ServiTecno
Technology 4.0 da 40 anni

La Safety incontra la Security: istruzioni per produttori di Macchine

(con riferimento a ISO/TR22100-4:2018, ISO12100 e Direttiva Macchine 2006/42/CE)

1979-2019 TECHNOLOGY 4.0 DA 40 ANNI
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

SOMMARIO

Introduzione

Ad inizio anno 2019, ISO, International Organization for Standardization, l'organizzazione internazionale per le normative dei settori industriali, ha emesso un documento ISO/TR Technical Report denominato "**ISO/TR 22100-4:2018, *Safety of Machinery*** – *Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*".


TECHNICAL REPORT

ISO/TR 22100-4

First edition
2018-12

Safety of machinery — Relationship with ISO 12100 —

Part 4:
Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

ISO

Reference number
ISO/TR 22100-4:2018(E)

© ISO 2018

In pratica si tratta di un **nuovo standard di sicurezza** (che a questo punto riguarda sia la Safety che la Security) **per macchinari, impianti ed Industrial of Things industriale (IIoT)** utilizzati in ogni settore dall'industria, al commercio, a trasporti e logistica, fino alle infrastrutture ed utility. Il documento è stato discusso e sviluppato dal comitato tecnico sulla standardizzazione di ISO/TC199.

Per la prima volta ISO ha inteso mettere nero su bianco che la sicurezza informatica non si applica solo ai dati, e riguarda anche alla Safety, ovvero a tutto ciò di reale che entra in contatto col mondo virtuale, compresi quindi i macchinari industriali.

Per la sicurezza di un macchinario "intelligente" sono richieste tecnologie "intelligenti". I dispositivi intelligenti sono esposti a minaccia di incidenti ed attacchi informatici, e non solo Internet of Things (IoT) in generale, ma anche i sistemi apparentemente isolati.

La Security informatica per la Safety dei macchinari

Il **rapporto tecnico ISO/TR 22100-4:2018** ci dà una classificazione di regolamentazione e normative ed una base fondamentale alla quale dovrebbe attenersi il produttore del macchinario.

Nell'attuale discussione sulle nuove tecnologie da impiagare per la digitalizzazione negli impianti produttivi, anche in vista di Industria 4.0, svolge un ruolo speciale la valutazione per gli effetti che incidenti ed attacchi alla sicurezza cyber possono avere sulla Safety di macchinari ed impianti.

Al fine di rendere oggettivo l'argomento, il **comitato di ISO/TC199 per la "Sicurezza dei macchinari" ha deciso di completare l'opera rilasciando questo ISO/TR22100-4:2018** a totale complemento, anche richiamato nel titolo, dello standard ISO12100.

L'obiettivo è quello di fornire al costruttore del macchinario un'assistenza pratica e propedeutica alla immissione sul mercato e consegna all'utilizzatore finale del macchinario stesso (analogo a quanto contenuto nella Direttiva).

Confronto tra Safety e Cyber Security

Grazie ad un confronto, viene dimostrato che gli argomenti, **Safety e Security**, **sono lontani** per quanto riguarda i loro **obiettivi**, le condizioni quadro (**rischi, metodi / misure**), le **dinamiche** e gli **attori coinvolti**.

Struttura del documento ISO/TR22100-4:2018

Il documento in oggetto, come tutte le norme/standard dopo la definizione di scopo ed altre norme di riferimento, da un accurato elenco di termini e definizioni, partendo da quelle già dichiarate nel richiamato **ISO12100**, specifiche della IT cyber Security.

Seguono quindi delle **tabelle ove sono evidenziati ed inquadrati gli obiettivi della Safety e della IT security** (cyber security) ed a seguire gli elementi di differenziazione tra le due discipline in questione: elementi di rischio, conseguenze per la valutazione del rischio.

Altri capitoli e parti del documento sono illustrati qui di seguito.

Inquadramento legale per la sicurezza del macchinario

Ciò che è importante per un assessment iniziale è la corretta classificazione dell'argomento rispetto alle attuali condizioni e normative vigenti.

La Direttiva Macchine 2006/42/CE è richiamata come "example of legal framework" nell'Allegato A della ISO/TR22100-4.
Come per altre disposizioni legislative nazionali sulla sicurezza dei macchinari (valide al di fuori dell'UE), **l'approccio della Direttiva Macchine 2006/42/CE è limitato esclusivamente a**:
- **uso PREVISTO** (intended use, come definito dal produttore) e
- **uso SCORRETTO** ragionevolmente prevedibile (reasonably foreseeable misuse) da parte dell'operatore.

Si può quindi sostenere che qualsiasi manipolazione non autorizzata da parte di terzi, che possa essere classificata come un attacco di cyber (atto criminoso de facto), NON rientra nella Direttiva Macchine **2006/42/CE**. Lo stesso vale per la standardizzazione per la sicurezza dei macchinari, poiché i principi di progettazione stabiliti nella **(EN) ISO 12100** corrispondono all'approccio contenuto nella Direttiva Macchine 2006/42/CE.
Nonostante ciò, i **fabbricanti di macchinari esposti a vulnerabilità per attacchi cyber a causa della rete alla quale il macchinario verrà connesso**, dovrebbero tenere conto dei possibili effetti sulla Safety di tali macchinari, nel momento e nella misura in cui la macchina verrà immessa sul mercato per la prima volta.

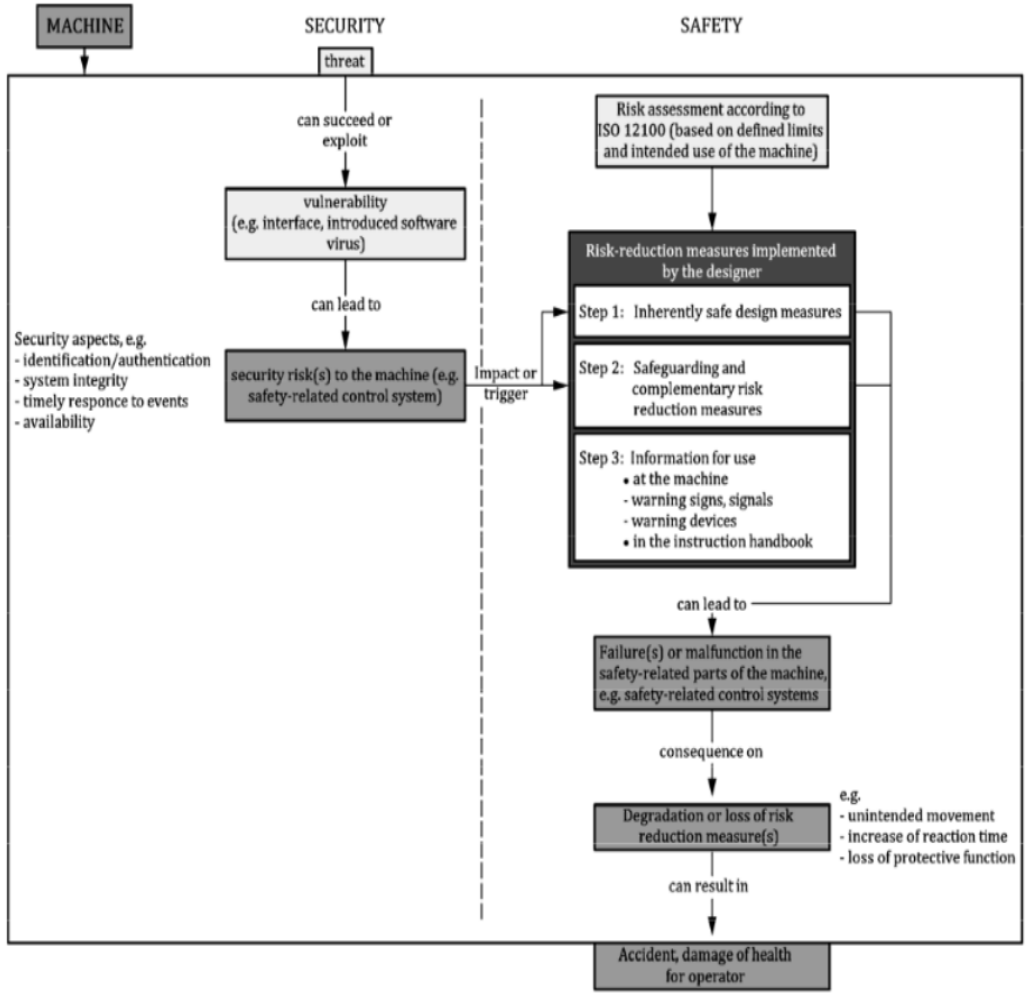
Relazione tra Safety del macchinario e Cyber Security

La figura mostra come **gli attacchi di Cyber Security possano NON rappresentare un'ulteriore minaccia in termini di Safety dei macchinari** (e quindi anche in conformità con la Direttiva Macchine 2006/42/CE).
Incidenti Cyber possono però generare il fatto che le misure di Safety previste ed implementate sul macchinario vengano compromesse o messe fuori servizio. Quindi ha senso effettuare un'attenta valutazione del rischio per la Safety del macchinario in conformità con lo standard **(EN) ISO 12100** prima di considerazioni dettagliate in merito alla sicurezza informatica.

Ne risulta che, in conformità **con (EN) ISO 12100** si dovrebbe a priori controllare se vulnerabilità a potenziali attacchi/incidenti Cyber possano diminuire la Safety e quindi, se necessario, adottare:

- **soluzioni di Safety intrinseche**
- **altre misure tecniche supplementari di protezione** (misure di mitigazione dei rischi)

Relationship between safety of machinery and cybersecurity



Source: ISO/TR 22100-4:2018

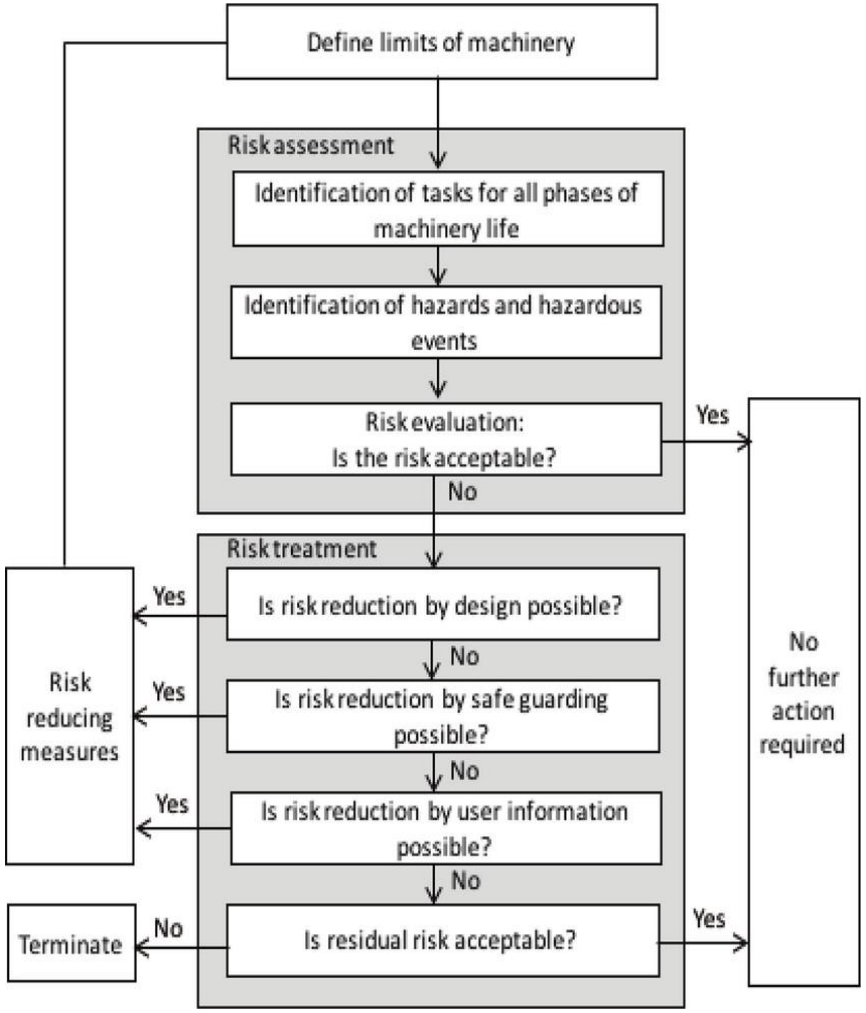
Valutazione del Rischio Safety e Rischio Cyber

Come abbiamo detto, la valutazione del rischio Safety di un macchinario secondo quanto previsto nella **ISO12100** deve precedere ogni considerazione sul rischio attacco/incidente cyber: quindi **dopo aver "messo in sicurezza safety" un macchinario con azioni e misure di mitigazione del rischio safety, il macchinario dovrebbe essere valutato per eventuali esposizioni alle minacce cyber**.

Ne risulta che il rischio cyber può essere mitigato con uno sforzo combinato da parte di fornitori dei componenti, costruttore del macchinario, il system integrator ed anche l'utilizzatore del macchinario.
Come detto nella **ISO12100**, è quindi necessario seguire la seguente gerarchia per la mitigazione del rischio:

- **Eliminare "by design" il rischio** per la security (evitare le vulnerabilità)
- **Mitigare il rischio per la security** con misure di riduzione del rischio (mitigare e limitare le vulnerabilità)
- **Dare** all'utilizzatore **informazioni sul "rischio residuo"** e di eventuali ulteriori misure da adottare

.



Chi deve fare cosa per la IT security che possa avere rilevanza sulla Safety: RUOLI

Il rischio IT che può influenzare la Safety dei macchinari evolve in continuazione durante tutto il ciclo di vita del macchinario, come d'altronde evolvono anche le contromisure da adottare ed adottate.
Considerando il ciclo di vita del macchinario, vengono definiti nel **ISO/TR22100-4:2018** diversi ruoli ed attività che spettano ad ogni singolo ruolo.

Abbiamo quindi il costruttore del macchinario, l'integratore e l'utilizzatore/utente finale.
Il costruttore del macchinario è responsabile anche della scelta del componente acquistato dal fornitore.
Nella **tabella 3 del ISO/TR20100-4:2018** viene riportato un lungo elenco di esempi di misure per la mitigazione del rischio per ridurre minacce IT/cyber che possano avere influenza sulla Safety del macchinario, suddivise per ruolo (Costruttore, Integratore, End-User)

Quali sono le possibili vulnerabilità e le misure per mitigarle

È ovvio che le vulnerabilità IT, ovvero nei confronti di attacchi/incidenti informatici, dipendono molto dal fatto se il macchinario possa essere connesso a sistemi IT esterni e quanto spesso possa avvenire. Ecco allora alcune domande da porsi per aiutare a limitare minacce e vulnerabilità IT:

ci chiediamo se il macchinario…

- **deve essere connesso**?
- deve restare **connesso sempre**?
- ne **viene monitorata la connessione**? (ad esempio, si utilizza VPN, virtual private network)
- la **connessione è configurabile**? (ad esempio, ristretta solo a persone autorizzate)
- la **connessione può essere "read only"?** (senza la possibilità di inviare variazioni o comandi)

Ne consegue che un macchinario senza interfacce dirette o indirette a sistemi IT esterni, possa essere considerato "non vulnerabile" ad attacchi/incidenti di IT cyber security. *
* N.B.: questo è quanto è scritto su **ISO/TR22100-4:2018** al punto 6. Sono però noti alcuni incidenti accaduti che possono mettere in dubbio questa affermazione.

Passi essenziali per la sicurezza IT durante tutto il ciclo di vita del macchinario

Come abbiamo detto, minacce e vulnerabilità IT richiedono la cooperazione e coordinazione tra fornitore dei componenti, produttore del macchinario, system integrator ed utilizzatore finale.

Ognuno ha un ruolo per prevenire attacchi/incidenti IT, durante tutte le fasi del ciclo di vita del macchinario e non si possono passare ad altri le proprie responsabilità e non si può addossare ad uno solo la responsabilità globale per la IT cyber security come d'altronde nessuno degli attori conosce tutte le informazioni disponibili per adeguata protezione IT del macchinario.

I 5 PASSI:

- Identificare
- Proteggere
- Visibilità
- Risposta
- Ripartenza

I 5 PASSI NEL DETTAGLIO

Ecco i cinque passi essenziali che produttore e integratore devono applicare per migliorare security e resilienza del macchinario.

Identificare:

- quali sono minacce e vulnerabilità per la IT security?
- perché dovrebbero mai attaccare il macchinario?
- cosa può avere l'utilizzatore di così prezioso?
- quali sono le porte/interfacce verso l'esterno?
- …

Proteggere:

- progettare e implementare contromisure appropriate per proteggere il macchinario

Visibilità:

- Prevedere e implementare adeguate misure per identificare un possibile attacco/incidente cyber (ad esempio monitoring e anomaly detection rete e sistema)

Risposta:

- Prevedere e implementare azioni adeguate da prendere in caso della scoperta di attacco/incidente cyber (possibilità di fermare o di contenere l'impatto negativo)

Ripartenza:

- Prevedere e implementare azioni adeguate a mantenere "resiliente" l'impianto, attivo e/o con possibilità di ripartenza in tempi brevi in caso di attacco/incidente cyber (emergency/recovery plan)

Raccomandazioni concrete per il produttore del macchinario

Le minacce di sicurezza informatica rilevanti per la Safety dei macchinari sono soggette a molti cambiamenti dinamici durante l'intero ciclo di vita di una macchina ("target mobile"). Lo stesso vale per le contromisure idonee / richieste.
D'altronde l'attenzione del produttore del macchinario si concentra nella fase di sviluppo e progettazione fino a quando la macchina viene immessa sul mercato per la prima volta**. Con riferimento a questo punto nel tempo, la ISO / TR 22100-4 contiene raccomandazioni concrete per il costruttore del macchinario, ovvero, nelle diverse fasi**:

• Nel **selezionare componenti adeguati** (sia hardware che software); le componenti relative alla Security che potrebbero essere potenzialmente gli obiettivi per gli attacchi/incidenti cyber dovrebbero avere un livello di sicurezza IT allo stato dell'arte, al fine di ridurre al minimo la vulnerabilità agli attacchi/incidenti cyber, valutare strumenti per controllo accessi, integrità del software, integrità dei dati, aggiornamenti del software, comunicazioni criptate, ecc.

• Nello **Sviluppare / progettare l'intera macchina**; conformità ai principi / alle misure di base volte a ridurre al minimo la vulnerabilità agli attacchi/incidenti cyber; prevedere una modalità di emergenza (trasferimento del macchinario in uno stato operativo sicuro nel caso in cui le funzioni di sicurezza critiche del macchinario siano limitate o rese inefficaci da un attacco/incidente cyber), attrezzare la macchina con dispositivi per un'adeguata protezione delle connessioni, ecc.

• Nello **stilare le istruzioni operative** (manuali per l'utilizzo); informazioni per l'operatore del macchinario dovranno contenere indicazioni su possibili rischi basati su potenziali minacce alla sicurezza informatica legate alla Safety del macchinario, gestione delle connessioni locali e remote, accessi al sistema, manutenzione in locale e da remoto, aggiornamenti del software, come agire in caso di problemi di cyber security IT, messa in stand-by, ripartenze, ecc.

CONCLUSIONI

Nel mondo iper-connesso, e quindi anche nelle fabbriche, la sicurezza IT copre non solo i nostri dati ma praticamente tutto ciò che si muove, inclusi i macchinari.

Gli attacchi informatici o malfunzionamenti IT nel Process & Manufacturing possono comportare rischi per le misure di Safety in atto, con un conseguente impatto sulla produzione, sugli impianti stessi, sulle persone e sull'ambiente. In questo documento **ISO / TR 22100-4:2018** sono stati pubblicati i nuovi orientamenti internazionali per identificare e affrontare tali rischi.

Industria4.0, Smart Manufacturing ovvero quella che sfrutta Internet e la tecnologia digitale, consente una produzione e un'integrazione senza soluzione di continuità lungo l'intera catena del valore. Consente inoltre di controllare i parametri, come ad esempio variabili come velocità, forza, pressioni, livelli e temperatura, da remoto.
I vantaggi sono molti, sicuramente la possibilità di tenere traccia di prestazioni, consumi, utilizzo e migliorare l'efficienza di macchinari ed impianti, ma esacerba anche il rischio di minacce alla sicurezza IT.

CONCLUSIONI

Aumentare la velocità o la forza di una macchina a livelli pericolosi, o variare le temperature di cottura o conservazione per provocare la contaminazione degli alimenti, sono solo alcuni esempi, riportati nel documento **ISO/TR22200-4:2018**, di come gli attacchi informatici possono non solo interrompere la produzione ma comportare seri rischi per noi. Questo nuovo documento ISO (TR) è stato pubblicato proprio per aiutare i produttori di macchinari a prepararsi e mitigare questi rischi.

ISO/TR 22100-4 ***"Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machine manufacturers for consideration of related IT-security (cyber security) aspects"*** infatti aiuta i produttori di macchinari a identificare e affrontare le minacce alla sicurezza IT che possono impatto sulla Safety del loro prodotto. Arriva e completa **lo standard di punta ISO per la sicurezza delle macchine, la ISO -12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*, che definisce i fondamenti per "risk assessment, hazard analysis" ed i requisiti documentali**.

Otto Görnemann, Presidente del comitato tecnico ISO responsabile della relazione tecnica, ha affermato: ***"Safety dei macchinari e la Cyber Security differiscono notevolmente per quanto riguarda obiettivi, metodi e le misure, ma in fabbrica sono inestricabilmente collegate.***
La ISO/TR 22100-4:2018 aiuterà i produttori di macchine a stringere la relazione tra sicurezza informatica e Safety delle macchine. Verranno quindi trattati aspetti quali i tipi di componenti che potrebbero essere potenziali bersagli per gli attacchi/incidenti cyber, la progettazione della macchina per ridurre al minimo vulnerabilità a tali attacchi e informazioni per l'operatore della macchina su possibili minacce".

Biografia e web

- ISO/TR 22100-4:2018 Safety of machinery -- Relationship with ISO 12100 -- Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects –
- https://www.iso.org/obp/ui/#iso:std:iso:tr:22100:-4:ed-1:v1:en
- https://www.ap-publishing.com/sicurezza-macchine-impianti/iso-tr-22100-4-la-sicurezza-dei-macchinari-dipende-anche-dalla-sicurezza-informatica/https://www.ap-publishing.com/sicurezza-macchine-impianti/nuova-iso-121002010/
- https://vdmaimpulse.org/article/-/article/render/203015
- http://tadviser.com/index.php/Article:ISO/TR_22100-4:2018_Security_of_a_production_equipment_%E2%80%93_Communication_with_ISO_12100_is_Part_4
- https://normung.vdma.org/en/viewer/-/v2article/render/26630426
- https://premiumresourcenetworkltd.com/information-security-management/smart-manufacturing-new-iso-guidance-to-reduce-the-risks-of-cyber-attacks-on-machinery/
- https://www.kan.de/en/publications/kanbrief/digitalization-and-industry-40/aspects-of-safety-and-security-in-the-emergence-of-industrie-40/
- https://www.theauditoronline.com/new-technical-report-to-mitigate-the-risk-of-cyber-attacks/
- http://www.sustainingedge.com/risks-of-cyber-attacks-on-machinery/

Appendice 1: Attacchi informatici, chiusura linee produzione in fabbrica con ricadute in Borsa e sul prezzo della materia prima

E' notizia di Marzo 2019 l'attacco informatico al colosso dell'alluminio Norsk Hydro: l'Azienda, uno dei maggiori produttori di alluminio a livello globale, è stata vittima di un attacco hacker, che ha portato progressivamente nei giorni seguenti ad una paralisi dell'attività

Un *ransomware* (un blocco dei sistemi IT con richiesta di riscatto, che ha poi coinvolto anche i sistemi OT) ha preso di mira i sistemi IT del gruppo norvegese con impianti distribuiti in diversi continenti, interessando varie sedi nel mondo.

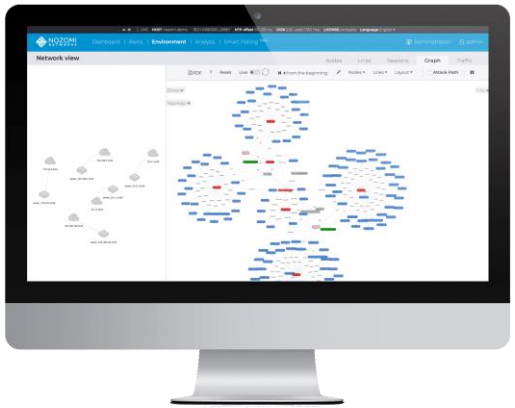
Si sono bloccati prima i computer negli uffici per poi arrivare fino bloccare alcuni sistemi di automazione e controllo su alcune linee di estrusione e di laminazione prodotti in alluminio.

L'Azienda ha dovuto fermare alcune linee di produzione fino a dover chiudere temporaneamente gli impianti di trasformazione dei metalli. Gli impianti di estrusione hanno potuto continuare la produzione con controllo in modo manuale. Fortunatamente l'attacco non ha toccato i sistemi di controllo nella produzione e distribuzione di energia nè i forni di fusione, e non si sono verificati rischi per incolumità e salute dei lavoratori ma sicuramente ci sono state pesanti ricadute sulla produzione e sulle consegne ai Clienti.

Nei giorni seguenti l'incidente, all'apertura dei mercati finanziari, il titolo in borsa del gruppo Norsk Hydro ha perso diversi punti ed il prezzo dell'alluminio è salito su tutti i mercati dei metalli.

Con questi incidenti e con quelli degli anni precedenti (quali ad esempio Cryptolocker nel 2016-7, WannaCry e Pethya nel 2017-8) si è visto quindi che la vulnerabilità di un sistema ai malware (in questi casi dei ransomware) comporta importanti interruzioni di produzione e di servizi con impatti spesso significativi sia in termini monetari che di immagine.

Appendice 2: Alcune soluzioni ServiTecno per la OT Security e la mitigazione dei rischi informatici con impatto sulla Safety.



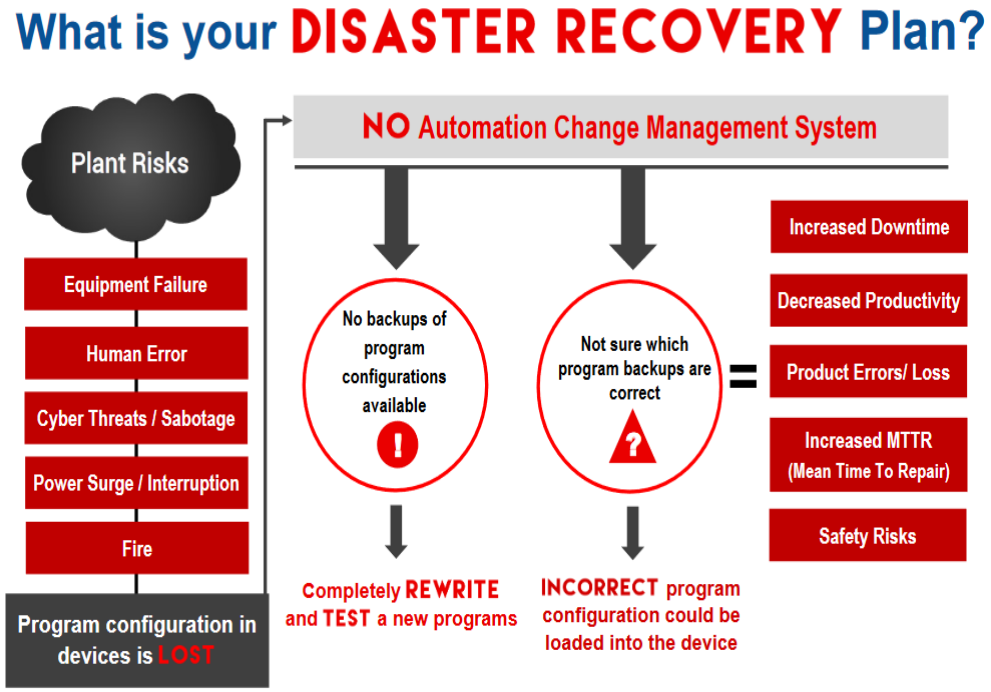
OT CyberSecurity a prova di ISO/TR22100-4:2018 e Direttiva Macchine 2006/42/CE
Uno dei punti cardini di ISO/TR22100-4:2018 è quello di incentivare l'attenzione nei confronti del rischio cyber, che potrebbe portare problemi di safety sulla macchina/impianto.
È necessario quindi da parte dei Machine Manufacturer porre attenzione particolare riguardo agli aspetti della continuità operativa e protezione da rischi informatici proprio in ambito sistemi OT (Operation Technology).
Sistemi di controllo macchina/impianto e reti industriali, un tempo considerate sicure perché fisicamente separate dal "resto del mondo" e costruite su protocolli proprietari, **sono diventate uno dei punti deboli sui quali le aziende di produzione devono intervenire**.

Un **primo step**, per esempio, dovrebbe essere il **monitoraggio delle attività della rete** per avere visibilità su eventuali attacchi/incidenti informatici
Un'anomalia del traffico potrebbe infatti essere **indice di un malfunzionamento o anche di un sabotaggio** indotto da un'intrusione non autorizzata nei sistemi di controllo o in quelli dell'Azienda.
I sistemi di monitoraggio dell'infrastruttura di rete e dei sistemi OT, come quello sviluppato da Nozomi Networks, oltre a dare visibilità su quanto avviene, forniscono funzioni di Anomaly Detection, e possono rappresentare un **buon livello di "early warning"** a protezione di reti e sistemi di controllo e a tutela dell'impianto controllato.

Si tratta soluzioni che fanno una mappatura completa della macchina e della rete alla quale viene connessa, identificando esattamente ogni singolo componente, che tipo, marca e modello sia, la versione del firmware e del software utilizzato, le regole di comunicazione, analizzano le relazioni tra i vari device, terminali ed altri dispositivi (PLC, RTU, switch, router, ecc.) partecipanti alla rete e i volumi di traffico, aiutando a definire le regole di una comunicazione "normale" , protocolli ammessi, porte e "conduit" da monitorare con attenzione, e, di conseguenza, a riconoscere eventuali comunicazioni e comportamenti illegittimi, connessioni non previste, dispositivi non aggiornati, regole di firewalling dubbie, mancanti o inutili, e molto altro.
In pratica permettono di avere sotto controllo tutta l'infrastruttura, ed in modo assolutamente passivo, accorgersi se ci siano in atto attacchi o malfunzionamenti sia dell'infrastruttura che nei dispositivi collegati.

La visibility sugli Asset, controllo configurazione e backup software a bordo macchina

Un tema critico per i sistemi di controllo di macchine ed impianti è poi quello legato alla gestione di asset (per esempio PLC, HMI-SCADA, robot, ICS, DCS, PC, server, switch, firewall, ma non solo) sempre più numerosi e distribuiti, spesso governati da firmware e software da aggiornare periodicamente o sporadicamente, con team di manutenzione a volte di terze parti ed operatori specializzati che si devono occupare di un parco installato molto variegato che richiede molte competenze diverse e costante attenzione per essere mantenuto con documentazione aggiornata ed attività controllata. Per non parlare di regolamentazione e relativa compliance, come ad esempio a ISO/TR22100-4:2018 e Direttiva Macchine 2006/42/CE
Per avere un'effettiva capacità di gestione di questi asset è importante dotarsi di **tool che tengano traccia di tutte le variazioni e conservano copia di backup di tutte le versioni degli applicativi installati**.
In questo modo, **in caso si renda necessario un ripristino a seguito di un guasto, incidente o di un attacco informatico**, sarà possibile **ripristinare il sistema in pochissimo tempo**, guadagnando preziose ore (se non giorni) in produzione e/o continuità nell'erogazione di servizio.



Un sistema come **MDT AutoSave Software, permette inoltre anche di rilevare eventuali differenze tra il runtime in esecuzione su un controllore e quello che "dovrebbe" esserci**, permettendo così di prevenire eventuali alterazioni del codice macchina ad opera di sabotatori, come già in passato si è verificato (ad esempio con Stuxnet nel 2010 ed in seguito in altri episodi, anche recenti, riportati su stampa e web).

Sistema di controllo macchinario: “SCADA tradizionale”, “SCADA ridondato” e “SCADA H.A.”

SCADA H.A. significa Sistema SCADA High Availability, SCADA ad Alta Disponibilità.
L’idea che sottende ad un sistema di controllo con SCADA H.A. è che per gestire, monitorare e supervisionare un macchinario o impianto che deve funzionare “senza interruzioni”, sia necessario un sistema di controllo che garantisca il massimo uptime e funzioni a sua volta “senza interruzioni”.
Utilizzato in numerose applicazioni realizzate in molti settori industriali, **lo SCADA iFIX di GE Digital** è utilizzato nei sistemi di automazione, controllo e telecontrollo, sia per applicazioni semplici su singolo macchinario, sia per applicazioni **SCADA** complesse e distribuite, come funzionalità di controllo distribuito, con anche analytics con aggregazione di dati (Big Data) e filtrazione e gestione distribuita degli allarmi.
iFix Soddisfa gli **standard industriali** di molteplici settori, sia nell’industria che nelle utility, ed è ideale se integrato con i sistemi di storicizzazione (come l’Historian integrato) e nell’ottica di una gestione estremamente informatizzata, secondo i canoni della Digitalizzazione4.0, industrial internet ed Industrial IoT (Internet of Things).

Il pacchetto software HMI/SCADA iFix di GE Digital, distribuito e supportato in Italia da ServiTecno (https://www.servitecno.it/prodotti/ge-ifix-hmi-scada/) è da sempre sinonimo di grande affidabilità ed è universalmente utilizzato in sistemi SCADA e applicazioni critiche sia nel mondo industriale che in quello delle utility.

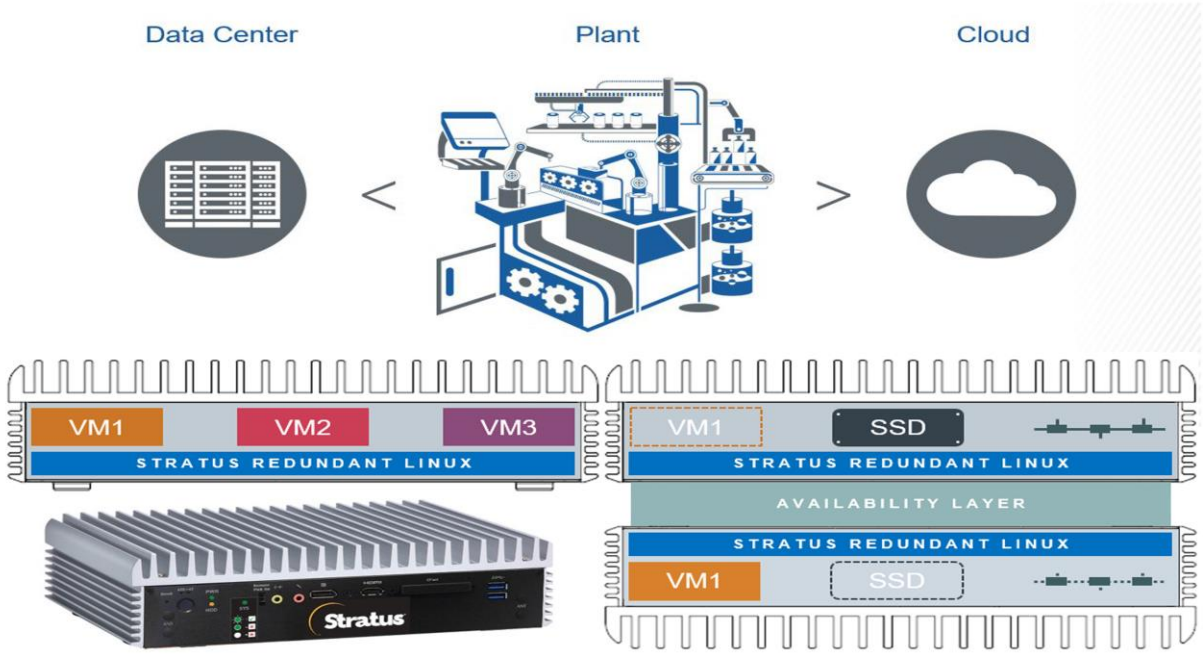
La Versione 6.0, innovativa per le eccellenti capacità di visualizzazione dei processi e di acquisizione dati, analisi, SUPERVISIONE e CONTROLLO aggiunge nuove ed avanzate prestazioni grafiche in ottica UX (User Experience, anche utilizzabili da dispositivi mobile), scalabilità e migliore manutenibilità, oltre alle più che testate e riconosciute affidabilità e sicurezza.

Sistema di controllo macchinario: “SCADA tradizionale”, “SCADA ridondato” e “SCADA H.A.”

Nel caso in cui sia richiesto, lo SCADA iFix prevede e supporta configurazioni SCADA ridondate, master/slave, con opzioni/funzioni di Fail-Over: abbiamo allora una coppia di server in configurazione ridondata, denominati uno Master ed il secondo Slave di back-up, collegati direttamente tra loro, per essere mantenuti allineati nei dati, eventi ed allarmi rilevati dal campo, oltre naturalmente a tutti i comandi dell’operatore.
In caso di anomalie ed eventuale caduta del server Master, il server slave di back-up subentra a tutti gli effetti nella funzione di controllo e supervisione, in modo da garantire la continuità di funzionamento ed operatività sul sistema SCADA.
Lo switch-over, il subentro da un sistema all’altro è configurabile con un watch-dog e può avvenire anche in termini di qualche secondo.
Questa soluzione sviluppata solo con le funzionalità insite in iFix, prescinde da eventuali problemi hardware e/o di sistema operativo che si potrebbero verificare e che potrebbero eventualmente inficiare la corretta funzionalità del sistema di controllo a bordo macchina e dello SCADA.

Sistemi di controllo macchine pensati per il 99,999% di Uptime e la Continuità Operativa

ztC Edge di Stratus Technology, è un sistema di computer "edge" per il controllo in locale di macchinari e possibilità di interfacciarsi con applicazioni in Cloud: **ztC Edge** è stato progettato per aiutare le aziende ad aumentare l'efficienza degli operatori, ridurre i costi e i tempi di fermo macchina. Questa soluzione si installa in meno di un'ora e può essere gestita completamente da remoto, riducendo significativamente gli sforzi normalmente richiesti all'IT per mettere in funzione una soluzione per sistemi di automazione e controllo a bordo macchina e l'elaborazione dei dati sul campo. Le funzionalità di autoprotezione e autocontrollo contribuiscono a ridurre i downtime non previsti e ad assicurare la massima disponibilità nelle applicazioni industriali business-critical. **ztC Edge** è fornito con una piattaforma di virtualizzazione integrata chiamata **Stratus Redundant Linux**: basata sul progetto open source KVM, è in grado di eseguire **fino a 3 macchine virtuali separate**, ognuna con differenti applicazioni di controllo industriale o IIoT.



Uno strumento di gestione, la ztC Console, semplifica l'impostazione, la configurazione e la gestione delle macchine virtuali, raggiungendo **l'ALTA DISPONIBILITA'** e fornendo in contemporanea la **"tecnologia ponte" per andare nel Cloud** e manutenzione da remoto
ztC Edge è composto da nodi ridondanti che agiscono come un unico sistema. Grazie a funzionalità come la migrazione VM live, la replica dei dati e il networking ridondante, offre istantaneamente protezione di dati e applicazioni. Il sistema può spostare in modo proattivo le macchine virtuali da un nodo all'altro, per garantire la continuità dell'applicazione: per sicurezza, i nodi **ztC Edge** possono essere fisicamente separati e a distanza, anche fino a 40 km (se la rete consente una latenza massima di 10 ms per la trasmissione bidirezionale dei dati). Se si rileva un guasto della rete o del disco su un nodo, reindirizza automaticamente il traffico o utilizza i dati sull'altro nodo, senza alcun intervento da parte dell'operatore. Le applicazioni in esecuzione in una posizione possono essere proseguite in un'altra location, con interruzione del servizio minima e in totale autonomia, garantendo il ripristino dei dati senza intervento dell'operatore.

Appendice 1: Attacchi informatici, chiusura linee produzione in fabbrica con ricadute in Borsa e sul prezzo della materia prima

E' notizia di Marzo 2019 l'attacco informatico al colosso dell'alluminio Norsk Hydro: l'Azienda, uno dei maggiori produttori di alluminio a livello globale, è stata vittima di un attacco hacker, che ha portato progressivamente nei giorni seguenti ad una paralisi dell'attività

Un *ransomware* (un blocco dei sistemi IT con richiesta di riscatto, che ha poi coinvolto anche i sistemi OT) ha preso di mira i sistemi IT del gruppo norvegese con impianti distribuiti in diversi continenti, interessando varie sedi nel mondo.

Si sono bloccati prima i computer negli uffici per poi arrivare fino bloccare alcuni sistemi di automazione e controllo su alcune linee di estrusione e di laminazione prodotti in alluminio.

L'Azienda ha dovuto fermare alcune linee di produzione fino a dover chiudere temporaneamente gli impianti di trasformazione dei metalli. Gli impianti di estrusione hanno potuto continuare la produzione con controllo in modo manuale. Fortunatamente l'attacco non ha toccato i sistemi di controllo nella produzione e distribuzione di energia nè i forni di fusione, e non si sono verificati rischi per incolumità e salute dei lavoratori ma sicuramente ci sono state pesanti ricadute sulla produzione e sulle consegne ai Clienti.

Nei giorni seguenti l'incidente, all'apertura dei mercati finanziari, il titolo in borsa del gruppo Norsk Hydro ha perso diversi punti ed il prezzo dell'alluminio è salito su tutti i mercati dei metalli.

Con questi incidenti e con quelli degli anni precedenti (quali ad esempio Cryptolocker nel 2016-7, WannaCry e Pethya nel 2017-8) si è visto quindi che la vulnerabilità di un sistema ai malware (in questi casi dei ransomware) comporta importanti interruzioni di produzione e di servizi con impatti spesso significativi sia in termini monetari che di immagine.