



La Progettazione Meccanica nell'era 4.0

Il quadro normativo

Ing. Giovanni TABASSO
*Commissione Meccanica Industriale
Ordine degli Ingegneri della Provincia di Roma*

Roma, 30 maggio 2024



UNI EN ISO 12100

- NORMA DI TIPO A
- Principi generali di progettazione del macchinario
- Strategia per la valutazione del rischio e la sua riduzione
- Base per norme di tipo B e C



UNI EN ISO 12100

FASI DELLA VALUTAZIONE DEL RISCHIO

- Determinazione dei limiti della macchina
- Identificazione del pericolo
- Stima del rischio

ANALISI DEL RISCHIO

- Ponderazione del rischio

PROCESSO ITERATIVO DI RIDUZIONE DEL RISCHIO

Rischio
accettabile?

SI

FINE

NO

- Misure di protezione adottate dal progettista
- Misure di protezione adottate dall'utilizzatore



UNI EN ISO 12100

MISURE DI PROTEZIONE ADOTTATE DAL PROGETTISTA

- 1) Misure di protezione adottate nella progettazione
- 2) Protezioni e misure di protezione complementari
- 3) Informazioni per l'uso



MISURE DI PROTEZIONE ADOTTATE DALL'UTILIZZATORE

- 1) Organizzazione e procedure
- 2) Dispositivi di protezione individuali
- 3) Formazione e addestramento



Misure di protezione da adottare nella progettazione in ambito "Industria 4.0"

riguardanti: **INTERCONNESSIONE – INTEGRAZIONE - CYBERSECURITY**



UNI EN ISO 12100

DETERMINAZIONE DEI LIMITI DELLA MACCHINA

- Limiti d'uso
- Limiti di spazio
- Limiti di tempo
- Altri limiti



COSA SI INTENDE?

LIMITI D'USO

- Uso previsto
- Uso scorretto ragionevolmente prevedibile
- Considerazione a parte merita il dolo, inteso come violazione della sicurezza informatica, che non è considerata utilizzo errato ragionevolmente prevedibile, ma non può essere ignorato



UNI EN ISO 12100

DETERMINAZIONE DEI LIMITI DELLA MACCHINA

- Limiti d'uso
- Limiti di spazio
- Limiti di tempo
- Altri limiti



COSA SI INTENDE?

LIMITI DI SPAZIO

- Raggio di movimento
- Requisiti spaziali per le interazioni uomo/macchina
- Interfaccia uomo/macchina
- Interfaccia macchina/fonte di energia/fonte di dati



UNI EN ISO 12100

DETERMINAZIONE DEI LIMITI DELLA MACCHINA

- Limiti d'uso
- Limiti di spazio
- Limiti di tempo
- Altri limiti



COSA SI INTENDE?

LIMITI DI TEMPO

- Limite di durata
- Intervalli di manutenzione raccomandati

Nel contesto 4.0, vedremo:

- Manutenzione predittiva
- Analisi dei rischi dinamica, cioè in tempo reale ed aggiornata



UNI EN ISO 12100

DETERMINAZIONE DEI LIMITI DELLA MACCHINA

- Limiti d'uso
- Limiti di spazio
- Limiti di tempo
- Altri limiti



ALTRI LIMITI

- Materiali da lavorare
- Ambientali



COSA SI INTENDE?



UNI EN ISO 12100

LIMITI D'USO

- Uso previsto
- Uso scorretto ragionevolmente prevedibile



**COSA DICE LA DIRETTIVA
2006/42/CE (Direttiva Macchine)?**

ALLEGATO 1

REQUISITI ESSENZIALI DI SICUREZZA

- Principi generali
 1. Con il processo iterativo della valutazione dei rischi e della riduzione dei rischi di cui sopra, il fabbricante o il suo mandatario:
 - stabilisce i limiti della macchina, il che comprende l'uso previsto e l'uso scorretto ragionevolmente prevedibile



UNI EN ISO 12100

LIMITI D'USO

- Uso previsto
- Uso scorretto ragionevolmente prevedibile



**COSA DICE LA DIRETTIVA
2006/42/CE (Direttiva Macchine)?**

ALLEGATO 1

REQUISITI ESSENZIALI DI SICUREZZA

- Gli obblighi previsti dai requisiti essenziali di sicurezza e di tutela della salute si applicano soltanto se esiste il pericolo corrispondente per la macchina in questione, allorché viene utilizzata nelle condizioni previste dal fabbricante, o dal suo mandatario, o nelle condizioni anormali prevedibili.



UNI EN ISO 12100

LIMITI D'USO

- Uso previsto
- Uso scorretto ragionevolmente prevedibile



**COSA DICE LA DIRETTIVA
2006/42/CE (Direttiva Macchine)?**

ALLEGATO 1

REQUISITI ESSENZIALI DI SICUREZZA

1.1.2 Principi di integrazione della sicurezza

[omissis]

La macchina deve essere progettata e costruita in modo da evitare che sia utilizzata in modo anormale, se ciò può comportare un rischio.



UNI EN ISO 12100

LIMITI D'USO

- Uso previsto
- Uso scorretto ragionevolmente prevedibile



**COSA DICE LA NORMA
UNI CEN ISO/TR 22100-4?**

UNI CEN ISO/TR 22100-4

Guida ai fabbricanti di macchinari per la considerazione degli aspetti relativi alla sicurezza informatica, intesa come resilienza alle minacce esterne che possono comprometterne il funzionamento corretto.



CIBERSECURITY



UNI EN ISO 12100

LIMITI D'USO

- Uso previsto
- Uso scorretto ragionevolmente prevedibile



**COSA DICE LA NORMA
UNI CEN ISO/TR 22100-4?**

UNI CEN ISO/TR 22100-4

La legislazione e la ISO 12100 restringono l'ambito della sicurezza della macchina all'uso previsto ed all'uso scorretto ragionevolmente prevedibile. Ogni tipo di violazione volontaria (sabotaggio, spionaggio) di una macchina è di fatto un atto criminale al di fuori degli scopi delle vigenti leggi e norme in materia di sicurezza della macchina

SAFETY ≠ SECURITY



UNI EN ISO 12100

6.2.11.7 Funzioni di sicurezza implementate da sistemi di comando elettronici programmabili

- Prestazione specificata, misurabile e misurata da SIL (Safety Integrity Level) e PL (Performance Level) 
 - Aspetti relativi all'hardware
 - Aspetti relativi al software
- Prestazioni per progettazione e realizzazione di sistemi di controllo relativi alla sicurezza per macchinari (SAFETY)
 - UNI EN ISO 13849-1
 - CEI EN 62061



UNI EN ISO 13849-1

Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza (SRP/CS) – Parte 1: principi generali per la progettazione

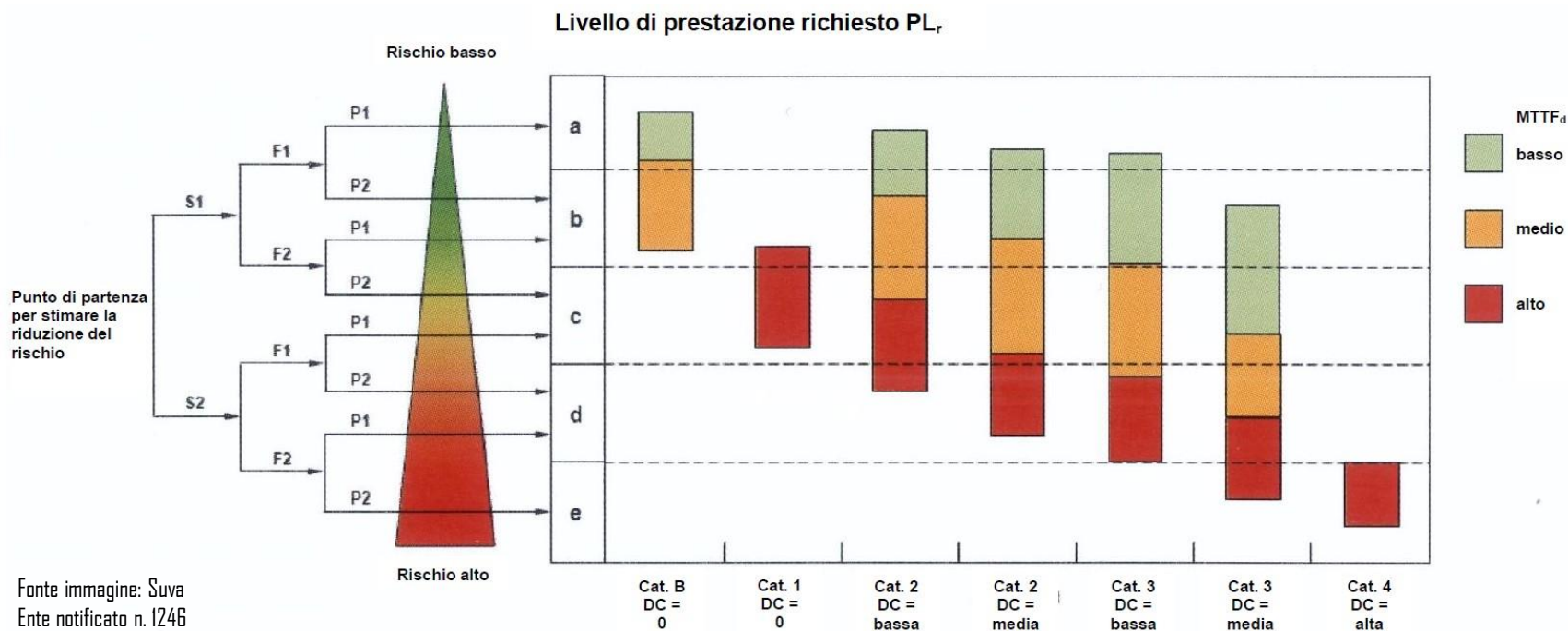
- PL (performance level) con cinque livelli di prestazione in ordine crescente: a, b, c, d, e
- Si determina il PL_r (PL richiesto) della funzione di sicurezza in base alla valutazione dei rischi e/o alla norma di tipo C, se esiste
- Si progetta la SRP/CS (Safety-Related Part of Control System) che applica la funzione di sicurezza
- Per ogni SRP/CS, si determina il PL in base a:
 - categoria o architettura della funzione di sicurezza
 - affidabilità dei componenti, espressa in termini di $MTTF_D$
 - copertura diagnostica (DC) intesa come rapporto tra la frequenza dei guasti pericolosi rilevati e quella dei guasti pericolosi totali
 - guasti da causa comune (CCF)
- Si confronta il PL della SRP/CS con il PL richiesto. Deve essere:

$$PL \geq PL_r$$



UNI EN ISO 13849-1

Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza (SRP/CS) – Parte 1: principi generali per la progettazione



S (severity) Gravità della lesione
S1 leggera (reversibile)
S2 grave (irreversibile)

F Frequenza/esposizione al pericolo
F1 rara/infrequente/esp. breve
F2 frequente/continua/esp. lunga

P Probabilità di evitare il pericolo
P1 possibile in condizioni specifiche
P2 improbabile



Ing. Giovanni TABASSO



CEI EN IEC 62061

Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili (E/E/PE) correlati alla sicurezza

- SIL (Safety Integrity Level) con 3 livelli di integrità della sicurezza in ordine crescente: 1, 2, 3
- Il SIL specifica le prescrizioni di integrità della sicurezza delle funzioni di controllo da assegnare al SRECS (Safety-Related Electrical Control System)
- Prescrizione di integrità della sicurezza espressa come PFH (Frequenza media dei guasti pericolosi per ora). PFH è un vecchio acronimo che sta per "Probability of dangerous Failure per Hour".
- Relazione tra SIL richiesto per ogni funzione di sicurezza e valori limite di PFH:

SIL	Valori limite di PFH (1/h)
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

- Una metodologia per la determinazione del SIL è basata sulla stima della gravità di un danno e sulla sua classe di probabilità, data dalla somma dei seguenti fattori:
 - Fr: frequenza e durata dell'esposizione
 - Pr: probabilità di accadimento dell'evento
 - Av: probabilità di evitare o limitare il danno



CEI EN IEC 62061

Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili (E/E/PE) correlati alla sicurezza

Conseguenze	Gravità (Se)	Classe CI = Fr + Pr + Av													
		3	4	5	6	7	8	9	10	11	12	13	14	15	
Decesso, perdita di un occhio o un braccio	4	SIL 1		SIL 2		SIL 2			SIL 3			SIL 3			
		PL _r b	PL _r c	PL _r d		PL _r d			PL _r e			PL _r e			
Lesione permanente, perdita di dita	3	Nessun SIL (o PL) richiesto		OM		SIL 1			SIL 2			SIL 3			
				PL _r a	PL _r b	PL _r c	PL _r d		PL _r e						
Lesione reversibile, intervento di un medico	2			OM			SIL 1			SIL 2					
				PL _r a	PL _r b	PL _r c	PL _r d								
Lesione reversibile, primo soccorso	1										OM		SIL 1		
											PL _r a	PL _r b	PL _r c		

OM = Other Measures; altre misure basate su parametri quali HFT (Hardware Fault Tolerance) e SFF (Safe Failure Fraction), per le quali si rimanda alla Tabella 7 della norma.



UNI EN ISO 12100

6.2.11.7 Funzioni di sicurezza implementate da sistemi di comando elettronici programmabili

- Prestazione specificata, misurabile e misurata da SIL (Safety Integrity Level) e PL (Performance Level)
 - Aspetti relativi all'hardware
 - Aspetti relativi al software
- 
- **TEORIA (ANALISI)**
 - CEI EN IEC 60812
 - CEI EN 61025
 - CEI EN IEC 61882
 - CEI EN IEC 62881
 - **PRATICA (VALIDAZIONE)**
 - Serie CEI EN 61508
 - Serie CEI EN 61511
 - CEI 65-186

UNI EN ISO 11161 – Sistemi di fabbricazione integrati – Requisiti di base



CEI EN IEC 60812

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Analisi dei modi e degli effetti di guasto (FMEA e FMECA)

- FMEA: Failure Modes and Effects Analysis



Analisi di tipo qualitativo dei singoli componenti di un sistema per determinare gli inconvenienti (Failure modes) e gli effetti sul sistema, basata su:

- FMECA: Failure Mode, Effects and Critical Analysis

- tutti i possibili modi di errore o di guasto
- i loro effetti
- le cause potenziali



CEI EN IEC 60812

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Analisi dei modi e degli effetti di guasto (FMEA e FMECA)

- FMEA: Failure Modes and Effects Analysis
- FMECA: Failure Modes, Effects and Criticality Analysis



Nella FMECA, i tre elementi della FMEA sono quantificati associandovi un valore su criteri predefiniti, per determinare un RPN (Risk Priority Number) o un ARPN (Alternative Risk Priority Number):

- Occurrence rating (O)
- Gravità degli effetti (S)
- Rilevabilità dell'errore (D)

$$\text{RPN} = O \times S \times D$$

$$\text{ARPN} = O + S + D$$



CEI EN 61025

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Analisi ad albero delle avarie (FTA)

- FTA: Fault Tree Analysis



Studio dei sistemi che consente di analizzare i rapporti esistenti tra vari eventi, a partire da eventi scatenanti e pervenendo a quelli intermedi e di guasto di entità più o meno grave.

- FTA costruito con porte logiche AND/OR e con simboli che rappresentano gli eventi e che formano la catena degli eventi.
- Eventi per la costruzione dell'albero (TOP-DOWN):
 - top event (evento di partenza, generalmente è il guasto da evitare)
 - intermedio
 - primario
 - base



CEI EN 61025

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Analisi ad albero delle avarie (FTA)

- FTA: Fault Tree Analysis



Studio dei sistemi che consente di analizzare i rapporti esistenti tra vari eventi, a partire da eventi scatenanti e pervenendo a quelli intermedi e di guasto di entità più o meno grave.

- **GUASTI:**

- primari, che si verificano in un contesto operativo normale;
- secondari, che si verificano in un contesto operativo anomalo ed imputabile a cause esterne;
- di comando, cioè malfunzionamenti per i quali il componente sbaglia tempo e spazio di intervento.



CEI EN 61882

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Studi di pericolo e operabilità (HAZOP)

- HazOp: Hazard and Operability



Studio di come un sistema potrebbe non corrispondere al comportamento previsto in fase progettuale, basato su:

- completezza ed accuratezza dei dati utilizzati;
- conoscenze tecniche del team di operatori;
- abilità nel definire ed esaminare i pericoli.

Termini dello studio HAZOP:

- nodi = parametri di processo;
- proprietà = obiettivi del sistema durante il funzionamento, cioè i valori-nodo;
- deviazioni;
- cause;
- conseguenze;
- parole-guida.



CEI EN 61882

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Studi di pericolo e operabilità (HAZOP)

- Parole-guida comunemente utilizzate nello studio HAZOP:
 - NO = assenza totale della proprietà attesa (obiettivo);
 - LESS = verificarsi dell'obiettivo con modalità ridotte;
 - MORE = verificarsi dell'obiettivo in maniera opposta al LESS;
 - PART OF = verificarsi parziale dell'obiettivo atteso;
 - REVERSE = verificarsi del fenomeno opposto all'obiettivo atteso;
 - OTHER THAN = verificarsi di un fenomeno diverso dall'obiettivo atteso.
- Parole-guida:
 - Proposte dal capo-squadra dello studio HAZOP
 - Convalidate ed approvate dai componenti della squadra



CEI EN IEC 62881

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Matrice di causa ed effetto

- **MATRICE:**
 - Intestazione delle righe -> le cause
 - Intestazione delle colonne -> gli effetti (obiettivi)
 - Intersezioni di righe e colonne -> relazioni richieste tra cause ed effetti
- **SCOPO:**
 - Evidenziare cause ed effetti, intesi come obiettivi da conseguire, per supportare:
 - la successiva stesura del codice di programmazione del PLC/DCS della macchina o dell'impianto;
 - verifica delle funzioni di sicurezza.



CEI EN IEC 62881

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Matrice di causa ed effetto - esempio

NORMAL STOP 01 END OF PRODUCTION FINE PRODUZIONE Legend; legenda: CL= Closed; chiuso/a OP= Opened; aperto/a ON= Switched on; acceso/a o in moto OFF= Switched off; spento/a o fermo/a									PID	Fail safe pos.	Service	Remarks	Rev.							
									Effect identifier	6" valve	XV02	XV03	XV004	TE01	DC POWER SUPPLY	Valve on vacuum package (HOLD 1) TBD	Valve on vacuum package TBD	D-BL-01	XV06	
									SIL	1	1	1	1	1	1	1	1	1	1	
									SIL	1	OP	CL	OP	OP	ON	OFF	CL	CL	OFF	CL
									1	"	OP	"	CL	"	"	"	"	"	"	"
									1	"	CL	CL	"	"	"	"	"	"	"	"
1	"	"	"	"	"	"	"	"	"	"	"									
1	"	"	"	"	OFF	"	OP	"	"	"	"									
1	"	"	"	"	"	"	CL	OP	"	"	"									
1	CL	"	"	"	"	"	"	"	"	"	"									

Ing. Giovanni TABASSO



CEI EN IEC 62881

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
TEORIA (ANALISI)

Matrici di causa ed effetto

Confronto con diagrammi a spina di pesce (fishbone) o di Ishikawa

- La testa del pesce rappresenta l'effetto
- Scopo
 - Elencare e raggruppare tutte le possibili cause di non conformità o malfunzionamenti.
 - Il metodo più completo applicabile alla progettazione ed alla fabbricazione è quello delle "8 M"



1. Macchine
2. Metodo (processo)
3. Materiale
4. Uomo (man)
5. Ambiente (Mother Nature)
6. Manutenzione
7. Sistema di misura
8. Management



Serie CEI EN 61508

UNI EN ISO 12100 - 6.2.11.7
HARDWARE/SOFTWARE
PRATICA (VALIDAZIONE)

Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili (E/E/PE) per applicazioni di sicurezza

- Parte 1 – Requisiti generali
- Parte 2 – Requisiti per sistemi E/E/PE
- Parte 3 – Requisiti del software
- Parte 4 – Definizioni e abbreviazioni
- Parte 5 – Esempi di metodi per la determinazione del SIL
- Parte 6 – Linee guida per l'applicazione delle parti 2 e 3
- Parte 7 – Panorama delle tecnologie e delle misure tecniche



Serie CEI EN 61511

UNI EN ISO 12100 – 6.2.11.7
HARDWARE/SOFTWARE
PRATICA (VALIDAZIONE)

Sicurezza funzionale – Sistemi strumentati di sicurezza per il settore dell'industria di processo (SIS = Safety Instrumented Systems)

- Parte 1 – Struttura, definizioni, sistema, prescrizioni per l'hardware e il software
- Parte 2 – Linee guida per l'applicazione della IEC 61511-1
- Parte 3 – Guida per la determinazione dei SIL richiesti
- CEI 65-186 – Linee guida per l'applicazione delle norme della serie CEI EN 61511



Da SAFETY a SECURITY

Norme che evidenziano la necessità della CYBERSECURITY in era 4.0,
poi ripresa dalla norma UNI CEN ISO/TR 22100-4

- UNI EN ISO 11161 –
Sicurezza del macchinario -
Sistemi di fabbricazione
integrati – Requisiti di base
 - Sistemi che incorporano
macchine interconnesse
 - IMS (Integrated
Manufacturing System),
definizione 3.1 della norma
 - Integratore, definizione 3.10
della norma
- **IMS:** gruppo di macchine che
lavorano insieme in maniera
coordinata, collegate da un sistema
di movimentazione dei materiali,
interconnesse da controlli, allo scopo
di fabbricare, trattare, movimentare
o confezionare singole parti o
insiemi.
- **Integratore:** entità che progetta,
fornisce, fabbrica o assembla un IMS
ed è responsabile della strategia
della sicurezza, incluse le misure di
protezione, le interfacce di controllo
e le interconnessioni dei sistemi di
controllo



Da SAFETY a SECURITY

Norme che evidenziano la necessità della CYBERSECURITY in era 4.0,
poi ripresa dalla norma UNI CEN ISO/TR 22100-4

- UNI/TR 11749 –
Tecnologie abilitanti per
Industry 4.0 –
Integrazione ed
interconnessione: aspetti
principali ed esempi
 - Interconnessione,
definizione 3.5 della norma
 - Integrazione, definizione
3.6 della norma

- **Interconnessione:** capacità del bene di:
 - scambiare informazioni con sistemi interni e/o esterni per mezzo di un collegamento basato su specifiche documentate, disponibili pubblicamente e internazionalmente riconosciute (TCP-IP, HTTP ecc.);
 - essere identificato univocamente, al fine di riconoscere l'origine delle informazioni, mediante l'utilizzo di standard di indirizzamento internazionalmente riconosciuti (per esempio: indirizzo IP).



Da SAFETY a SECURITY

Norme che evidenziano la necessità della CYBERSECURITY in era 4.0,
poi ripresa dalla norma UNI CEN ISO/TR 22100-4

- UNI/TR 11749 –
Tecnologie abilitanti per
Industry 4.0 –
Integrazione ed
interconnessione: aspetti
principali ed esempi
 - Interconnessione,
definizione 3.5 della norma
 - Integrazione, definizione
3.6 della norma

Integrazione: è uno degli elementi centrali del paradigma 4.0 attraverso il quale le architetture aziendali possono garantire l'interconnessione trasparente, sicura ed affidabile dei diversi dispositivi hardware e delle applicazioni software tramite l'implementazione di un modello di dati comune ed il supporto di vari protocolli ed interfacce.

L'integrazione della parte fisica dell'impresa con i sistemi informativi impiegati (integrazione IT/OT) permette di elaborare dati disponibili provenienti da macchine, dispositivi e sistemi (interni ed esterni), trasformandoli in informazioni e dati interpretati, capaci di migliorare le varie fasi di creazione del valore.



Da SAFETY a SECURITY

Progettazione meccanica in era 4.0: interconnessione avanzata e integrazione tra parte fisica e sistemi informativi

- Ruolo dell'integratore, non più semplice progettista meccanico, ma vero e proprio coordinatore tra:
 - sistema logistico della fabbrica;
 - rete di fornitura, intesa come qualsiasi soggetto con il quale l'impresa interagisce stabilmente nel processo di creazione del valore;
 - con altre macchine del ciclo produttivo.

INTEGRATORE

artefice dell'interconnessione avanzata e dell'integrazione tra parte fisica e sistemi informativi, che sono due delle tecnologie abilitanti per l'Industria 4.0



Da SAFETY a SECURITY

VANTAGGI E CRITICITÀ IN ERA 4.0

VANTAGGI

- Miglioramento delle varie fasi del processo di creazione del valore
- Manutenzione predittiva
- Analisi dei rischi dinamica, aggiornata in tempo reale

CRITICITÀ

- Nuovi rischi emergenti, soprattutto rischi sistemici
 - Database ARIA (Analyse, Recherche et Informations sur les Accidents) del Ministero francese per l'Ambiente
 - Motore di ricerca "EsOpIA" dell'INAIL: Esperienze Operative di Intelligenza Artificiale, che utilizza tecniche di IA per l'analisi di documenti su esperienze operative di incidenti, quasi-incidenti e anomalie, al fine di migliorare i SGS
 - Utilizzo critico e coordinato delle norme di tipo B, delle serie CEI EN 61508 e CEI EN 61511 sulla sicurezza dei sistemi
- Esposizione alle minacce informatiche
 - UNI CEN ISO/TR 22100-4
 - Serie CEI EN IEC 62443

CYBERSECURITY





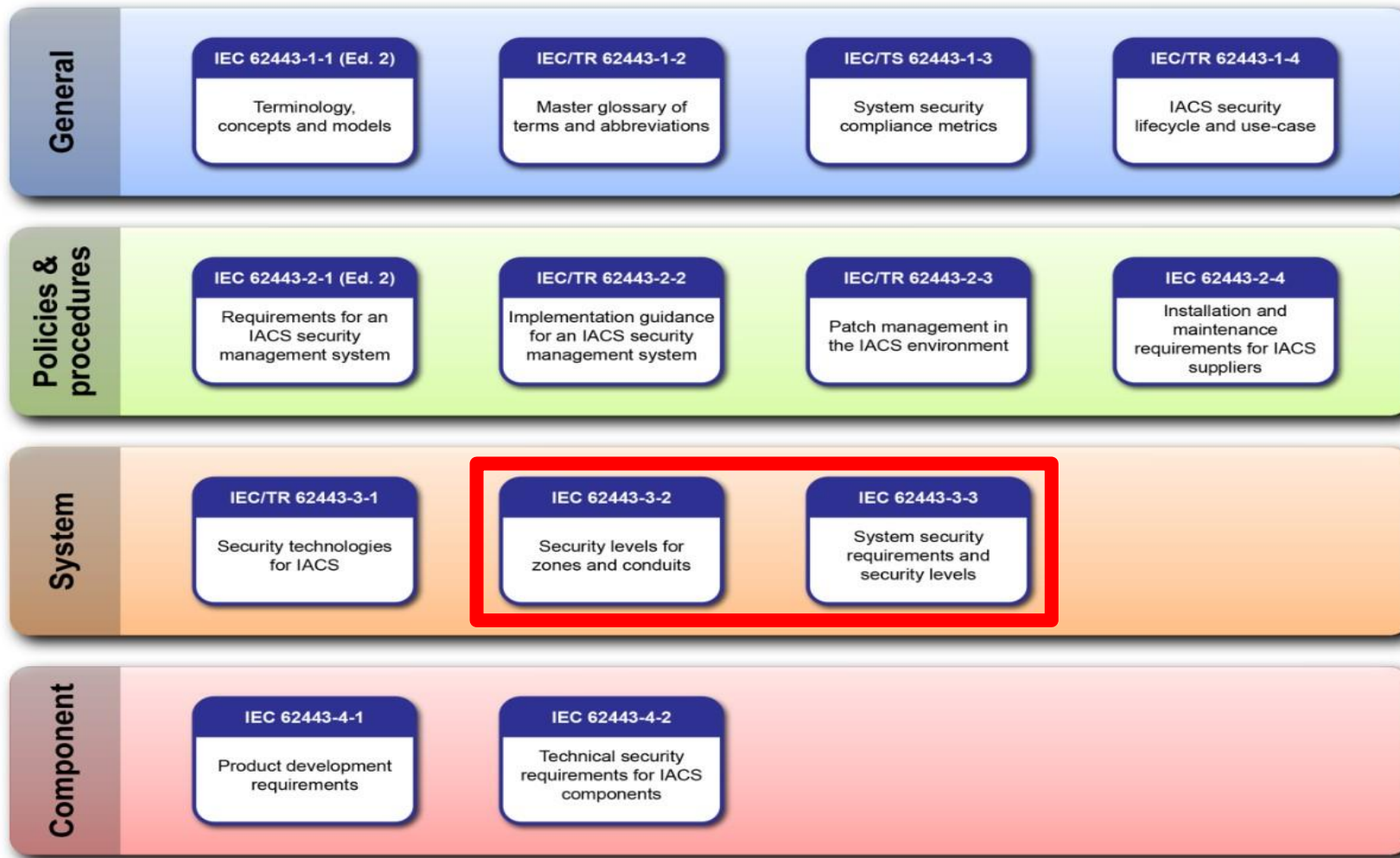
UNI CEN ISO/TR 22100-4

- NORMA DI TIPO A
- Guida ai fabbricanti di macchinari per la considerazione degli aspetti relativi alla sicurezza informatica
- Sicurezza informatica (**Cybersecurity**) intesa come resilienza alle minacce esterne che possono comprometterla
- Base per norme di tipo B e C



Serie IEC 62443

Sicurezza dei sistemi di automazione e controllo industriale (IACS)





CEI EN IEC 62443-3-2

Sicurezza dei sistemi di automazione industriale e controllo (IACS) Parte 3-2: valutazione del rischio di sicurezza nel progetto di sistema

- Suddivisione del sistema in esame (SUC) in:
 - zone
 - canali di comunicazione (conduit)
- Definizione dei livelli di sicurezza-obiettivo (Security Level Targets o SL-Ts)
- Quattro livelli di SL (Security Level):
 - SL 1: Protezione contro violazioni casuali o incidentali
 - SL 2: Protezione contro violazioni volontarie attuate con mezzi semplici con basse risorse, competenze generiche e bassa motivazione
 - SL 3: Protezione contro violazioni volontarie attuate con mezzi sofisticati con risorse moderate, competenze specifiche su IACS e motivazione moderata
 - SL 4: Protezione contro violazioni volontarie attuate con mezzi sofisticati con risorse cospicue, competenze specifiche su IACS e motivazione elevata



CEI EN IEC 62443-3-3

Reti di comunicazione industriale – Sicurezza di rete e di sistema

Parte 3-3: requisiti per la sicurezza informatica e i livelli di sicurezza informatica di sistema

- Determinazione dei livelli di sicurezza richiesti (Security Level Capabilities SL-Cs)
- Comparazione con i livelli di sicurezza-obiettivo (Security Level Targets o SL-Ts) definiti con la CEI EN IEC 62443-3-2
- Distingue tra:
 - FR: Foundational requirements (requisiti fondamentali):
 - FR 1: Controllo dell'identificazione e dell'autenticazione
 - FR 2: Controllo dell'utilizzo
 - FR 3: Integrità di sistema
 - FR 4: Riservatezza dei dati
 - FR 5: Flusso di dati ristretto
 - FR 6: Risposta temporale agli eventi
 - FR 7: Disponibilità di risorse
 - SR: System requirement (requisiti di sistema) all'interno dei singoli FRs



UN CASO DI ATTUALITÀ

L'Olanda rassicura gli USA: "Possiamo spegnere le macchine per i chip di TSMC in caso di invasione cinese di Taiwan"

- La società olandese ASML costruisce macchine per realizzare i semiconduttori più sofisticati al mondo, molte delle quali in servizio presso la taiwanese TSMC (Taiwan Semiconductor Manufacturing Company)
- **La ASML sarebbe in grado di disabilitarle da remoto!** Un'opzione che potrebbe essere tenuta in conto nel caso di un'invasione cinese di Taiwan, già testata in alcune simulazioni.
- Lo spegnimento a distanza riguarda la linea di macchine con litografia ultravioletta estrema (EUV), utilizzata per disegnare i circuiti: onde luminose ad alta frequenza stampano i più piccoli chip esistenti al mondo, creando prodotti che hanno applicazioni in IA e nel campo militare.
- ASML è l'unico produttore al mondo di tali macchine e gli USA ne hanno già vietato la vendita alla Cina, che era il primo cliente di ASML: si teme lo spionaggio industriale ed il controllo del mercato dei microchip.



ISO/TS 15066

Robots and robotics devices – Collaborative robots

- Integra la Serie UNI EN ISO 10218 – Robot e attrezzature per robot – Requisiti di sicurezza per robot industriali
 - Parte 1: robot
 - Pericoli di base associati ai robot
 - Requisiti per eliminarli o ridurli
 - Parte 2: sistemi ed integrazione di robot
 - Pericoli di base per i sistemi e le isole robotizzate come parte di un sistema di produzione integrato.
 - Cobot (collaborative robot) al requisito 5.11 e in Appendice "E": operatività possibile solo quando tutte le misure di protezione sono attive.



RIPRENDIAMO LA SAFETY



UNI EN ISO 12100

6.3.2.5 Selezione e implementazione di dispositivi di protezione sensibili

- Utilizzati per:
 - rilevare il superamento di un limite;
 - rilevare una presenza;
 - riavviare il funzionamento della macchina, pratica soggetta a condizioni severe.
- **6.3.2.5.2 Implementazione:** i dispositivi di protezione sensibili devono essere integrati nella parte operativa ed associati al sistema di comando in modo tale che:
 - sia inviato un comando non appena una persona o una sua parte è rilevata;
 - il riavviamento della funzione pericolosa sia volontario da parte dell'operatore esterno alla zona pericolosa;
 - la macchina non possa funzionare durante l'interruzione da parte del dispositivo di protezione sensibile, eccetto che durante le fasi di inibizione;
 - il ritiro della persona non riavvii automaticamente la macchina.



UNI EN ISO 12100

6.3.2.5 Selezione e implementazione di dispositivi di protezione sensibili – Norme di tipo B attinenti al requisito

- **Serie (CEI) EN IEC 61496** – Sicurezza del macchinario – Apparecchi elettrosensibili di protezione (ESPE = Electro-Sensitive Protective Equipment)
 - Parte 1: Prescrizioni generali e prove
 - Parte 2: Prescrizioni particolari per l'equipaggiamento che utilizza dispositivi di protezione fotoelettrici attivi (AOPD)
 - Parte 3: Prescrizioni particolari per dispositivi di protezione fotoelettrici attivi che rispondono alla riflessione diffusa (AOPDDR)
 - Part 4-2: Particular requirements for equipment using vision based protective devices (VBPD) - Additional requirements when using reference pattern techniques (VBPDPP)
 - Part 4-3: Particular requirements for equipment using vision based protective devices (VBPD) - Additional requirements when using stereo vision techniques (VBPDST)
- **CEI EN IEC 62046** – Sicurezza del macchinario – Applicazione dei dispositivi di protezione per rilevare la presenza di persone



LEGISLAZIONE

Direttiva 2006/42/CE

- o "Direttiva Macchine";
- ad oggi in vigore fino al 19/1/2027.

Regolamento (UE) 2023/1230

- o "Regolamento Macchine";
- in vigore dal 19/7/2023 e già applicabile in alternativa alla Direttiva Macchine;
- rimarrà il solo applicabile dal 20/1/2027 in poi, quando la Direttiva Macchine sarà definitivamente abolita.



LEGISLAZIONE

"Quasi-macchina" (Almost-completed machinery)

- Definizione: un insieme che non costituisce ancora una macchina in quanto, da solo, non è in grado di eseguire un'applicazione specifica e che è soltanto destinato ad essere incorporato o assemblato ad altre macchine o apparecchi per costituire una macchina.
- Dichiarazione di incorporazione, redatta secondo:
 - Allegato II Parte B della Direttiva "Macchine" 2006/42/CE
 - Allegato V Parte B del Regolamento "Macchine" (UE) 2023/1230
- La dichiarazione di incorporazione contiene l'elenco delle norme e dei rispettivi requisiti applicati alla macchina.



LEGISLAZIONE

"Quasi-macchina" (Almost-completed machinery)

- La quasi-macchina non deve essere messa in servizio finché la macchina finale in cui deve essere incorporata non sia stata dichiarata conforme alla Direttiva o al Regolamento dal proprio fabbricante: infatti, la dichiarazione di incorporazione lo vieta esplicitamente.
- Esempio: skid monoblocco per la produzione di acqua calda sanitaria, privo di pompe e dotato soltanto di:
 - quadro di programmazione dei parametri di processo;
 - scambiatore di calore;
 - valvole manuali ed attuate, strumenti, tubazioni e basamento.



LEGISLAZIONE

"Quasi-macchina" (Almost-completed machinery)

Stralcio della dichiarazione di incorporazione

Rispetta i seguenti requisiti essenziali applicati:

1.1.1; 1.1.2; 1.1.3; 1.1.5; 1.2.1; 1.2.2; 1.2.3; 1.2.4.1; 1.2.4.3; 1.2.4.4; 1.2.5; 1.2.6; 1.3.1; 1.3.2; 1.5.1; 1.5.2; 1.5.5; 1.6.1; 1.6.3; 1.6.4; 1.6.5; 1.7.1; 1.7.1.1; 1.7.3; 1.7.4; 1.7.4.1; 1.7.4.2

È conforme alle direttive comunitarie:

Direttiva 2014/68/UE

La documentazione tecnica pertinente è stata compilata in conformità all'allegato VII parte B. Il fabbricante si impegna a trasmettere, in risposta a una richiesta adeguatamente motivata delle autorità nazionali, informazioni pertinenti la quasi-macchina e ne

VIETA

la messa in servizio finché la macchina finale in cui deve essere incorporata non sia stata dichiarata conforme, se del caso, alle disposizioni della presente direttiva.



LEGISLAZIONE

"Quasi-macchina" (Almost-completed machinery)

- In quali casi i robot destinati ad essere integrati in isole robotizzate ed in sistemi di robot rientrano in tale definizione?
- Importanza del ruolo dell'*integratore* ai sensi della definizione 3.10 della UNI EN ISO 11161 per i sistemi di fabbricazione integrati, che qui sotto si riporta ancora:
- **Integratore:** entità che progetta, fornisce, fabbrica o assembla un IMS (Integrated Manufacturing System) ed è responsabile della strategia della sicurezza, incluse le misure di protezione, le interfacce di controllo e le interconnessioni dei sistemi di controllo.



MATCH STANDARDS, GET CONNECTED, STAY HUMAN

GRAZIE PER L'ATTENZIONE

Ing. Giovanni TABASSO

Studio di ingegneria
Progettazione e normativa di impianti industriali

mail@giovannitabasso.com

06 906 14 85

-

347 32 50 458