INAIL

Sicurezza funzionale dei sistemi di controllo delle macchine: requisiti ed evoluzione della normativa

Edizione 2013

Pubblicazione realizzata da

INAIL
Settore Ricerca, Certificazione e Verifica
Dipartimento Tecnologie di Sicurezza

AUTORI
Fabio Pera
Giovanni Luca Amicucci
Massimo Giuffrida
Francesca Ceruti

COLLABORAZIONE REDAZIONALE
Daniela Gaetana Cogliani

CONTATTI
INAIL - Dipartimento Tecnologie di Sicurezza
Via Alessandria, 220/E - 00198 Roma
r.dts@inail.it

www.inail.it

ISBN 978-88-7484-360-2

Tipolitografia INAIL - Milano, febbraio 2014

Premessa

Lo sviluppo tecnologico ha condotto ad utilizzare componenti elettrici, elettronici ed elettronici programmabili per la realizzazione dei sistemi di controllo delle macchine. Accanto alle normali funzioni, tali sistemi realizzano anche le funzioni di sicurezza.
Ciò, a livello normativo, ha spinto all'esecuzione di studi ed analisi per approfondire i rischi connessi con la realizzazione pratica di funzioni di sicurezza, per mezzo di sistemi intrinsecamente più difficili da gestire degli usuali sistemi a logica cablata, in quanto dotati di un numero esponenzialmente più grande di stati possibili.

Gli studi e le analisi sono serviti da base per la pubblicazione di una serie di norme tecniche relative alla valutazione e gestione del rischio connesso con l'utilizzo di funzioni di sicurezza realizzate con tecnologie elettriche, elettroniche ed elettroniche programmabili.
Una volta disponibili le norme, i fabbricanti e gli assemblatori di macchine hanno cominciato ad utilizzarle, chi più e chi meno. Anche perché, dopo un primo entusiasmo dovuto alla pubblicazione di una norma non troppo onerosa (EN 954-1), vi è stata una sorta di rallentamento dovuto alla pubblicazione di due norme evidentemente più onerose (EN ISO 13849-1 e EN IEC 62061) e con un campo di applicazione un po' sovrapposto, cosa che ha creato nei costruttori anche il dilemma della scelta.

Pertanto, è sorta spontanea la curiosità di conoscere quanto effettivamente tali norme fossero utilizzate a livello industriale o se, viceversa, fossero inutilizzabili, poiché lacunose o troppo costose da applicare, e vi fosse la necessità di rivederle per integrarle e correggerle.
Lo studio e l'analisi delle problematiche connesse alla pratica applicazione delle norme è stato affrontato predisponendo un questionario conoscitivo ad hoc e somministrandolo in forma anonima a diverse aziende produttrici di macchine.

Il presente monografico inizia con un richiamo alle definizioni ed ai concetti rilevanti nel campo dell'affidabilità.

Il volume prosegue con l'analisi delle complesse relazioni tra i documenti che costituiscono il corpo normativo. Nell'ambito di tale analisi ci si è soffermati sui metodi per il calcolo dei dati relativi ai tassi di guasto dei componenti (con un cenno anche allo standard industriale SN 29500).

La sezione successiva tratta delle architetture con cui sono realizzati i PLC, cercando di illustrare in modo mirato le specifiche caratteristiche delle singole tecnologie.

Un sistema affidabile, nella sua complessità, presenta prestazioni migliori quanto più riesce a trasmettere le informazioni in modo corretto ed esente da errori. Per questo è stata inclusa anche una sezione sui sistemi di interconnessione e comunicazione a bus.

Chiude il lavoro l'analisi delle risposte al già ricordato questionario sull'applicabilità delle norme e sull'affidabilità dei sistemi di controllo in vigore nel settore delle macchine, in modo da mettere in luce le criticità e le eventuali difficoltà di applicazione.

Il presente volume è destinato ad una vastissima platea di fruitori, che va da chi cerca spunti di approfondimento fino a chi deve occuparsi dell'evoluzione normativa.

Indice

Capitolo 1 - Affidabilità 7
La determinazione del Tempo Medio tra due Guasti Pericolosi 10

Capitolo 2 - Panorama normativo 12
Le Architetture designate della norma EN IEC 62061 18
Le Categorie della norma EN ISO 13849-1 21
Il B_{10} per i componenti pneumatici, meccanici ed elettromeccanici 25
I dati sui tassi di guasto 26
I valori di tasso di guasto determinati secondo lo standard SN 29500 26

Capitolo 3 - I PLC nei sistemi di controllo 28
Funzionamento di un PLC 28
Architettura di un PLC 29
Differenze tra PLC per applicazioni standard e PLC fail-safe 35
Il software 39

Capitolo 4 - I bus di comunicazione 40
I sistemi PROFIBUS 41
Tipologie di dispositivi nelle reti PROFIBUS 42
Caratteristiche principali di PROFIBUS-DP 43
I sistemi AS-Interface 44
Campo di impiego e struttura di una rete AS-Interface 45
Tipologie di interconnessione 46

Capitolo 5 - Indagine sull'adozione delle norme per i sistemi di controllo delle macchine nel panorama produttivo nazionale 48
Contesto aziendale 51
Adozione di norme per i sistemi di controllo 52
Tipologia di organizzazione 61
Reperimento di informazioni 62
Prestazioni 65
Motivi della mancata adozione 69

Conclusioni 79

Bibliografia 80

Capitolo 1 - Affidabilità

La corretta esecuzione di una funzione da parte di un sistema di controllo ed il conseguente soddisfacimento degli eventuali requisiti di sicurezza sono strettamente connessi all'*affidabilità* del sistema di controllo stesso.

Un componente, o più in generale un sistema, è definito essere affidabile quando riesce a completare il suo compito in un tempo prestabilito sotto l'azione delle sollecitazioni "*previste*", dove per previste si intendono le sollecitazioni tipiche a cui può essere sottoposto durante il suo impiego.
Da ciò si comprende che l'*affidabilità* non ha una compiuta definizione se non quando è correlata al concetto di *sollecitazione*.

L'importanza dell'affidabilità ha spinto i comitati normatori internazionali e nazionali ad inserire in modo sostanziale il concetto di *affidabilità dei sistemi di controllo* all'interno del corpus delle norme relative alla sicurezza delle macchine.

Nelle norme relative a tale argomento è definito un parametro tramite il quale quantificare il livello di prestazione affidabilistica di un sistema di controllo.
In generale, per determinare l'affidabilità di un sistema o di un componente, è necessario calcolare la Probabilità di Guasto Pericoloso PFH_D.

Per la EN ISO 13849-1 la capacità di un sistema di controllo di realizzare una funzione di sicurezza è espressa tramite il Performance Level (punto 4.5). Tale parametro è determinato in base agli intervalli di probabilità di guasto pericoloso del sistema. La probabilità di guasto pericoloso, a sua volta, può essere calcolata grazie alla stima di diversi parametri, tra i quali il $MTTF_d$ (Mean Time To dangerous Failure).
Appare quindi evidente l'importanza del $MTTF_d$ quale figura di merito per valutare il grado di affidabilità di un sistema di controllo. Ciò può essere fatto, almeno in linea di principio, a partire dalla conoscenza circuitale e funzionale del sistema e da una stima dello stesso parametro per i singoli componenti costituenti il sistema.
Per la determinazione del $MTTF_d$ dei componenti è necessaria la conoscenza di informazioni sul componente, relative alla sua realizzazione fisica, ai materiali utilizzati ed a statistiche qualitative del processo costruttivo. Ad esempio, nel caso di componenti elettromeccanici può essere utile conoscere il B_{10}, ovvero il numero medio di cicli entro cui il 10% dei componenti subisce un guasto pericoloso.

I guasti possono essere suddivisi in:

- guasti infantili;
- guasti casuali;
- guasti per usura.

I *guasti infantili* sono quelli dovuti a fattori strettamente attinenti al periodo iniziale della vita del componente o del sistema. Tali guasti possono essere ricondotti a fattori di inadeguatezza nel ciclo produttivo, assenza di controllo della qualità al termine della produzione, errato collaudo prima della messa in esercizio. In genere, possono essere ridotti con un opportuno periodo di prova per il componente, prima della messa in esercizio.

I *guasti casuali* (o accidentali) sono quelli che si verificano a causa delle sollecitazioni sopportate dal sistema o da un suo componente durante il periodo di normale

funzionamento (vita utile), cioè dopo il periodo di prova per eliminare i componenti soggetti a guasti infantili. L'incidenza di manifestazione dei guasti casuali (rateo di guasto) è stazionaria (costante nel tempo). I guasti casuali sono dovuti a fattori incontrollabili che neanche un buon progetto ed una buona realizzazione possono eliminare (mortalità standard). Sono causati da fluttuazioni statistiche delle condizioni di esercizio che determinano forti sollecitazioni casuali sui componenti compromettendone, a volte, le capacità operative.

I *guasti per usura* (o per vecchiaia) sono causati dal progressivo processo di invecchiamento del sistema o del componente, in riferimento al suo periodo di esercizio.

Le tre tipologie di guasti, per modalità di accadimento e dinamica di manifestazione, sono studiate per mezzo di modelli matematici e funzioni statistiche tra loro distinte. I parametri relativi a tali funzioni sono stimati con analisi statistiche condotte all'interno dei rispettivi periodi di esistenza. Ciò consente di avere, con determinati margini di approssimazione, informazioni sull'affidabilità del sistema o del componente che si sta studiando.
Senza approfondire le questioni matematiche, è opportuno richiamare le definizioni fondamentali della teoria dell'affidabilità di un componente, in modo da comprendere chiaramente a cosa ci si riferisce quando se ne parlerà nel seguito.

Se si indica con $F(t)$ la probabilità di avere un guasto all'istante t, l'affidabilità di un componente o di un sistema è definita come la probabilità di non avere il guasto, ovvero:

$$R(t) = 1 - F(t)$$

Il parametro che però interessa per la definizione dell'affidabilità è il *tasso di guasto*, definito come l'attitudine di un componente o di un sistema a subire un guasto durante un determinato intervallo di tempo:

$$h(t) = f(t)/R(t)$$

dove $f(t) = \mathrm{d}F(t)/\mathrm{d}t$

Conoscere l'andamento nel tempo del tasso di guasto consente di ricavare l'andamento nel tempo dell'affidabilità. É possibile verificare tale affermazione per mezzo della funzione di densità di probabilità esponenziale.
Assumendo di considerare un numero molto alto di componenti uguali che subiscono guasti casuali indipendenti tra di loro e tali che la probabilità di guasto di ciascun componente in un dato intervallo di tempo sia indipendente dalla durata della vita del componente già trascorsa, si può dimostrare che la densità di probabilità di guasto di ciascun componente è decrescente nel tempo ed è descritta dalla funzione: $f(t) = \lambda e^{-\lambda t}$ con λ costante rispetto al tempo.

Dalla densità di probabilità di guasto si può ricavare la probabilità di guasto:

$$F(t) = \int_0^t f(\tau)d\tau = \int_0^t \lambda e^{-\lambda\tau} d\tau = 1 - e^{-\lambda t}$$

Una volta nota la probabilità di guasto è possibile ottenere l'affidabilità:

$R(t) = 1 - F(t) = e^{-\lambda t}$

È quindi possibile ricavare il valore del *tasso dei guasti casuali*, ovvero:

$$h(t) = f(t)/R(t) = (1/R(t))(dF(t)/dt) = (1/e^{-\lambda t})(d(1 - e^{-\lambda t})/dt) = \lambda$$

che, come atteso, è indipendente dal tempo.

Da una analisi delle funzioni che definiscono le varie tipologie di guasti, è possibile vedere che i guasti per mortalità infantile, quelli casuali e quelli dovuti all'usura in sostanza coesistono, pertanto si avrà un andamento del tasso di guasto di fatto variabile nel tempo, del tipo raffigurato in figura 1.

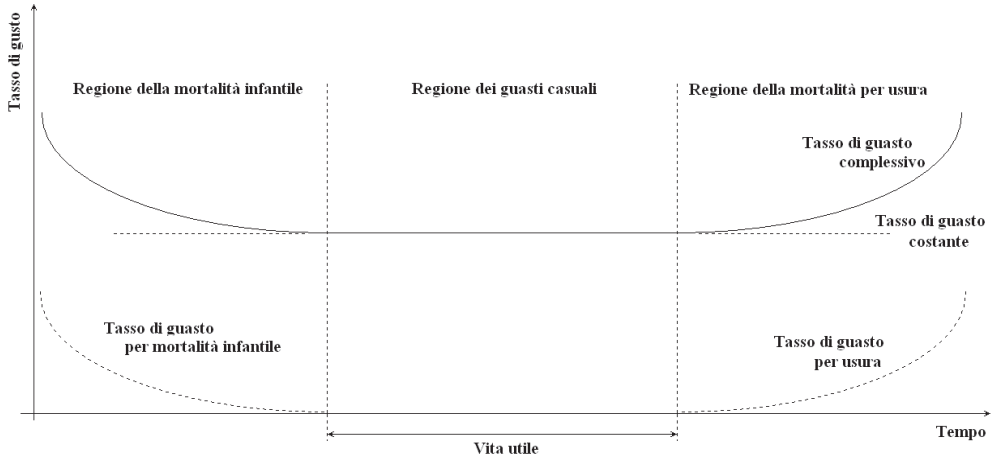


Figura 1: Andamento tipico del tasso di guasto di un componente (tasso di guasto complessivo)

I guasti per mortalità infantile e per usura possono essere rappresentati con funzioni di affidabilità del tipo $R(t) = \exp[-(t/\alpha)^{\beta}]$, relative a densità di probabilità di guasto del tipo di Weibull:

$f(t) = (\beta t^{\beta-1}/\alpha^{\beta})\exp[-(t/\alpha)^{\beta}]$,

dove α e β sono parametri di scala riferiti anche al tempo in cui viene calcolata la funzione. Se $\beta < 1$ la funzione di Weibull ha un tasso di guasto decrescente e può essere utilizzata per descrivere i casi di mortalità infantile; se $\beta > 1$ la funzione di Weibull ha un tasso di guasto crescente e può essere utilizzata per descrivere i casi di mortalità per usura, infine se $\beta = 1$ la funzione di Weibull ha un tasso di guasto costante (si riduce ad una funzione esponenziale) e può essere utilizzata per descrivere i guasti casuali durante la vita utile del componente.

Un esempio di applicazione della formula di Weibull è dato dalla determinazione del valore della probabilità di guasto per mortalità infantile di un condensatore dopo un anno di funzionamento (8760 ore). La densità di probabilità di guasto del condensatore può essere descritta da una funzione di Weibull con parametri $\alpha = 100000$ (ore)$^{-1}$ e $\beta = 0,5$.
La probabilità di guasto è data da: $F(8760) = 1 - \exp[-(8760/100000)^{0,5}] = 0,26$.

Per cui, dopo 8760 ore di utilizzo, l'affidabilità del condensatore è pari a $R(t) = 1 - F(t) =$ 0,74 (ovvero il 74%).

La determinazione del Tempo Medio tra due Guasti Pericolosi

Il parametro che definisce l'affidabilità di un sistema o di un componente è il Tempo Medio al primo Guasto Pericoloso, identificato con l'acronimo $MTTF_d$ (Mean Time To dangerous Failure).

Nei contesti produttivi in cui sono utilizzati sistemi e componenti elettronici riparabili, l'obiettivo primario è quello di conoscere l'intervallo temporale tra due possibili guasti che possano comportare un rischio per la sicurezza, di conseguenza il parametro che definisce l'affidabilità è il Tempo Medio tra due Guasti Pericolosi, identificato con l'acronimo $MTBF_d$ (Mean Time Between dangerous Failure).

I parametri che definiscono i valori dei tempi medi di guasto sono legati tra loro dalla seguente relazione:

$$MTBF_d = MTTF_d + MTTR,$$

dove MTTR (Mean Time To Repair) è il valore atteso del tempo di ripristino, presente in caso di manutenzione.
Nei casi in cui il valore del tempo di ripristino possa essere trascurato, si ha:

$$MTBF \cong MTTF_d.$$

La norma EN ISO 13849-1 utilizza il $MTTF_d$ dei componenti del sistema di controllo, l'architettura con cui sono interconnessi (la categoria) e altri parametri per risalire alla Probabilità di Guasto Pericoloso. Negli Allegati C e D a tale norma sono proposti alcuni metodi di calcolo del $MTTF_d$, sia per singoli componenti, sia per singoli canali di un sistema. In particolare, il punto C.3 propone un metodo di calcolo del $MTTF_d$ per singoli componenti idraulici, mentre il punto C.4 propone un metodo di calcolo per componenti meccanici ed elettromeccanici.

Per valutare l'affidabilità di sistemi con complessità maggiore di quella di un singolo componente, si può ricorrere a svariate tecniche di calcolo che consentono di analizzare nel dettaglio le modalità di guasto e la loro probabilità.
Tra tali tecniche le più utilizzate sono la F.M.E.A. (Failure Mode Effects Analysis) e l'albero dei guasti.

La FMEA è un'analisi che prevede la suddivisione del sistema in esame in sottoparti, per esempio sottosistemi o componenti. Per ognuna di queste parti elementari bisogna individuare:

- i modi di guasto che si ritengono possibili;
- le cause e gli effetti dei possibili modi di guasto;
- le misure di riconoscimento del guasto (segnali, sintomi…);
- i sistemi di prevenzione e controllo;
- i parametri di guasto: probabilità di guasto, tempo medio fra i guasti, etc.

La FMEA è in sostanza un metodo di analisi induttivo, che dal particolare (singolo componente) va al generale (il sistema) ed è per questo definito del tipo bottom-up.

La FMECA è una derivazione della FMEA rispetto alla quale include un'analisi delle criticità individuando la gravità delle conseguenze dei modi di guasto.

L'albero dei guasti è invece un procedimento *top-down,* deduttivo, perché parte da un guasto del sistema per individuare il guasto del singolo componente che l'ha causato. Tramite relazioni di tipo logico, impostate attraverso il percorso individuato con l'albero dei guasti, si identificano le relazioni fra i vari componenti durante il funzionamento del sistema, per giungere alla valutazione dell'affidabilità del sistema stesso.

Capitolo 2 - Panorama normativo

Il rapido sviluppo tecnologico nel settore dei sistemi di controllo ha portato i normatori a cercare di regolare con criteri quantitativi il livello di affidabilità dei sistemi di controllo che assolvono funzioni di sicurezza.
Le due norme che più nel dettaglio stabiliscono criteri e requisiti di sicurezza funzionale per i sistemi di controllo sono la EN IEC 62061 e la EN ISO 13849-1.

La EN IEC 62061 fornisce prescrizioni riguardanti i sistemi di controllo elettrici, elettronici ed elettronici programmabili, in applicazioni di sicurezza. Tali sistemi sono costituiti dall'insieme delle implementazioni di tutte le funzioni di sicurezza individuate nel processo di riduzione sistematica dei rischi, come previsto nella norma EN ISO 12100.

La EN ISO 13849-1 è una norma di tipo B1 nata dalla collaborazione tra il CEN/TC 114 e l'ISO/TC 199 (Safety of Machinery Technical Committee), al fine di dare a progettisti e costruttori di sistemi di controllo delle macchine uno strumento in linea con lo sviluppo tecnologico, considerato soprattutto l'impiego, sia in ambito meccanico che idraulico e pneumatico, di componenti elettrici ed elettronici programmabili e lo sviluppo della meccatronica nell'ambito industriale.

Entrambe le norme fondano la loro applicazione su un parametro di valutazione delle prestazioni delle funzioni di sicurezza realizzate dal sistema di controllo, legato a figure di merito di affidabilità. Per la EN IEC 62061 tale parametro è il *SIL* (*Safety Integrity Level*), mentre per la EN ISO 13849-1 è il *PL* (*Performance Level*). In entrambi i casi, si tratta di intervalli di valori della probabilità che possano verificarsi dei guasti pericolosi in un'ora.
Il cambiamento rispetto al passato è sostanziale, in quanto si passa da una visione deterministica, in cui un sistema di controllo veniva realizzato secondo strutture ed architetture definite da regole rigide, ad una metodologia basata sulla valutazione della prestazione ottenibile dal sistema e dalle sue parti in termini di probabilità di guasto. Non più, dunque, schemi rigidamente prefissati, ma da scegliere in base a valutazioni affidabilistiche e probabilistiche.

In entrambe le norme sono descritte procedure per la progettazione e la realizzazione di sistemi di controllo di sicurezza, in modo che questi tendano ad avere valori di probabilità di guasto pericoloso entro parametri predeterminati e ritenuti tollerabili per un certo tipo di applicazione. In entrambe le norme, la valutazione dei parametri che misurano il grado di sicurezza è connessa alla tipologia di architettura adottata per il sistema di controllo.

Nella norma EN ISO 13849-1 il livello di prestazione voluto (*PL*) per l'affidabilità del sistema di controllo, si ottiene facendo riferimento a 5 categorie (cat. B, cat. 1, cat. 2, cat. 3, cat. 4) ed a parametri di affidabilità a queste associati, quali il $MTTF_d$ (tempo medio al guasto pericoloso), la copertura diagnostica DC (il rapporto fra la frequenza dei guasti pericolosi rilevati λ_{dd} e la frequenza dei guasti pericolosi totali λ_d) ed i guasti di causa comune CCF. Le categorie non sono altro che architetture che indicano come il sistema di controllo è stato realizzato (es. ridondanza, canale singolo, test…). Per ciascuna di esse sono indicati il comportamento al guasto, i requisiti richiesti, i principi da utilizzare per raggiungere la sicurezza funzionale ed in generale il comportamento della parte che implementano. Utilizzando sistemi con categoria più alta, è possibile raggiungere livelli di sicurezza più alti in termini di probabilità di guasto, viceversa se si fissa un determinato livello di sicurezza, alcune categorie potrebbero non essere utilizzabili per ottenerlo: in

ogni caso bisogna tener presente che il livello di sicurezza, nonché la prestazione e la probabilità di guasto, devono essere correttamente armonizzate al rischio da ridurre con la funzione da implementare e quindi all'analisi preventivamente fatta prima di iniziare la realizzazione del sistema.

Nella EN IEC 62061 il *SIL* è il parametro che in base al suo valore determina il grado di affidabilità richiesto ad una SRCF (Safety Related Control Function – funzione di controllo relativa alla sicurezza) in riferimento al rischio considerato ed è l'analogo del *PL* per la norma EN ISO 13849-1, tanto che è possibile stabilire una corrispondenza. Tale parametro è espresso sulla base di una scala di probabilità oraria che si verifichino guasti pericolosi (Probability of dangerous Failure per Hour), indicata con la sigla PFH_D. La classificazione del SIL della EN IEC 62061 è riportata nella tabella 1.
Il concetto di SIL, ed indirettamente quello di *PL*, è stato ripreso dalla norma IEC 61508, documento dal quale derivano sia la norma EN IEC 62061 sia la norma EN ISO 13849-1.

Probabilità media di un guasto pericoloso (PFH_D) [h^{-1}]	***SIL* (IEC 61508)**
$10^{-6} \leq PFH_D < 10^{-5}$	1
$10^{-7} \leq PFH_D < 10^{-6}$	2
$10^{-8} \leq PFH_D < 10^{-7}$	3

Tabella 1: Classificazione del *SIL* (EN IEC 62061)

Come è possibile notare, al crescere dei valori del *SIL*, la probabilità che possano verificarsi guasti pericolosi è via via sempre più bassa, di modo che si possa assumere che il sistema di controllo sia sempre più affidabile.

Anche nella ISO EN 13849-1 il *PL* è quantificato con la probabilità che si verifichino guasti pericolosi in un'ora (PFH_D).
La norma definisce cinque intervalli probabilistici ad ognuno dei quali è assegnato un *PL*, come indicato nella tabella 2. Nella stessa tabella è riportata la corrispondenza con il *SIL*.
A titolo esemplificativo, una probabilità oraria media di guasto pericoloso di 10^{-6} h^{-1} esprime la possibilità che si verifichi mediamente un guasto pericoloso ogni milione di ore e corrisponde ad un valore di *PL* = *c* e di *SIL* = 1.

***PL* (EN ISO 13849)**	**Probabilità media di un guasto pericoloso (PFH_D) [h^{-1}]**	***SIL* (IEC 61508)**
a	$10^{-5} \leq PFH_D < 10^{-4}$	Non definito
b	$3 \cdot 10^{-6} \leq PFH_D < 10^{-5}$	1
c	$10^{-6} \leq PFH_D < 3 \cdot 10^{-6}$	1
d	$10^{-7} \leq PFH_D < 10^{-6}$	2
e	$10^{-8} \leq PFH_D < 10^{-7}$	3

Tabella 2: Classificazione del *PL* e confronto con il *SIL* (EN ISO 13849-1)

Dopo la prima fase di analisi e valutazione dei rischi, connessi all'utilizzo della macchina, durante il processo di riduzione del rischio e quindi all'atto dell'applicazione di misure per

una progettazione intrinsecamente sicura (EN ISO 12100), vengono identificate le funzioni di sicurezza necessarie, con le loro specifiche e caratteristiche e viene determinato per ciascuna di esse il *PL* richiesto (PL_r) oppure il *SIL assegnato*, a seconda della norma applicata. Infatti, il progettista del sistema di controllo, dopo aver individuato la funzione di sicurezza per uno specifico compito della macchina, deve individuare quale valore di *PL* sia da ritenere accettabile per la data applicazione; tale valore è indicato come PL_r. Per far questo si utilizza un processo decisionale come il grafico ad albero suggerito dalla norma e riportato nella figura 2 seguente.

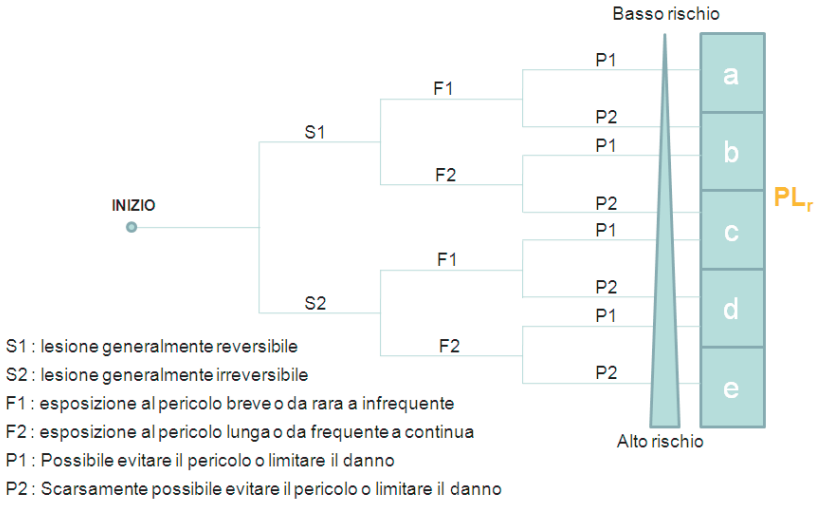


Figura 2: Determinazione del PL_r (livello di prestazione richiesto - EN ISO 13849-1)

Il compito successivo è quello di definire la parte del sistema di controllo relativa alla sicurezza (SRP/CS), cioè che esplica la funzione di sicurezza, rappresentarla con uno schema logico e determinarne il *PL* in base alla categoria, al $MTTF_d$, al DC ed al CCF. L'opera si conclude verificando che *PL* sia ≥ PL_r.

La norma EN ISO 13849-1 propone un metodo semplificato per la determinazione del *PL* di una funzione di sicurezza, che si basa sull'applicazione del modello di Markov ad architetture designate dette categorie (la norma ne prevede 5, le stesse della norma EN 954, ritirata), descritte nei paragrafi successivi. L'applicazione ha portato alla seguente rappresentazione grafica (figura 3), che mette in relazione le Categorie, il $MTTF_d$, il DC ed il CCF con i *PL* ottenibili.

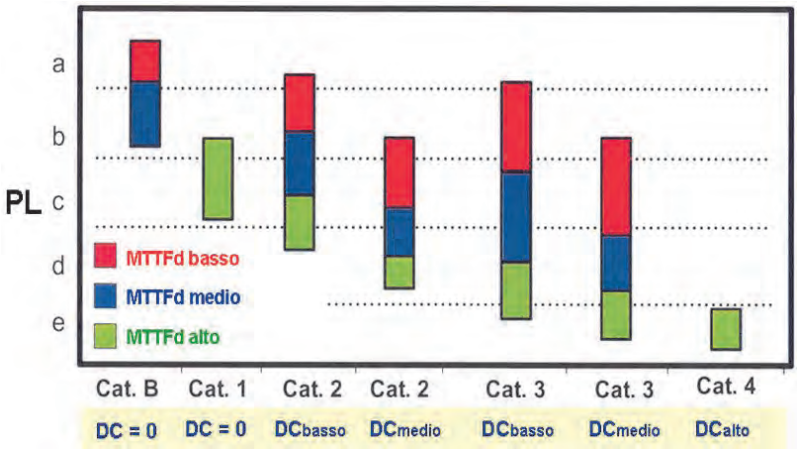


Figura 3: Relazione tra Categorie, $MTTF_d$, DC e CCF con i *PL* ottenibili (EN ISO 13849-1)

Dal grafico di figura 3 è possibile risalire, una volta determinati i parametri significativi, al *PL* della SRP/CS.
È anche disponibile una rappresentazione numerica dei valori del *PL* (Allegato K della norma EN ISO 13849-1), in termini di probabilità di guasto pericoloso per ora (PFH_D).

Per il $MTTF_d$ ed il DC sono considerati i seguenti intervalli (tabelle 3 e 4).

Basso	3 anni ≤ $MTTF_d$ < 10 anni
Medio	10 anni ≤ $MTTF_d$ < 30 anni
Alto	30 anni ≤ $MTTF_d$ ≤ 100 anni

Tabella 3: Intervalli per $MTTF_d$ (EN ISO 13849-1)

Nessuna	DC < 60%
Bassa	60% ≤ DC < 90%
Media	90% ≤ DC < 99%
Alta	99% ≤ DC

Tabella 4: Intervalli per DC (EN ISO 13849-1)

Il processo è riassunto dalla procedura iterativa mostrata in figura 4. In tale figura la fase che richiede un'ulteriore iterazione è necessaria quando alla fine della validazione si individua il mancato rispetto di un requisito.

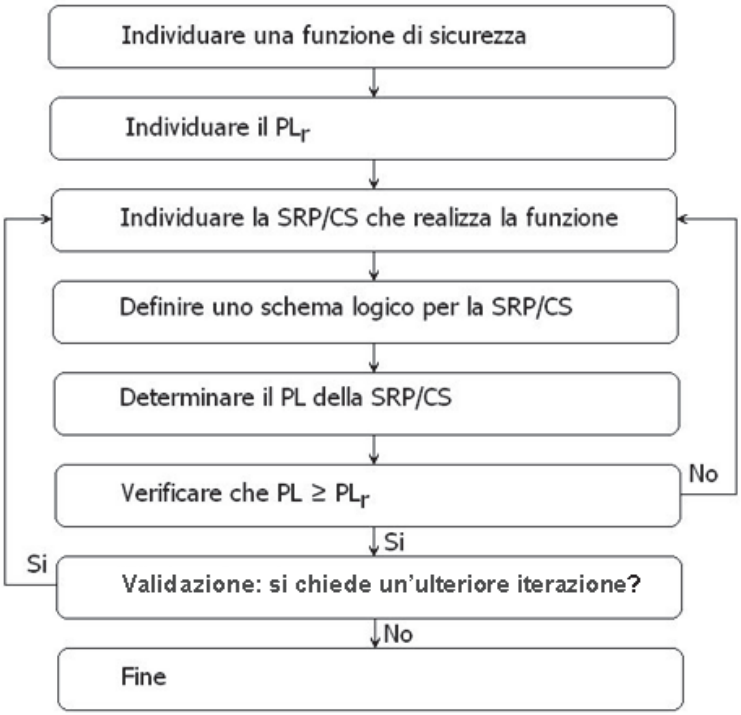


Figura 4: Procedura descritta nella norma ISO EN 13849-1

Il CCF rappresenta i guasti da causa comune che derivano da un unico evento ma che non dipendono gli uni dagli altri. Un metodo semplificato attribuisce ad ogni misura applicata un punteggio fisso ed un punteggio minimo da rispettare.

Analogamente, per la EN IEC 62061, viene assegnato un SIL alla funzione di sicurezza con una procedura che utilizza una matrice del rischio come indicato in tabella 5.

Conseguenze	Gravità	Classe					Durata		Probabilità	Evitabilità
		3-4	5-7	8-10	11-13	14-15				
Morte, perdita braccio/occhio	4	*SIL*2	*SIL*2	*SIL*2	*SIL*3	*SIL*3	≤1 ora	5	Molto alta 5	
Permanente, perdita dita	3		OM	*SIL*1	*SIL*2	*SIL*3	da >1 ora a ≤ 1 giorno	5	Probabile 4	
Reversibile, cure mediche	2			OM	*SIL*1	*SIL*2	da >1 giorno a ≤ 2 settimane	4	Possibile 3	Impossibile 5
Reversibile, pronto soccorso	1				OM	*SIL*1	da > 2 settimane a ≤ 1 anno	3	Scarsa 2	Possibile 3
							> 1 anno	2	Trascurabile 1	Probabile 1

Tabella 5: Matrice del rischio (EN IEC 62061)

In base alla somma dei punteggi di durata, probabilità ed evitabilità, assegnati per un evento pericoloso, si determina la classe e successivamente, nella tabella 5, dall'intersezione fra la colonna "conseguenze" e la colonna "classe", si ricava il *SIL* da assegnare alla funzione di sicurezza; OM sta per "altre misure" (other measures) da utilizzare a livello di raccomandazione.

Successivamente, viene eseguita la progettazione del sistema di controllo secondo una procedura che ricorda molto da vicino quella descritta nella figura 4.
Tale procedura prevede la suddivisione dell'intero sistema di controllo in funzioni di sicurezza; in seguito tali funzioni sono suddivise in blocchi funzionali e ciascun blocco funzionale è associato ad un sottosistema hardware per la realizzazione fisica (uno stesso sottosistema hardware può realizzare blocchi funzionali di funzioni diverse).
Ciascun sottosistema è sottoposto a vincoli di architettura che definiscono le caratteristiche della struttura ed il suo comportamento al guasto: tali vincoli sono complessivamente rappresentati nella tabella 6 seguente, in cui compaiono i parametri Safe Failure Fraction (SFF) e tolleranza all'avaria (N).

Frazione di guasti in sicurezza SFF	**Tolleranza N all'avaria dell'hardware**		
	0	**1**	**2**
SFF < 60%	Non permesso	*SIL*1	*SIL*2
60% ≤ SFF < 90%	*SIL*1	*SIL*2	*SIL*3
90% ≤ SFF < 99%	*SIL*2	*SIL*3	*SIL*3
99% ≤ SFF	*SIL*3	*SIL*3	*SIL*3

Tabella 6: Vincoli di architettura (EN IEC 62061)

SFF è il rapporto fra i guasti non pericolosi (λ_s+ λ_{dd}) ed i guasti totali (λ_s + λ_d), dove λ_s sono i guasti sicuri, λ_{dd} quelli pericolosi rilevati e λ_d sono quelli pericolosi. Si fa notare che per λ_s = 0, SFF e DC coincidono.
La tolleranza all'avaria rappresenta la capacità di un sottosistema di continuare ad eseguire una funzione richiesta in presenza di avarie: una tolleranza N indica che N+1 guasti possono causare la perdita della funzione di sicurezza (per esempio N=0 significa che un guasto può causare la perdita della funzione di sicurezza).
I valori di SFF e tolleranza all'avaria stabiliti per un sottosistema in funzione della sua architettura (ridondanza, monitoraggio, scelta dei componenti) determinano il valore massimo di *SIL* che può essere richiesto per un sottosistema.
La probabilità di guasto casuale dell'hardware PFH_D del sistema viene calcolata come la somma delle probabilità di guasto pericoloso per ora del sottosistema o di tutti i sottosistemi che implementano la funzione di controllo di sicurezza, compresa la probabilità di errori pericolosi di trasmissione PTE:

$$PFH_D = PFH_D + \ldots\ldots + PFH_D + PTE$$

La norma suggerisce un metodo semplificato per il calcolo della probabilità di guasto pericoloso dell'hardware PFH_D di un sottosistema per 4 architetture base indicate con "A", "B", "C", "D", descritte nei paragrafi successivi.

Entrambe le norme EN ISO 13849-1 e EN IEC 62061 prevedono misure per evitare i guasti sistematici ed una lunga serie di criteri per la sicurezza del software applicativo ed incorporato.

Le Architetture designate della norma EN IEC 62061

Come anticipato, la norma EN IEC 62061 propone un metodo semplificato di valutazione del PFH_D complessivo dello schema logico che realizza la funzione di sicurezza, che si basa su quattro architetture prestabilite, denominate rispettivamente Architettura A, B, C e D, per ognuna delle quali vengono fornite formule per il calcolo.
È opportuno notare che un'architettura costituisce un sottosistema e che il sottosistema è rappresentato da blocchi logici quali elementi costituenti.

Architettura A - Tolleranza zero ai guasti e nessuna funzione di diagnostica

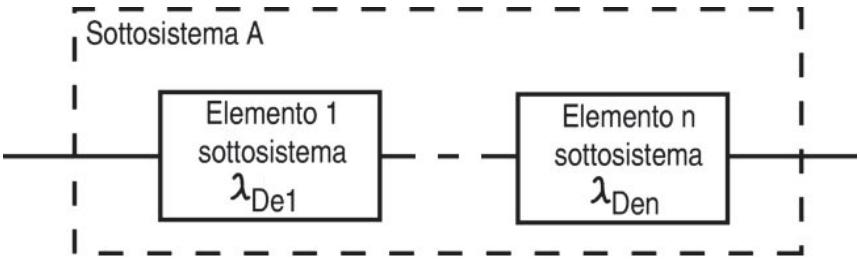


Figura 5: Schema logico Architettura A (EN IEC 62061)

L'architettura è costituita da più blocchi che si trovano in serie logica (figura 5), per cui il guasto di uno solo di essi determina la perdita della funzione di sicurezza.
Se si conoscono i valori dei tassi di guasto pericoloso per ogni singolo elemento, allora è possibile determinare il tasso di guasto pericoloso del sottosistema per mezzo della seguente relazione:

$PFH_{DSSA}=\lambda_{DSSA}\times 1\ [h]$

dove

$\lambda_{DSSA}= \lambda_{De1}+.....+ \lambda_{Den}$

λ_{Dei}= tasso dei guasti pericolosi dell'elemento e_i, per i=1,...n.

Architettura B - Tolleranza singola ai guasti e nessuna funzione di diagnostica

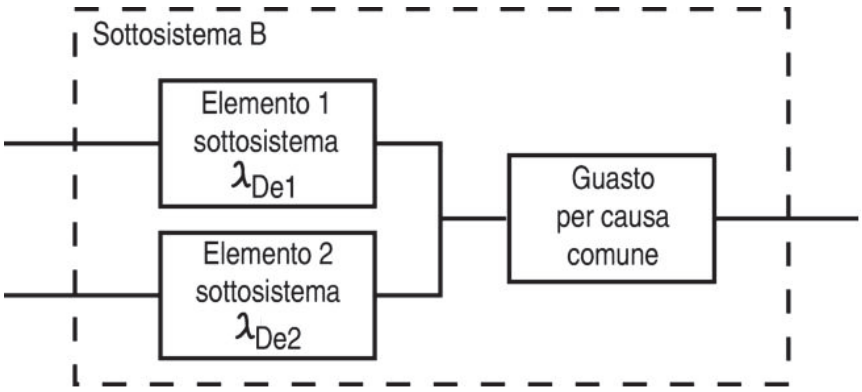


Figura 6: Schema logico Architettura B (EN IEC 62061)

L'architettura è costituita da due blocchi che si trovano in parallelo logico (figura 6), per cui la perdita della funzione di sicurezza si ha solo nel caso di guasto di entrambi i blocchi. Una volta noto il peso dei guasti di causa comune (CCF – *Common Cause Failure* – il parametro β della coppia di sottosistemi *De*1 e *De*2), si determina il tasso di guasto del sistema complessivo per mezzo della seguente relazione:

$PFH_{DSSB}=\lambda_{DSSB}\times 1$ [*h*]

dove

$\lambda_{DSSB}= (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2}\times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

β =suscettibilità a guasti per cause comuni (frazione dei guasti per causa comune);

T_1= valore inferiore tra l'intervallo di verifica periodica ed il ciclo di vita.

Gli altri simboli hanno il significato usuale.

Architettura C - Tolleranza zero ai guasti con funzione di diagnostica

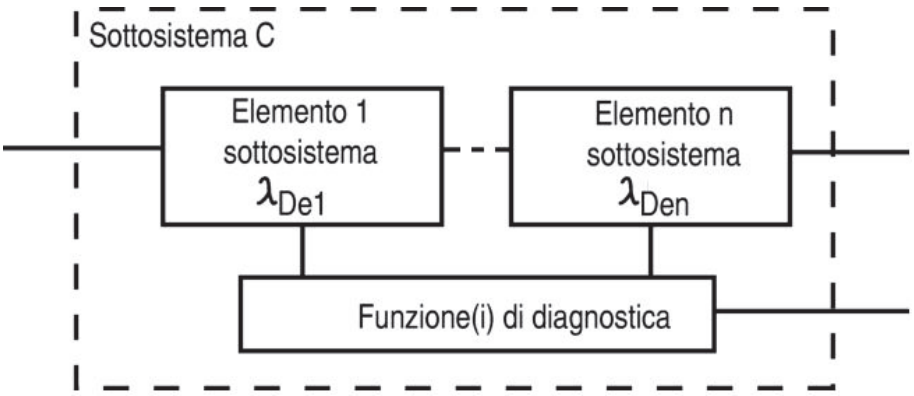


Figura 7: Schema logico Architettura C (EN IEC 62061)

L'architettura è costituita da più blocchi che si trovano in serie logica (figura 7), per cui il guasto di uno solo di essi, in assenza di eventuali interventi volti a ripristinare la funzionalità, determina la perdita della funzione di sicurezza.
Allo scopo di contrastare la perdita è inserito un blocco diagnostico, eventualmente integrato a livello del singolo sottosistema, che, nel caso rilevi il guasto, attiva una reazione successiva all'avaria stessa.
Ciò garantisce un intervento tempestivo ed evita la perdita della funzione di sicurezza. In questo caso si avrà:

$PFH_{DSSC}=\lambda_{DSSC}\times 1$ [*h*]

dove

$\lambda_{DSSC}= \lambda_{De1}\times(1-DC_1)+...+\lambda_{Den}\times(1-DC_n)$

$\lambda_D=\lambda_{DD}+\lambda_{DU}$ è il tasso dei guasti pericolosi;

λ_{DU} è il tasso dei guasti pericolosi non rilevabili $\lambda_{DU}=\lambda_D(1-DC)$;

λ_{DD} è il tasso dei guasti pericolosi rilevabili $\lambda_{DD}=\lambda_D DC$;

DC_1, DC_2,...DC_n, è la percentuale degli errori rilevati dalla copertura diagnostica (*Diagnostic Coverage*) per ciascuno degli elementi del sottosistema.

Gli altri simboli hanno il significato usuale.

Architettura D - Tolleranza singola ai guasti con funzione di diagnostica

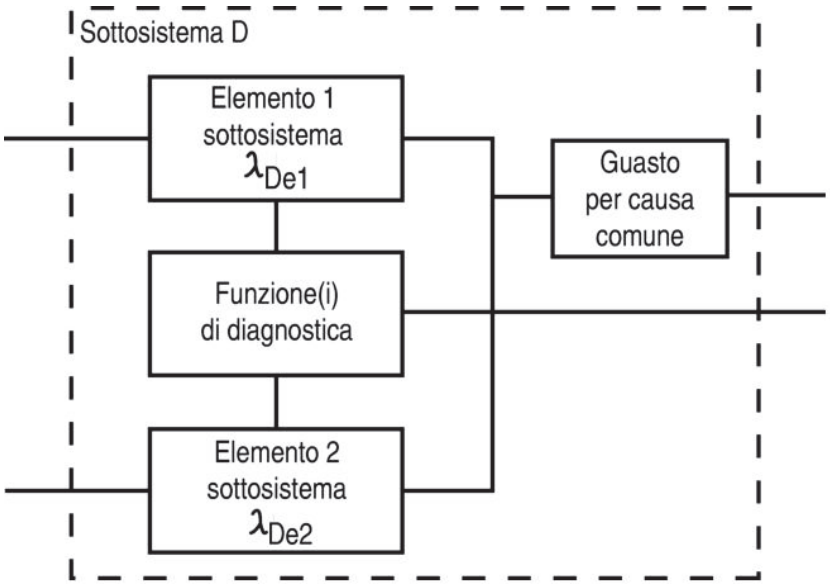


Figura 8: Schema logico Architettura D (EN IEC 62061)

L'architettura è costituita da due blocchi che si trovano in parallelo logico (figura 8), per cui la perdita della funzione di sicurezza si ha solo nel caso di guasto di entrambi i blocchi. Allo scopo di contrastare la perdita è inserito un blocco diagnostico, eventualmente integrato a livello del singolo sottosistema che, nel caso rilevi guasti, attiva opportune azioni correttive.
La probabilità oraria che si verifichino guasti pericolosi è data da:

$PFH_{DSSD}=\lambda_{DSSD}\times 1\ [h]$

dove

$$\lambda_{DSSD}= (1-\beta)^2\{[\lambda_{De1}\times\lambda_{De2}\times(DC_1+DC_2)]\times T_2/2+[\lambda_{De1}\times\lambda_{De2}\times(2-DC_1-DC_2)]\times T_1/2\}+\beta\times(\lambda_{De1\ x}\,\lambda_{De2})^{1/2}$$

T_1= valore inferiore tra l'intervallo di verifica periodica ed il ciclo di vita;

T_2= intervallo di prova diagnostica.

Gli altri simboli hanno il significato usuale.

Le Categorie della norma EN ISO 13849-1

Nel caso della norma EN ISO 13849-1, le architetture base utilizzate per l'applicazione del metodo semplificato sono le categorie. Per analogia con la norma EN IEC 62061 diremo

che una categoria equivale ad un sottosistema. Le categorie proposte, come già indicato,sono cinque, hanno caratteristiche diverse e con esse è possibile realizzare interamente una parte del sistema di controllo (SRP/CS) che implementa una specifica funzione di sicurezza.

Figura 9: Schema logico (architettura) delle categorie B e 1 (EN ISO 13849-1)

La categoria B è strutturata come un'architettura a canale singolo, composta da tre elementi (figura 9): un blocco di Input (blocco I), un blocco per la logica per l'elaborazione dei dati (blocco L) ed un blocco di attuazione per le uscite (blocco O). Il canale è progettato per soddisfare requisiti minimi di affidabilità intrinseca del sistema e dei suoi componenti.
Tali requisiti prevedono l'applicazione delle norme e dei principi di base per garantire la resistenza della funzione di sicurezza agli stress ed alle sollecitazioni (anche ambientali) previste. Soddisfare tali requisiti è una prescrizione comune per tutte le categorie. Non è prevista copertura diagnostica, il valore del $MTTF_d$ può variare da basso a medio, la valutazione del CCF non è applicabile. Un guasto nel canale può portare alla perdita della funzione di sicurezza.

La categoria 1 è anch'essa strutturata come un'architettura a canale singolo e per essa continua a valere lo schema a blocchi di figura 9. Per tale categoria, ai requisiti previsti per la categoria B, è aggiunto l'obbligo di utilizzare componenti e principi di sicurezza di valore ben provato (well tried). Un componente è tale quando la sua affidabilità è garantita dal fatto che è stato già utilizzato in moltissime altre applicazioni e pertanto se ne conoscono bene limiti, modi di guasto e comportamento al guasto, oppure quando è progettato, costruito e verificato utilizzando criteri e principi ritenuti universalmente idonei per la sicurezza. Anche in questa architettura non è prevista copertura diagnostica e la valutazione del CCF non è applicabile; viceversa il valore del $MTTF_d$ deve essere alto.

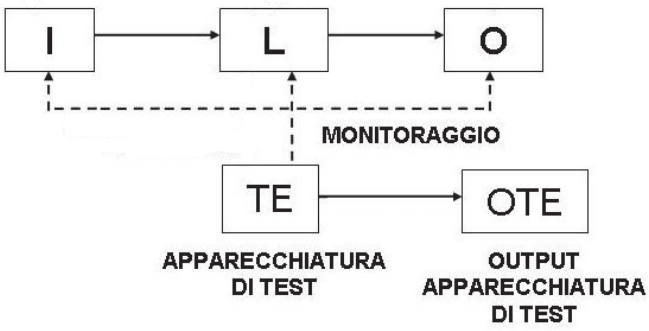


Figura 10: Schema logico (architettura) della categoria 2 (EN ISO 13849-1)

La categoria 2 è anch'essa strutturata come un'architettura a canale singolo (figura 10), a cui, però, è aggiunto un ramo per il test della funzione di sicurezza. Tra i requisiti, oltre a quelli validi per la categoria B, vi è l'adozione di principi di sicurezza di comprovato valore (well tried safety principles) e la verifica (test) della funzione di sicurezza ad opportuni intervalli di tempo. Con ciò si intende che i test devono essere effettuati dal sistema di controllo nei momenti e nelle fasi ritenute più significative, come l'avvio o l'esecuzione di movimenti e procedure pericolose. È evidente che la funzione di sicurezza può essere persa nell'intervallo fra due test, ma tale perdita deve essere necessariamente rivelata al momento dell'esecuzione del test.
Quando il guasto è rivelato, il sistema di controllo porta la macchina in una condizione sicura che è mantenuta finché il guasto non è eliminato.
Il livello previsto di copertura diagnostica è basso o medio, il valore del $MTTF_d$ può essere basso, medio od alto e devono essere presi in considerazione i guasti dovuti a cause comuni (CCF).
Come facilmente constatabile dalla figura 10, l'architettura corrispondente alla categoria 2 presenta una struttura semplice a canale singolo con controlli diagnostici; il risultato del test di verifica è demandato ad un blocco denominato OTE che, in caso di guasto rilevato, è in grado di segnalarne la presenza ed eventualmente di avviare opportune azioni di allarme e correttive. La categoria 2 ha due importanti vincoli:

- frequenza di richiesta di un'azione di sicurezza pari ad 1/100 della frequenza di test;
- $MTTF_d$ del canale di test maggiore della metà del $MTTF_d$ del canale della funzione.

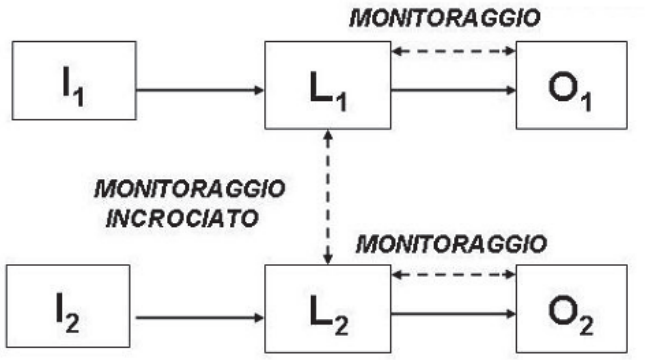


Figura 11: Schema logico (architettura) delle categorie 3 e 4 (EN ISO 13849-1)

La categoria 3 è strutturata come un'architettura a canale doppio (figura 11). Le unità logiche dei due canali sono dotate di funzione di diagnostica e tale diagnostica è effettuata sia sulla base di segnali di monitoraggio che per mezzo dell'analisi dei dati scambiati. Per la categoria è richiesto che siano rispettati, oltre ai requisiti della categoria B, anche i principi di sicurezza di comprovato valore come nel caso precedente. Inoltre, è necessario che un singolo guasto non porti alla perdita della funzione di sicurezza e, quando possibile, sia rivelato.
Questo significa che non tutti i guasti possono essere individuati e che il loro accumulo potrebbe portare alla perdita della funzione di sicurezza.

Il livello previsto di copertura diagnostica è basso o medio, il valore del $MTTF_d$ può essere basso, medio o alto e devono essere presi in considerazione i guasti dovuti a cause comuni (CCF).

La categoria 4 è strutturata anch'essa come un'architettura a canale doppio (figura 11). Per la categoria è richiesto che siano rispettati, oltre ai requisiti della categoria B, anche i principi di sicurezza di comprovato valore come nel caso precedente. Il singolo guasto non deve portare alla perdita della funzione di sicurezza e deve essere rivelato in occasione della richiesta della funzione di sicurezza o prima della richiesta successiva. Per tale categoria i requisiti prevedono la possibilità che si verifichi un accumulo dei guasti, ma devono essere presi provvedimenti affinché questo non comporti la perdita della funzione di sicurezza.
Il livello previsto di copertura diagnostica è alto, il valore del $MTTF_d$ è anch'esso alto e devono essere presi in considerazione i guasti dovuti a cause comuni (CCF).

Nella tabella 7 seguente sono riassunte le caratteristiche delle diverse categorie.

	Requisiti caratteristici	**DC**	**$MTTF_{dB}$**	**CCF**
B	Adozione di norme e principi di base (requisito valido anche per le altre categorie).	Nulla	Basso, Medio	No
1	Adozione di principi di sicurezza ben provati. Adozione di componenti ben provati.	Nulla	Alto	No
2	Adozione di principi di sicurezza ben provati Monitoraggio periodico e in determinate situazioni.	Bassa, Media	Basso, Medio, Alto	Si
3	Adozione di principi di sicurezza ben provati. Monitoraggio periodico e in determinate situazioni. Un singolo guasto non porta alla perdita della funzione di sicurezza.	Bassa, Media	Basso, Medio, Alto	Si
4	Adozione di principi di sicurezza ben provati. Monitoraggio periodico e in determinate situazioni. Un singolo guasto non porta alla perdita della funzione di sicurezza, l'accumulo di guasti non rilevati non porta alla perdita della funzione di sicurezza.	Alta + tolleranza all'accumulo dei guasti	Alto	Si

Tabella 7: Caratteristiche delle diverse categorie

La categoria B e la categoria 1 hanno la stessa struttura logica; la categoria 1 ha semplicemente requisiti più severi per i componenti e per il $MTTF_d$. Per la categoria 1 è richiesto in più l'uso di componenti ben provati (well tried).
Le altre tre categorie (2, 3 e 4) richiedono il ricorso anche a misure protettive sistemiche, come risulta evidente dai diagrammi più complessi. Infatti, richiedono una progettazione che, oltre all'affidabilità dei componenti, prenda in debita considerazione due ulteriori principi: il monitoraggio (monitoring) e la tolleranza ai guasti. La categoria 3 e la categoria 4 hanno la stessa struttura logica; la categoria 4 ha semplicemente requisiti più severi per la copertura diagnostica (DC) e per il $MTTF_d$, il singolo guasto deve essere rilevato e l'accumulo dei guasti non deve portare alla perdita della funzione di sicurezza. Il doppio canale è adottato per poter ottenere la tolleranza ai guasti. Da notare che la struttura a doppio canale consente anche il monitoraggio incrociato (cross monitoring) tra i due canali.

Il B_{10} per i componenti pneumatici, meccanici ed elettromeccanici

Per componenti soggetti a guasto meccanico (es. relè, elettrovalvole) il parametro generalmente utilizzato per definire l'affidabilità è il B_{10}. Tale parametro è definito come il tempo o il numero di cicli in corrispondenza dei quali il 10% dei componenti presenta dei guasti. Tra i guasti che si possono verificare assumono particolare rilevanza quelli definiti pericolosi; in questo caso l'indicazione è espressa con B_{10d}, dove il pedice *d* (dangerous) indica proprio il fatto che si tratta di guasti pericolosi. Se il valore B_{10d} non è dato esplicitamente, allora è possibile assumere che la frazione dei guasti pericolosi sia il 50% del totale. Ciò significa che il numero di cicli al termine dei quali il 10% dei componenti presenterà un guasto pericoloso è il doppio del numero di quelli relativi al B_{10}. La norma EN ISO 13849-1 propone quindi $B_{10d} = 2 \cdot B_{10}$ come valore raccomandato per tale parametro.

Il valore del $MTTF_d$ può essere determinato grazie ai due parametri B_{10d} e n_{op}; quest'ultimo individua il numero medio di operazioni l'anno effettuate dal componente. La relazione da utilizzare è la seguente:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

dove

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cycle}}$$

d_{op} = numero medio di giorni di lavoro per anno,
h_{op} = durata media di una giornata di lavoro, in ore al giorno,
t_{cycle} = tempo medio tra l'inizio di due cicli successivi di un componente, in secondi per ciclo.

Il *tempo operativo* di un componente è limitato dal valore di T_{10d} che è il tempo medio in corrispondenza del quale il 10% dei componenti presenta un guasto pericoloso. Pertanto si ha:

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

La EN ISO 13849-1 assume, in prima approssimazione, una funzione di distribuzione dei guasti di tipo esponenziale, ovvero: $F(t) = 1 - e^{(-\lambda_d t)}$. Nel caso in cui si sostituiscano in tale espressione i seguenti valori: $t = T_{10d}$ e $F(T_{10d})$=10%, e si cerchi di risolvere esplicitando il tasso di guasto λ_d, questo può essere approssimato con la seguente relazione:

$$\lambda_d \approx \frac{0{,}1}{T_{10d}} \approx \frac{0{,}1 \times n_{op}}{B_{10d}}$$

Con $MTTF_d = 1/\lambda_d$ si ha quindi la formula per il calcolo del $MTTF_d$ in funzione di B_{10d} e di n_{op} presentata in precedenza.

I dati sui tassi di guasto

Ai fini progettuali, per mezzo della scomposizione del sottosistema che realizza una data funzione di sicurezza nel suo schema logico, la determinazione del $MTTF_d$ per ogni singolo componente consente poi di ricavare il valore di tale parametro per l'intero sottosistema.
Pertanto, la domanda preliminare ai processi di progettazione e realizzazione di un sistema di controllo è: *dove è possibile reperire i dati di affidabilità di un componente*?

Il problema non è sempre semplice, data la vastità di componenti in commercio la necessità spesso spinge i costruttori ad operare scelte sui componenti da adottare, in base alla reperibilità delle informazioni. Ciò penalizza quei fabbricanti di componenti, che non compiono sui propri componenti quegli studi che si rendono necessari per fornire dati sull'affidabilità.

Oltre ai valori forniti dai fabbricanti, è possibile trovare dati sui tassi di guasto di taluni componenti anche nell'allegato C della EN ISO 13849-1 ed informazioni nell'Allegato D della EN ISO 13849-2, soprattutto nel caso di componenti elettrici, elettronici ed elettromeccanici.
È opportuno notare che, stante la riconosciuta carenza di dati per componenti idraulici, l'Allegato C di cui sopra fornisce informazioni per la determinazione, sotto prefissate condizioni, del valore di $MTTF_d$ di questi specifici componenti. Per essi si segnala anche che non esiste purtroppo una lista di componenti ben provati (well tried) all'interno della norma EN ISO 13849-2.

Si ricorda comunque che nell'Allegato C della ISO EN 13849-1 sono riportati i valori di $MTTF_d$ per differenti tipi di componenti: meccanici, idraulici, pneumatici, elettrici, elettromeccanici. Nel caso di applicazioni specifiche è preferibile l'utilizzo di dati più precisi, laddove i progettisti di sistemi di controllo ne dispongano.

Altri dati possono essere reperiti in apposite banche dati. In particolare, i dati che si possono trovare nelle norme prima citate sono stati tratti soprattutto dai seguenti standard industriali:

- SN 31920 "*Standard B_{10} values with continuous demand rate and failure rates in low demand mode of electromechanical components*"
- SN 29500 "*Failure rates of components*".

I valori di tasso di guasto determinati secondo lo standard SN 29500

Lo standard SN 29500 è uno standard industriale, ovvero uno standard elaborato da un costruttore per i propri fornitori o per altri costruttori interessati a realizzare sistemi in qualche modo compatibili con quelli da lui prodotti.

In tale standard l'unità di misura del tasso di guasto λ è definita con l'acronimo FIT (*Failure In Time*). Un FIT è equivalente ad un guasto ogni 10^9 ore.
Nello standard, quando si parla di *valore atteso del tasso di guasto,* si intende fare riferimento ad un valore del tasso di guasto ottenuto in *condizioni predeterminate.* Ciò significa che, cambiando le condizioni al contorno, i valori di tasso di guasto possono anche cambiare.

Lo scopo della parte 2 della SN 29500 è quello di fornire la metodologia di calcolo dei parametri relativi all'affidabilità di circuiti integrati realizzati in logica TTL e CMOS e distinti in relazione al grado di integrazione.

I valori di affidabilità dei parametri variano da un minimo di 2 FIT per transistori bipolari in logica TTL fino ad un massimo di 50 FIT per dispositivi BICMOS.

In generale, nello standard l'affidabilità dei singoli componenti è ottenibile con la relazione:

$$\lambda = \lambda_{ref} \times \pi_u \times \pi_T \times \pi_D$$

dove:

λ_{ref} = valore di riferimento del tasso di guasto, calcolato nelle condizioni tipiche di utilizzo dei componenti nella maggior parte delle applicazioni (parte 2.3, SN 29500-1),

π_u = parametro dipendente dalla tensione,

π_T = parametro dipendente dalla temperatura,

π_D = parametro dipendente dalla tensione di alimentazione.

Capitolo 3 - I PLC nei sistemi di controllo

Il crescente sviluppo tecnologico dei sistemi di controllo e l'esigenza di una maggiore produttività, hanno spinto negli ultimi anni i maggiori costruttori di sistemi di comando basati sui PLC (Programmable Logic Controller) a cercare di integrare in un unico sistema le funzioni della sicurezza e quelle di controllo.
Tali sistemi sono sempre più utilizzati sia per le macchine che per i grandi processi industriali.
Ciò è possibile grazie al notevole progresso nello sviluppo delle reti locali di comunicazione per lo scambio dei dati, dei protocolli di comunicazione e dei bus ridondanti per la comunicazione *fail-safe* tra CPU (Central Processing Unit), memorie e dispositivi di I/O (Input/Output).

Su questi aspetti i maggiori produttori mondiali di componentistica elettronica si confrontano, ed il confronto ha portato ad una notevole ridondanza dell'offerta di sistemi di controllo basati sull'utilizzo dei PLC in grado di integrare funzioni normali e funzioni di sicurezza.

L'elevato grado di flessibilità di impiego e la relativa semplicità di programmazione hanno reso l'uso di simili componenti molto diffuso.
Lo sviluppo dei linguaggi di programmazione dei PLC ha ulteriormente incrementato il livello di prestazione generale dei controllori.
Le specifiche tipiche dei linguaggi di programmazione dei PLC sono contenute nella parte 3 della norma IEC 61131 (EN 61131-3).

Soffermarsi sull'analisi dei moderni PLC è, quindi, necessario per capirne principi di funzionamento, architetture e possibili campi di impiego.

Funzionamento di un PLC

Il PLC è un computer industriale specializzato in origine nella gestione dei processi industriali. Il PLC esegue un programma ed elabora i segnali digitali ed analogici provenienti da sensori e diretti agli attuatori. Nel tempo, con la progressiva miniaturizzazione della componentistica elettronica e la diminuzione dei costi, è entrato anche nell'uso domestico (per le applicazioni domotiche).

I PLC sono costruiti per essere robusti: infatti, normalmente sono posti in quadri elettrici collocati in ambienti con interferenze elettriche, con temperature elevate o con grande umidità. In alcuni casi sono in funzione 24 ore su 24, per 365 giorni all'anno, su impianti che non possono fermarsi mai.

I sistemi a PLC hanno strutture che possono essere scelte in base al processo da automatizzare. Durante la progettazione del sistema di controllo, vengono scelte le schede adatte alle grandezze elettriche in gioco. Le varie schede sono quindi inserite sul *rack* del PLC e connesse ai bus.

Normalmente il PLC legge tutti gli ingressi, sia digitali che analogici (anche quelli sulle schede remote collegate al PLC con una connessione dedicata o con una rete di comunicazione). Dopo di ciò, memorizza il loro stato in una memoria che è detta *registro*

immagine degli ingressi. A questo punto le istruzioni di comando sono elaborate in sequenza dalla CPU e il risultato è memorizzato nel *registro immagine delle uscite*. Infine, le uscite fisiche sono attivate.

Poiché l'elaborazione delle istruzioni si ripete continuamente, essa è ciclica. Il tempo che il controllore impiega per una singola elaborazione viene detto tempo di ciclo (solitamente da 1 a 10 millisecondi).

Architettura di un PLC

La struttura di un PLC può essere schematizzata in modo semplice con la seguente distinzione in blocchi (figura 12):
- Unità di alimentazione;
- Bus indirizzi, dati e controllo;
- Unità di acquisizione (per i dati in ingresso);
- Unità centrale di elaborazione (CPU);
- Unità di memoria RAM;
- Unità di memoria ROM;
- Unità di uscita (per il condizionamento dei segnali e l'attuazione).

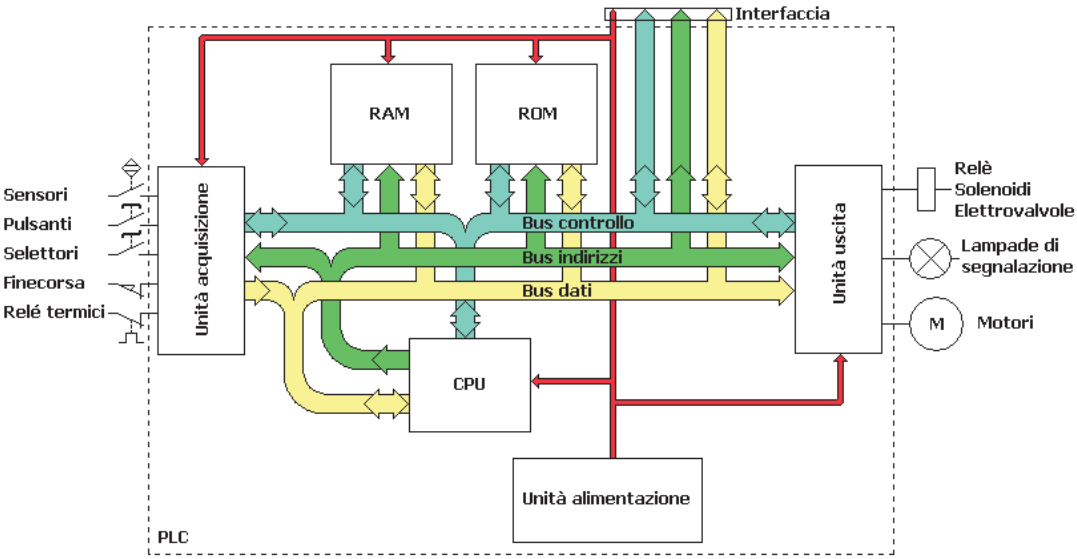


Figura 12: Architettura di un PLC

Il PLC esegue le operazioni in funzione del software (di sistema e/o applicativo) residente nella memoria.
Per il software applicativo esistono apposite unità di programmazione (figura 13), oppure, per sfruttare al meglio le possibilità offerte da interfacce grafiche più potenti, il software è sviluppato su PC o terminali esterni che possono essere connessi al PLC per il trasferimento dei programmi.
Ciascun blocco assolve ad una funzione specifica.

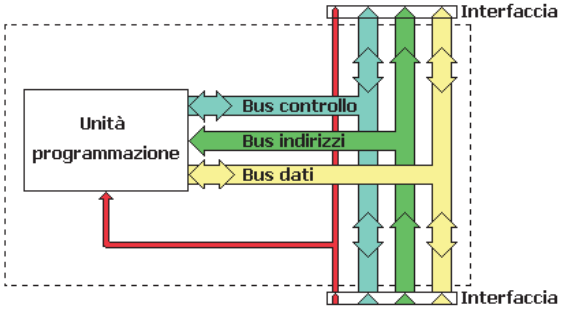


Figura 13: Architettura di un'unità di programmazione

Dal punto di vista costruttivo, i PLC sono distinti in *compatti* e *modulari.*
I PLC *compatti* sono costituiti da un unico dispositivo che racchiude al suo interno tutti i blocchi funzionali.
I PLC *modulari*, invece, sono dispositivi studiati per esigenze industriali più articolate, che necessitano di piattaforme di controllo espandibili. Sono composti da un dispositivo di base, che contiene oltre ai Bus ed alle unità della struttura tipica di un PLC anche una Unità di interfaccia e comunicazione.

I *moduli di espansione* (figura 14), connessi per mezzo dell'unità di interfaccia e comunicazione, vengono aggiunti in relazione alle esigenze industriali e sono costituiti da blocchi contenenti:
- Unità di acquisizione dei dati in ingresso;
- Unità di condizionamento dei segnali in uscita;
- Unità di interfaccia e comunicazione.

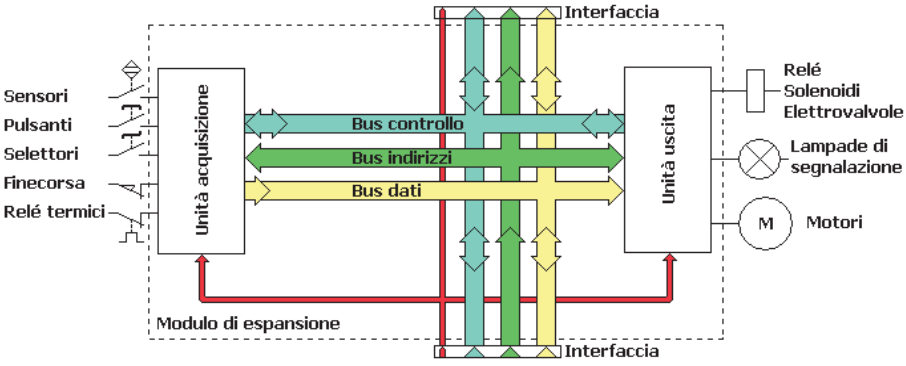


Figura 14: Architettura di un modulo di espansione

In relazione alla tipologia di operazioni, i PLC si dividono anche in PLC *sequenziali* e PLC *multifunzione*.

I primi sono impiegati laddove i processi prevedano l'esecuzione di sequenze preordinate di azioni, mentre i secondi consentono di gestire e sovrintendere processi che prevedano, oltre alle funzioni caratteristiche della logica sequenziale, anche prestazioni riconducibili a:
- Controllo e regolazioni di processo;
- Dialogo tra PLC e periferiche di I/O (anche tramite rete), dialogo tra PLC in rete.

Unità di alimentazione
L'unità di alimentazione si occupa di trasformare la tensione di rete in una serie di tensioni direttamente utilizzabili dai circuiti interni del PLC e dall'unità di uscita di quest'ultimo.
Valori tipici per le unità di alimentazione dei PLC sono:
- Tensione nominale di ingresso: 110V o 220V in AC $\pm$ 10%, con f=50Hz;
- Tensione nominale di uscita: 5V e 12V (o 24V) in DC;
- Corrente di uscita: variabile da 1 a 15A in relazione all'assorbimento dei moduli collegati.

In alcuni casi di PLC modulari anche gli alimentatori sono caratterizzati da un sistema modulare di collegamento: in caso di guasto di un'unità, la potenza richiesta è divisa tra le unità rimanenti, fino alla sostituzione del modulo difettoso (localizzabile di solito tramite lo stato di un LED).

Unità di acquisizione
L'unità di acquisizione serve a trasmettere informazioni al PLC.
I segnali, dal campo, vengono fatti arrivare con cavi elettrici fino alla morsettiera della scheda ed ogni singolo canale può essere protetto da fusibili di adeguato amperaggio.
Le informazioni possono essere di tipo *digitale* (lo stato di un interruttore, di un finecorsa, la presenza o l'assenza di un segnale, ecc.) o di tipo *analogico* (il valore di una grandezza continua).

Non sempre i segnali digitali possono essere gestiti direttamente dalla CPU. Infatti, mentre la tensione di funzionamento interna della CPU è bassa (di solito 5 V), i segnali digitali in ingresso al PLC possono presentarsi con livelli di tensione diversi (12, 24, 48, 110, 220 V). Inoltre, i segnali possono necessitare di amplificazione o essere affetti da rumore, disturbi, valori di *offset* e *portanti*. In tal caso devono essere *condizionati*, ovvero adattati di livello, demodulati e liberati da tutto ciò che non è funzionale al contenuto informativo.
Adattare il livello e le caratteristiche del segnale è uno dei compiti svolti dalle schede d'ingresso dell'unità di acquisizione.

Quando le informazioni che il PLC deve acquisire sono di tipo analogico, per poter essere elaborate o memorizzate, devono essere trasformate in valori numerici. Ciò avviene per mezzo di opportuni dispositivi detti convertitori analogico-digitali (A/D converter).
Non tutti i PLC sono in grado di gestire direttamente segnali analogici. Quelli in grado di farlo hanno una parte dell'unità di acquisizione dotata di schede di ingresso con in cascata uno stadio di condizionamento opportuno (per adattare il livello del segnale, eventualmente demodularlo e liberarlo da rumore e disturbi) e un convertitore analogico-digitale.
Queste schede sono disponibili con varie risoluzioni (8, 12, 14, 16 bit) e con 1 o più ingressi separati galvanicamente disponibili in morsettiera.
Le grandezze da convertire possono essere in tensione o in corrente. Ad esempio, sono disponibili schede per ingressi analogici in corrente, con un intervallo variabile tra 4mA e 20mA.

Molti costruttori di PLC rendono disponibili schede con ingressi analogici per sonde di temperatura, sia termoresistenze che termocoppie (T, J, K, ecc.).

All'interno dell'unità di acquisizione può essere contenuto il registro immagine degli ingressi, quando è realizzato con un *buffer* dedicato e non è contenuto nella RAM o tra le memorie interne della CPU.

Esistono poi opportuni segnali di interrupt che viaggiano sui bus di controllo in grado di avvisare l'unità centrale quando vi sono malfunzionamenti nell'unità di acquisizione, in modo che sia possibile avviare un'opportuna sub-routine di gestione del problema.

Unità centrale di elaborazione (CPU)
Il tipo di CPU influisce sull'affidabilità del PLC, sulla qualità delle sue prestazioni e sulla quantità di operazioni che possono essere svolte nell'unità di tempo.

Indipendentemente dalla complessità e dal contesto di utilizzo, la struttura di una CPU può essere schematizzata come nella figura 15 (che contiene molte semplificazioni e parti non indicate).

In fase di scelta di un PLC occorre valutare le capacità della CPU per conoscere se sarà in grado di gestire, nei tempi e nei modi dovuti, la complessità delle operazioni necessarie per il controllo da realizzare.

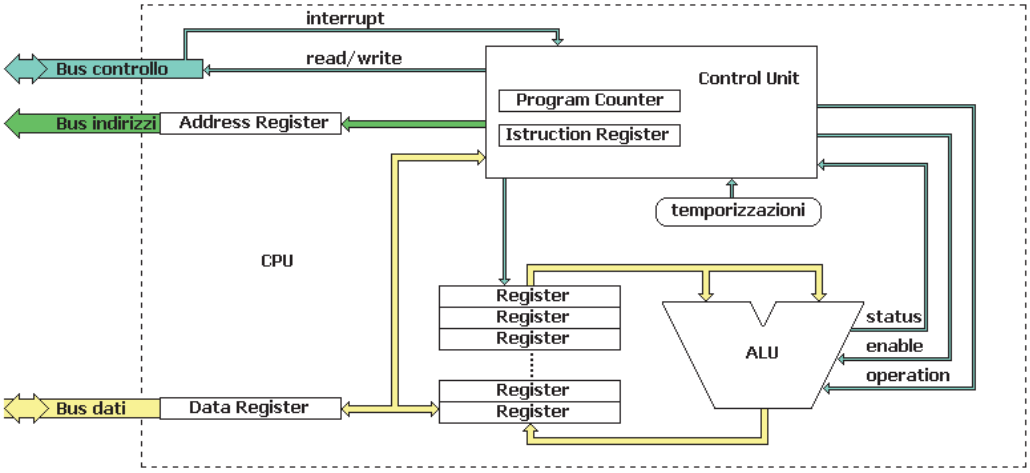


Figura 15: Schematizzazione di una CPU

All'interno della CPU vi è la Arithmetic Logic Unit (ALU) che esegue le operazioni sui dati conservati nei registri interni. Le operazioni sono eseguite quando la Control Unit (CU) dà l'abilitazione ad eseguire la specifica azione richiamata dal microprogramma attivato dall'istruzione corrente contenuta nell'Istruction Register (IR).
Una volta terminato il microprogramma, il Program Counter (PC) è incrementato e l'istruzione successiva, contenuta in memoria all'indirizzo indicato dal PC, è caricata nell'IR per essere eseguita.

I risultati sono poi trascritti, con altre istruzioni, dai registri interni alla memoria o all'unità di uscita, per essere utilizzati successivamente da altre istruzioni o per l'eventuale pilotaggio degli attuatori.

Tra i parametri utilizzati per la scelta di una CPU vi è il *tempo medio di esecuzione di un'istruzione*. I costruttori forniscono questo parametro caratterizzandolo in funzione delle operazioni eseguite dalla CPU. Viene fornito pertanto il tempo di esecuzione delle operazioni di lettura/scrittura, o su una singola parola, o su un singolo bit, o in virgola mobile.
Valori tipici sono:
- Tempo per un'operazione di lettura/scrittura: 0.075 ms
- Tempo per un'operazione su singolo bit: 0.075 ms
- Tempo per un'operazione su singola parola: 0.075 ms
- Tempo per un'operazione in virgola mobile: 0.225 ms

Naturalmente un ciclo del PLC è composto da tante operazioni, per cui la durata di un ciclo può raggiungere anche una decina di millisecondi.

Memorie
In funzione del tipo di informazioni da memorizzare, le memorie dei PLC possono essere suddivise in:
- Memoria di sistema;
- Memoria per i dati;
- Memoria per le istruzioni.

La **memoria di sistema** (comunemente denominata *firmware*) contiene le istruzioni per il funzionamento interno del PLC, come le routine di autodiagnosi, e il controllo dei moduli di espansione. In genere è realizzata con tecnologia ROM (o EPROM o EEPROM) e non è accessibile all'utente.

La **memoria per i dati**, contiene il risultato dell'elaborazione della CPU ed i valori dei dati provenienti dalle unità di acquisizione, o da inviare alle unità di uscita. È realizzata con tecnologia RAM.
Una parte di tale memoria, realizzata di solito in modo da non essere volatile con la mancanza dell'alimentazione (ad es. per mezzo di batterie tampone o di memoria FLASH), ha le stesse protezioni di accesso della memoria di sistema, poiché è deputata a memorizzare lo stato interno del PLC (incluso il registro istruzioni), in modo che, se dovessero verificarsi problemi dovuti proprio alla mancanza dell'alimentazione, possa essere possibile far ripartire correttamente l'impianto al ritorno della condizione di normalità.

La **memoria per le istruzioni** contiene il programma da eseguire, in forma di istruzioni.
I programmi che non devono essere modificati dall'utente sono memorizzati su una parte di memoria realizzata con tecnologia ROM (o EPROM o EEPROM), mentre i programmi realizzati dall'utente sono memorizzati su una parte di memoria realizzata con tecnologia RAM (eventualmente con accorgimenti per non renderla volatile con la mancanza dell'alimentazione).
Le memorie ROM e RAM non devono necessariamente essere distinte dalla CPU, ma possono anche essere interne a questa (realizzate sullo stesso chip, che spesso è dotato anche di unità di ingresso e di unità di uscita). In questo caso possono aversi anche

memorie esterne oltre a quelle interne, quando queste ultime sono di capacità insufficiente (figura 16).
Ricapitolando, nella ROM sono contenute la memoria di sistema e quella parte di dati e di programmi che assolutamente non sono modificabili dall'utente, mentre nella RAM sono contenuti i programmi realizzati dall'utente, i dati di ingresso, quelli di uscita e quelli risultanti dall'elaborazione.

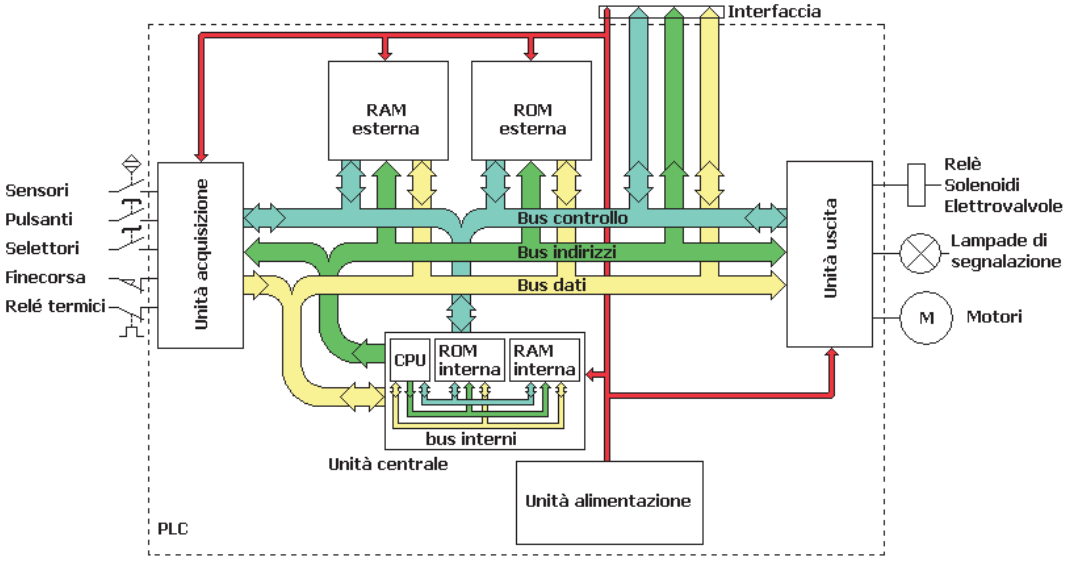


Figura 16: Esempio di architettura di PLC realizzata con unità centrale dotata di memorie interne

Recentemente, per la realizzazione di memorie non volatili, si è vista la diffusione di memorie FLASH. Sono anche diventate di uso comune le memorie FLASH in formato Micro Memory Card (MMC). Vantaggi delle MMC sono l'affidabilità, l'immunità ai campi elettromagnetici, la facile programmabilità e la possibilità di essere rimosse; inoltre, in caso di necessità, possono essere facilmente duplicate.

Unità di uscita
L'unità di uscita serve a trasmettere ordini e segnali dal PLC agli attuatori (ad es. bobine di comando di relè o di elettrovalvole, armature di motori) e ai segnalatori (lampade e segnalatori acustici).

Di solito gli ordini di uscita sono di tipo digitale e realizzati con tensione bassa (5 V), ma possono aversi casi in cui è utile avere tensioni più alte (24, 48, 110, 220 V) o di tipo analogico (per rappresentare una grandezza continua). Per tali motivi alcuni PLC possono avere un'unità di uscita dotata di schede con stadi di potenza o con convertitori digitale-analogici (D/A converter, in grado di trasformare un valore numerico in una tensione con una certa regolarità).

Le schede di uscita analogiche permettono di controllare attuatori variabili. Possono essere in corrente o in tensione ed avere una determinata risoluzione esprimibile in bit. Ad

esempio, è possibile comandare un motore elettrico tramite un inverter variandone la velocità, tramite la frequenza, da zero alla sua massima velocità.

Anche per le unità di uscita esistono opportuni segnali di *interrupt* che viaggiano sui bus di controllo in grado di avvisare l'unità centrale quando vi sono malfunzionamenti, in modo che sia possibile avviare un'opportuna sub-routine di gestione del problema.

Unità di programmazione
Un altro elemento fondamentale per un PLC è rappresentato dall'unità di programmazione.
A seconda dei costruttori, i PLC possono essere collegati ad un comune PC per la loro programmazione, attraverso le porte RS232, RS422/RS485 o la porta USB.

Tutti i PLC possono essere usati in almeno due diverse modalità operative selezionabili tramite un comando esterno.
Una è la modalità di esecuzione del programma (*run*) e l'altra è la modalità di programmazione (*stop/prog*). In modalità programmazione le uscite sono disabilitate per permettere di introdurre o modificare i programmi.

Alcuni PLC hanno una terza modalità di lavoro detta di monitoraggio (*monitor/term*).Tale modalità consente di forzare o riassegnare i valori delle uscite, dei relè interni, dei temporizzatori, dei contatori e di controllare i valori degli ingressi.

Differenze tra PLC per applicazioni standard e PLC fail-safe

Se, oltre a gestire il controllo delle funzioni ordinarie, il PLC è scelto per svolgere anche il controllo delle funzioni di sicurezza, le caratteristiche e le prestazioni della CPU vanno vagliate attentamente.
I PLC per applicazioni di sicurezza, impropriamente chiamati *fail-safe* sono, a volte, dotati di CPU con architetture particolari, oppure di doppia o tripla CPU. Le architetture particolari consistono in configurazioni ridondanti dei bus interni in modo da avere affidabilità dei dati, degli indirizzi e dei controlli o in opportuni circuiti di validazione delle operazioni svolte (ad es. *watchdog*, controllori, dispositivi di diagnostica). Invece, nelle CPU multiple si cerca di raggiungere gli stessi risultati per mezzo di un confronto incrociato tra le CPU, in modo da riconoscere eventuali malfunzionamenti. Il confronto è effettuato da un software di sistema opportuno o da un'unità hardware dedicata.

Quando il PLC è utilizzato in applicazioni di sicurezza ed è riconosciuto un malfunzionamento, possono essere attuate opportune azioni correttive per conservare il livello di sicurezza, ad esempio l'avvio di un programma che porti al raggiungimento di uno stato sicuro del sistema controllato in caso di guasto pericoloso.

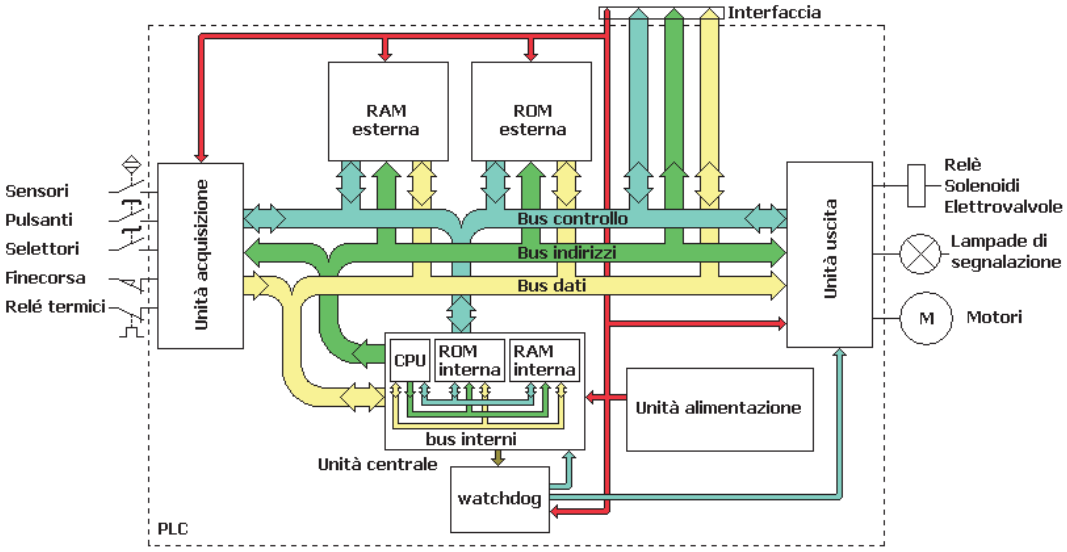


Figura 17: Esempio di architettura di PLC fail-safe con watchdog

In figura 17 è mostrato un PLC fail-safe, dove è presente un circuito di monitoraggio della CPU realizzato con un watchdog.

Il watchdog è un sistema di temporizzazione hardware che permette la rilevazione di un loop infinito di programma o di una situazione di stallo.
Tale rilevazione consente di prendere provvedimenti per correggere il problema, generalmente effettuando un reset del sistema. Possono essere implementati watchdog più complessi che permettano la memorizzazione delle informazioni di contesto, per effettuare il *debugging* delle applicazioni che hanno causato lo stallo.
Particolari watchdog possono innescare, inoltre, azioni di sistemi di controllo per effettuare operazioni di messa in sicurezza di apparati secondari, come ad esempio spegnimento di motori, alimentazioni o altro, in attesa che la condizione di errore sia eliminata.

Un semplice watchdog può essere implementato facilmente con un contatore di *n*-bit in un sistema che funzioni con un *clock* di *m* MHz, in questo modo il sistema verrà resettato se il timer non viene riazzerato ogni $2^n/(m \cdot 10^6)$ secondi.

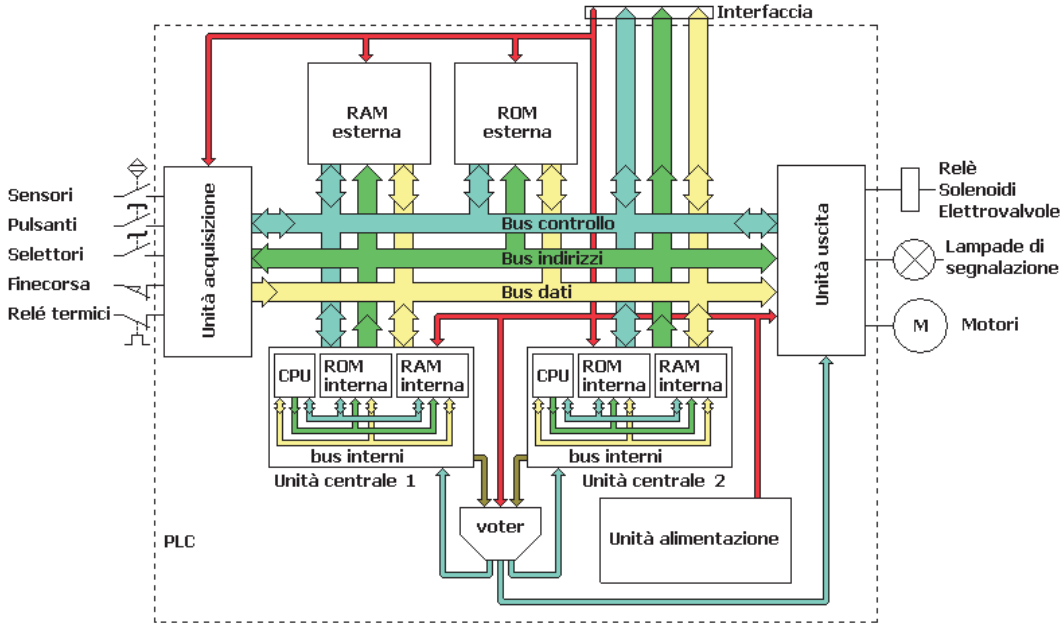


Figura 18: Esempio di architettura di PLC fail-safecon CPUridondante

In figura 18 è mostrata una coppia di CPU che si controllano a vicenda per mezzo di un circuito di sincronismo/comparazione (*voter*): ciascun processore esegue in parallelo anche le elaborazioni dell'altro e a intervalli regolari i risultati sono comparati. In caso di discordanza il voter disabilita le uscite, oppure, se con opportune azioni diagnostiche è possibile capire quale delle due sia la CPU in errore, abilita in uscita i risultati della CPU funzionante, oltre ad avvisare della presenza di un guasto.

Esistono vari metodi per individuare quale CPU si trova in errore e/o se l'errore è temporaneo o permanente; senza presunzione di esaustività la maggior parte di tali metodi sono basati sui seguenti principi:

- l'uso di codici ridondanti sui bus;
- l'esecuzione di sub-routine di gestione degli errori;
- la ripetizione dell'ultimo ciclo di acquisizione, elaborazione e comparazione.

In pratica, i codici ridondanti sono utilizzati per escludere errori hardware nella comunicazione tra le varie unità. Infatti, in caso di tali errori, il codice ridondante può permettere un recupero parziale, tramite l'avvio di opportune sub-routine software o tramite decoder hardware (quest'ultimo potrebbe essere incluso nel voter e potrebbe indicare in tempo reale il dispositivo in errore).

Allo stesso modo, la ripetizione dell'ultimo ciclo permette di vedere se l'errore è temporaneo o se tende a ripresentarsi.

Infine, le subroutine di gestione degli errori possono avviare le operazioni software di decodifica dei codici e/o di ripetizione dei cicli e/o potrebbero imporre alle diverse unità

l'esecuzione di operazioni in grado di rivelare la presenza di guasti capaci di generare gli errori.

Un caso tipico di discordanza dei valori di uscita si ha, ad esempio, quando le due unità centrali, operando in maniera asincrona, hanno eseguito le elaborazioni su ingressi differenti perché relativi ad istanti diversi. In tal caso la sub-routine di gestione degli errori può cercare di sincronizzare gli istanti di campionamento degli ingressi o può far eseguire ad ogni unità centrale un'elaborazione con gli ingressi dell'altra unità, in modo da comparare i risultati ottenuti per gli stessi ingressi.

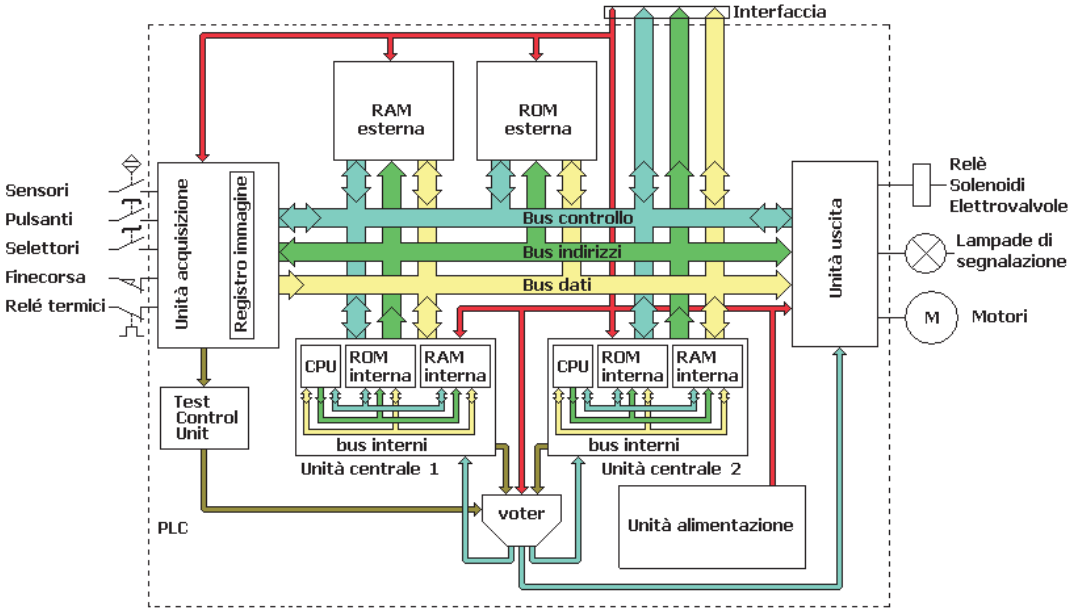


Figura 19: PLC con CPU ridondante e Test Control Unit per l'unità di acquisizione

Per quanto riguarda gli ingressi, un PLC per applicazioni standard non possiede, di solito, alcun sistema interno per la validazione degli stessi. I segnali di ingresso, dopo essere stati memorizzati nel registro immagine degli ingressi (previa eventuale conversione A/D, se analogici), sono inviati alla CPU per essere elaborati.

Un PLC fail-safe potrebbe essere dotato di un dispositivo di validazione degli ingressi (Test Control Unit, figura 19), in grado di rivelare eventuali anomalie in una delle unità di acquisizione e di generare un segnale di avvertimento per la CPU o per il voter (nel caso di CPU ridondanti).
Molto spesso, però, il controllo è fatto direttamente dalla CPU prima di qualsiasi elaborazione dei dati acquisiti.

Per quanto riguarda le uscite, un PLC fail-safe ha di solito un watchdog o un voter che abilita l'unità di uscita quando le uscite sono validate dalla comparazione; inoltre i già ricordati interrupt che viaggiano sui bus di controllo sono in grado di avvisare le unità centrali in caso di malfunzionamenti sulle schede di uscita, che potrebbero richiedere l'esecuzione di sub-routine particolari.

Il software

Il software definisce le operazioni che il PLC deve compiere sui componenti del sistema di controllo. I moderni PLC utilizzano differenti linguaggi di programmazione, in relazione alla complessità delle operazioni che sono in grado di eseguire e alle specifiche esigenze del sistema da controllare.

Per uniformare l'uso dei PLC, nel 1993 è nata la norma internazionale IEC 61131 (CEI EN 61131). Lo scopo è stato quello di definire un unico standard di progettazione per consentire ai costruttori, indipendentemente dalla specifica tipologia di CPU, di ottenere PLC con prestazioni confrontabili.

La parte terza della IEC 61131 (CEI EN 61131-3) si occupa dei linguaggi di programmazione, definendo la tipologia dei linguaggi, la sintassi e la semantica. Ogni costruttore, infatti, utilizza una differente CPU e ciò potrebbe creare qualche problema di uniformità tra modelli di costruttori diversi, soprattutto nella programmazione, essendo questa legata all'architettura della CPU. Nella pratica, ogni costruttore utilizza un proprio ambiente software di programmazione.

Linguaggi grafici

- *Ladder diagram (LD o KOP)* tradotto in italiano con *Linguaggio a contatti*: è stato il linguaggio più usato fino a pochi anni fa, in quanto è la trasposizione informatica degli schemi per i circuiti elettrici usati dagli elettrotecnici. L'automazione industriale, infatti, era basata su sistemi a logica cablata che sono stati poi sostituiti dai PLC, ciò ha indicato come naturale il ricorso a schemi grafici in grado di trasportare i concetti della logica cablata nel linguaggio di programmazione. Il programmatore semplicemente utilizza simboli logici corrispondenti a segnali di ingresso e di uscita per implementare la logica, non cablando i relè, ma disegnando gli schemi elettrici nell'interfaccia grafica del software di programmazione.

- *Sequential function chart (SFC),* tradotto in italiano con *Diagramma funzionale sequenziale*: è usato anche come strumento di specifica, è un linguaggio grafico molto simile ai diagrammi usati per descrivere le reti di Petri. Permette di implementare facilmente automi a stati finiti.

- *Function Block Diagram (FBD o FUP),* tradotto in italiano con *Diagramma a blocchi funzionali*: è costituito da diagrammi a blocchi che descrivono funzioni tra le variabili di ingresso e le variabili di uscita.

Linguaggi testuali

- *Instruction List (IL o AWL),* tradotto in italiano con *Lista di istruzioni*: linguaggio di alto livello, molto utilizzato, per la sua leggibilità, dalla maggior parte delle Società di Software per PLC, molto simile all'Assembler. Può essere facilmente ricavato dal Ladder diagram.

- *Structured Text (ST),* tradotto in italiano con *Testo strutturato*: linguaggio di alto livello simile al Pascal.

Capitolo 4 - I bus di comunicazione

L'importanza della comunicazione e interconnessione tra dispositivi e sistemi all'interno di un processo industriale è importante, oltre che sotto l'aspetto produttivo, anche sotto quello della sicurezza funzionale. Infatti, particolare rilevanza è assunta dalla comunicazione dei segnali di sensori ed attuatori che sovrintendono a funzioni di sicurezza.
Nella fase di progettazione e successiva realizzazione del processo è necessario valutare la possibilità di intercomunicabilità tra dispositivi realizzati da produttori diversi.
Poter connettere tra loro, e far quindi comunicare, simili dispositivi, assicura un forte abbattimento dei costi e un incremento dell'efficienza del processo industriale. Una delle possibili soluzioni a tale problema è quella di ricorrere all'adozione di un protocollo comune di comunicazione.
Così, sono nati e si sono diffusi i *bus di campo*.
In figura 20 è schematizzata una possibile gerarchia delle comunicazioni in un processo industriale.

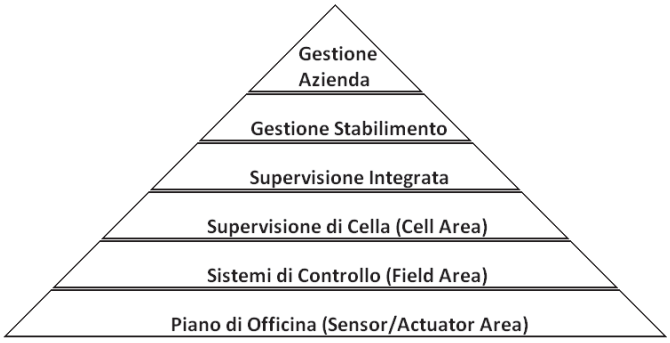


Figura 20: Gerarchia delle comunicazioni in un processo industriale

Nella tabella 8 sono rappresentati i parametri caratteristici dei segnali di comunicazione in relazione alle esigenze del processo.
Ciascun livello utilizza una specifica tipologia di rete:

- il livello gestionale utilizza una rete per le *informazioni gestionali*;
- il livello di produzione utilizza una rete per il *controllo*;
- il livello degli attuatori/sensori una rete per i segnali di *campo*.

	Quantità di dati	**Durata della comunicazione**	**Frequenza**
Gestione e supervisione	Mbyte	Ore/Minuti	Giorni/Turni
Area di cella	Kbyte	Secondi	Ore/Minuti
Area di campo (field)	Byte	Centinaia di μs… 100ms	10ms… 100ms
Area attuatori/sensori	bit	μs… ms	ms

Tabella 8: Parametri caratteristici dei segnali di comunicazione in un processo industriale

Nella schematizzazione di figura 20, il livello più basso (attuatore/sensore) è quello che influisce di più sulla sicurezza dei lavoratori. Si pensi ad esempio al caso di un sensore (ad esempio una barriera ottica a protezione di un'area) che aziona un dispositivo di

sicurezza. A tale livello la comunicazione avviene con lo scambio di pochi bit di informazione, in tempi che vanno dal μs al ms. Per la gestione e l'interconnessione di periferiche e dispositivi che agiscono a livello di processo vengono utilizzati i bus di campo (e vedremo come esempio i sistemi PROFIBUS), mentre a livello di sensore/attuatore vengono utilizzati anche altri sistemi (e vedremo come esempio i sistemi AS-Interface).

I sistemi PROFIBUS

PROFIBUS (PROcess Field BUS) è un bus di campo seriale, il cui sviluppo è stato affidato ad un'organizzazione denominata PROFIBUS Trade Organization (PTO), composta da membri provenienti dall'industria, da istituti di ricerca e da utenti finali. Attualmente vi sono più associazioni (Regional PROFIBUS & PROFINET Associations) interessate alla sua diffusione in tutto il mondo.
La tecnologia PROFIBUS è nata come standard con la norma DIN 19245 (1991), successivamente è stata emanata la norma armonizzata EN 50170 e tale tecnologia è stata inclusa tra gli standard europei (1996).
PROFIBUS supporta i seguenti tre protocolli di comunicazione:

- FMS (*Fieldbus Message Specification*),
- DP (*Decentralized Peripherals*),
- PA (*Process Automation*).

Il complesso protocollo PROFIBUS FMS, oggi poco utilizzato, rappresenta la soluzione *general-purpose* per la comunicazione, anche a livello di cella. È utilizzato per la comunicazione (non deterministica) dei dati tra dispositivi master.
Il protocollo PROFIBUS DP è rivolto soprattutto alla comunicazione tra sistemi di controllo (*masters*) e dispositivi distribuiti di I/O (*slaves*). La sua maggiore semplicità rispetto al protocollo FMS ha favorito la sua diffusione.
PROFIBUS DP realizza i livelli 1 e 2 del modello a 7 livelli ISO/OSI[1], rappresentato in tabella

	7	Dati	**Applicazione** Dai processi di rete all'applicazione
host	**6**	Dati	**Presentazione** Presentazione dei dati e criptazione
layers	**5**	Dati	**Sessione** Controllo comunicazioni tra applicazioni
	4	Segmenti	**Trasporto** Connessione end-to-end e affidabilità
media	**3**	Pacchetti	**Rete** Determinazione e traduzione degli indirizzi
layers	**2**	Struttura	**Collegamento** Indirizzamento fisico
	1	Bit	**Fisico** Media, segnale e trasmissione binaria

Tabella 9: Layer dello standard ISO/OSI

[1]Modello creato dall'ISO (International Organization for Standardization) per descrivere le comunicazioni tra computer.

Il protocollo PROFIBUS PA è stato progettato principalmente per l'automazione di processo. Consente di collegare sensori ed attuatori su una linea di comunicazione comune in aree a sicurezza intrinseca. Con esso è possibile trasmettere dati e alimentazioni su un bus a due conduttori, in accordo con lo standard internazionale IEC 61158-2 (codifica del bit tramite segnale di corrente). Ciò consente di operare in condizioni di sicurezza intrinseca (zone Ex 0 ed Ex 1) permettendo ai dispositivi di essere alimentati direttamente sul bus. A livello fisico il protocollo PA può essere interfacciato con il protocollo DP per mezzo di un bridge-accoppiatore. PA utilizza per la trasmissione dei dati un protocollo DP esteso oltre ad un Profilo PA nel quale viene definito il comportamento dei dispositivi di campo.

Tipologie di dispositivi nelle reti PROFIBUS

La gestione dell'accesso al bus di campo è realizzata, nel protocollo PROFIBUS, secondo la filosofia *master*/*slave*, mentre per ridurre i conflitti di accesso al bus tra master, si utilizza una procedura basata sul *token passing*.

I principali dispositivi che possono essere connessi al bus sono:

- I dispositivi *master*, che controllano la comunicazione sul bus. Un master può spedire messaggi senza richiesta esterna quando detiene il controllo della linea di comunicazione (possesso del *token*). Anche chiamati stazioni attive.
- I dispositivi *slave,* che costituiscono le periferiche di I/O (tra cui anche sensori ed attuatori),non possono accedere al bus direttamente, se non per divulgare informazioni diagnostiche che li riguardano. Sono in grado solo di riconoscere i messaggi ricevuti o di spedire messaggi al master quando interrogati. Dal momento che richiedono piccole porzioni di protocollo, la loro gestione è particolarmente economica. Anche chiamati *stazioni passive*.

La procedura *token passing* garantisce che il permesso d'accesso al bus, concesso al master che possiede il token, sia definito per un intervallo di tempo predeterminato e costante, pertanto il tempo che ogni master dovrà attendere per accedere al bus dipenderà dal numero di dispositivi attivi presenti nella rete e dal massimo tempo di utilizzo del bus permesso (*token hold time*). Il token viene passato da un master all'altro secondo un ordine prefissato (anello logico). La procedura master/slave consente alla stazione attiva che in un preciso momento possiede il token di accedere alle stazioni passive a lui assegnate. Il master può spedire messaggi agli slave o richiedere messaggi dagli slave.
Il protocollo PROFIBUS, al fine di soddisfare diverse esigenze, in termini di velocità di trasmissione, distanza raggiungibile, sicurezza e possibilità di alimentazione lungo il bus, supporta diverse soluzioni tecnologiche:

- la trasmissione RS-485 per i protocolli DP e FMS,
- la trasmissione con fibre ottiche per i protocolli DP e FMS,
- la trasmissione in conformità allo standard IEC 61158-2 per il protocollo PA.

La semplice ed economica tecnica di trasmissione RS 485 a due conduttori è perfettamente adatta all'impiego con reti in struttura lineare/ad albero con elevata velocità di trasmissione.
L'estensione della rete è complessivamente inferiore rispetto ad una rete realizzata con sistemi in fibra ottica; mediante la segmentazione e la rigenerazione dei segnali con max. 9 *repeater* sono però raggiungibili anche distanze da 1 km (a 12 Mbit/s) fino a 10 km (a 187,5 kbit/s).

Al posto dei repeater standard sono impiegabili anche repeater diagnostici, che eseguono oltre alla rigenerazione dei segnali anche la sorveglianza online del segmento di bus collegato. Un segmento può avere fino a 32 nodi/partner (master/slave), l'intera rete fino a 126 nodi/partner. All'inizio e alla fine di ogni segmento va prevista una terminazione attiva del cavo, che è già integrata nell'apparecchiatura (ad es. repeater) oppure è disponibile come elemento di chiusura RS 485 attivo.

Viceversa, l'impiego di sistemi a fibra ottica è utile negli ambienti ad alta interferenza elettromagnetica oppure per aumentare la distanza massima raggiungibile dalla comunicazione o la velocità massima impiegabile. Infatti, in tali sistemi la larghezza di banda, e quindi la velocità di trasmissione, risulta inversamente proporzionale alla lunghezza del collegamento e non al suo quadrato, come nei sistemi che utilizzano conduttori metallici. Il segnale digitale pilota un diodo emettitore di luce affacciato alla fibra ottica. All'altra estremità un dispositivo fotosensibile trasforma gli impulsi luminosi in impulsi elettrici. Possono essere utilizzati due tipi di conduttori:

- Un cavo economico di accoppiamento in fibra di plastica per interno e per applicazioni di ridotta estensione (distanze inferiori ai 50m);
- Un cavo in fibra in vetro per interno ed esterno per distanze inferiori al chilometro. Molti costruttori realizzano connettori speciali che integrano convertitori da fibra ottica a RS-485 e viceversa.

Infine, lo standard IEC 61158-2 risponde alle esigenze delle applicazioni ATEX, che richiedono comunicazioni intrinsecamente sicure. È basato sulla codifica dei bit per mezzo di segnali di corrente ed è spesso individuato con la sigla H1. La trasmissione si fonda sui seguenti principi:

- ogni segmento ha una sola fonte di alimentazione, l'unità di alimentazione non riversa potenza sul bus quando una stazione invia dati;
- ogni dispositivo consuma una corrente di base (tipicamente 10 mA) nel suo stato di attesa, ogni dispositivo si comporta come un pozzo passivo di corrente;
- ad entrambi i capi del bus sono presenti terminazioni passive (RC serie, R=100Ω, C=1μF);
- sono permesse reti lineari, ad albero o a stella;
- è possibile aggiungere tratti ridondanti di bus per aumentare l'affidabilità.

I dispositivi sono alimentati con una corrente continua di almeno 10 mA, mentre il segnale è caratterizzato da una modulazione di 9 mA rispetto alla componente continua. Il numero massimo di unità collegabili è 32, anche se il numero in realtà è limitato dal tipo di protezione contro le esplosioni scelta. La compresenza sul bus di dispositivi alimentati esternamente è possibile solo se questi ultimi sono dotati di un appropriato isolamento in accordo con lo standard EN 60079-27.

Caratteristiche principali di PROFIBUS-DP

La versione DP del protocollo PROFIBUS è stata pensata per la comunicazione tra sistemi di controllo (PC, PLC) e dispositivi d'ingresso/uscita distribuiti (sensori, attuatori). È ottimizzata per comunicazioni ad alta velocità e per connessioni poco costose. Gran parte dello scambio di dati in tale contesto avviene in modo ciclico; tuttavia per permettere lo svolgimento di procedure di configurazione, di diagnostica o di gestione degli allarmi, il protocollo supporta anche funzioni di comunicazione aciclica. L'aumento significativo di velocità rispetto al protocollo FMS deriva sostanzialmente dall'utilizzo del servizio SRD

(*Send and Receive Data*), che consente la trasmissione di dati di ingresso e uscita in un singolo messaggio.

PROFIBUS DP prevede due tipologie di master (figura 21): DPM1per la gestione degli slave e DPM2 per lo svolgimento delle funzioni di diagnostica e programmazione. Possono essere presenti più DPM1, ciascuno con il suo gruppo di slave, anche se tra loro i DPM1 non comunicano.
È possibile invece la comunicazione tra un DPM1 e un DPM2.

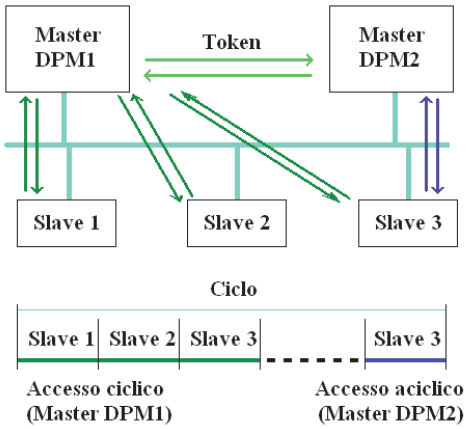


Figura 21: Esempio di ciclo di comunicazione PROFIBUS DP

I sistemi PROFIBUS, per impieghi in sistemi a sicurezza intrinseca, sono chiamati PROFI*safe*. Per tali sistemi il processo di progettazione deve essere certificato da un ente terzo, secondo il cosiddetto modello FISCO (Fieldbus Intrinsically Safe Concept). Il profilo PROFI*safe* viene implementato come strato software addizionale nelle apparecchiature e nei sistemi, senza che siano modificati i meccanismi di comunicazione standard di PROFIBUS. È pertanto possibile impiegare, senza modifiche, i componenti standard interessati alla comunicazione nei nodi/partner PROFI*safe* (ad es. unità di comunicazione, connettori o cavi).

I sistemi AS-Interface

Per i collegamenti tra attuatori e sensori, lo standard AS-Interface è quello attualmente più diffuso ed utilizzato. Si tratta di uno standard aperto, le cui specifiche elettriche e meccaniche sono state concordate e definite da 11 costruttori di sensori e attuatori binari. La sua introduzione sul mercato risale al 1994. Nel 1999 il sistema AS-interface è entrato a far parte degli standard europei con la pubblicazione delle norme EN 50295 e IEC 62026-2.

I componenti dei sistemi AS-Interface sono compatibili tra loro indipendentemente dal costruttore che li ha prodotti. AS-Interface, in quanto sistema aperto, può essere utilizzato universalmente e può essere collegato direttamente ad un controllore programmabile

(PLC) o ad una rete di bus di campo di livello superiore, come ad esempio una rete PROFIBUS.

Campo di impiego e struttura di una rete AS-Interface

AS-Interface è un sistema di connessione progettato per operare tramite un cavo bifilare in grado di trasportare dati e potenza. È adatto alla circolazione di un volume di dati limitato. È particolarmente indicato per operare con numerosi dispositivi di campo che forniscono informazioni semplici, di tipo binario, e che devono interfacciarsi ad un'unità di controllo elettronica come un PLC o un elaboratore.

Il sistema AS-Interface è pensato per sostituire la tecnologia di cablaggio tradizionale utilizzata normalmente. Quest'ultima prevede che i dati provenienti dal livello di processo siano trasmessi tramite cavi paralleli e moduli di ingresso/uscita; di conseguenza ciascun attuatore e sensore è collegato ad un gruppo di ingresso/uscita tramite un cavo individuale ad esso riservato. Con AS-interface la connessione è realizzata tramite un unico cavo, al quale tutti i dispositivi di campo - sensori e attuatori - sono collegati. Sullo stesso cavo vengono trasportati segnali ed alimentazione. I vantaggi sono evidenti, soprattutto quando i singoli sensori/attuatori devono essere installati in modo distribuito sulla macchina.

Nella figura 22 è schematizzata la tipica interconnessione di vari componenti.

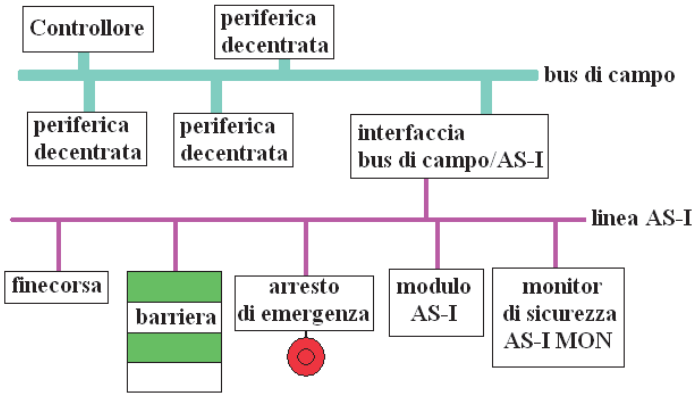


Figura 22: Interconnessione tra dispositivi realizzata con due reti operanti su bus diversi

Una rete AS-Inteface può essere composta dai seguenti componenti:

- Master AS-I;
- Alimentatore master;
- Linea AS-I;
- Programmatore di indirizzi;
- Slave AS-I standard con interfacciamento AS-I, che si collegano alla rete tramite i moduli slave di ingresso/uscita. Ciascun slave permette la trasmissione in parallelo di 4 bit di segnale di ingresso e 3 bit in uscita. Ad ogni ingresso può essere rilevato lo stato di un dispositivo, ad ogni uscita può essere inviato un comando (necessitano di un modulo di collegamento alla rete AS-I);

- Slave moduli AS-I, dispositivi che possono essere connessi direttamente al cavo AS-I. Tali apparecchi sono da considerarsi come moduli indipendenti, ad ognuno dei quali è riservato un nodo, corrispondente a 4 canali per la trasmissione di dati (4 bit di dati). Rispetto ai dispositivi standard, sono componenti AS-I a tutti gli effetti e possiedono i requisiti richiesti dalla norma EN 50295;
- Monitor di sicurezza AS-I MON, dispositivo a logica programmabile, in grado di svolgere operazioni logiche (logica booleana, flip-flop ecc.) e funzioni di temporizzazione. Ha il vantaggio, rispetto alle normali unità, di elaborare i segnali ricevuti dai sensori, permettendo la realizzazione di operazioni complesse, come ad esempio funzioni di intervento condizionate da più variabili.
  Possono essere scelti diversi modi operativi, a seconda dell'applicazione può variare il tipo di intervento effettuato. Tra le funzioni disponibili, le più importanti sono la funzione di arresto d'emergenza, la funzione di ritenuta, la scelta della categoria di arresto.
  Inoltre, collegando un PC al monitor, è possibile effettuare operazioni di diagnostica.
  Sono disponibili due varianti di monitor, la cui differenza principale sta nella complessità di operazioni logiche realizzabili:
  - Monitor di sicurezza di base;
  - Monitor di sicurezza ampliato, dotato di funzioni logiche più complesse.

  Entrambe le varianti sono disponibili con uno o due circuiti di abilitazione a due canali. Il monitor si inserisce all'interno della rete AS-I come se fosse un normale modulo e agisce leggendo le informazioni che circolano in rete, senza interferire con il master AS-I.
  Dopo la chiamata da parte del master, gli slave di sicurezza inviano al master le informazioni di cui sono in possesso allo stesso modo in cui lo fanno gli slave standard. Il monitor di sicurezza controlla la trasmissione dagli slave di sicurezza al master e può intervenire in maniera indipendente. Un intervento del monitor provoca l'apertura dei relè di sicurezza.
  A seconda della causa dell'intervento, si distinguono due stati di arresto:
  - stato di arresto d'emergenza, in caso di guasti o anomalie segnalate dagli slave di sicurezza;
  - stato di sicurezza, in seguito ad una richiesta di arresto.

Tipologie di interconnessione

Le tipologie di connessione di una rete AS-I sono quelle indicate nelle figure 23a e 23b seguenti:

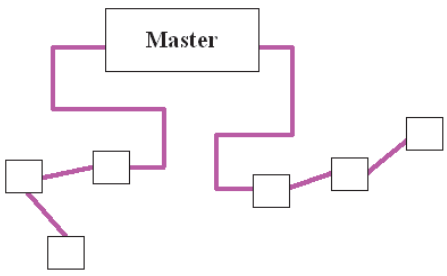


Figura 23a: Collegamento seriale

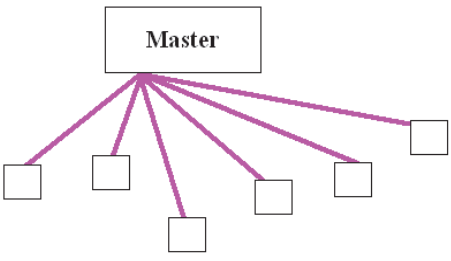


Figura 23b: Collegamento a stella

Con tali collegamenti gli unici limiti al numero di slaves collegabili sono dovuti alla tipologia di sistema ed alle funzioni da realizzare (figura 24). Alcune varianti prevedono sistemi AS-I con controllo locale, naturalmente ciò è possibile quando il sistema è a bassa complessità.

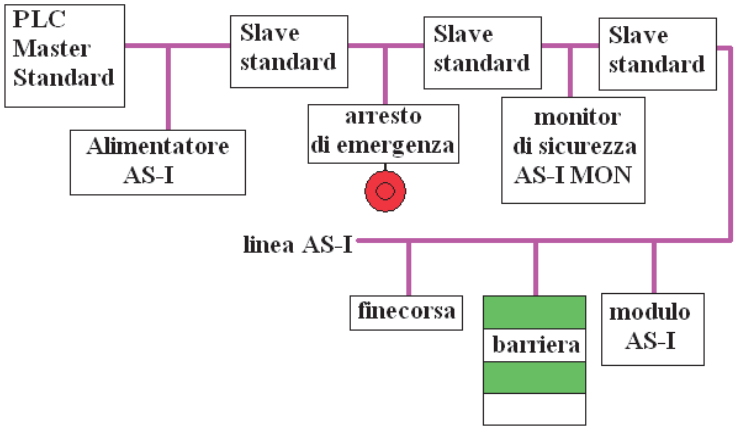


Figura 24: Esempio di collegamento ed interconnessione dei vari moduli

Capitolo 5 - Indagine sull'adozione delle norme per i sistemi di controllo delle macchine nel panorama produttivo nazionale

La nuova Direttiva Macchine (recepita in Italia con il D.Lgs. 17/2010 [1]) prevede che le macchine commercializzate o messe in servizio siano conformi ai requisiti essenziali di sicurezza contenuti nell'All. I alla Direttiva stessa (art.3, comma 3).

Tra i requisiti di sicurezza contenuti nell'All. I, quelli che riguardano la sicurezza e l'affidabilità dei sistemi di comando si trovano al punto 1.2.1: i sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose e in modo tale che:

- resistano alle previste sollecitazioni di servizio e agli influssi esterni;
- un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose;
- errori della logica del sistema di comando non creino situazioni pericolose;
- errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose.

Commercializzare macchine in grado di resistere alle sollecitazioni previste è alla base della competitività produttiva. A tal fine, i progettisti ricorrono in genere ad una scelta oculata dei materiali e delle tecnologie.
Agli errori umani ragionevolmente prevedibili si può ovviare con una buona progettazione.
Una progettazione anche corretta, oltre che buona, permette di fare a meno degli errori della logica di comando, in modo da non dover affrontare situazioni pericolose a causa di tali errori. A tal proposito, esistono tecniche di progettazione che, se applicate, aiutano ad eliminare eventuali errori nella logica di comando.
Quanto alle avarie nell'hardware o nel software, si può far in modo che non creino situazioni pericolose ricorrendo a ridondanza e diversità dei canali del sistema di comando.

Le norme sull'affidabilità dei sistemi di comando indicano le procedure da seguire per decidere in quali casi, su base probabilistica e sulla base delle caratteristiche richieste al sistema di comando, sia sufficiente un unico canale logico per realizzare una funzione di sicurezza o sia necessario ricorrere a parti aggiuntive, come un controllo diagnostico sul canale o l'adozione di almeno due canali separati che siano in grado di effettuare controlli diagnostici uno sull'altro in modo da garantire la sicurezza della macchina, eventualmente anche in presenza di guasti.

La prima norma armonizzata (fin dalla prima Direttiva Macchine, recepita con D.P.R.459/96 [2]), appositamente pubblicata per rendere disponibili procedure e criteri comuni per la progettazione e la valutazione di affidabilità dei sistemi di comando, è stata la EN 954-1 [3].
Tale norma è stata studiata per l'applicazione a diversi tipi di tecnologie, da quelle elettriche, che comprendono anche i sistemi a logica programmabile, a quelle meccaniche, idrauliche e pneumatiche.
Nella norma sono introdotti i principi base affinché i sistemi di comando siano progettati e costruiti in modo da evitare situazioni pericolose. In pratica, il sistema di comando deve essere inserito nel ciclo di vita della macchina, che parte dall'identificazione dei pericoli, e che prevede l'individuazione delle funzioni di sicurezza da realizzare per mezzo del

sistema di comando stesso. Il progettista, per ciascuna funzione, deve scegliere una Categoria, tra cinque disponibili, per la realizzazione effettiva. Il sistema di comando ottenuto deve essere validato, per verificare che le caratteristiche richieste per la Categoria scelta siano state ottenute. A questo punto, la progettazione è terminata e la macchina può essere realizzata e, dopo aver soddisfatto gli adempimenti per l'immissione sul mercato, commercializzata. Il ciclo di vita non finisce con la vendita, ma prosegue con la manutenzione, con le modifiche a seguito di incidenti, con gli adeguamenti a nuove disposizioni legislative (ove necessario), per terminare solo con la dismissione effettiva della macchina.

Nella realtà, la EN 954-1 non è mai stata una norma troppo vincolante: le definizioni con le caratteristiche delle Categorie non fornivano un'idea univoca di come realizzare queste ultime, inoltre non erano date indicazioni per poter effettuare valutazioni quantitative in maniera oggettiva.
Per tale motivo è stato naturale, come era auspicabile fin dall'inizio, far evolvere la norma EN 954-1 nella norma EN ISO13849-1 [4]. In essa è stato posto in rilievo il fatto che le Categorie rappresentassero in realtà delle Architetture (con o senza ridondanza), con cui realizzare il canale logico di una data funzione di sicurezza all'interno del sistema di comando. Inoltre, è stato finalmente spiegato che il parametro di valutazione della bontà di un sistema di comando è la probabilità di fallimento dello stesso quando viene richiesta l'attivazione di una data funzione di sicurezza: più è bassa tale probabilità e più è difficile che si verifichino situazioni pericolose per il mancato intervento di una funzione di sicurezza.
La valutazione del rischio serve a stabilire qual è l'intervallo di livello di probabilità da raggiungere per una data funzione di sicurezza, in modo tale che il rischio residuo sia tollerabile (Required Performance Level). Inoltre, il processo di progettazione della funzione di sicurezza deve essere integrato e deve essere reiterato, finché non si raggiunge un livello di probabilità di fallimento della funzione di sicurezza inferiore al valore tollerabile.

Poco prima della pubblicazione della EN ISO 13849-1, per il settore delle macchine è stata pubblicata la norma EN IEC 62061 [5], che copre più o meno gli stessi aspetti (solo per i sistemi di comando elettrici, elettronici ed elettronici programmabili).
La filosofia della EN IEC 62061 è un po' diversa: non ci sono architetture rigide per la realizzazione dei canali logici del sistema di comando, ma la scelta dell'architettura è delegata al progettista, così come la scelta del tipo di ridondanza da adottare per accrescere l'affidabilità di tale sistema.
Cambia anche la nomenclatura: il Required Performance Level è chiamato Safety Integrity Level Claimed, anche se non vi è una corrispondenza biunivoca tra i due concetti.

Attualmente, a livello normativo, è allo studio l'unificazione della EN ISO13849-1 con la EN IEC 62061, con una serie di modifiche ed integrazioni allo scopo di rendere la norma che ne risulterà più applicabile delle due norme che l'hanno generata.

Pertanto, per poter intervenire più efficacemente nel processo di realizzazione normativa, è stato preparato dal Dipartimento Tecnologie di Sicurezza dell'INAIL– Settore Ricerca, Certificazione e Verifica un questionario per verificare l'effettiva adozione ed attuazione delle norme sui sistemi di comando delle macchine nel panorama produttivo nazionale.
Il questionario si proponeva di fornire un'analisi anche dello stato dell'arte attuativo riscontrabile nelle imprese italiane costruttrici di macchine.

L'indagine è stata condotta mediante la diffusione del questionario alle principali associazioni di costruttori di macchine – in rigoroso ordine alfabetico: Assofluid, Assomacchine, Aziende del settore delle macchine di sollevamento (piattaforme elevabili, PLE, e gru su autocarro), Federmacchine, Ucimu. Le aziende che hanno risposto al questionario proposto sono state in totale 36 e rappresentano un'ampia percentuale del mercato nazionale.

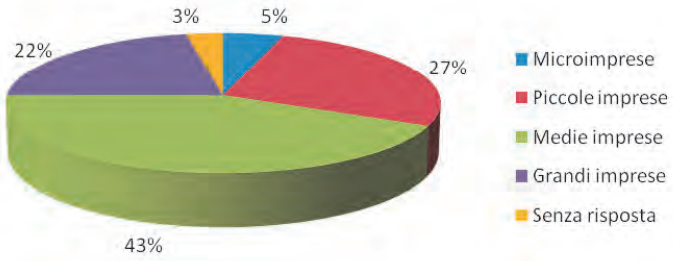
L'obiettivo dell'indagine era valutare la reale diffusione delle norme, mettendo in luce sia gli effettivi vantaggi della loro adozione, sia i motivi dell'eventuale mancata adozione.
Il questionario non è stato somministrato a fini ispettivi, ma solo a fini statistici e per future proposte di miglioramento normativo ed è stato costruito in modo da soddisfare gli obiettivi citati. Veniva richiesto, perciò, di rispondere con serietà e con onestà anche se non a tutte le domande obbligatoriamente, essendo il questionario in forma anonima.
La suddivisione in aree tematiche ha fatto sì che le domande riguardanti lo stesso tema fossero disposte consecutivamente, in modo da rendere più facili la lettura ed il processo di risposta, coniugando il più possibile caratteristiche di dettaglio e di rapidità di compilazione. Inoltre, le 71 domande a filtro hanno permesso di evitare che gli intervistati fossero costretti a rispondere a quesiti non di interesse.

Grazie al questionario, è stato possibile acquisire utili informazioni sia di carattere qualitativo che quantitativo relativamente ai dati richiesti ed è stato possibile elaborare alcune considerazioni sullo stato dell'arte in materia di applicazione delle norme, relativamente ad un ampio squarcio della realtà produttiva italiana del settore delle macchine.
Le principali indicazioni che è stato possibile estrapolare dalle risposte fornite hanno riguardato la diffusione delle norme citate dal questionario, la difficoltà di applicazione delle stesse e la difficoltà di reperimento dei dati sui singoli componenti e sui sistemi completi.
Dall'analisi della percentuale di risposte per ogni singola domanda emergono alcune interessanti considerazioni.
In primo luogo, come era ovvio, è emerso che il campo di interesse delle aziende che hanno risposto non è esclusivamente quello della produzione di sistemi di comando per la realizzazione di funzioni di sicurezza; molte aziende realizzano macchine che hanno come componente essenziale un sistema di comando, altre volte, invece, è possibile che il sistema di comando sia fabbricato da un fornitore esterno, che non specifica al costruttore della macchina quali norme sono state seguite per la progettazione e la realizzazione.
In secondo luogo, è emerso che in alcuni casi risulta effettivamente difficile reperire informazioni attinenti l'affidabilità dei singoli componenti del sistema di controllo.
In ogni caso, questa prima indagine apre uno scenario sul livello di conoscenza delle norme posseduto dalle aziende che operano nel panorama nazionale e sullo sforzo da queste sostenuto per applicare e mettere in pratica i contenuti normativi.
Grazie al contributo delle aziende che hanno partecipato all'indagine, è stato possibile comprendere quali aspetti delle norme possono essere migliorati.

Di seguito sono riportate le principali informazioni estratte dal questionario.

Contesto aziendale

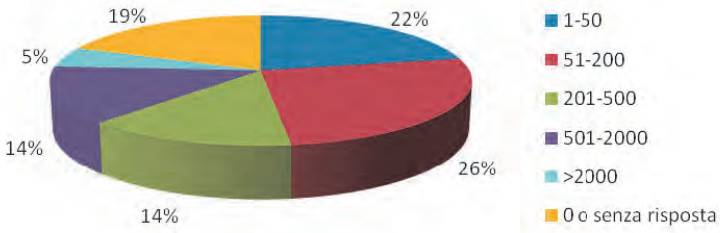
Allo scopo di comprendere il contesto aziendale di chi ha partecipato all'indagine, è stata prevista una sezione del questionario rivolta ad indagare sui dati generali delle aziende e sul livello di sicurezza dei sistemi di controllo da queste progettati/realizzati/utilizzati. Questa è stata l'unica sezione del questionario per cui si è chiesto che i dati fossero forniti in forma quantitativa.



QUESITO N. 1: Dimensione aziendale (numero di dipendenti)

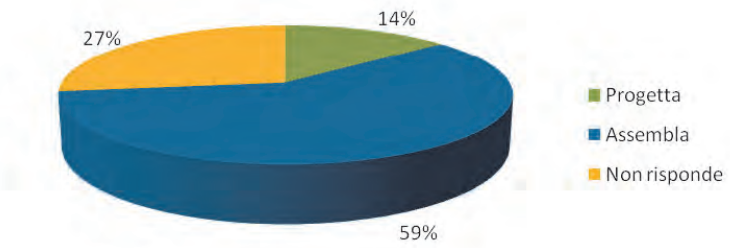
A tutela della privacy, il quesito n. 1 sulla dimensione aziendale è stato formulato in modo da richiedere il numero dei dipendenti delle aziende coinvolte nella compilazione del questionario.
Secondo la definizione della Gazzetta Ufficiale delle Comunità Europee n.107 del 30 aprile 1996, soggetta a revisione il 1 gennaio 2005, è stato possibile classificare le aziende che hanno risposto in base al numero di lavoratori dipendenti, nella seguente maniera:

- microimprese: imprese da1a 9 dipendenti;
- piccole imprese: imprese da10 a 49 dipendenti;
- medie imprese: imprese da 50 a 249 dipendenti;
- grandi imprese: imprese con più di 250 dipendenti.



QUESITO N. 2: Dimensione aziendale
(numero di macchine/quasi macchine/sistemi di controllo venduti)

Non è stato possibile considerare, ai fini della classificazione, anche il fatturato, per motivi di privacy. In compenso, un'idea indicativa delle capacità produttive delle aziende è ricavabile sulla base del numero di macchine prodotte (quesito n. 2), anche se tale dato non è facilmente correlabile con il fatturato.

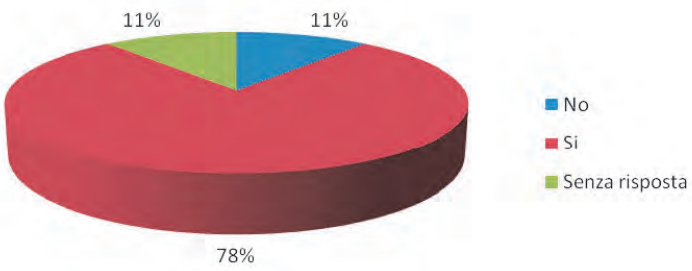


QUESITO N. 3: Progettazione di sistemi di controllo

È stata posta anche una domanda che aveva lo scopo di comprendere in che percentuale le aziende intervistate producessero sistemi di controllo, a partire dalla progettazione fino alla vendita, oppure utilizzassero sistemi fabbricati da altri sulla base di specifiche da loro prodotte, oppure utilizzassero sistemi di controllo completamente chiavi in mano (quesito n.3). Dalla percentuale di risposte date al quesito n. 3 emerge che il 14% delle aziende progetta i sistemi di controllo per le macchine/quasi macchine che vende, il 59% assembla nei propri prodotti sistemi di controllo chiavi in mano, il 27% non risponde.

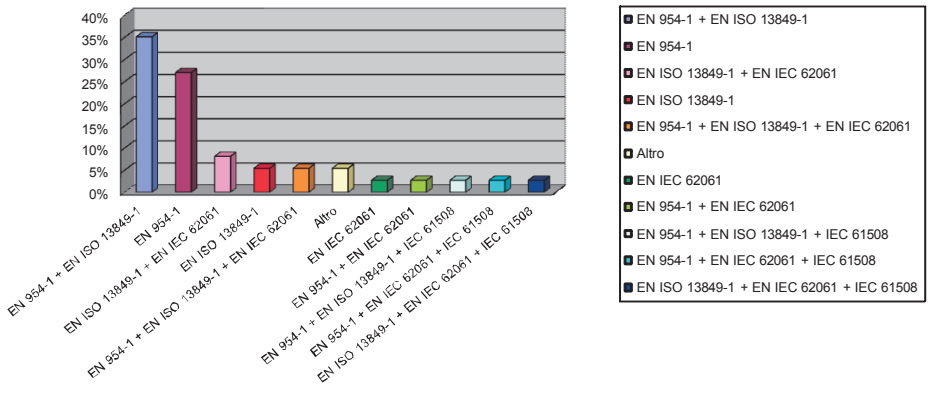
Adozione di norme per i sistemi di controllo

Il gruppo successivo di domande è stato inserito nel questionario con l'obiettivo di indagare sull'adozione di norme specifiche sulla sicurezza dei sistemi di controllo delle macchine. Quasi tutte le domande sono state poste in termini dicotomici (si/no). Tale sezione ha rappresentato uno spartiacque del questionario: chi ha affermato di non aver adottato norme sulla sicurezza dei sistemi di controllo delle macchine ha poi proseguito direttamente con l'ultima sezione, saltando le altre.



QUESITO N. 4: L'azienda applica le norme armonizzate sulla sicurezza dei sistemi di controllo?

Le risposte date al quesito n. 4 sottolineano un dato interessante circa la diffusione ed applicazione delle norme armonizzate sui sistemi di controllo: la maggioranza delle aziende le applica.
Anche se, sulla base del fatto che le risposte sono pervenute da aziende appartenenti a settori produttivi diversi (meccanica, elettromeccanica, pneumatica, elettrica, idraulica),si è indotti a credere che la risposta in questione potrebbe riguardare l'applicazione di norme armonizzate specifiche del settore produttivo di interesse, senza particolare riferimento alle norme per i sistemi di controllo, come è possibile evincere confrontando il dato con le risposte al quesito n. 5.

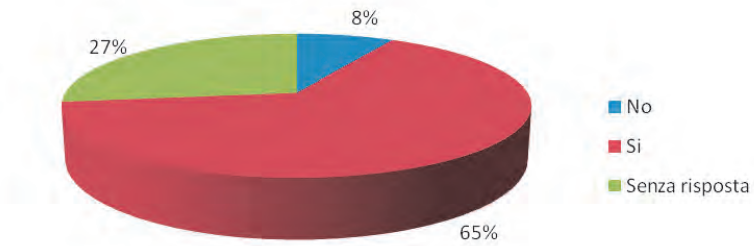


QUESITO N. 5: Per la realizzazione dei prodotti o dei sistemi, quali norme tecniche sono seguite?

La norma EN 954-1 è senz'altro la più utilizzata dalle aziende ed è evidente che quelle che si stanno preparando per applicare anche la sua evoluzione, EN ISO 13849-1, sono la maggior parte; basta vedere la percentuale delle aziende che applicano entrambe (quesito n. 5). La causa di tale successo è storica, inoltre la EN 954-1, prima di essere ritirata, ha avuto una proroga del proprio periodo di validità, arrivando a coesistere con la EN ISO 13849-1. Segue la classifica, ma molto alla lontana, la norma EN IEC 62061. Curioso è il

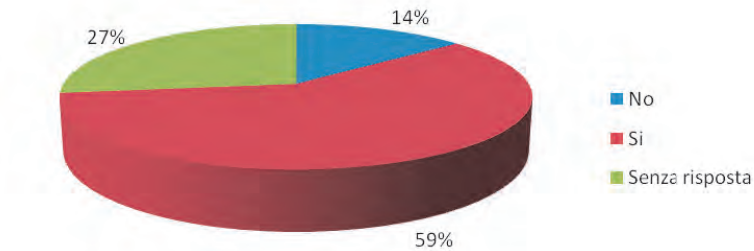
fatto che molte aziende applicano coppie di norme e altre applicano tre norme in contemporanea. Ciò può voler dire che i sistemi di controllo da loro prodotti/utilizzati verificano in contemporanea più norme, allo scopo di essere appetibili a fette di mercato più ampie o, viceversa, che parte della produzione di tali aziende è conforme ad una norma e parte ad un'altra; è questo il caso di chi assembla macchine e si rivolge per i sistemi di controllo una volta ad un fornitore che segue una norma e una volta ad un fornitore che ne segue un'altra.
Significativo è il fatto che alcune aziende abbiano dichiarato di far riferimento alla IEC 61508 [6], da cui sia la EN ISO 13849-1 che la EN IEC 62061 sono state tratte.
Infine, una piccola percentuale di aziende applica altro (norme specifiche di prodotto); ciò può essere dovuto al fatto che tali aziende non producono sistemi di controllo; è questo il caso di chi produce quasi-macchine o componenti di macchine.

Il gruppo di quesiti da 6 a 10 cerca di indagare l'applicabilità della norma EN ISO 13849-1.



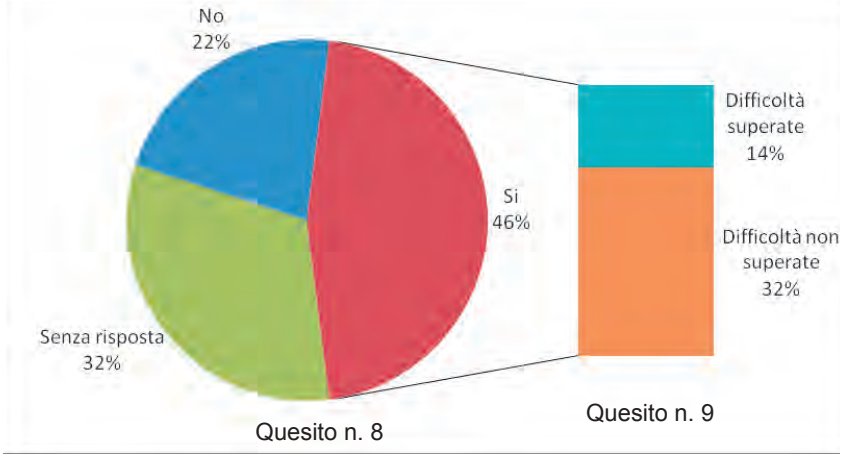
QUESITO N. 6: La norma EN ISO13849-1 è comprensibile?

Il 65% delle risposte al quesito n. 6 lascia intendere che la EN ISO 13849-1 sia abbastanza comprensibile: le prescrizioni e le indicazioni contenute nella norma sono ritenute comprensibili da una maggioranza di coloro che ha risposto.



QUESITO N. 7: La norma EN ISO 13849-1 è applicabile?

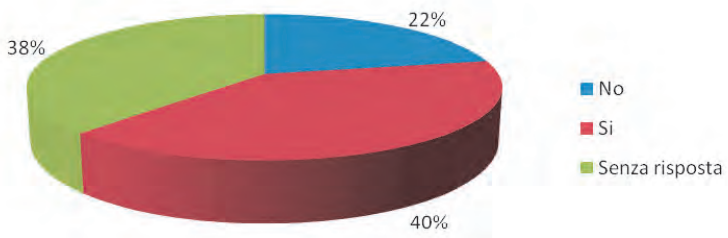
Le risposte al quesito n. 7 mostrano che, nel complesso, la norma EN ISO 13849-1 è giudicata applicabile dagli intervistati.



QUESITO N. 8: Si sono incontrate difficoltà a realizzare i sistemi di controllo secondo le architetture indicate nella norma EN ISO13849-1 per le categorie?

QUESITO N. 9: Le difficoltà (del quesito n. 8) sono state superate?

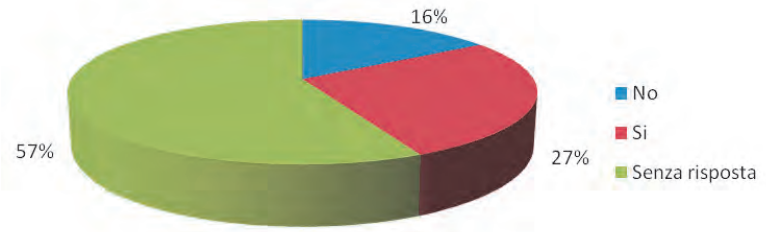
Anche se la maggior parte delle aziende ritiene la norma EN ISO 13849-1 comprensibile e la applica, ciò non di meno una percentuale significativa (circa il 71% di coloro che l'hanno compresa, che hanno risposto “si” al quesito n. 6 e il 78% di quelli che la applicano, che hanno risposto “si” al quesito n. 7) ha incontrato delle difficoltà nell’applicazione (quesito n. 8). È quindi naturale chiedersi se le difficoltà siano relative alla prima applicazione della norma e poi scompaiono una volta messe a punto le procedure operative, oppure se vi siano delle difficoltà di carattere sostanziale. Il dato relativo al superamento delle difficoltà, contenuto nelle risposte al quesito n. 9, confrontato con la percentuale di aziende che le hanno sperimentate, di cui al quesito n. 8, evidenzia che il 30% di coloro che hanno trovato difficoltà (14% delle risposte al questionario) è poi riuscito a superarle. Allo stesso tempo, è significativa anche la percentuale di coloro che non sono riusciti a superarle: ciò è indice di problemi nell'approccio alla norma o di effettive difficoltà insite nella norma stessa. Nel primo caso, se ne può concludere che le difficoltà sono superabili persistendo nell’intento di voler applicare la norma, mentre nel secondo caso si comprende che la versione attuale della norma può essere sicuramente migliorata nel futuro.



QUESITO N. 10: Si sono incontrate difficoltà a realizzare lo schema a blocchi logici del sistema di controllo secondo quanto richiesto nella norma EN ISO13849-1?

Anche il dato relativo alle risposte date al quesito n. 10 è consistente con la percentuale di aziende che al quesito n.8 hanno risposto di aver incontrato difficoltà e indica che una parte rilevante delle difficoltà incontrate dipende dalla prescrizione della norma relativa alla richiesta di realizzare uno schema a blocchi del sistema di controllo. Tale richiesta è evidentemente un punto critico della norma, considerato che crea difficoltà anche a progettisti esperti.

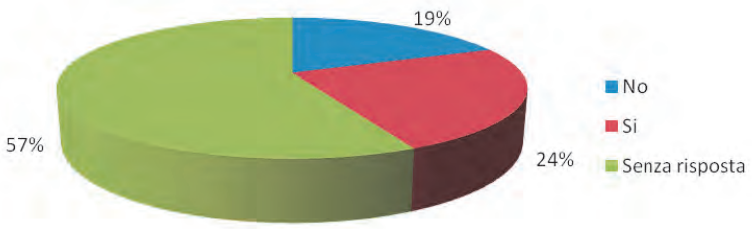
Il gruppo di quesiti 11–15 cerca di indagare l'applicabilità della norma EN IEC 62061.



Quesito n. 11: La norma EN IEC 62061 è comprensibile?

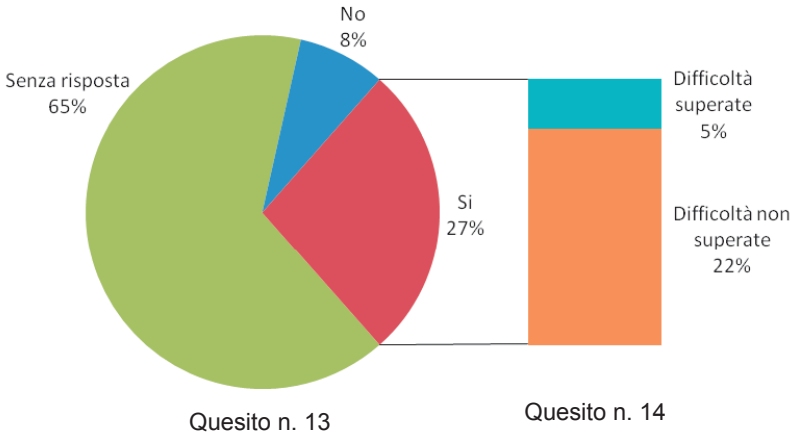
Già dalle risposte date al quesito n. 5 era risultato evidente che la norma EN IEC 62061 ha una diffusione minore rispetto alla EN ISO 13849-1, dato confermato dalla percentuale di risposte al quesito n. 11 (il 57% delle aziende che hanno risposto non ha dato informazioni sulla comprensibilità della EN IEC 62061). A ciò può aver contribuito anche il fatto che molte delle aziende intervistate non producono componenti o parti di sistemi che contemplino l'applicazione della norma EN IEC 62061, che è specifica per i sistemi di controllo elettrici, elettronici ed elettronici programmabili.

In ogni caso l'impressione è che la EN IEC 62061 sia sembrata agli intervistati meno comprensibile della EN ISO 13849-1.
È da notare che la percentuale dei soggetti che ha dichiarato di aver compreso la EN IEC 62061 è leggermente superiore alla percentuale dei soggetti che effettivamente la applicano (come è verificabile per confronto con le risposte date al quesito n. 12).



QUESITO N. 12: La norma EN IEC 62061 è applicabile?

Le risposte al quesito n. 12 mostrano che la maggioranza delle aziende che hanno risposto che la norma era comprensibile (quesito n. 11), l'ha ritenuta anche applicabile (la percentuale di coloro che hanno ritenuto la EN IEC 62061 applicabile è numericamente compatibile con la percentuale di coloro che nel quesito n. 5 hanno dichiarato di applicarla, da sola o in contemporanea con altre norme).



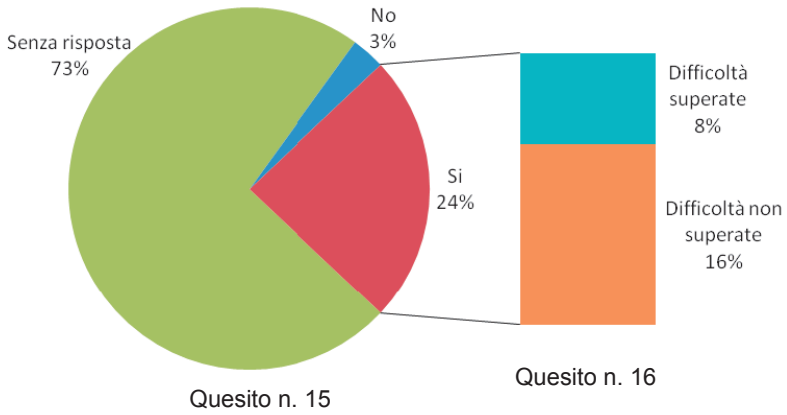
QUESITO N. 13: Si sono incontrate difficoltà nella norma EN IEC 62061 a suddividere la funzione di sicurezza in blocchi funzionali e ad associare a questi il corrispondente sottosistema?

QUESITO N. 14: Le difficoltà (del quesito n. 13) sono state superate?

Tra coloro che hanno risposto al quesito n. 13 la maggioranza delle aziende ha ritenuto complesso o comunque difficoltoso il processo di suddivisione in blocchi funzionali del sistema di controllo, in analogia a quanto già evidenziato per la EN ISO 13849-1 nel

quesito n.10. Sempre per confronto con il quesito 10, è possibile notare che chi applica la EN IEC 62061 senza problemi è un gruppo più ristretto rispetto a chi applica la EN ISO 13849-1 senza problemi (l'8% del quesito n. 13 contro il 22% del quesito n. 8).

Le risposte al quesito n. 14 mostrano che le difficoltà incontrate per l'applicazione della norma EN IEC 62061 non hanno trovato metodiche efficaci di soluzione, che possano aiutare i progettisti ed i produttori di sistemi di controllo al loro superamento. Evidentemente la EN IEC 62061 presenta maggiori difficoltà applicative rispetto alla EN ISO 13849-1. Infatti, dal confronto con il quesito precedente si evince che la maggior parte di coloro che hanno avuto difficoltà ad applicare la norma non sono poi riusciti a superarle.



QUESITO N. 15: Si sono riscontrate difficoltà a realizzare sistemi di controllo secondo le architetture semplificate indicate nella norma EN IEC 62061?

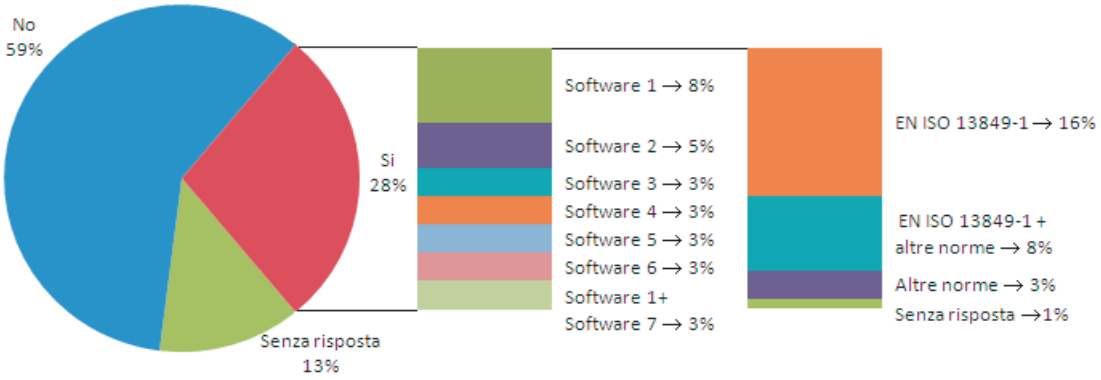
QUESITO N. 16: Le difficoltà (del quesito n. 15) sono state superate?

Le risposte al quesito n. 15 mostrano che anche l'applicazione delle architetture semplificate, descritte nel paragrafo 6.7.8.2. della norma EN IEC 62061, ha costituito un problema per le aziende che hanno risposto al questionario. Le ragioni possono essere molteplici e saranno analizzate in dettaglio nel seguito; si può comunque anticipare che gran parte dei problemi sono spesso dovuti alla difficoltà di reperimento delle informazioni.

Le risposte al quesito n. 16 mostrano che solo un terzo di coloro che hanno incontrato difficoltà sono poi riusciti a superarle. Già era emerso dai quesiti n. 13 e n. 14 il fatto che l'applicazione delle metodiche generali della norma potesse creare problemi, ma ora si vede che anche l'applicazione delle metodiche semplificate è altrettanto problematica.

Alla diffusione delle norme EN ISO13849-1 e EN IEC 62061 ha, di sicuro, contribuito la sempre crescente diffusione di software che consentono ai progettisti di realizzare la documentazione e i calcoli secondo le prescrizioni delle norme stesse. L'applicabilità di una norma è, in tale contesto, il risultato di un continuo sviluppo di ambienti e piattaforme che permettono a chi deve mettere in pratica i dettami della norma di poter entrare nei

singoli aspetti della progettazione, secondo le prescrizioni normative, a qualsiasi livello di dettaglio, dall'intero sistema fino alle caratteristiche dei singoli componenti.
Il gruppo di quesiti da 17 a 22 cerca di indagare le possibilità di applicabilità delle norme, legate all'uso di pacchetti software specifici.



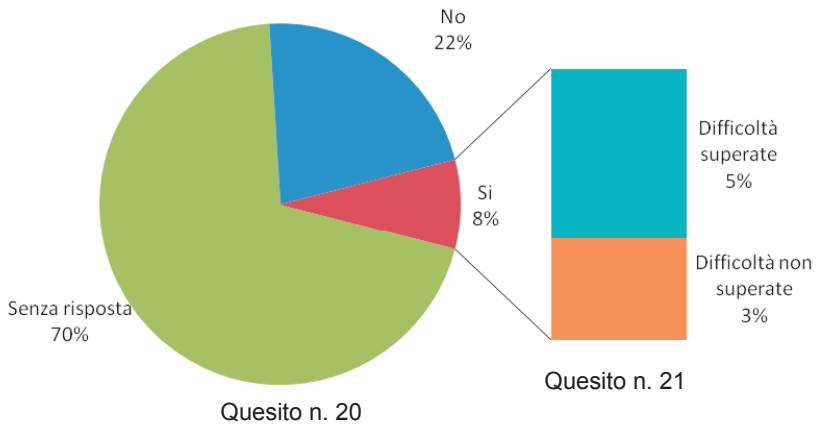
Quesito n. 17 Quesito n. 18 Quesito n. 19

QUESITO N. 17: È usato un software specifico per l'applicazione delle norme sulla sicurezza dei sistemi di controllo (ad es. un software per la valutazione dell'affidabilità)?

QUESITO N. 18: Se (si è risposto) si (al quesito n. 17) specificare il nome (del software).

QUESITO N. 19: Specificare le norme per cui si utilizza il software

Le risposte al quesito n. 17 mostrano che la maggior parte delle aziende non utilizza dei software specifici. Ciò potrebbe essere legato al fatto che la maggioranza delle aziende si occupa soltanto di "assemblare" il sistema di controllo all'interno delle architetture delle macchine che produce.
Le risposte al quesito n. 18 mostrano che il mercato dei software specifici, seppur limitato, comincia già ad essere sufficientemente differenziato. In ogni caso, non vi sono software specifici che abbiano percentuali di diffusione significative e rilevanti.
Le risposte al quesito n. 19 mostrano che i software specifici sono utilizzati quasi esclusivamente per l'applicazione della norma EN ISO 13849-1.

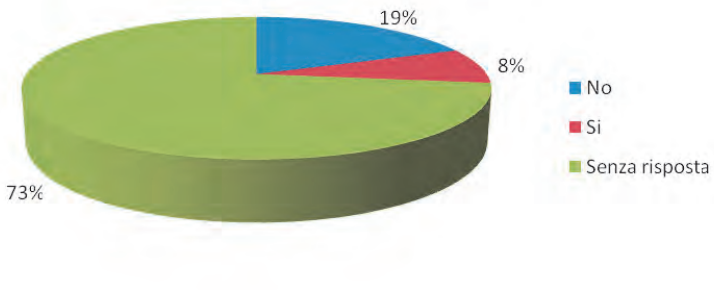


QUESITO N. 20: Si sono incontrate difficoltà ad applicare il software?

QUESITO N. 21: Le difficoltà (del quesito n. 20) sono state superate?

Le risposte al quesito n. 20 mostrano che, tra le aziende che utilizzano un software per gestire l'applicazione delle norme, quasi la totalità (il 78% di coloro che hanno risposto "si" al quesito n. 17) ha dichiarato di non aver incontrato difficoltà nella sua applicazione. È probabile che tali aziende abbiano del personale dedicato all'uso di simili software.

Le risposte al quesito n. 21 mostrano che la percentuale di chi non ha superato le difficoltà è quasi uguale alla metà di chi aveva incontrato tali difficoltà (quesito n. 20).

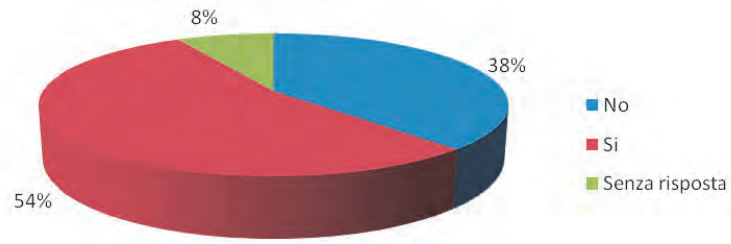


QUESITO N. 22: Il software contiene una base dei dati di fidatezza?

Le risposte al quesito n. 22 rivelano che vi è una scarsa presenza di librerie di dati all'interno dei software disponibili sul mercato.

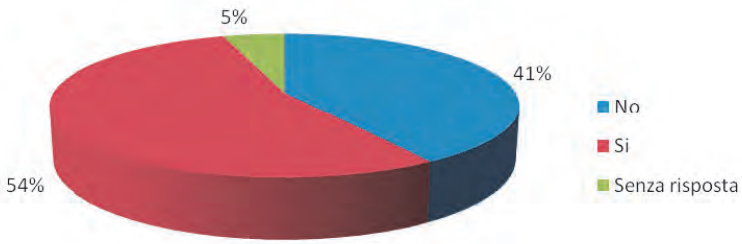
Tipologia di organizzazione

Un gruppo di domande è stato dedicato ad indagare sulle caratteristiche di quella parte di organizzazione aziendale preposta a garantire il rispetto delle norme specifiche sulla sicurezza dei sistemi di controllo delle macchine. Quasi tutte le domande sono state poste in termini dicotomici.



QUESITO N. 24: Esistono all'interno delle aziende delle procedure per definire compiti e responsabilità in merito alla progettazione in sicurezza delle macchine e dei sistemi di controllo?

Il quesito n. 24 chiedeva informazioni specifiche sulle capacità organizzative e gestionali delle aziende; l'analisi era volta a far luce su di un aspetto del processo produttivo che non è prettamente organizzativo, ma può essere direttamente correlato all'efficacia e alla sicurezza dei prodotti poi realizzati. È però da evidenziare il fatto che il 38% del campione non possiede procedure e figure ben definite in merito ai compiti e alle responsabilità in fase di progettazione.



QUESITO N. 25: Esistono all'interno delle aziende delle procedure per definire compiti e responsabilità per gli aspetti di valutazione e verifica in fase di progetto, realizzazione/assemblaggio?

Le risposte al quesito n. 25 rivelano che, in analogia all'alta percentuale di risposte negative al quesito precedente, il 41% delle aziende intervistate non hanno definito al proprio interno alcun processo di gestione per gli aspetti legati alla verifica e alla

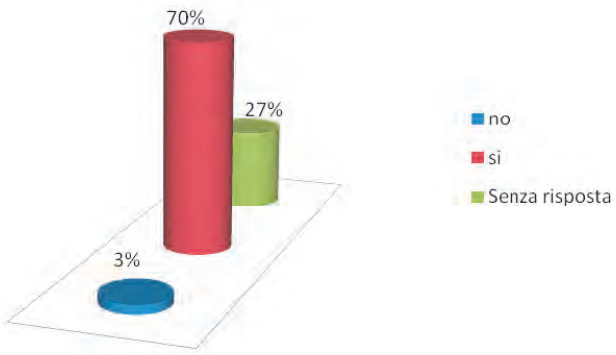
valutazione del rispetto delle norme e dei requisiti di sicurezza, oltre che dei requisiti funzionali e delle specifiche in fase di progetto.

Tra le aziende che hanno contribuito a rendere rilevanti le percentuali di risposte negative ai quesiti n. 24 e n. 25 vi sono probabilmente quelle aziende che acquistano da altri il sistema di controllo e non si occupano della sua progettazione.
Però, le alte percentuali di "no" fanno desumere che ciò potrebbe essere dovuto alla mancanza di un sistema di qualità dei prodotti e/o della produzione e/o aziendale.

Reperimento di informazioni

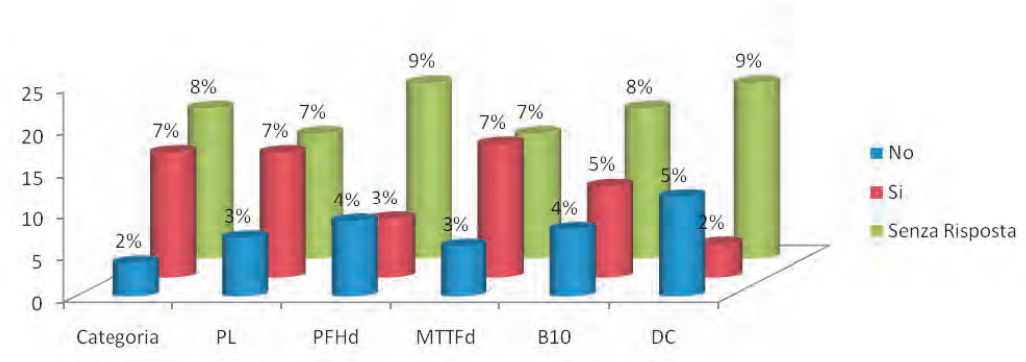
Un gruppo di domande è stato dedicato ad indagare sul livello di utilizzo delle norme armonizzate per la sicurezza dei sistemi di controllo e sulla loro effettiva diffusione. Il metodo per svolgere tale indagine è stato quello di verificare se i fornitori mettono a disposizione delle aziende le informazioni su alcuni dei parametri che riguardano i singoli componenti e che sono necessari per l'applicazione delle norme stesse. Allo stesso tempo, dal tipo delle risposte fornite è stato possibile evincere quanto chi avrebbe dovuto utilizzare tali informazioni fosse consapevole di ciò che stava facendo. Quasi tutte le domande sono state poste in termini dicotomici.

Scopo del quesito n. 26 era quello di vedere quali informazioni, sull'affidabilità dei sistemi/componenti, i fornitori mettevano a disposizione dei costruttori/assemblatori. In realtà, alcune delle informazioni riguardavano esclusivamente i sistemi ed altre i componenti anche se, per come era posto il quesito, tale fatto non traspariva. Ad esempio, tanto per rendere più chiaro il concetto, la copertura diagnostica (DC) ha senso se riferita a componenti complessi, quali schede logiche, microcontrollori, ecc.



QUESITO N. 26: In riferimento alle norme utilizzate, quali parametri sono dichiarati dai fornitori sui singoli prodotti? **La Categoria** (con riferimento alla EN 954-1)?

Per quanto riguarda la EN 954-1, si riscontra come la Categoria rientri ormai tra i parametri dichiarati (la percentuale di risposte negative o di mancanza di risposte è dovuta senz'altro all'adozione di altre norme).

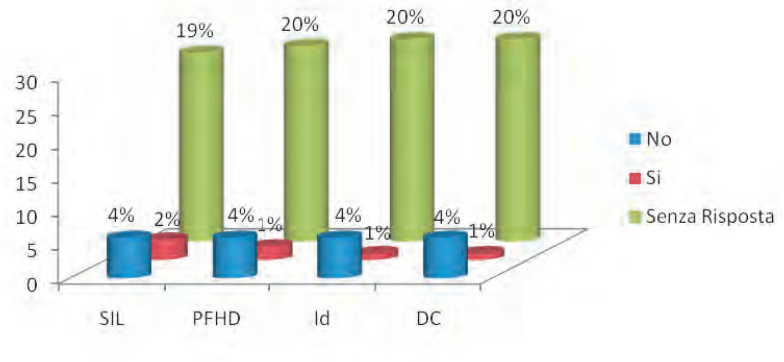


QUESITO N. 26: In riferimento alle norme utilizzate, quali parametri sono dichiarati dai fornitori sui singoli prodotti? **La Categoria, il PL, il PFH_D, il $MTTF_d$, il B_{10}, la DC** (con riferimento alla EN ISO 13849-1)?

Per quanto riguarda la EN ISO 13849-1, si riscontra come la Categoria, il PL, il PFH_D, il $MTTF_d$, il B_{10}, la DC, facciano ormai parte del bagaglio culturale dei fornitori di sistemi/componenti e rientrino quindi tra i parametri dichiarati (la percentuale di risposte negative o di mancanza di risposte è dovuta anche all'adozione di altre norme).

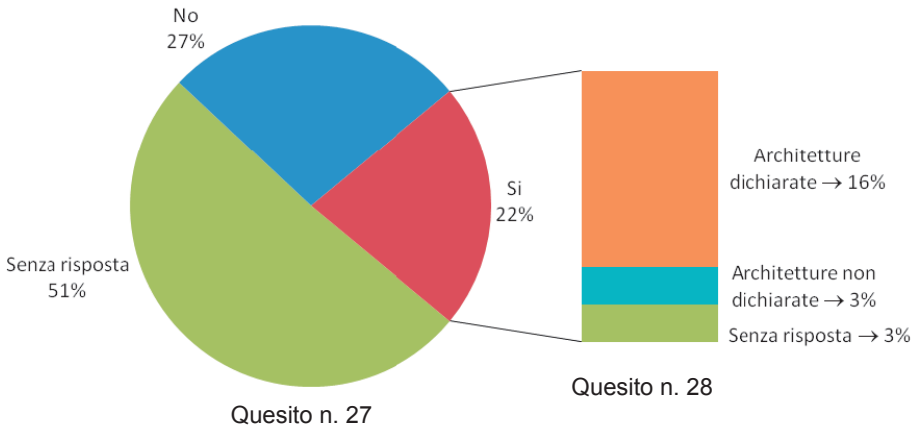
QUESITO N. 26: In riferimento alle norme utilizzate, quali parametri sono dichiarati dai fornitori sui singoli prodotti? **Il SIL, il PFH_D, il λ_D, la DC** (con riferimento alla EN IEC 62061)?

Per quanto riguarda la EN IEC 62061,si riscontra come il SIL, il PFH_D, il λ_D=1/$MTTF_d$, la DC, facciano ormai parte del bagaglio culturale dei fornitori di sistemi/componenti e rientrino quindi tra i parametri dichiarati (la percentuale di risposte negative o di mancanza di risposte è dovuta anche all'adozione di altre norme).



QUESITO N. 26: In riferimento alle norme utilizzate, quali parametri sono dichiarati dai fornitori sui singoli prodotti? **Il SIL, il PFH_D, il λ_D, la DC** (con riferimento alla IEC 61508)?

Per quanto riguarda la IEC 61508, si riscontra come il SIL, il PFH_D, il $\lambda_D=1/MTTF_d$, la DC, facciano ormai parte del bagaglio culturale dei fornitori di sistemi/componenti e rientrino quindi tra i parametri dichiarati (la percentuale di risposte negative o di mancanza di risposte è dovuta anche all'adozione di altre norme).



QUESITO N. 27: Nel caso di sistemi di controllo acquistati "chiavi in mano", è dichiarata dal fornitore la categoria/architettura utilizzata per ogni funzione di sicurezza?

QUESITO N. 28: In caso di risposta affermativa sono dichiarate dal fornitore del sistema di controllo anche le categorie/architetture utilizzate per realizzare i sottosistemi?

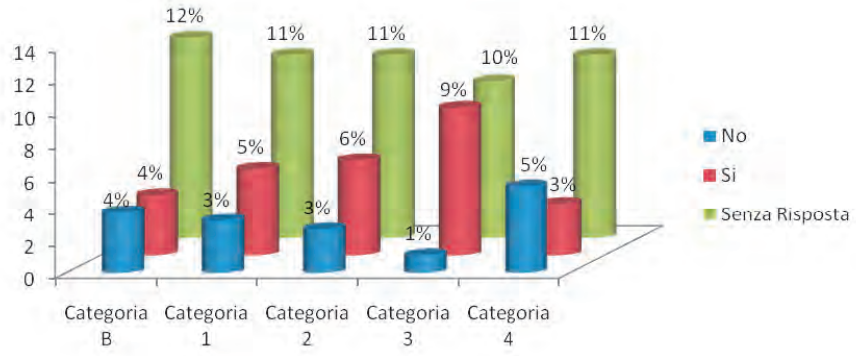
Le risposte al quesito n. 27 mostrano che, per coloro che hanno risposto "si" o "no" (il 49% del campione), alcuni fornitori dei sistemi di controllo non dichiarano alcun tipo di caratteristica architetturale per le funzioni di sicurezza che i sistemi forniti andranno a

realizzare. Ovviamente, a tale domanda non hanno risposto coloro che non acquistano sistemi di controllo “chiavi in mano”.

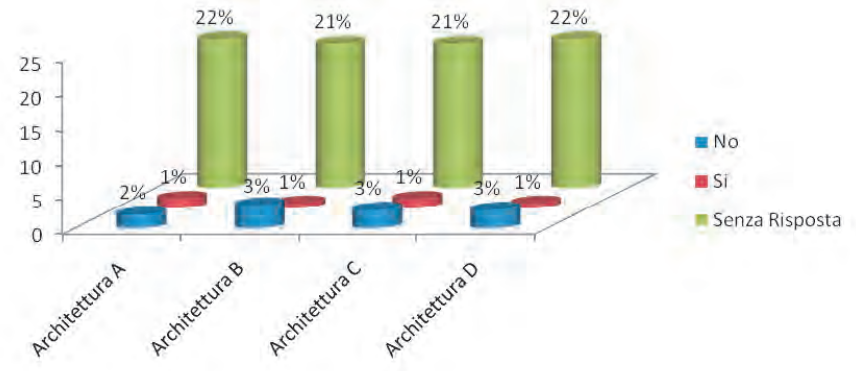
Le risposte al quesito n. 28 mostrano che solo il 16% della totalità dei fornitori dichiara le categorie/architetture utilizzate per realizzare i sottosistemi (anche se qualcuno dichiara la Categoria dell’intero sistema di controllo “chiavi in mano”).

Prestazioni

Un gruppo di domande è stato dedicato ad indagare sulle prestazioni raggiunte dall’azienda nell’adozione delle norme sulla sicurezza dei sistemi di controllo delle macchine. Quasi tutte le domande sono state poste in termini dicotomici.

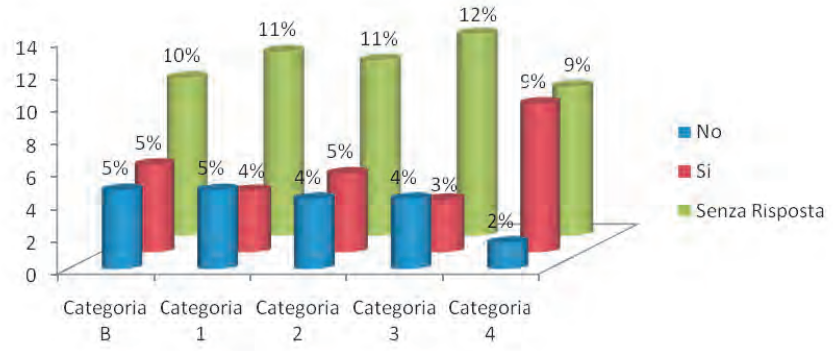


QUESITO N. 29: Dare un’indicazione delle categorie/architetture utilizzate prevalentemente, con riferimento alla EN ISO 13849-1

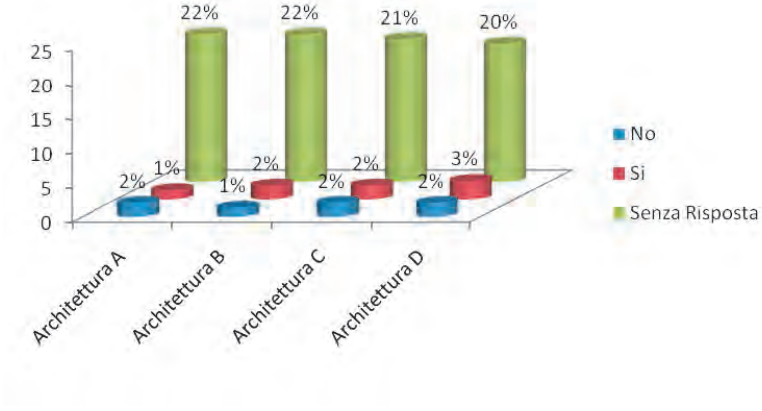


QUESITO N. 29: Dare un’indicazione delle categorie/architetture utilizzate prevalentemente, con riferimento alla EN IEC 62061

Le risposte al quesito n. 29 confermano che la norma più adottata è la EN ISO 13849-1 in quanto evoluzione della EN 954-1.

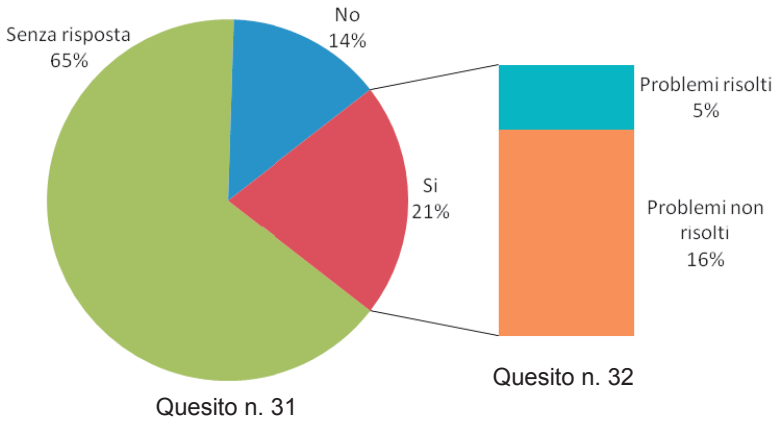


QUESITO N. 30: Dare un'indicazione delle categorie/architetture utilizzate raramente o mai, con riferimento alla ISO EN13849-1



QUESITO N. 30: Dare un'indicazione delle categorie/architetture utilizzate raramente o mai, con riferimento alla EN IEC 62061

Le risposte al quesito n. 30 confermano (anche se in termini di negazione) che la norma più adottata è la EN ISO 13849-1.

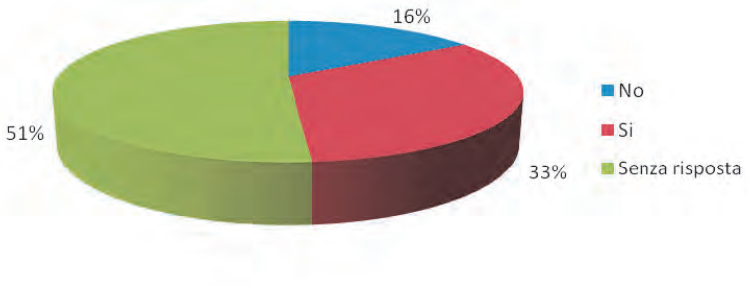


QUESITO N. 31: Si sono incontrati problemi per ottenere un software embedded compatibile con il SIL/PL richiesto?

QUESITO N. 32: I problemi (del quesito n. 31) sono stati risolti?

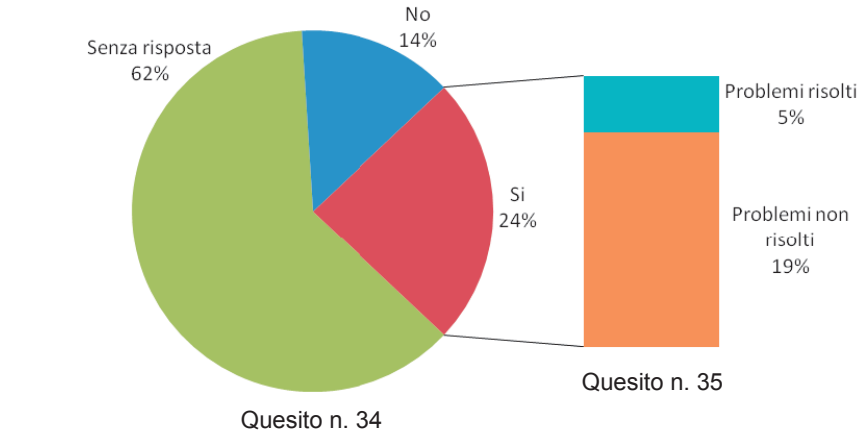
Le risposte al quesito n. 31 mostrano che alcune aziende hanno incontrato difficoltà nel reperire software embedded che fossero compatibili con le esigenze di carattere progettuale.

Le risposte al quesito n. 32 mostrano che tra le aziende che hanno incontrato delle difficoltà, alcune non le hanno risolte.



QUESITO N. 33: Il software applicativo per il sistema di controllo è progettato all'interno dell'azienda?

Il quesito n. 3 aveva mostrato che circa il 59% delle aziende assemblava macchine impiegando componenti prodotti da altri, mentre il quesito n. 27 aveva mostrato che circa il 49% delle aziende faceva ricorso a sistemi di controllo “chiavi in mano”. È importante tenere a mente le citate percentuali nel prendere in considerazione il quesito n. 33, a cui ha risposto ancora un 49% delle aziende.
Le risposte mostrano come circa due terzi delle aziende che hanno risposto produca da sé il software applicativo.

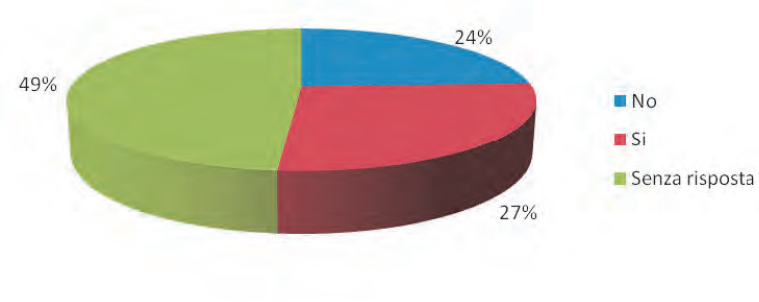


QUESITO N. 34: Si sono incontrati problemi per ottenere un software applicativo compatibile con il SIL/PL richiesto?

QUESITO N. 35:I problemi sono stati risolti?

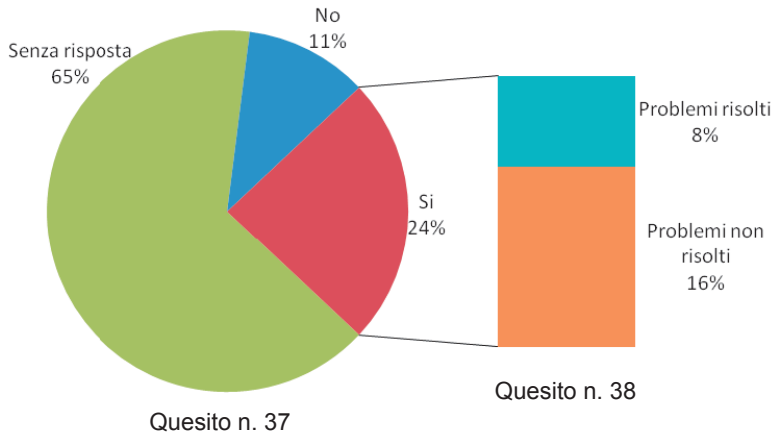
Le risposte al quesito n. 34 mostrano che alcune aziende hanno incontrato difficoltà nell'ottenere software applicativi che fossero compatibili con le esigenze di carattere progettuale.

Le risposte al quesito n. 35 mostrano che tra le aziende che hanno incontrato delle difficoltà, alcune non le hanno risolte.



QUESITO N. 36: Il software applicativo per il sistema di controllo è validato all'interno dell'azienda?

Le risposte al quesito n. 36 mostrano che, per il 27% delle aziende, esiste un sistema di valutazione del software. I processi di validazione assicurano che le prestazioni del software rispondano in modo efficiente alle specifiche del sistema di controllo.



QUESITO N. 37: Si sono incontrati problemi per la validazione del software applicativo?

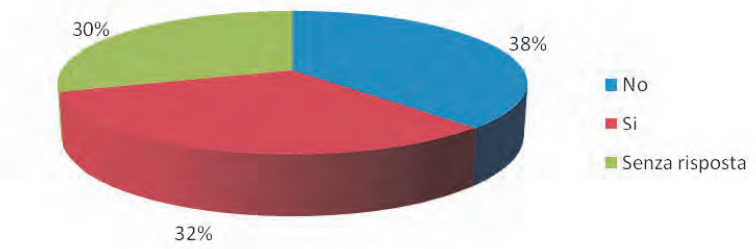
QUESITO N. 38: I problemi sono stati risolti?

Le risposte al quesito n. 37 mostrano che alcune aziende hanno incontrato difficoltà nel processo di validazione del software. Ciò potrebbe in parte dipendere dalla scarsa chiarezza delle norme sui requisiti del software e sul processo di validazione relativo.

Le risposte al quesito n. 38 mostrano che, tra le aziende che hanno incontrato delle difficoltà, alcune non le hanno risolte. In realtà, la validazione del software si rivela spesso un processo complesso che solo realtà aziendali ben strutturate e di notevoli dimensioni, con uno staff di sviluppatori dedicato alla progettazione e alla realizzazione del software, possono affrontare.

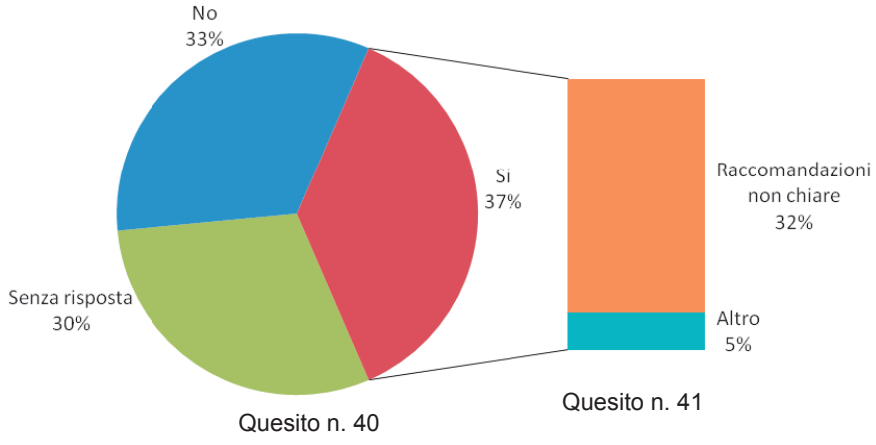
Motivi della mancata adozione

Un gruppo di domande è stato dedicato ad indagare sui motivi della mancata adozione delle norme sulla sicurezza dei sistemi di controllo delle macchine. Tale sezione poteva essere omessa se nella sezione 2 si era dichiarato di aver adottato tali norme. Tuttavia, anche chi avesse adottato le norme poteva rispondere alle domande sulle eventuali difficoltà incontrate. Quasi tutte le domande sono state poste in termini dicotomici.
Per quanto riguarda le risposte ai quesiti della sezione, è da considerare il fatto che dei partecipanti al questionario il 70% ha risposto alla sezione, così suddiviso: il 46% ha risposto sulla EN ISO 13849-1, l'11% sulla EN IEC 62061 ed il 13% su entrambe.



QUESITO N. 39: Le difficoltà applicative delle norme EN IEC 62061 e EN ISO13849-1 sono tali da pregiudicarne l'applicazione?

Le risposte al quesito n. 39 mostrano che, tra coloro che hanno risposto (il 70% del campione), un 46% circa ha avuto difficoltà nell'applicare le norme.

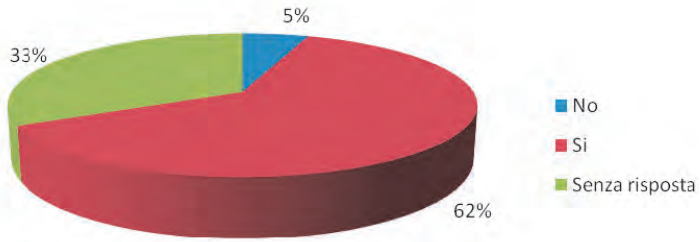


QUESITO N. 40: Si sono incontrate difficoltà nella scelta della norma da applicare?

QUESITO N. 41: In caso affermativo ciò è dovuto a raccomandazioni non chiare sull'applicazione delle norme?

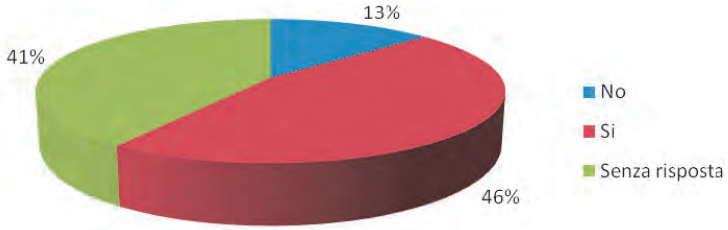
Le risposte al quesito n. 40 mostrano che, tra coloro che hanno risposto (il 70% del campione), il 54% circa ha avuto difficoltà nella scelta stessa della norma da applicare.

Le risposte al quesito n. 41 mostrano che, tra coloro che hanno avuto difficoltà a scegliere quale norma applicare, la maggior parte ha incontrato difficoltà a comprendere le raccomandazioni applicative contenute all'inizio delle norme.



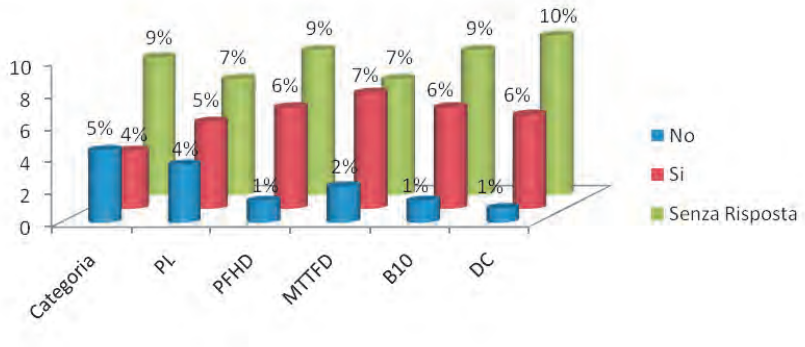
QUESITO N. 42: Si ritiene necessaria la predisposizione di una norma unica in luogo della EN IEC 62061 e della EN ISO13849-1?

Le risposte al quesito n. 42 mostrano che la maggioranza di chi ha risposto (il 70% del campione) auspica una semplificazione del panorama normativo.
La serie di quesiti che segue, dal n. 43 al n. 61, riguarda la norma EN ISO 13849-1.



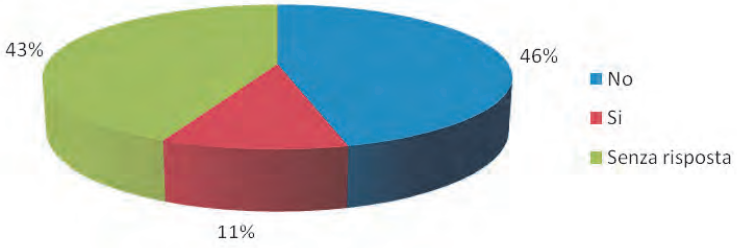
QUESITO N. 43: Si sono incontrate difficoltà ad accedere alle basi di dati sulla fidatezza dei componenti (per quanto concerne le informazioni utilizzate dalla norma EN ISO 13849-1)?

Le risposte al quesito n. 43 mostrano che sono ancora troppo poche le basi di dati da cui reperire le informazioni sulla fidatezza dei componenti richieste dalle norme.



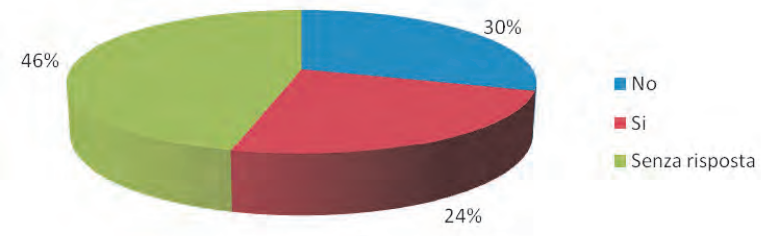
QUESITON. 44: Per la norma EN ISO13849-1 si sono incontrate difficoltà a reperire i dati sottoelencati?

Le risposte al quesito n. 44 mostrano che la difficoltà di reperimento dei dati sulla fidatezza dei componenti non dipende molto dal tipo di parametro cercato.



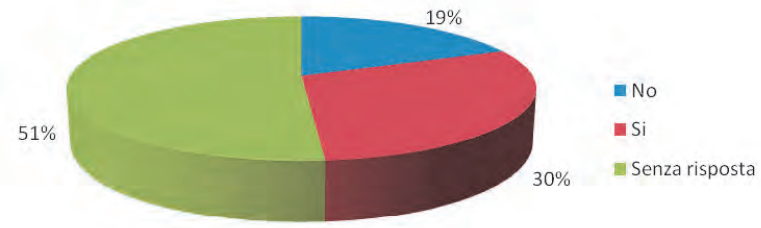
QUESITO N. 45: Si ritiene troppo semplicistica la procedura suggerita per la valutazione del PL_r?

Le risposte al quesito n. 45 mostrano che la maggior parte di coloro che hanno risposto ai quesiti della sessione non ritiene semplicistica la procedura suggerita dalla norma EN ISO 13849-1 per la valutazione del PL_r.



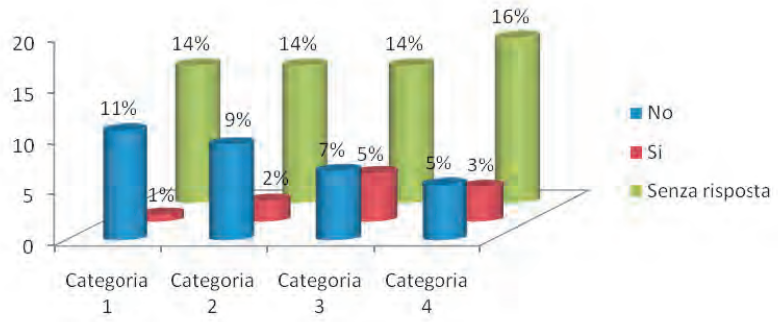
QUESITO N. 46: Si ritiene applicabile la procedura suggerita per la valutazione della copertura diagnostica (DC)?

Le risposte al quesito n. 46 mostrano che la procedura suggerita nell'Allegato E della norma EN ISO 13849-1 per la valutazione della copertura diagnostica non è ritenuta applicabile da tutti. Evidentemente, non sono considerate abbastanza complete o aderenti alle esigenze dei progettisti le indicazioni riportate nella tabella E.1 dell'Allegato E.



QUESITO N. 47: Si ritiene applicabile la procedura suggerita per la valutazione del CCF?

Le risposte al quesito n. 47 mostrano che la procedura suggerita nell'Allegato F della norma EN ISO 13849-1 per la valutazione del CCF non è ritenuta applicabile da tutti. Evidentemente, non sono considerate abbastanza complete o aderenti alle esigenze dei progettisti le indicazioni riportate nella tabella F.1 dell'Allegato F, anche se si nota un incremento delle risposte affermative rispetto al quesito precedente.



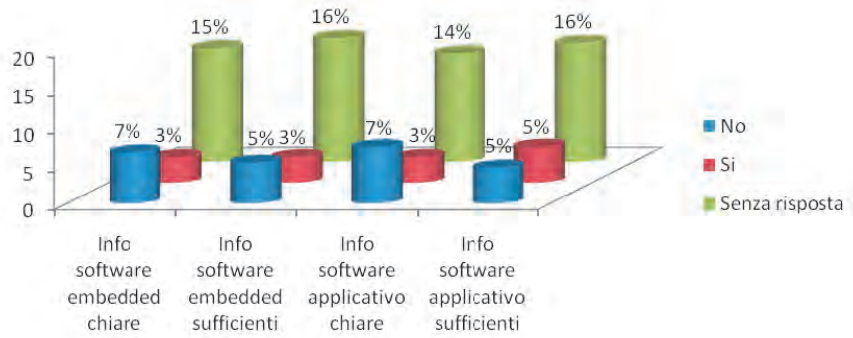
QUESITO N. 48: Si sono incontrate difficoltà per la realizzazione di sistemi conformi alla Categoria 1?

QUESITO N. 50: Si sono incontrate difficoltà per la realizzazione di sistemi conformi alla Categoria 2?

QUESITO N. 52: Si sono incontrate difficoltà per la realizzazione di sistemi conformi alla Categoria 3?

QUESITO N. 54: Si sono incontrate difficoltà per la realizzazione di sistemi conformi alla Categoria 4?

Le risposte ai quesiti n. 48, 50, 52, 54 mostrano che, tra coloro che hanno risposto, la maggioranza non incontra difficoltà nella realizzazione di sistemi di controllo conformi alle varie Categorie della EN ISO 13849-1.



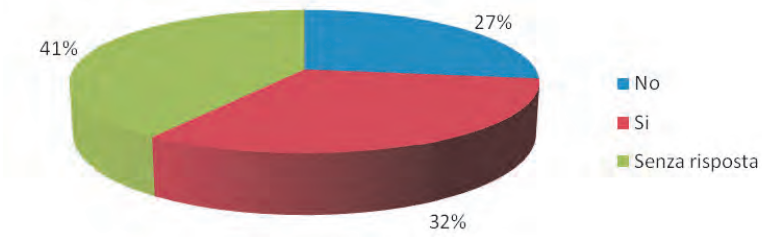
QUESITO N. 56: Le indicazioni fornite dalla EN ISO 13849-1 sul software embedded sono chiare?

QUESITO N. 57: Le indicazioni fornite dalla EN ISO 13849-1 sul software embedded sono sufficienti?

QUESITO N. 58: Le indicazioni fornite dalla EN ISO 13849-1 sul software applicativo sono chiare?

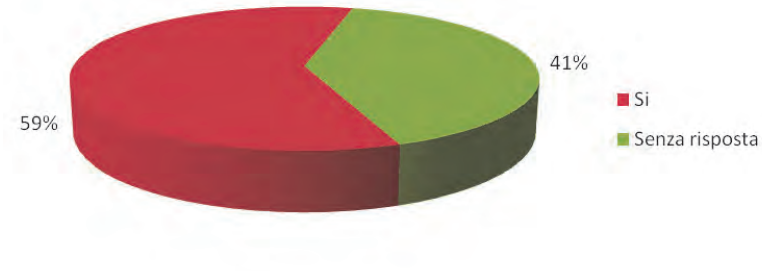
QUESITO N. 59: Le indicazioni fornite dalla EN ISO 13849-1 sul software applicativo sono sufficienti?

Le risposte ai quesiti n. 56, 57, 58, 59 mostrano che, per coloro che hanno risposto, le informazioni fornite dalla norma EN ISO 13849-1, sia per il software embedded che per quello applicativo (parte 4.6.2 parte 4.6.3), non sono né chiare, né sufficienti.



QUESITO N. 60: A fronte delle difficoltà evidenziate si ritiene sufficiente il prolungamento fino a dicembre 2011 della EN 954-1?

Le risposte al quesito n. 60 mostrano che, al momento della somministrazione del questionario, molte aziende preferivano continuare ad utilizzare una norma come la EN 954-1, più semplice da applicare.

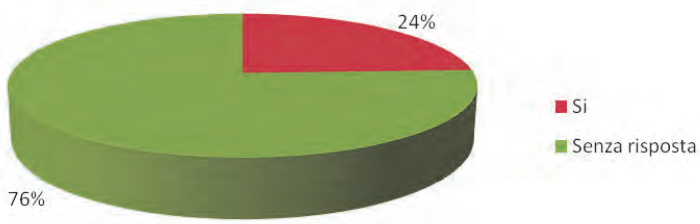


QUESITO N. 61: La conformità alla norma EN ISO 13849-1 è più onerosa rispetto alla conformità alla norma EN 954-1?

Le risposte al quesito n. 61 mostrano che la maggior parte delle aziende che hanno risposto ritengono che realizzare sistemi di controllo che rispettino i requisiti imposti della EN ISO 13849-1 sia più oneroso rispetto a realizzare sistemi di controllo che rispettino i requisiti imposti dalla EN 954-1. Tale aspetto riflette anche le difficoltà incontrate per rispettare i requisiti del software e per implementare un efficiente sistema di validazione.

La serie di quesiti che segue, dal n. 62 al n. 71, riguarda la norma EN IEC 62061. Va ricordato che a tale sezione ha risposto circa il 24% del campione, di cui l'11% ha risposto

ai quesiti sulla sola EN IEC 62061 e 13% ai quesiti che riguardavano anche la EN ISO 13849-1.

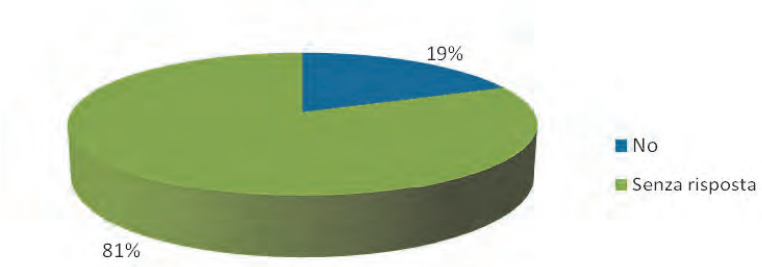


QUESITO N. 62: Si sono incontrate difficoltà ad accedere alle basi di dati sulla fidatezza dei componenti (per quanto concerne le informazioni utilizzate dalla norma EN IEC 62061)?

Le risposte al quesito n. 62 confermano, come quelle del quesito n. 43, che sono ancora troppo poche le basi di dati da cui reperire le informazioni sulla fidatezza dei componenti richieste dalle norme.

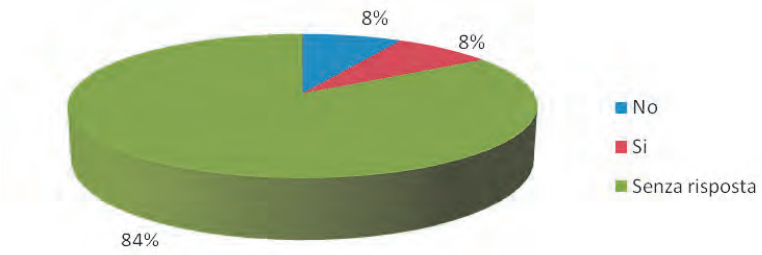
QUESITO N. 63: Si sono incontrate difficoltà a reperire i dati sottoelencati per la norma EN IEC 62061?

Le risposte al quesito n. 63 mostrano che la difficoltà di reperimento dei dati sulla fidatezza dei componenti non dipende molto dal tipo di parametro cercato.



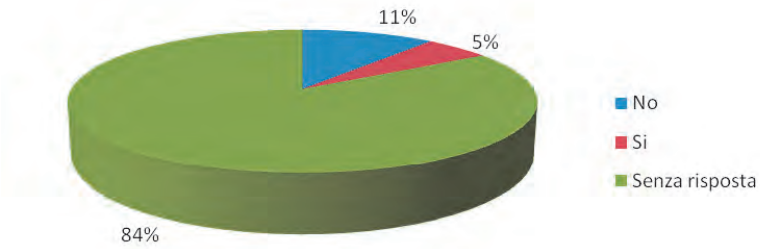
QUESITO N. 64: Si ritiene troppo semplicistica la procedura suggerita per l'assegnazione del SIL?

Le risposte al quesito n. 64 mostrano che la maggior parte di coloro che hanno risposto ai quesiti dal n. 62 al n. 71 non ritiene semplicistica la procedura suggerita dalla norma EN IEC 62061 per l'assegnazione del SIL.



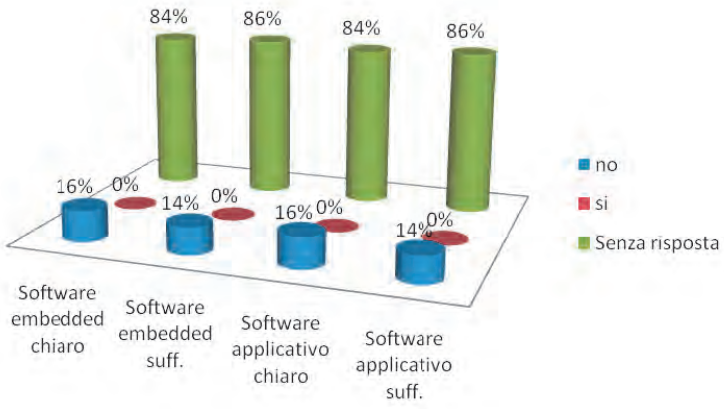
QUESITO N. 65: Si ritiene applicabile la procedura suggerita per la valutazione del CCF?

Le risposte al quesito n. 65 mostrano che, tra le aziende che hanno deciso di rispondere ai quesiti dal n. 62 al n.71 (circa il 24% del totale), quelle che ritengono applicabile la procedura per la valutazione del CCF sono circa un terzo.



QUESITO N. 66: Si sono incontrate difficoltà per la realizzazione di sistemi conformi alle architetture semplificate?

Le risposte al quesito n. 66 mostrano che, tra le aziende che hanno deciso di rispondere ai quesiti dal n. 62 al n.71 (circa il 24% del totale), quelle che, almeno con le architetture semplificate, non hanno incontrato difficoltà sono meno della metà.



QUESITO N. 68: Le indicazioni fornite dalla EN IEC 62061 sul software embedded sono chiare?

QUESITO N. 69: Le indicazioni fornite dalla EN IEC 62061 sul software embedded sono sufficienti?

QUESITO N. 70: Le indicazioni fornite dalla EN IEC 62061 sul software applicativo sono chiare?

QUESITO N. 71: Le indicazioni fornite dalla EN IEC 62061 sul software applicativo sono sufficienti?

Le risposte ai quesiti n. 68, 69, 70, 71 mostrano che, per circa due terzi di coloro che hanno risposto, le informazioni fornite dalla norma EN IEC 62061, sia per il software embedded che per quello applicativo, non sono né chiare, né sufficienti.

Conclusioni

La diffusione, tra i sistemi di comando delle macchine, di sistemi a logica programmabile ha reso necessaria l'emanazione di norme specifiche per regolamentare i metodi di valutazione dell'affidabilità di tali sistemi, in modo da garantire la sicurezza delle macchine su cui sono montati.

L'evoluzione del panorama normativo ha indotto il Dipartimento Tecnologie di Sicurezza dell'INAIL – Settore Ricerca, Certificazione e Verifica - a svolgere un'indagine sulle difficoltà di applicazione di tali norme.

L'indagine è stata svolta per mezzo della somministrazione di un questionario alle aziende aderenti a diverse associazioni di costruttori.

Dalle risposte fornite all'interno dei questionari, emergono evidenti difficoltà in merito all'adozione delle norme EN ISO 13849-1 e EN IEC 62061.
Molte delle risposte fanno intendere che le difficoltà cominciano dalla scelta della norma da applicare e proseguono con l'interpretazione di alcune parti della stessa.
Anche se una larga maggioranza delle aziende reputa la EN ISO 13849-1 applicabile e comprensibile, cosa che spingerebbe a credere che non vi siano grossi problemi nell'applicazione pratica di tale norma, nella realtà sono state evidenziate difficoltà anche a realizzare i sottosistemi secondo le architetture designate.
Difficoltà ad applicare la EN ISO 13849-1 sono state incontrate anche per la progettazione e la validazione del software.
Le stesse anomalie, anche se con percentuali meno significative, sono state riscontrate con la EN IEC 62061.

Probabilmente molte aziende non hanno ancora raggiunto un sufficiente grado di comprensione dei vantaggi che l'applicazione delle norme potrebbe comportare.
La scelta tra la EN ISO 13849-1 e la EN IEC 62061 dipende dalla complessità del sistema da progettare, dalle sue finalità e dal campo di impiego, oltre che dalla successiva integrazione con altri sistemi.
L'impiego di sistemi di controllo di ultima generazione basati sui controllori programmabili rende irrinunciabile il ricorso ad una delle due norme citate, per quantificare il livello di sicurezza raggiunto. In ogni caso, gli enti normatori non possono ritardare ulteriormente la pubblicazione di linee guida applicative che chiariscano meglio scopi, campi di applicazione e, soprattutto, forniscano indicazioni applicative semplificate.

Bibliografia

[1] Decreto Legislativo 27 gennaio 2010 , n. 17, Attuazione della direttiva 2006/42/CE, relativa alle macchine e che modifica la direttiva 95/16/CE relativa agli ascensori.

[2] Decreto del Presidente della Repubblica 24 luglio 1996, n.459, Regolamento per l'attuazione delle Direttive 89/392/CEE, 91/368/CEE, 93/44/CEE e 93/68/CEE concernenti il riavvicinamento delle legislazioni degli Stati membri relative alle macchine.

[3] EN 954-1:1996, Parti dei sistemi di controllo correlate alla sicurezza. Parte 1. Principi generali per la progettazione.

[4] EN ISO13849-1:2006, Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione + EC1:2009.

[5] EN IEC 62061:2005, Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando elettrici, elettronici ed elettronici programmabili correlati alla sicurezza (CEI 44-16).

[6] IEC 61508: 2010, Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza - Requisiti Generali.

[7] CEI EN 61131-3:2009 (CEI 65-1000), Controllori programmabili - Parte 3: Linguaggi di programmazione.

[8] EN 50170:1998, PROFIBUS specification normative parts.

[9] IEC 61158-2, Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition.

[10] EN 60079-27:2008 (CEI 31-76) Concetto di bus di campo a sicurezza intrinseca (FISCO).

[11] EN 50295:1999, Low-voltage switchgear and controlgear - Controller and device interface systems - Actuator Sensor interface (AS-I)

[12] IEC 62026-2:2008, Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) – Part 2: Actuator sensor interface (AS-I)