QUADERNO

"PHARMA 4.0: OPPORTUNITÀ E VINCOLI DELLA DIGITALIZZAZIONE DELL'INDUSTRIA FARMACEUTICA"

"PHARMA 4.0: OPPORTUNITIES AND CONSTRAINTS OF THE PHARMACEUTICAL INDUSTRY DIGITALIZATION"

La cyber security in Industria 4.0 e Pharma 4.0

Cyber security in Industry 4.0 and Pharma 4.0

Enzo Maria Tieghi

A.D. ServiTecno S.r.l., GE Digital Alliance Partner, Docente CLUSIT, Coordinatore GdL IOT CSA Cloud Security Alliance, Italy Chapter, Milano

Questo articolo mira a presentare come la cyber security possa essere declinata nei campi dell'Industry 4.0 e Pharma 4.0. Nello specifico, il paper presenta i vari ingredienti dei sistemi e network industriali e discute le principali differenze tra cyber security IT e OT. Successivamente, il paper si focalizza sulla relazione tra security e data integrity nel campo del Pharma 4.0, per poi discutere ulteriormente le discrepanze tra sicurezza IT e OT, tenendo conto degli standard ISA95 e ISA99/IEC62443. Infine, l'articolo confronta la sicurezza nei contesti Internet of Things e Industrial Internet of Things.

Parole chiave: IoT, SCADA, SCADA Security, GAMP, IIoT, ISA95, ISA99, IEC62443, Pharma4.0, Industria4.0, Industry4.0, OT, Operation Technology, IT, Information Technology, IT Security, OT Security, ICS Cyber Security, Anomaly Detection, Data Integrity, Compliance, GMP, GxP, ALCOA, NIST, SP800-53, SP800-82, Cloud Computing, CSA, Cloud Security Alliance

This paper aims at presenting how cyber security can be declined in the contexts of Industry 4.0 and Pharma 4.0

In particular, the paper will first discuss the main ingredients of industrial systems and networks, then it will discuss the differences between IT and OT cyber security. After a focus on the relation between security and data integrity in Pharma 4.0, the paper will further discuss IT vs OT Security with respect to the ISA95 and ISA99/IEC62443 standards. Finally, the paper will compare security in the contexts of Internet of Things, and Industrial Internet of Things.

***Key words**: IoT, SCADA, SCADA Security, GAMP, IIoT, ISA95, ISA99, IEC62443, Pharma4.0, Industry4.0, OT, Operation Technology, IT, Information Technology, IT Security, OT Security, ICS Cyber Security, Anomaly Detection, Data Integrity, Compliance, GMP, GxP, ALCOA, NIST, SP800-53, SP800-82, Cloud Computing, CSA, Cloud Security Alliance*

Address for correspondence
Indirizzo per la corrispondenza

Enzo Maria Tieghi
ServiTecno Srl
via F. Koristka 10, 20154 Milano
e-mail: etieghi@servitecno.it

Industria 4.0/Pharma 4.0 e la cyber security

In tutti i piani Industria 4.0, e a maggior ragione anche in quelli mirati al settore industriale del Life Science denominati Pharma 4.0, la cyber security è uno dei pilastri sui quali deve basarsi la cosiddetta "trasformazione digitale".

Quando si parla di cyber security in ambiente industriale si fa riferimento alla protezione da rischi informatici di reti e sistemi di automazione di fabbrica e di controllo dei processi di produzione.

Reti e sistemi industriali: ma di quali sistemi stiamo parlando e dove si trovano?

Spesso si utilizzano delle sigle, ben note a chi si occupa di reti e sistemi di fabbrica. Eccone qui un elenco esemplificativo, sicuramente non esaustivo:

- *Distributed Control Systems* (DCS), spesso utilizzati in impianti a processo continuo, soprattutto chimici;
- PLC o controllori a logica programmabile, con tutti i Bus di fabbrica che utilizzano per le lor comunicazioni;
- SCADA/HMI, che sulle reti di impianto permettono la visualizzazione, la raccolta di dati e la gestione degli allarmi;
- Database e Historian, per la memorizzazione e la storicizzazione di quanto avviene in produzione;
- DNC/CNC, Robot, Cobot, AGV, Stampanti 3D ecc., e tutti gli altri dispositivi "smart/intelligenti" che sono presenti nei centri di lavoro e collegati sulla rete di impianto;
- MES, EBRS *& Production Management Systems, Traceability, Track and Trace, Efficiency monitoring and Analysis*, OEE ecc. Sono tutti i sistemi che gestiscono la produzione, stato di avanzamento e tracciabilità/genealogia di quanto si produce;
- LIMS, QA/QC, *Calibration Systems, Measurement and Smart Instrumentation* e tutti gli strumenti "intelligenti" presenti in laboratorio Qualità o connessi direttamente per analisi sulla linea di produzione;
- connessioni remote e sistemi connessi per *Asset Performance Monitoring and Maintenance* (Portali, CMMS, IoT, Industrial IoT ecc.) e tutti i sistemi per la gestione della manutenzione, della documentazione degli impianti di produzione;
- reti di impianto, sistemi per *Smart Building and Facility/ Building* BMS, HVAC, WFI, e ogni altra cosa sia connessa alla rete di fabbrica.

Come detto, questo elenco riporta molti ma non sempre tutti i dispositivi presenti in fabbrica che siano in grado di acquisire dati/informazioni e siano connessi con altri dispositivi in rete: tutti questi devono in qualche modo essere protetti.

La differenza tra cyber security IT e quella OT

Nelle aziende di produzione ci sono solitamente due "domini" di sistemi: IT (*Information Technology*) e OT (*Operation Technology*).

I primi sono i cosiddetti sistemi gestionali: posta, office e produttività individuale, mentre i secondi sono quelli che fanno "funzionare la fabbrica".

Tra i due domini, è evidente ci sono differenze sostanziali, che si riflettono anche sulla cyber security e sulle contromisure e metodi di protezione da adottare, poiché i rischi sono sostanzialmente differenti: nell'IT la security si occupa della protezione del dato, mentre per la parte OT è cruciale la difesa dell'asset produttivo (impianto o macchinario che sia) e la continuità operativa. Il rischio infatti fa riferimento sia alla Security che per alla Safety, ovvero proteggere l'integrità di persone, ambiente e impianti.

Un'altra differenza riguarda le superfici di attacco: per la IT è forse più facilmente definibile (anche se con l'avvento del Cloud e dei dispositivi mobile ora risulta più "liquida"). Per quanto riguarda la OT, la superficie di attacco è spesso "più larga" e labile, spesso distribuita geograficamente, in ogni caso composta da dispositivi più difficili da proteggere con gli strumenti tipici della security, in quanto non sono solo PC e server.

Anche le priorità risultano differenti, secondo i tipici dettami dei sistemi di gestione (tipo ISO27000 e simili): nell'IT abbiamo a scalare "riservatezza", "integrità" e infine "disponibilità". Nell'OT sono esattamente capovolti e abbiamo prime per importanza "disponibilità" e "integrità", e la "riservatezza" risulta spesso solo accessoria.

In effetti nell'agenda del CISO dell'azienda abbiamo ben in evidenza la difesa delle informazioni e dati di business, del sito web dell'azienda, la protezione della proprietà intellettuale (IP), la privacy e GDPR, la reputazione.

Per chi produce le maggiori preoccupazioni riguardano le performance dell'impianto, l'OEE, la *Supply-chain*, la tracciabilità e genealogia del prodotto, la continuità operativa ecc.

Security e data integrity nel Pharma

Ovunque, ma soprattutto nel mondo del Life Science, abbiamo un'interdipendenza diretta tra sistemi IT e OT: se l'impianto si ferma per un problema informatico, non si riesce a produrre, consegnare il prodotto, fatturare, e incassare. Ma in un'industria altamente regolamentata come quella del farmaco, anche se l'impianto produce a regime e per un problema cyber perdiamo i dati del prodotto, quel prodotto è come se "non esistesse" e i risvolti finali hanno ugualmente un impatto fragoroso sul business.

Diversi standard e in particolare le GAMP (Martin, Perez, 2008) (*Good Automated Manufacturing Practices*, ormai giunte alla versione 5 e corredate da numerose integrazioni con *Good Practices Guide* e altri documenti emessi dal GAMP Committee di ISPE a livello internazionale) e le ultime regolamentazioni sulla data integrity fanno menzione della security: spessò però si limitano agli aspetti del control-

lo accessi e non sempre ricordano che la security è uno dei capisaldi per garantire continuità operativa in produzione.

In particolare, quando si parla di "data integrity" si fa riferimento all'acronimo ALCOA (Smith, 2014), ovvero il dato "protetto e integro" deve avere una serie di caratteristiche e specifiche:

- "attibutable", ovvero chi l'ha generato e perché;
- "legible": deve essere nel tempo accessibile e consultabile;
- "contemporaneus": deve essere registrato nel momento in cui viene generato;
- "original": l'informazione deve essere autentica e originale, o una copia autentica;
- "accurate": senza errori, o nel caso di correzioni, con una documentazione dell'accesso.

Inoltre, sono state aggiunte anche queste altre caratteristiche per la data integrity:

- "complete": bisogna raccogliere e registrate TUTTI i dati dei test, anche le ripetizioni;
- "consistent": con "date/time stamp" progressivo;
- "enduring": se i dati devono essere memorizzati elettronicamente, i sistemi devono essere convalidati;
- "available": i dati devono essere sempre accessibili per revisioni e audit durante tutto il ciclo di vita.

Dobbiamo inoltre segnalare che nelle GAMP5 alcuni aspetti di "security" sono presenti anche nelle appendici operative:

- O3, Performance Monitoring;
- O4, Incident Management;
- O5, Corrective & Preventive Action;
- O6, Operational Change and Configuration Management;
- O8, Periodic Review;
- O9, Backup & Restore;
- O10, Business Continuity Management;
- Oltre naturalmente alla O1, Security Management.

ISA95, ISA99/IEC62443: IT *vs* OT Security

Lo standard ISA95 (2012) ci propone una gerarchia funzionale dei sistemi utilizzati nelle aziende di produzione. Partendo dal livello zero ove fisicamente si produce, abbiamo in sequenza:

- Livello 1: ove sono sensori e attuatori, oltre alla strumentazione di impianto;
- Livello 2: ove abbiamo controllori e supervisione di macchina e SCAD di impianto;
- Livello 3: ove si "gestisce la produzione" attraverso sistemi con funzioni di gestione ricetta, raccolta dati, schedulazione fine, sistemi MES (*Manufacturing Execution Systems*) e MOMS (*Manufacturing Operation Management Systems*), sistemi per analisi e ottimizzazione della produzione, manutenzione di impianto, calcolo efficienza/efficacia/OEE ecc.
- Livello 4: con MRP/ERP, pianificazione e gestione di tutto il ciclo produttivo.

Fino al Livello 3 abbiamo sistemi appartenenti al "dominio OT (*Operation Technology*), dal livello 4 in su i sistemi solitamente rientrano nel dominio IT (*Information Technology*).

Mentre di solito i sistemi IT sono ben presidiati in termini di cyber security, lo stesso non si può dire ancora per la parte OT: proprio per questa ragione ISA (Associazione internazionale per automazione e controllo, www.isa.org) ha costituito il Comitato ISA99, che ha iniziato a pubblicare i technical report e documenti che hanno portato allo standard internazionale IEC62443 (2009).

Alcuni dei capisaldi di tale standard IEC62443 sono la definizione di terminologia e modelli da utilizzare nella vita quotidiana dei responsabili di reti e sistemi di fabbrica: qui s'inizia con la considerazione che i sistemi in rete di fabbrica possono essere facilmente compromessi se hanno standard di protezione differenti tra loro. Meglio quindi avere un approccio di segmentazione della rete in zone, con presidi e device che possano gestire le comunicazioni in modo controllato, e segregare in zone DMZ gli asset critici come server e altri sistemi che raccolgono e smistano dati tra le differenti zone con criteri diversi e specifici di protezione.

Quali tool per la protezione di sistemi OT e quali standard?

Abbiamo accennato alla segmentazione in zone delle reti di fabbrica e segregazione degli asset informatici critici, mediante dispositivi attivi per permettere o meno la comunicazione tra sistemi differenti: utilizziamo quindi firewall e devices con funzioni IDS/IPS (*Intrusion detection & prevention*) e utilizzo di tool di protezione da malware e altre minacce.

Strumenti sempre più utilizzati e che si stanno molto evolvendo a livello di tecnologie e prestazioni/funzioni sono i cosiddetti sistemi per la rilevazione di anomalie (*Anomaly Detection*): questi sistemi sono in grado di "studiare" il comportamento della rete e dei sistemi che scambiano dati tra loro in rete, ed evidenziare quando avvengono comportamenti "non profilati" che potrebbero essere delle anomalie che evidenziano possibili attacchi o il sorgere di incidenti informatici.

A livello internazionale, la comunità della security è sempre attiva nello studio di procedure e strumenti per contrastare attacchi e incidenti. Vengono quindi proposti e approvati standard e best practice per la protezione dei sistemi in produzione. Oltre al già citato Standard IEC62443 (in aggiornamento e completamento) e le *Good Practice Guide* delle GAMP, possiamo anche menzionare alcuni interessanti documenti rilasciati dal NIST USA (*National Institute of Standard and Technology*, dello US Department of Commerce):

- NIST SP 800-53 (2008): *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*;
- NIST SP 800-82 (2008): *Guide to Industrial Control Systems* (ICS) *Security.*

E possiamo aggiungere anche questi, molto pertinenti con le architetture di sistemi più evolute che contemplano IOT (*Internet of Things*) e *Cloud Computing*:

- NIST SP 800-183 (2016): *Network of "Things" (Computer Security)*;
- NIST SP 800-144 (2011): *Guidelines on Security and Privacy in Public Cloud Computing.*

La security IoT e IIoT (*Internet of Things*, e *Industrial Internet of Things*)

Proprio sul tema IoT Security, NIST a inizio 2018 ha pubblicato (con la richiesta di commenti) in bozza il report NIST IR8200 *Interagency Report on Status of International CyberSecurity Standardization for the Internet of Things* (IoT), che riporta alcuni concetti e soprattutto alcuni esempi di come la IOT può avere impatti anche nel settore della salute e cura pazienti.

Si parte dal presupposto che non sempre gli scopi della security sono coincidenti con quelli della tutela della privacy, in particolare per tutti quei casi che possano coinvolgere informazioni che portino all'identificazione della persona (PII, *Personally Identifiable Information*).

Inoltre le priorità dei requisiti per la IoT/IIoT (sopra abbiamo già ricordato le differenti priorità tra IT e OT) sono ancora differenti da quelli tipici dell'IT: per l'IoT si deve partire dall'autenticazione dell'oggetto/dispositivo collegato in Internet, si passa poi per i requisiti tipici dell'IT come *Availability, Confidentiality & Integrity*, per aggiungere anche la "non-repudiation", per evidenti possibili impatti a livello di responsabilità e tracciabilità riferito a dati generati e azioni espletate dall'oggetto collegato in rete.

Seguono nel report NIST interessanti considerazioni sia sulle applicazioni riportate come esempi dell'IoT in molti settori di utilizzo quotidiano, come ad esempio veicoli connessi, smart city e smart building, medicina di precisioni, smart factory ecc. Per ogni esempio vengono identificati i fattori critici e ove sia necessario approfondire gli impatti, rischi e contromisure da adottare.

Conclusioni

Siamo già in un mondo connesso e stiamo ulteriormente proseguendo sulla strada di una maggiore interconnessione tra sistemi tra solo differenti.

Industria 4.0/Phrama4.0, Cloud e IoT non possono prescindere dal tema della cyber security: la protezione deve essere pensata e "messa dentro" sin dall'inizio dello studio e implementazione dei sistemi e sottosistemi tra solo collegati.

Le minacce delle quali siamo al corrente oggi, potrebbero non essere più attive domani, e potrebbero però prossimamente ripresentarsi, anche in forma differente: sistemi pensati con criteri di resilienza e di "riconoscimento" di anomalie potranno sicuramente aiutarci nel garantire continuità di funzionamento e produzione secondo gli standard qualitativi definiti, e la tecnologia in evoluzione ci darà un mano in questa direzione.

Bibliografia

International Electrotechnical Commission. *IEC 62443: Industrial communication networks-network and system security-security for industrial automation and control systems*, 2009.

ISA-95. *ISA-95: the international standard for the integration of enterprise and control systems*, 2012.

Martin KC, Perez A. *GAMP 5 quality risk management approach*. Pharmaceut Engin 2008;28:24.

NIST SP. *800 82: Guide to Industrial Control Systems (ICS) Security.* Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), 2008.

NIST SP. *800-144. DRAFT Guidelines on Security and Privacy in Public Cloud Computing*, 2011.

NIST SP. *800-53. Recommended Security Controls for Federal Information Systems*, 2003, pp. 800-53.

Smith P. *Data integrity in the analytical laboratory.* Pharmaceut Technol 2014;38:58-60.

Voas J. *Networks of 'Things' (NIST Special Publication 800-183).* National Institute of Standards and Technology, 2016, p. 30.