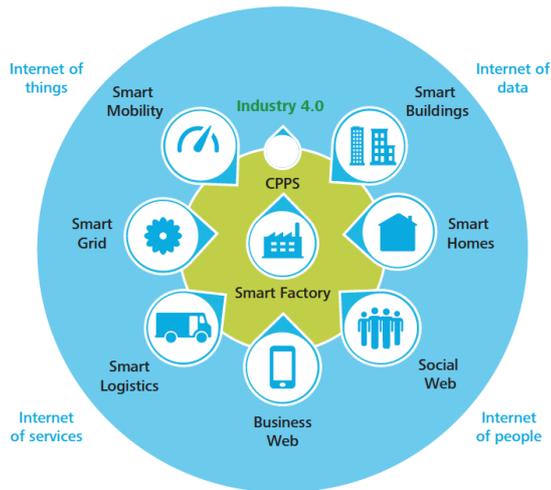
Si noti anche che la stessa focalizzazione sugli aspetti di IoT e Big Data è alla base dell'iniziativa *Industrial Data Space (IDS)*² guidata dal Fraunhofer in Germania, il principale ente di ricerca tedesco orientato all'innovazione industriale. In particolare, IDS è visto come il fattore abilitante per tutte le soluzioni Industry 4.0, ed è focalizzato sulla raccolta, gestione ed analisi dei dati su tutta la catena produttiva, sia nell'ambito delle diverse unità della stessa azienda, che nell'ambito delle varie aziende di una stessa catena produttiva.

² Fraunhofer, "INDUSTRIAL DATA SPACE – Digital Sovereignty over Data", 2016, <https://www.fraunhofer.de/en/research/lighthouse-projects-fraunhofer-initiatives/industrial-data-space.html>

4.1. Scopi e vantaggi di IoT e Big Data

Contestualizzata nel mondo di Industria 4.0, la Cyber-Physical Convergence permette una continua interazione tra *cose*, *dati*, *persone* e *servizi*, che è alla base di molti dei concetti fondamentali di Industry 4.0 (Figura 6). In particolare, è grazie a questa interazione che diventa possibile quel processo circolare continuo di (i) produzione di dati (ii) analisi di dati e (iii) manutenzione e riconfigurazione dei processi produttivi.

Figura 6. L'ambiente Industry 4.0 abilitato dai Cyber-Physical Production Systems (CPPS)



Vi possono essere diversi ambiti di applicazione del processo circolare sopra illustrato. Se applicato ad un singolo processo produttivo, ad esempio, tale approccio consente di monitorare il processo in maniera accurata e continua in modo da controllarlo efficacemente, migliorarlo costantemente nel corso del tempo e riadattarlo rispetto alla variabilità del contesto esterno (con benefici in termini di costi, tempi e flessibilità del processo in questione in ottica “zero-defect”). Se esteso a diversi reparti e linee della stessa azienda, esso consente di ottenere un’integrazione interna ottimale, andando a migliorare le performance a livello aziendale (integrazione verticale). Se esteso al di fuori delle imprese (cioè se anche altre imprese esterne adottassero tecnologie IoT e Big Data), le nuove tecnologie offrirebbero la possibilità, finora mai stata così potente, di integrarsi in filiere più ampie, andando a identificare dinamicamente partner manifatturieri in network produttivi che sarebbe altrimenti impossibile agganciare, anche solo per produzioni temporanee (integrazione orizzontale). Infine, se l’approccio di IoT e Big Data venisse esteso anche al mondo dei clienti, il flusso di informazioni sui prodotti durante il loro ciclo di vita e sui clienti stessi permetterebbe di far evolvere i modelli di business aziendali nella direzione dell’offerta di servizi ad alto valore aggiunto e di circular economy.

4.2. A che punto siamo

In molte realtà Europee e mondiali sono già in atto iniziative industriali per realizzare pilots di sistemi Industry 4.0 e per convertire processi produttivi secondo tali nuovi modelli. Si veda, a tale proposito, il recente report di McKinsey³ sullo stato di avanzamento dell'adozione di Industry 4.0 in US, Germania e Giappone, oppure i pilot realizzati nell'infrastruttura Smart Factory di DFKI⁴, fino ad esperienze in tal senso di singole aziende, anche italiane⁵⁶.

Visto che le tecnologie IoT e Big Data sono al momento mature (benché sempre in evoluzione nel settore della ricerca) è possibile programmare interventi puntuali ed immediati di adozione di tecnologie IoT e BigData sin da subito, nell'ottica di una migrazione a più lungo termine verso modelli Industria 4.0. Come anche indicato nel già citato report McKinsey sull'adozione di Industry 4.0 negli ultimi anni, tipicamente i primi interventi che vengono pianificati e realizzati riguardano il miglioramento dell'efficienza produttiva (*operational effectiveness*) nell'ambito di singole unità produttive o nell'insieme di unità produttive di una stessa azienda, grazie a tecnologie IoT e BigData.

A titolo di esempio, si possono indicare le seguenti tecnologie che sono al momento già disponibili sul mercato. Per quanto riguarda le tecnologie IoT:

- ARDUINO e RASPBERRY PI. Permettono la realizzazione di piccoli sistemi integrati a bassissimo costo (~100 euro a soluzione). Sono essenzialmente piattaforme hw generali, su cui è possibile “montare” sensori di vario tipo (luce, umidità, movimento, etc.) e schede per la comunicazione wireless che implementano i più diffusi standard di comunicazione (wifi, zigbee, ...). Dispongono anche di processori locali che possono essere programmati per l'analisi dei dati raccolti “sul posto”.
- Zigbee. E' il nome di soluzioni commerciali basate sullo standard iee 802.15.4 per la realizzazione di reti di sensori (iot) a basso consumo energetico. I dispositivi zigbee possono comunicare tra loro e ricevere comandi da remoto, per modificare il loro stato. Sono spesso usati per applicazioni di controllo, come ad esempio la domotica, ma hanno applicazioni in molti settori, come retail, smart parking, illuminazione intelligente, smart metering, etc.
- Bluetooth low energy. E' l'evoluzione della tecnologia bluetooth per dispositivi iot a bassissimo consumo energetico. Permette la comunicazione

³ McKinsey, “Industry 4.0 after the initial hype - Where manufacturers are finding value and how they can best capture it”, 2016, <http://www.mckinsey.com/business-functions/operations/our-insights/industry-40-looking-beyond-the-initial-hype>.

⁴ DFKI, SmartFactory^{KL}, <http://www.smartfactory.de/>

⁵ Il Sole24Ore, 16 Agosto 2016, “Varese, Industria 4.0 dal basso”, <http://www.ilsole24ore.com/art/impresa-e-territori/2016-08-25/varese-industria-40-basso-152257.shtml?uuid=ADGEuAAB>

⁶ Il Sole 24 Ore, 11 Agosto 2016, “Manifattura 4.0, la via Emilia che batte i tedeschi”, http://www.ilsole24ore.com/art/impresa-e-territori/2016-08-10/manifattura-40-via-emilia-che-batte-tedeschi-145935_PRV.shtml?uuid=ADV8QL4

wireless tra oggetti fisici in prossimità, come dispositivi indossabili (smart watches, smart badges, etc.) e con dispositivi inseriti nell'ambiente fisico circostante (es. termostati intelligenti).

- Sigfox, lora, cellular-iot. Sono tecnologie per la copertura wireless di grandi aree geografiche per dispositivi iot a bassissimo consumo. Applicazioni tipiche sono illuminazione intelligente o smart metering. Ad esempio, nel caso sigfox, un operatore del servizio di rete (concettualmente simile ad un operatore cellulare) garantisce copertura in particolari aree geografiche (l'Italia è attualmente in fase di coperta tramite il concessionario nettrotter⁷). Acquistando dispositivi iot (tipicamente sensori) che possano comunicare sulla rete sigfox si ha automaticamente la possibilità di creare sistemi per il monitoraggio ed il controllo di oggetti fisici. In particolare, sigfox raccoglie i dati generati dai sensori e li fornisce all'utente che li ha installati sottoscrivendo un servizio di accesso tramite cloud.
- libelium. E' uno dei principali produttori di sensori e dispositivi iot fisici⁸. I dispositivi disponibili permettono di raccogliere dati su una grandissima varietà di grandezze fisiche. E' possibile associare a tali sensori schede di rete per abilitare la trasmissione dei dati sulle principali tecnologie iot (zigbee, wifi, lora, sigfox, cellulariot).

Per quanto riguarda le tecnologie Big Data, si possono citare:

- Hadoop. È il framework tecnologico open di riferimento per la programmazione di sistemi di analisi su grandi quantità di dati.
- Hive. Permette l'esecuzione efficiente di richieste (queries) per la raccolta e l'analisi di dati su sistemi distribuiti, compatibili con Hadoop.
- Spark. Tecnologia di riferimento per la programmazione efficiente di sistemi paralleli per l'analisi di dati su larga scala.
- HBase e Cassandra. Tecnologie per la gestione di grandi quantità di dati su sistemi distribuiti con prestazioni particolarmente elevate.

Applicando tali tecnologie, è possibile, per esempio, sin da ora:

- integrare dispositivi IoT per il monitoraggio delle varie fasi della produzione;
- analizzare BigData provenienti dal processo di produzione o dall'utilizzo dei prodotti da parte dei clienti.

⁷ Copertura SigFox: <http://www.sigfox.com/en/coverage>

⁸ Libelium, <http://www.libelium.com/>

- costruire processi circolari secondo lo schema Information Value Loop. Al momento è ragionevole pensare ad implementazioni in tal senso all'interno di una singola realtà produttiva o, nel caso di aziende più grandi, come supporto all'integrazione "verticale" di varie unità produttive della stessa azienda. Uno degli esempi più immediati di questo approccio è la predictive maintenance dei macchinari.

È da notare che implementare questo tipo di processi a livelli puntuali della singola azienda viene comunemente visto ad oggi come un approccio pragmatico all'adozione di modelli Industry 4.0. È esperienza comune nei Paesi che si stanno muovendo in questa direzione di cominciare ad implementare strumenti per la raccolta e l'analisi dei dati nelle singole aziende, non necessariamente in modo collegato con le altre aziende della stessa *value chain*. In questo modo si riesce a "partire", evitando di rimanere bloccati in attesa che si verifichino le condizioni complessive di eco-sistema per una completa migrazione verso nuovi modelli di business (si veda ancora il report McKinsey già citato).

La realtà industriale italiana è, per molti aspetti, ben posizionata per sfruttare appieno le potenzialità dei modelli di Industria 4.0. Tra tutte, le caratteristiche legate alla tipica dinamicità ed inventiva delle PMI italiane, una consolidata attitudine alla competizione in mercati internazionali, la produzione di oggetti "di nicchia" ad altissimo valore aggiunto, sono tutti elementi che ben si sposano con modelli di filiera produttiva dinamica, orientata al cliente, continuamente riconfigurabile. Inoltre, le nuove tecnologie consentirebbero di "allungare le filiere" nazionali andando ad identificare in maniera dinamica partner che attualmente è difficile intercettare per le PMI italiane.

D'altro canto, come anche indicato in un recente report di Confindustria⁹, esistono diverse barriere all'adozione di tali modelli, tra cui la scarsa tendenza all'investimento e all'avanzamento tecnologico, l'assenza di piattaforme aperte per la condivisione e l'analisi dei dati ed i rapporti non organici con ecosistemi di start-up realtà di Ricerca e Sviluppo. Si noti che al momento IoT e Big Data sono tematiche presenti nell'offerta formativa a livello di corsi e Master Universitari. Corsi su IoT e Data Mining sono attualmente in quasi tutti i corsi universitari in Ingegneria dell'Informazione ed Informatica, e recentemente sono stati attivati anche Master dedicati su questi argomenti¹⁰¹¹¹². Ciò che al momento sembra mancare è un travaso di tali competenze per la ristrutturazione dei processi manifatturieri.

4.3. La strada verso IoT e Big Data

A fronte delle barriere individuate, emergono chiaramente alcune necessità per l'adozione di tecnologie IoT e Big Data, in particolare rispetto al contesto italiano (si veda ancora il già citato rapporto di Confindustria). Si segnalano i seguenti punti quali prioritari:

⁹ Confindustria, Audizione Parlamentare 22 Marzo 2016, Commissione Attività Produttive della Camera dei Deputati,

http://www.confindustria.it/wps/wcm/connect/www.confindustria.it/5266/26cb8a9f-545d-40f3-a4fb-87cdcf80bee6/Audizione+industria+4.0+Camera+dei+Deputati_22.3.2016.pdf?MOD=AJPERES

¹⁰ Master in "Big Data Analytics & Social Mining" dell'Università di Pisa, <http://masterbigdata.it/>

¹¹ Master in "Data Science" dell'Università di Bologna, <http://www.bbs.unibo.it/hp/master-fulltime/data-science/>

¹² Master in "Business Intelligence and BigData Analytics", Università di Milano Bicocca.

- Adozione massiccia di tecnologie IoT per la raccolta ed il monitoraggio dei dati a tutti i livelli, e tecnologie BigData per la loro elaborazione. Il rinnovamento dei macchinari, spesso indicato come uno dei bisogni fondamentali, dovrebbe includere una profonda adozione di tecnologie abilitanti IoT e Big Data (ed investimenti in appropriate tecnologie IT in generale), che sono il supporto di base a tutte le innovazioni discusse in precedenza.
- *Acquisizione di skills su tecnologie IoT e Big Data*, o direttamente in azienda, o tramite la creazione di rapporti organici con *Digital Innovation Hubs*, che possano fornire supporto all'integrazione di soluzioni avanzate di IoT e Big Data nello sviluppo di processi produttivi. È fondamentale che, al di là dei singoli casi di aziende che già vanno in questa direzione, ci sia un'esposizione maggiore delle aziende nazionali (PMI in particolare) verso le tecnologie IoT e Big Data, per capire come inserirle nei propri processi produttivi. Si segnala come esempio in tal senso lo specifico programma I4MS (*ICT innovation for manufacturing SMEs*) all'interno del programma di Ricerca ed Innovazione H2020 della Commissione Europea¹³.
- Necessità di progetti pilota che, in modo incrementale, permettano alle aziende di provare e capire a fondo *i benefici dei nuovi modelli di business ed organizzazioni produttive di I4.0*, ad esempio stimolando progetti nelle aree della mass customisation e della servitisation, quindi "aprendo" il processo produttivo (ed in particolare, la raccolta ed analisi dei dati tramite IoT e Big Data) anche ai clienti finali e focalizzando la produzione non solo sull'oggetto prodotto, ma soprattutto sui servizi associati.
- *Creazione di piattaforme aperte* basate su open standard per la condivisione e l'analisi dei dati su larga scala, prevedendo opportune interfacce per l'integrazione dei sistemi IoT delle singole aziende. Tali piattaforme dovranno in prospettiva supportare il "bus orizzontale" dei dati per la loro condivisione ed analisi a livello di filiera integrata.
- Costituzione di *Competence Centres* sulle tematiche IoT e Big Data e creazione di rapporti stabili ed organici tra soggetti di ricerca, innovazione ed aziende per l'adozione di tali tecnologie in modo rapido ed efficace.

¹³ I4MS (ICT innovation for manufacturing SMEs), <http://i4ms.eu/>

5. Cyber security

Recentemente il mercato globale del cyber crime è stato valutato in circa 1 trilione di Dollari. Senza una adeguata protezione alle infrastrutture informatiche che sono alla base della Industria 4.0, vi saranno inevitabilmente una serie di criticità che rallenteranno l'avvento del nuovo paradigma. La protezione dei sistemi informatici, e quindi la cyber security sono elementi necessari nello sviluppo della tecnologia.

Nel tempo gli attacchi ai sistemi informatici (o cyber) si sono evoluti. Inizialmente (anni '80) erano compiuti da hackers interessati a dimostrare il proprio "valore" e le proprie abilità. In seguito, gli attaccanti si sono compiuti per ottenere un vantaggio economico da cyber criminali effettuando delle cyber frodi, vedi casi di ransom-ware ("materiale per chiedere il riscatto") ed attacchi ai sistemi finanziari. Nei tempi più recenti stanno emergendo le problematiche di cyber terrorismo, vista la rilevanza di sistemi industriali complessi come quello energetico e del trasporto.

Il cyber crime è diventato esso stesso un mercato in cui le metodologie e gli strumenti di attacco possono essere acquisiti ed acquistati come servizio nel dark web e pagati con moneta elettronica (bitcoins), ovvero *cyber crime as a service*. La tecnologia per la cyber security permettono di proteggere i sistemi informatici e quindi di evitare o limitare i danni a tali sistemi e più in generale ai sistemi che dipendono da questi (come i sistemi di controllo industriale (ICS)). Nel momento in cui c'è una evidente convergenza di sistemi cyber e quelli fisici (*cyber physical convergence*) tali attacchi esulano dal puro danno al sistema informatico e possono espandersi verso attacchi che riguardano la sicurezza stessa delle persone fisiche e delle strutture ed infrastrutture industriali come dimostra il recente attacco ad una fonderia in Germania nel 2014¹⁴.

La cyber security prevede una serie di fasi del tipo: *pianifica, rileva e reagisci (plan, detect, react)* che possono essere a loro volte scomposte in altre sotto fasi per cui sono state sviluppate varie metodologie e tecnologie. In particolare,

- *Pianifica*: In questa fase si possono ulteriormente considerare due sotto fasi:
 - *Identifica*. In questa fase si identificano i beni da proteggere o *assets*, le possibili minacce, le vulnerabilità
 - *Analizza*. Analizza il rischio e se ne deriva un piano di gestione di tale rischio. Sono stati sviluppati a tal proposito molti approcci, modelli e standard per l'analisi del rischio informatico (e.g., ISO 27005).
- *Proteggi*. In questa fase si implementano una serie di meccanismi di protezione dei sistemi informatici. In questa fase sono numerosissime le tecnologie che possono

¹⁴ Annual report, German Federal Office for Information Security (BSI), December 2014.

essere usate per la protezione dei sistemi informatici:

- Tecniche di cifratura dei dati per garantire la confidenzialità ed integrità.
 - Cifratura dei canali di comunicazione e protocolli di comunicazione di rete quali SSL (Secure Socket Layer) per TCP/IP.
 - Autenticazione e controllo accessi. Esistono molti protocolli di autenticazione ed identificazione che usano sia certificati digitali, quali x.509, oppure altre credenziali, incluse informazioni biometriche. Al contempo esistono vari linguaggi usabili per esprimere e garantire politiche di controllo accessi ai sistemi informatici (quali XACML).
 - Protezione dell'hardware. Tra le varie tecnologie hardware ha ricevuto molto interesse l'uso di Trusted Platform Modules (TPM) che offrono una serie di meccanismi di garantire l'integrità dei sistemi.
- *Rileva*: In questa fase si applicano una serie di meccanismi di raccolta ed analisi delle informazioni, spesso da varie sorgenti che permettono di rilevare attacchi al sistema Intrusion Detection Systems (IDS) (oppure situazioni di rischio aumentato che richiedono azioni ulteriori). In questa fase si usano varie tecnologie, sia basate su riconoscimento efficiente di *signatures* note di attacchi (efficiente ma poco utile per gli zero-day-attacks, ovvero sconosciuti) che tecniche di *machine learning* per classificazione di comportamenti (quali k-nearest-neighbors (kNN), *supporting vector machine* (SVN)) per identificare possibili anomalie nel comportamento dei sistemi, utile per gli zero-day attacks, ma foriero di possibili falsi allarmi.
 - *Reagisci*: In questa fase si possono ulteriormente considerare due sotto fasi:
 - *Rispondi*. In questa fase una serie di azioni immediate possono essere prese, come la chiusura di certi canali di comunicazione, la rimozione di possibili programmi malevoli nel sistema (malware), etc.. Esistono per questo scopo vari sistemi per la prevenzione degli attacchi e processi di rimozione del malware.
 - *Ripara*: In questa fase, in base al piano di gestione del rischio identificato si tende a compiere quella serie di operazioni per riportare il sistema in (piena) operatività. Si possono qui utilizzare dei *Decision support systems* per rimediare agli effetti degli attacchi e politiche di reazione possono essere automaticamente eseguite.

Esistono molte varianti alla serie di passi precedentemente descritta, ad esempio nella fase di reazione aspetti di *cyber forensic* possono essere considerati, come acquisizione di evidenza di reati informatici che debbano essere poi portati in giudizio. Le fasi precedentemente descritte sono elementi basilari di ogni processo di protezione dei sistemi.

Le necessità e l'opportunità di ricerca ed innovazione legate al mondo dei sistemi industriali e della rivoluzione tecnologica legata alla convergenza del mondo fisico e quello cyber sono state investigate anche a livello Europeo e descritte in vari report di molte organizzazioni, quali ENISA e dal WG3 della piattaforma Europea su Network and Information Security (NIS)¹⁵, dalla organizzazione Europea per la Cyber Security (ECSO)¹⁶, e da varie organizzazioni industriali specializzate nel settore come Symantec¹⁷.

5.1. Scopi e vantaggi delle tecnologie di cyber security

I sistemi industriali ed i relativi macchinari sono sempre più dotati di tecnologie che acquisiscono in tempo reale dati dettagliati sul proprio funzionamento e comunicano e distribuiscono tali dati ad altri sistemi informatici in rete (in particolare Internet). Questi dati vengono aggregati, filtrati ed utilizzati dalle imprese al fine di (micro/macro) gestione e controllo dei processi industriali, ma possono essere anche usati da altri attori (ad esempio fornitori, utenti finali) per offrire servizi aggiuntivi (servitization). Un esempio classico può essere il settore energetico in cui sono attualmente in corso di sviluppo concetti quali gli smart grids o "reti intelligenti". Anche se ci sono molti tipi di reti intelligenti, centrale è l'esistenza di una infrastruttura di rete integrata che consente ai sistemi in tutta la rete (ad esempio generatori di energia, contatori intelligenti, veicoli elettrici, elettrodomestici) di comunicare tra loro. Sistemi di controllo industriale permettono di misurare costantemente quanto l'elettricità fluisce attraverso la griglia e consentono ai vari attori (operatori, ma anche consumatori) di ottenere vantaggi da questo incremento di controllo.

In questo contesto sono molti gli elementi da proteggere, dai sistemi embedded, alle reti di comunicazione, ai sistemi informatici che analizzano e immagazzinano tali dati (es. cloud). E' importante notare come per la convergenza cyber physical, che l'Industria 4.0 richiede, la protezione del mondo cyber implica anche un contributo alla usuale protezione fisica dei sistemi, e quindi alla protezione aziendale.

In particolare, la trattazione dei dati acquisiti richiederà particolare attenzione. Per i sistemi di controllo industriale, e più in generale per la mass consumerization e circularization della Industria 4.0, avremo che più flussi di dati, da più sorgenti e con più destinatari, dovranno essere integrati e trattati con analisi complesse e, dall'interpretazione di questi dati, dovranno essere eseguite azioni di risposta e di controllo, per cui gli aspetti di integrità, confidenzialità, non ripudio e fiducia/credibilità avranno un ruolo fondamentale. E' inoltre importante considerare le problematiche di privacy (ovvero acquisizione di *personal identifiable information*, PII), che nascono dall'aver miliardi di sensori attorno alle persone (siano esse partecipi del processo produttivo o consumatori), sia al lavoro ma anche a casa (smart buildings).

L'aumento dei dispositivi collegati determina una crescita della cosiddetta superficie di attacco (*attack surface*) che include infrastrutture industriali, robot, macchine di

¹⁵ European Cyber Security Strategic Research Agenda (Eds. P. Bisson, R.R. Granadino, F. Martinelli). Available at <https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents>

¹⁶ www.ecs-org.eu

¹⁷ SMARTER SECURITY FOR MANUFACTURING IN THE INDUSTRY 4.0 ERA

assemblaggio, macchine di smistamento logistico e simili. E' interessante notare come il cambiamento tecnologico implicato dalla Industria 4.0 e dall'Internet come rete globale, possa portare ad un cambiamento alle condizioni assunte nel progettare le protezioni dei sistemi, spesso basate sul concetto di prossimità (o non prossimità) fisica. In effetti l'evoluzione della tecnologia per *industrial control systems* ed in generale per Industria 4.0 è in gran parte dipendente ed in relazione ai sistemi preesistenti ed ai sistemi che vengono connessi. Risultano evidenti i possibili problemi di collegamento di sistemi *legacy* e stand-alone per reti proprietarie e Internet, e tali problematiche cresceranno rapidamente di pari passo con i nuovi concetti e le nuove possibilità alla base della Industria 4.0. Molti sistemi di sicurezza, ad esempio, erano basati sul concetto che un attaccante dovesse essere fisicamente presente per compiere un attacco; tali assunzioni non sono più valide nel momento in cui le varie componenti vengono messe in rete, rendendo in tal modo insicura una componente del sistema che prima lo era. Ad esempio, in ambiente *automotive*, l'introduzione di collegamento remoto, sia per telecontrollo e diagnostica che per *infotainment* ha introdotto delle vulnerabilità gravi in molte auto di nuova generazione. Quindi non solo il numero di devices che possono essere attaccati cresce, ma la presenza stessa di una componente nuova che aggiunge altre caratteristiche non previste rende più insicure altre parti del sistema globale e richiede una analisi del rischio dinamica, che vada oltre il puro dominio ICT e riguardi anche i domini specifici.

Risulta evidente dalla trattazione precedente che la dipendenza dei sistemi produttivi della Industria 4.0 dai sistemi informatici richiede la protezione di questi ultimi come prerequisito essenziale per ogni sviluppo credibile e sostenibile della Industria 4.0 stessa.

E' anche importante notare come le nuove tecnologie aprano scenari di sicurezza non previsti / prevedibili e che le tecnologie informatiche sono un beneficio per la manifattura ma al contempo lo sono anche per i possibili attaccanti. Come abbiamo già evidenziato, sia la superficie di attacco può essere allargata dalla Industria 4.0, sia gli strumenti stessi di attacco possono evolvere con il miglioramento delle tecnologie. Consideriamo il caso di sensori *embedded* nel mondo fisico direttamente connessi alla rete (IoT), come ad esempio le telecamere per controllare via remoto i sistemi produttivi. Se tali strumenti di per sè utili per la protezione fisica non sono perfettamente configurati, possono essere vulnerabili e quindi utilizzabili per effettuare degli attacchi. Esistano addirittura dei servizi web¹⁸ che con una ricerca estensiva su tutti gli indirizzi Internet cercano dispositivi (anche sensori) vulnerabili o non protetti e forniscono a terzi queste informazioni, permettendo loro di accedere e controllare tali dispositivi anche in modo remoto.

Nel caso della cyber security, più che descrivere i benefici dell'applicazione della tecnologia, è più facile parlare dei danni derivanti dalla sua omissione. In particolare:

- Danni alla produzione (incluso sabotaggio);
- Danni alla proprietà intellettuale;
- Danni alle infrastrutture industriali;

¹⁸ Ad esempio: shodan.io (ultimo accesso eseguito nell'Agosto 2016).

- Danni alle persone fisiche (inclusi addetti e clienti);
- Danni di reputazione ed immagine;

5.2. A che punto siamo

Le tecnologie per la protezione dei sistemi, che siano meccanismi di cifratura end-to-end, sistemi di controllo accessi avanzati e di gestione delle identità in ambienti altamente aperti e distribuiti, devono essere propriamente configurate e utilizzate. In un ambiente complesso ed interconnesso come quello della Industria 4.0, esistono varie barriere che devono essere superate per una fruttuosa adozione della tecnologie.

Tutte le metodologie e gli strumenti utili ad incrementare la sicurezza dei dispositivi informatici saranno indispensabili, ma dato il contesto e la convergenza *cyber physical*, vi sono nuove sfide specifiche da affrontate.

- *Interdipendenze fra aspetti di safety e security.* Nel settore dei sistemi di controllo industriale è stata data sempre grande enfasi alla sicurezza, intesa come sicurezza fisica delle persone (safety). Con la presenza di sistemi cyber, la protezione da attacchi di natura antropica dovrà essere maggiormente garantita. La sicurezza informatica e la safety potrebbero sembrare talvolta in conflitto - un firewall o un livello di crittografia su canale di comunicazione possono aggiungere una buona protezione informatica, ma anche un ulteriore punto di guasto da una prospettiva di sicurezza e dependability. In effetti, la necessità/comodità di una facile manutenzione è anche uno dei motivi per cui molti sistemi controllo industriale non hanno sistemi di controllo accessi molto complessi, che invece sono uno dei controlli di sicurezza primari nei sistemi informatici. Inoltre, una caratteristica specifica della comunicazione nei dispositivi industriali è la necessità di elaborazione in tempo reale. Questo a volte può essere in contrasto con l'applicazione di tecniche di sicurezza informatica come ad esempio la cifratura delle comunicazioni che richiedono un costo in termini di risorse di tempo e computazionali (spesso le telecamere di sorveglianza hanno la possibilità di cifrare il contenuto delle comunicazioni, per esempio con protocollo SSL, ma non la usano in quanto degrada le prestazioni). E' necessario quindi avere dei meccanismi di decisione che permettano di mediare tra i vari parametri, anche durante l'esecuzione dei sistemi, e che permettano di ottimizzare le risorse disponibili. In questo ambito, spesso si parla di modelli quantitativi per la sicurezza (più che qualitativi), intendendo che in molti casi è necessario cercare soluzioni abbastanza sicure e non necessariamente totalmente sicure che, oltre a non essere tecnicamente realizzabili, avrebbero un costo proibitivo.
- *Necessità di gestione dei sistemi legacy/tradizionali.* A differenza delle normali componenti IT, le componenti per il controllo industriale hanno di solito una lunga durata, a volte decenni. Così, ogni nuovo meccanismo di sicurezza che sia da inserire nel sistema, deve spesso dover interagire con sistemi *legacy*. Quindi le architetture ed i nuovi sistemi devono essere pronti per requisiti di sicurezza che possano valere per un lungo periodo. In questo senso si parla anche di sistemi di

sicurezza che possono evolvere ed adattarsi con lo sviluppo dei sistemi che proteggono. Un ulteriore problema generato da questa lunga durata di impiego è la disponibilità dei fornitori; pochi fornitori sono disposti a impegnarsi per fornire patch di manutenzione e di sicurezza molto a lungo, e vi è un'alta probabilità che alcuni fornitori o loro subappaltatori possono non durare a lungo quanto i loro dispositivi. Un esempio recente è Windows XP, che è ancora ampiamente usato nel dominio ICS, ma che è in fase di esaurimento da parte del fornitore e avrà il supporto molto limitato in futuro. Tutti questi aspetti sono già presenti negli attuali sistemi e non potranno che essere esacerbati nel futuro.

- *Difficile analisi del rischio.* Anche semplicemente in un ambiente di sicurezza informatica *tout court*, l'esecuzione di una corretta analisi del rischio può essere un compito arduo, ed è difficile ottenere numeri significativi ed affidabili. In un sistema di controllo industriale, o in esempi di Industria 4.0, questa analisi può risultare ancora più difficile. Con i sistemi ICS sempre più collegati, c'è anche un livello crescente di dipendenze, molti delle quali non sono ben definite. Un certo numero di sistemi di controllo, ad esempio, richiede alta precisione di sincronizzazione, ed il tempo comune viene acquisito dal sistema GPS. Questo però diviene naturalmente un *single point of failure* di tali sistemi. Inoltre, molti produttori richiedono la possibilità di fare manutenzione a distanza, e questo complica gli aspetti di sicurezza. Inoltre i sistemi possono raggiungere un enorme livello di complessità – l'esempio più significativo è forse la smart grid, che si estende su un intero continente con un sistema che ha centinaia di milioni di componenti. È ben noto che i servizi software di questo livello di complessità sono difficili da progettare e quindi da eseguire in maniera corretta dal semplice punto di vista funzionale, ed a maggior ragione da un punto di vista di sicurezza.
- *Gestione e protezione integrata di grandi moli di dati.* Il numero enorme di sensori/attuatori collegati ai sistemi industriali che stanno alla base della Industria 4.0 generano informazioni che hanno valore (*data deluge*) e devono quindi essere protette. Inoltre i dispositivi contengono anche molte informazioni relative al processo ed al prodotto per cui la protezione di tali sistemi ha anche un impatto diretto sulla protezione dei diritti intellettuali. E' necessario porre in essere una serie di meccanismi che garantiscano il controllo sui dati prodotti e disseminati (*data usage control*) e permettano facilmente di definire chi può ricevere i risultati della elaborazione. Nella Industria 4.0 il dato è elemento di assoluto valore e tutte le problematiche di *data protection* hanno un ruolo molto rilevante, amplificato dalla convergenza cyber physical e da inevitabili aspetti di privacy.
- *Gestione della privacy.* La pervasività dei sensori, la capacità di elaborare grandi quantità di dati, la possibilità di interagire ed aggregare informazioni, dalla creazione del prodotto al suo riciclo, passando per gli usi ed i costumi dei clienti che lo posseggono, apre delle sfide molto significative dentro l'azienda, tra aziende e tra consumatori ed aziende. E' chiaro che la gestione della privacy è anche uno degli elementi per lo sviluppo della fiducia tra i vari stakeholder della filiera della Industria 4.0. Si dovrebbero utilizzare quando possibile tecnologie del tipo *privacy-by-design*, che permettano comunque un controllo fine da parte dell'utente dei dati personali che lo riguardano. Tali aspetti sono molto difficili da gestire.
- *Manca di skills, risorse umane e procedura di formazione.* L'aumento del tasso tecnologico della Industria 4.0 implica la crescente domanda di risorse umane con

capacità e skill varie ed interdisciplinari. In questo ambito è quindi importante avere la possibilità, ad ogni livello, di far crescere la consapevolezza sul ruolo della sicurezza informatica per la protezione della società e di promuovere le tecniche più avanzate per operare in questo settore. E' necessaria una serie di azioni per migliorare la formazione del personale in questo settore specifico.

Una delle specificità italiane è la costituzione del tessuto industriale fatta in gran parte di PMI. Gli aspetti di gestione della sicurezza informatica in generale e in particolare della Industria 4.0 sono specifici e vanno affrontati in maniera particolare. Le specifiche necessità delle PMI sono identificate da varie organizzazioni, quali ECSO (European Cyber Security Organization), che ha un gruppo di lavoro specifico nel settore, ed ENISA, che ha creato dei documenti specifici.

Una delle possibili soluzioni per le PMI è quindi nell'adozione di soluzioni informatiche in cui la gestione sia affidata a terzi, per quanto possibile. Il cloud è un esempio in questo senso. In particolare, ENISA ha elencato alcuni vantaggi per le PMI nell' utilizzare il cloud¹⁹ anche per migliorare gli aspetti di sicurezza:

- *Patch e aggiornamento.* Patch tempestive e l'aggiornamento del software sono aspetti fondamentali per la sicurezza, visto che spesso gli attaccanti hanno bisogno solo di una piccola finestra temporale per attaccare e sfruttare una vulnerabilità rilevata in un sistema. In realtà, molti attacchi informatici sfruttano il fatto che le organizzazioni sono lente ad aggiornare i sistemi con le patch di sicurezza, e questo vale in particolar modo per le PMI che spesso non hanno personale dedicato per la sicurezza. Poter quindi contare su servizi cloud che sono continuamente aggiornati e protetti è un vantaggio.
- *Security-as-a-service.* Alcuni compiti della protezione informatica possono essere automatizzati ed offerti tramite servizi cloud, ad esempio il data protection (cifatura dei dati). Nel cloud computing è spesso più facile esternalizzare alcuni di questi compiti di sicurezza a terze parti o al fornitore stesso (se offre tali servizi). In questa ottica *security as a service* è un elemento importante della sicurezza delle PMI.
- *Certificazione e conformità.* Nel cloud computing, uno stesso servizio cloud è utilizzato da molti clienti. La certificazione rispetto agli standard di sicurezza delle reti e dell'informazione (come ISO27001) della piattaforma cloud, potrebbe essere utilizzata dai clienti per adempiere il proprio obbligo di conformità, delegando questo passo in genere oneroso alla conformità del cloud stesso.

¹⁹ ENISA's Security Guide and Online Tool for SMEs when going Cloud

5.3. La strada verso la cyber security in Industry 4.0

Si riportano di seguito alcune considerazioni per lo sviluppo di efficaci tecnologie di cyber security quali condizione indispensabile per la diffusione di Industria 4.0.

- *Gestione della fiducia negli apparati.* Dato che molti processi decisionali vengono eseguiti automaticamente in uno scenario di Industria 4.0, una particolare attenzione deve essere data alla sicurezza basata su hardware; per esempio il *trusted computing* può essere utilizzato per identificare in modo sicuro dispositivi e convalidare l'integrità del software installato (anche in maniera remota – *remote attestation*). Tale possibilità è cruciale per poter gestire in maniera remota risorse significative ed essere comunque in grado di attestare l'integrità dei dispositivi, incluse le componenti software.
- *Necessità di evitare silos tecnologici.* E' importante, specialmente nel settore della sicurezza informatica, evitare di creare dei silos tecnologici separati tra i vari domini di applicazione. Questo rende difficile far cooperare e comunicare le varie componenti e quindi renderle partecipi di un sistemi di controllo e protezione globale.
- *Responsabilità definite.* Mentre il fallimento/danneggiamento di una infrastruttura industriale, magari critica, ha possibili ripercussioni per tutta la società, il costo di proteggere tale infrastruttura è spesso compito solo proprietario della infrastruttura stesso, creando una certa asimmetria. Questo chiaramente vale in particolar modo per sistemi industriali critici. E' importante creare degli standard di sicurezza comuni per tutti e di livello soddisfacente. Lo sviluppo di tali norme è un compito non banale ed è necessario tener conto di molti fattori per evitare di sovraccaricare gli operatori e creare un bilanciamento tra i vari interessi. Recentemente, la Comunità Europea ha definito la prima direttiva Europea²⁰ sulla Network and Information Security (NIS) che definisce livelli minimi di sicurezza per gli operatori di servizi essenziali.
- *Condivisione delle informazioni sugli incidenti, in particolare modo per ICS.* Soprattutto per quello che riguarda i sistemi di controllo industriale per applicazioni critiche è utile prevedere dei gruppi di condivisione dell'informazione che possano permettere in tempo reale la risoluzione dei problemi dovuti a cyber attacchi. Dato il livello di esperienza nel settore relativamente basso, è importante per i partecipanti alla comunità imparare a condividere le *best practices*. Per la maggior parte dei sistemi ICS, almeno sul lato operatore, la sicurezza non è un elemento di differenziazione competitiva, ma un elemento di condivisione all'interno della comunità per non mettere a repentaglio gli obiettivi di business.
- *Formazione e training.* E' fondamentale nel settore della cyber security avere personale preparato alla gestione dei sistemi e delle possibili emergenze che in questi sistemi possano verificarsi. Si stima che nel mondo saranno necessari circa 6 milioni di posti di lavoro nella cyber security e solo 4.5 saranno disponibili. La necessità di formare

²⁰ <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

risorse umane adatte è quindi palese. A livello Europeo, ENISA in cooperazione con la piattaforma NIS ha fatto una ricognizione sui corsi in cyber security disponibili a livello Universitario²¹.

- *Cyber insurance*. Data la difficoltà di analisi e di protezione dei sistemi ICS, è comunque importante poter usufruire di strumenti anche economici come una cyber insurance per le società, che permetta loro di poter trasferire parte del rischio residuo su terzi (le assicurazioni). La cyber insurance è stata definita *the next big thing* nel mondo cyber, anche se in Italia e in Europa si sta procedendo più lentamente in questa direzione rispetto agli Stati Uniti.

²¹ <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities>

Elenco Ricerche pubblicate:

- “Best practice e limiti da superare per il rilancio delle imprese M3 (Medie, Manifatturiere, Multinazionali)” N° 01/2015
- ““Far volare” le PMI con nuove competenze manageriali” N° 02/2015
- “L’accessibilità dei Comuni della Città Metropolitana di Milano e della Provincia di Monza e Brianza” N° 03/2015
- “Tre anni di formazione continua a Milano: i progetti Territoriali finanziati da Fondimpresa dal 2010 al 2012” N° 04/2015
- “E-Government: tra aspettative e realtà” N° 05/2015
- “Alternanza scuola-lavoro: le condizioni per il successo” N° 01/2016
- “L’accessibilità dei Comuni della Città Metropolitana di Milano e della Provincia di Monza e Brianza. Focus sull’accessibilità agli ambiti produttivi di cinque Comuni” N° 02/2016
- “Modelli di partenariato didattico università-impresa” N° 03/2016
- “Le performance delle imprese europee: un'analisi benchmark” N° 04/2016
- “Analisi e strumenti per un territorio attrattivo” N° 05/2016
- “Strategie di internazionalizzazione: export strategy ed export performance” N° 06/2016
- “The Chemical and Pharmaceutical Industry in Lombardy” N° 07/2016

www.assolombarda.it
www.farvolaremilano.it
www.assolombardanews.it

