GIORNATA DI FORMAZIONE SULLE APPARECCHIATURE ELETTRICHE DEGLI IMPIANTI A FUNE

AOSTA, 23 GIUGNO 2015

ing. Gabriele Cappello, NIDEC ASI S.p.A.
ing. Andrea Fornasa, EEI S.p.A.

TEMI TRATTATI - 1

- 1 - FIDATEZZA E SICUREZZA FUNZIONALE
  - Definizioni fondamentali e norme principali
  - Analisi RAMS e calcolo del livello di sicurezza
- 2 - EVOLUZIONE NORMATIVA ITALIANA ED EUROPEA SUGLI IMPIANTI ELETTRICI FUNIVIARI
  - Regolamentazione UNIFER-CEI e Circolare D.G.159/89
  - Prescrizioni tecniche speciali per gli I.E.F.A.T.
  - Direttiva europea 2000/9/CE e norme CEN

TEMI TRATTATI - 2

- 3 – LA REGOLAMENTAZIONE EUROPEA ATTUALE:
  - Punti focali della direttiva e della certificazione
  - Norme elettriche armonizzate e principi di sicurezza
- 4 - SCHEMI ELETTRICI ED ASPETTI OPERATIVI IN RELAZIONE ALLE NORME DI PROGETTO:
  - Regolamentazione UNIFER-CEI
  - Prescrizioni tecniche speciali per gli I.E.F.A.T.
  - Direttiva europea 2000/9/CE e norme CEN

PARTE 1

FIDATEZZA E SICUREZZA FUNZIONALE

ing. Gabriele Cappello, NIDEC ASI S.p.A.

FIDATEZZA: DEFINIZIONI - 1

- FIDATEZZA (Dependability): valutazione del livello di fiducia che può essere attribuito ad un sistema riguardo al suo buon funzionamento.
- SICUREZZA (Safety): Condizione di rischio accettabile nei confronti di eventi pericolosi casuali.
- ANALISI RAMS: analisi delle caratteristiche di:
  - AFFIDABILITA' (Reliability)
  - MANUTENIBILITA' (Manutenibility)
  - DISPONIBILITA' (Availability)
  - SICUREZZA (Safety)

FIDATEZZA: DEFINIZIONI - 2

- AFFIDABILITA': Probabilità che un sistema rimanga continuativamente in grado di eseguire una funzione richiesta, in condizioni stabilite, per un intervallo di tempo dato (t_1,t_2).
  - ➢In particolare, per $t_1 = 0$, è la probabilità di conservare lo stato sano a partire dall'attivazione iniziale.
  - ➢E' sempre una funzione decrescente: probabilmente, o prima o poi, il sistema si guasta.
  - ➢E' una caratteristica posseduta da tutti i sistemi, sia riparabili che non riparabili.

FIDATEZZA: DEFINIZIONI - 3

- MANUTENIBILITA': Probabilità che un sistema guasto, utilizzato in condizioni stabilite, sia sottoposto ad una manutenzione correttiva che lo faccia tornare allo stato sano, in un intervallo di tempo dato (t_1,t_2).
  - ➢E' ovviamente una caratteristica dei soli sistemi riparabili.
  - ➢E', in sintesi, la probabilità di tornare dallo stato guasto allo stato sano in un lasso di tempo stabilito.
  - ➢E' una funzione crescente: probabilmente o prima o poi il sistema viene aggiustato, se viene manutenuto.
  - ➢In genere viene calcolata assumendo i ricambi disponibili e senza contare i tempi logistici di intervento.

FIDATEZZA: DEFINIZIONI - 4

- DISPONIBILITA': Probabilità di un sistema riparabile di trovarsi in grado di eseguire una funzione richiesta, in condizioni stabilite, ad un istante dato t_1 o per un intervallo di tempo dato (t_1,t_2).
  - E' una funzione risultante dai valori di affidabilità e di manutenibilità (riparabilità).
  - E', in sostanza, la probabilità che il sistema si trovi nello stato sano ad un certo istante, indipendentemente dal fatto che in precedenza sia sempre stato sano oppure sia stato riparato dopo essersi guastato.

PARAMETRI AFFIDABILISTICI - 1

- TASSO DI GUASTO (Failure rate) $\lambda(t)$: frequenza di guasto di un componente o di un sistema.
  - ➢In linea di principio è espresso in n° di guasti all'ora.
  - ➢Praticamente, si usa spesso il FIT (Failure In Time):

    $1\ FIT = 10^{-9}$ guasti / ora $\qquad (\lambda_{FIT} = \lambda_h \cdot 10^9)$

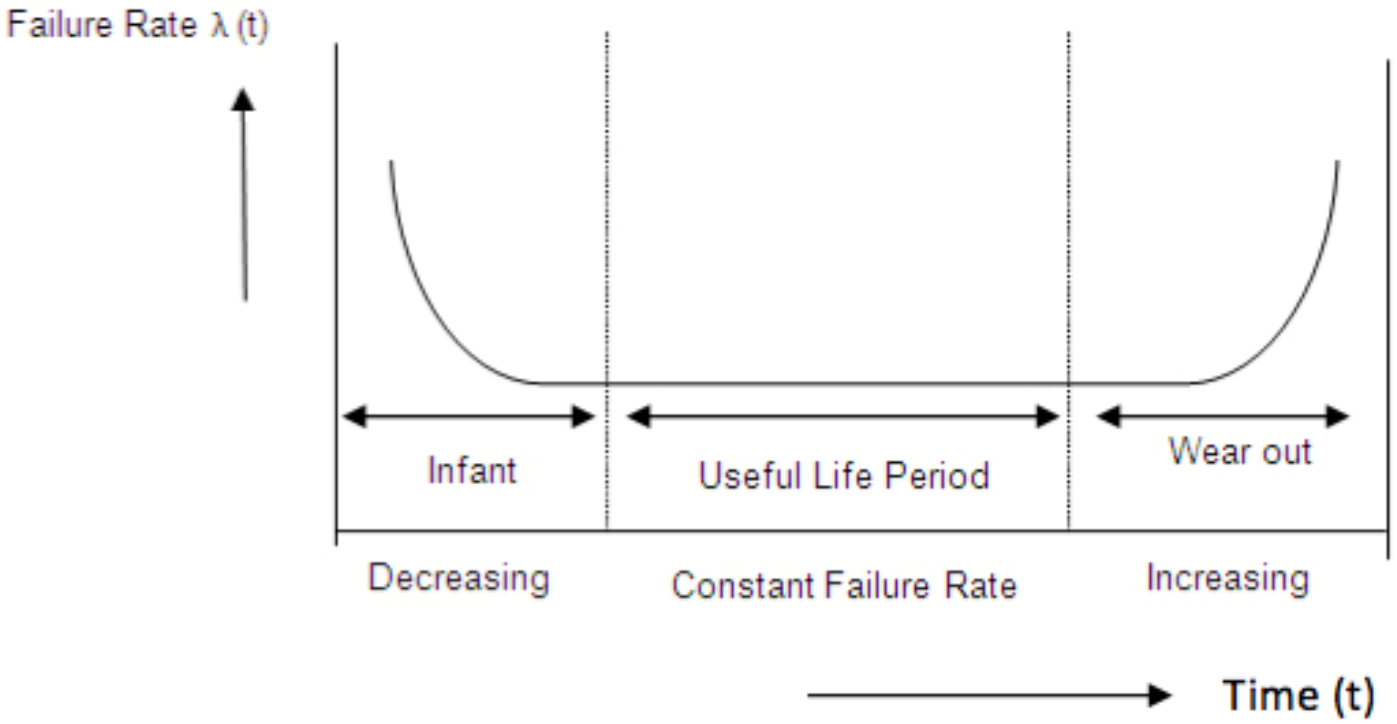
    corrispondente a ppm/kh, cioè 1 guasto per milione di componenti in 1000 ore di funzionamento.
  - ➢E' espresso spesso anche in %/kh (1 %/kh = 1 guasto su 100 componenti in 1000 ore di funzionamento).

PARAMETRI AFFIDABILISTICI - 2

- Il failure rate λ(t) varia durante la vita del sistema:
  - Inizialmente, spesso tende a scendere (assestamento dopo la mortalità infantile);
  - Alla lunga, aumenta (invecchiamento, usura, fatica).
- Nei sistemi elettronici, si riconosce che, per un lungo tempo successivo all'assestamento iniziale, l'affidabilità decresce esponenzialmente. Ciò corrisponde ad avere un failure rate λ = costante.
- Il periodo a tasso di guasto costante costituisce la vita utile del componente (lifetime).

PARAMETRI AFFIDABILISTICI - 3

- L'evoluzione del failure rate λ(t) nei sistemi elettronici è espresso dalla curva a vasca da bagno:



PARAMETRI AFFIDABILISTICI - 4

- La costanza del failure rate dei componenti è importante perché li rende sommabili.
  - ➢Il tasso λ non è una probabilità, ma vi è legato; per il teorema della probabilità totale, il tasso di guasto di un sistema è la somma dei tassi dei singoli componenti.
  - ➢Esempi di ordine di grandezza del tasso di guasto:
    - ✓ resistore: 1 ÷ 25 FIT
    - ✓ encoder: 20’000 FIT
    - ✓ elementi di PLC (CPU, moduli I/O): 1 FIT (ciascuno!)
    - ✓ centraline di sicurezza (check motore fermo): 5 FIT

PARAMETRI AFFIDABILISTICI - 5

- TEMPO MEDIO AL GUASTO (MTTF, Mean Time To Failure): tempo mediamente trascorrente affinché il sistema inizialmente sano si guasti.
  - Con MTTF in ore e se λ è costante, risulta:

$$MTTF = 1 / \lambda$$

- TEMPO MEDIO DI RIPARAZIONE (MTTR, Mean Time To Repair): tempo mediamente richiesto affinché il sistema guasto venga riparato.

PARAMETRI AFFIDABILISTICI - 6

- TEMPO MEDIO FRA DUE GUASTI (MTBF, Mean Time Between Failures): tempo mediamente trascorrente fra due guasti successivi.
  - ➢Evidentemente, riguarda i soli sistemi riparabili e vale il lasso di tempo mediamente comprendente un intervallo di up-time ed uno di down-time. Pertanto:

$$MTBF = MTTF + MTTR$$

  - ➢Nei sistemi molto affidabili e rapidamente riparabili, si ha $MTTR << MTTF$, per cui $MTBF \approx MTTF$. Per questo, si trova spesso scritto $MTBF = 1 / \lambda$.

PARAMETRI AFFIDABILISTICI - 7

- B_{10} = n° medio di cicli di lavoro che vede guastarsi il 10% degli esemplari del componente.
  - ➢Spesso, i componenti come pulsanti, contattori e relé vengono caratterizzati dal B_{10} piuttosto che dall' MTTF.
  - ➢Si dimostra che:

$$MTTF = (10 \cdot B_{10}) / n_{op}$$

dove n_{op} è il n° medio di cicli che il componente è chiamato ad eseguire in un anno.

PARAMETRI AFFIDABILISTICI - 8

ATTENZIONE AL SIGNIFICATO DELL'ESPRESSIONE

$$MTTF = 1 / \lambda$$

- Il valore di MTTF dei singoli componenti può essere nell'ordine di milioni di ore, corrispondenti centinaia di anni di servizio affidabile.
- Questi ordini di grandezza NON hanno nulla a che vedere con la vita utile, ma sono solo valori statistici validi entro il lasso di tempo della vita utile (periodo a λ costante), che è normalmente molto più breve!

PARAMETRI AFFIDABILISTICI - 9

- PROBABILITA' ORARIA DI GUASTO (PFH, Probability of Failure per Hour): è l'espressione usata in certe norme per esprimere il tasso di guasto.
  - ➢A rigore non è una probabilità, ed il nome corretto attualmente usato è Average Failure Frequency.
  - ➢I valori di MTTF ed MTBF sono spesso espressi in anni.
    - ✓ In questo caso, ovviamente non si ha più MTTF = 1 / λ con λ in h^{-1}, ma occorre dividere per 8760 = 24 x 365.
  - ➢Se è noto l'MTTF in anni, si ha quindi

$$PFH = 1 / (8760 \ \ MTTF)$$

RIDONDANZA - 1

- La ridondanza, intesa come moltiplicazione delle risorse singolarmente sufficienti a svolgere in modo autonomo una funzione, è lo strumento più potente e semplice per elevare la disponibilità.
- Però:
  - i canali devono essere realmente indipendenti;
  - la funzionalità dei canali dev'essere testata;
  - in linea di principio è costosa.

RIDONDANZA - 2

- Tipi di ridondanza:
  - ➢calda: i canali sono sempre operativi;
  - ➢fredda (‘stand-by’): il canale alternativo è di riserva, e subentra in caso di necessità, in modo automatico o no.

  - ➢omogenea: i canali ridondanti sono identici;
  - ➢diversificata: i canali ridondanti sono diversi.
    - ✓ in particolare, diversi per concezione, tecnologia, costruttore, principio fisico di funzionamento.
    - ✓ antivalenti: costruiti in logica complementare.

RIDONDANZA - 3

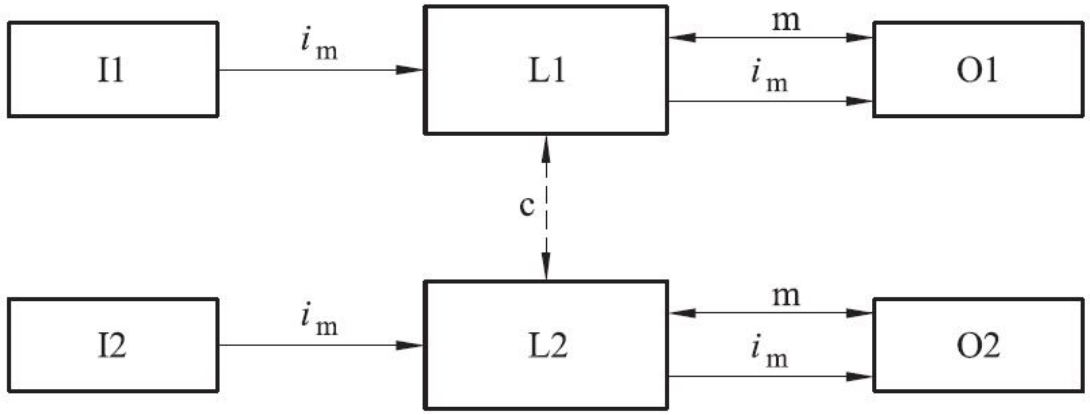
- L'incremento della disponibilità si basa sul fatto che la probabilità di accadimento di un doppio guasto aleatorio contemporaneo è «minima».
  - ➢La probabilità composta di due eventi indipendenti vale il prodotto delle probabilità dei singoli accadimenti.
  - ➢La totale indipendenza è difficile da ottenere: occorre analizzare i GUASTI DI CAUSA COMUNE (CCF: Common Cause Failures), che giocano un ruolo pesante.
  - ➢Il sistema dev'essere riparabile in modo sufficiente-mente rapido (LRU = Line Replaceable Units).

RIDONDANZA - 4

- A proposito di ridondanza calda e fredda:
  - La ridondanza calda garantisce continuità assoluta in caso di guasto di un canale, ma espone al rischio di CCF.
  - La ridondanza fredda è utilizzabile solo quando il tempo di commutazione è tollerabile, ma in genere è molto più robusta verso i CCF (es.: EMI, fulminazioni); richiede di garantire la vitalità dei canali (es.: scambio).
- A proposito di ridondanza diversificata:
  - Costituisce uno strumento molto efficace contro i CCF;
  - E' complessa e costosa (doppia progettazione).

RIDONDANZA - 5

- Affinché la disponibilità si mantenga elevata, è indispensabile rilevare tempestivamente il guasto di un canale.
  - ➢L'architettura più semplice prevede un sistema di test basato sul confronto continuo fra i canali. Ad es.:



RIDONDANZA - 6

- Non è facile diagnosticare tutti i possibili guasti «interessanti»; occorre valutarli con attenzione e stimare il TASSO DI COPERTURA DIAGNOSTICA (DC, Diagnostic Coverage):

$$TCD = \frac{\text{Frequenza dei guasti rilevati}}{\text{Frequenza dei guasti totali}}$$

- ATTENZIONE: la ridondanza senza un test continuo o periodico di operatività dei canali è inutile.

SICUREZZA FUNZIONALE - 1

- PERICOLO (Hazard): sorgente potenziale di danno.
- DANNO (Harm): lesione fisica o danneggiamento della salute di persone, o della proprietà, o dell'ambiente.

  - SITUAZIONE PERICOLOSA (Hazardous situation): situazione in cui un soggetto si trova esposto ad un pericolo.
  - EVENTO PERICOLOSO (Hazardous event): accadimento in cui una situazione pericolosa può determinare un danno.
  - EVENTO DANNOSO (Harmful event): accadimento in cui una situazione pericolosa determina un danno.

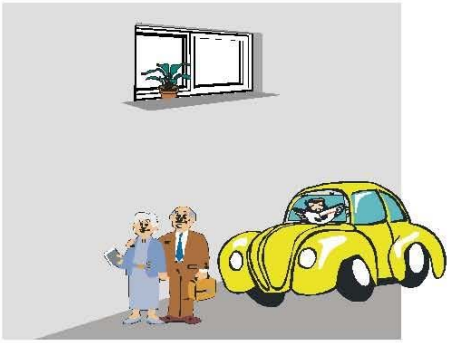
SICUREZZA FUNZIONALE - 2

IEC

From hazard to harm

Hazard

Hazardous Situation



Hazardous Event

Harm

SICUREZZA FUNZIONALE - 3

- QUANTIFICAZIONE DEL PERICOLO E DEL DANNO
  - ➢Il pericolo è caratterizzato quantificando in modo opportuno (per classi o mediante statistiche) la probabilità di accadimento dell'evento dannoso.
  - ➢Il danno viene quantificato con una opportuna scala di gravità (severity), detta anche magnitudo.
  - ➢La scala di gravità più efficace è «logaritmica», sia che venga espressa numericamente sia in modo descrittivo (es.: ferite recuperabili, lesioni permanenti, morte di un singolo o di pochi, morte di molte persone).

SICUREZZA FUNZIONALE - 4

- RISCHIO (Risk): funzione proporzionale al prodotto della probabilità dell'evento dannoso per la magnitudo del danno determinatosi.

  - RISCHIO ORIGINARIO: rischio presentato dal sistema prima di adottare contromisure che lo mitighino.
  - RISCHIO RESIDUO: rischio presentato dal sistema dopo aver adottato contromisure per mitigarlo.
  - MITIGAZIONE DEL RISCHIO: contromisure adottate per ottenere un rischio residuo desiderato.

SICUREZZA FUNZIONALE - 5

- VALUTAZIONE DEI RISCHI (Risk assessment):
  - ➢ANALISI DEI RISCHI (Risk analysis): individuazione dei pericoli e stima quantitativa dei rischi ad essi connessi, entro le limitazioni d'uso del sistema.
  - ➢QUANTIFICAZIONE DEI RISCHI (Risk evaluation): valutazione del conseguimento degli obiettivi di riduzione dei rischi, effettuata iterativamente dopo l'introduzione delle contromisure di mitigazione.
    - ✓ Le contromisure sono sufficienti quando il rischio residuo ha raggiunto un livello accettato, cioè quando l'uso della macchina si può ritenere sufficientemente sicuro.

SICUREZZA FUNZIONALE - 6

- SICUREZZA FUNZIONALE: insieme delle misure di mitigazione del rischio fornite dall'automazione della macchina mediante funzioni di sicurezza.
  - ➢In genere, il rischio residuo accettabile (cioè il funzionamento sicuro) è legato ai requisiti normativi e allo stato dell'arte, e segue il criterio «ALARP» (As Low As Reasonably Possible);
  - ➢le misure di sicurezza funzionale non sono (quasi) mai sufficienti e vanno (quasi) sempre integrate da istruzioni operative (manuali, prescrizioni d'uso e manutenzione).

SICUREZZA FUNZIONALE - 7

- Approfondiamo il concetto di guasto:
  - AVARIA (Fault): **stato** di incapacità di svolgere la missione richiesta («stato guasto»).
  - GUASTO (Failure): **transizione** dallo stato di capacità di svolgere la missione richiesta («stato sano») allo stato guasto.
    - ✓ Attenzione: nella comune terminologia italiana, anche tecnica, i lemmi Avaria e Guasto sono spesso confusi.
    - ✓ Un componente elettrico / elettronico può avere diversi modi di guasto; ad es.: corto circuito, interruzione, deriva.
    - ✓ Il software NON si guasta, ma può contenere errori.

SICUREZZA FUNZIONALE - 8

- IMPORTANTI CATEGORIE DI GUASTO:
  - ➢GUASTO PERICOLOSO (Dangerous failure): guasto che implica il fallimento della funzione di sicurezza.
  - ➢G. NON PERICOLOSO: guasto che determina una avaria nel sistema ma non fa fallire la missione di sicurezza.
  - ➢GUASTO DIAGNOSTICATO (Detected failure): guasto tale da essere rilevabile dalla diagnostica di sistema.
    - ✓ Un guasto può essere latente fino al test successivo.
  - ➢GUASTO NON DIAGNOSTICATO (Undetected failure): guasto non rilevabile dalla diagnostica di sistema.

SICUREZZA FUNZIONALE - 9

- RELAZIONE CON LA CASUALITA':
  - ➢GUASTO CASUALE (Random failure): guasto a distribuzione aleatoria non riconducibile a causa sistematica.
    - ✓ Dipende in genere da effetti delle sollecitazioni elettriche e termiche che possono colpire il componente casualmente ed in anticipato rispetto alla sua vita media.
  - ➢GUASTO SISTEMATICO (Systematic failure): guasto correlato in modo deterministico ad una data causa.
    - ✓ Dipende da errori di concezione, progetto (spesso dimensionamento), fabbricazione, procedura operativa…
    - ✓ Gli errori del software sono sempre guasti sistematici.

SICUREZZA FUNZIONALE - 10

- RELAZIONE CON LA CAUSALITA':
  - ➢ Ogni GUASTO deve essere inteso come l'insieme del primo guasto e di ogni altro guasto propagato, cioè susseguente al primo e scatenatosi come conseguenza.
    - ✓ Una siffatta sequenza di guasti è come un guasto singolo.
  - ➢ Affinché sia giustificata l'ipotesi di esclusione di un doppio guasto contemporaneo, prevista da alcune norme, deve potersi applicare il teorema della probabilità composta di eventi indipendenti, cioè si deve trattare di due guasti INDIPENDENTI nella STESSA funzione di sicurezza.

SICUREZZA FUNZIONALE - 11

Lo studio della sicurezza funzionale avviene applicando i concetti e i metodi della fidatezza ai sistemi che svolgono funzioni di sicurezza. In particolare, dalla definizione:

- SICUREZZA (Safety): Probabilità che un sistema rimanga continuativamente in condizioni tali che il rischio derivante dal suo impiego permanga al di sotto di un livello prefissato.

si evince che la sicurezza funzionale è quantificabile come **disponibilità dei sistemi di sicurezza**.

SICUREZZA FUNZIONALE - 12

- Nella sicurezza funzionale, si adottano quindi i termini relativi alla fidatezza focalizzandosi focalizzandosi sui guasti pericolosi e puntando a minimizzare, fra questi, quelli non diagnosticati.
- Assumendo che i sistemi siano riparabili e che MTTR << MTTF, il sistema è tanto più sicuro quanto più è basso il suo failure rate. Pertanto, tutte le norme moderne in materia legano il livello di sicurezza alla probabilità di guasto pericoloso, in genere espressa in termini orari (PFHd).

SICUREZZA FUNZIONALE - 13

- Per quanto detto, si definiscono tutte le funzioni affidabilistiche in termini di guasti pericolosi (MTTFd, PFHd, DC, …).
  - ➢Le norme attuali definiscono le prestazioni dei sistemi di sicurezza con varie scale (SIL, PL, AK), i cui gradi sono tutti riconducibili, in maniera più o meno diretta, ad un intervallo di valori di PFHd, in genere correlato con l'architettura circuitale, la DC e le misure di contrasto ai CCF.
- Tutti i concetti inerenti i calcoli probabilistici di fidatezza riguardano i soli **guasti aleatori**.

SICUREZZA FUNZIONALE - 14

- Relativamente ai **guasti sistematici**, inclusi i bachi del software, ci si focalizza su:
  - ➢Progettazione seguendo un diagramma di verifica e validazione, che prevede un'accurata stesura delle specifiche e dei protocolli di prova;
  - ➢Processo produttivo sotto controllo di qualità;
  - ➢Esecuzione approfondita dei protocolli di prova da parte di persone diverse dai progettisti, ricerca di un'estesa gamma di sollecitazioni ai percorsi logici del software, adeguatamente strutturato.

SICUREZZA FUNZIONALE - 15

- TIPI DI SISTEMI DI SICUREZZA:
  - ➢SISTEMI SICURI AL GUASTO (FAIL-SAFE SYSTEMS): sistemi in grado di svolgere la missione in caso di guasto, ma che non è detto rimangano in grado di farlo dopo l'evento, o almeno non col livello di sicurezza richiesto in condizioni normali.
  - ➢SISTEMI A TOLLERANZA DI GUASTO (FAULT-TOLERANT Systems): sistemi in grado di continuare a svolgere la missione anche in caso di guasto, mantenendo il livello di sicurezza richiesto in condizioni normali.

SICUREZZA FUNZIONALE - 16

- OSSERVAZIONE TERMINOLOGICA:
  - ➢Spesso, per i componenti o i dispositivi sicuri al guasto (fail-safe), viene utilizzata la locuzione «**a sicurezza intrinseca**», traduzione di «inherent safety» oppure di «intrinsic safety», ma è fuorviante e sbagliata:
    - ✓ **inherent safety** è un concetto di sicurezza degli impianti chimici, basato sulla limitazione dei pericoli, cioè sull'incrementare la sicurezza eliminando alcuni pericoli piuttosto che mantenendoli e dovendoli controllare.
    - ✓ **intrinsic safety** è un concetto di sicurezza negli ambienti esplosivi, basato sulla limitazione dell'energia disponibile per l'innesco e della temperatura.

SICUREZZA FUNZIONALE - 17

- RIDONDANZE PER SICUREZZA E PER CONTINUITA':
  - ➢Un sistema multicanale adeguatamente diagnosticato permette di conseguire anzitutto il livello di sicurezza richiesto (fail-safe system).
  - ➢L'adozione di ridondanze e di diagnostica superiori a quelle richieste ai soli fini della sicurezza permette di arrivare alla conservazione della piena sicurezza anche in caso di guasto (fault-tolerant fail-safe system)
    - ✓ Anche se i due approcci hanno obiettivi diversi e sembrano antitetici, un sistema fault-tolerant deve prima di tutto essere anche fail-safe.

SICUREZZA FUNZIONALE - 18

- Esempi:
  - ➢Impianti elettrici funiviari PTS a tre canali A, B, C: A+C o B+C sono sufficienti ai fini del pieno livello di sicurezza, quindi i canali A e B sono in ridondanza reciproca a soli fini di continuità (fault-tolerance).
  - ➢Impianti di segnalamento ferroviario a tripla ridondanza con votazione ad autorità 2oo3.
  - ➢Sistemi di calcolo per avionica (es. Space shuttle: cinque computer, ognuno dei quali esegue diagnostica sugli altri, con schema di votazione 3oo5).

SICUREZZA FUNZIONALE - 19

- STATO SICURO DEL SISTEMA PROTETTO: le funzioni di sicurezza devono essere distinte in base allo stato sicuro in cui può essere posto il sistema protetto, in caso di intervento della funzione:
  - ➢Sistemi protetti che ammettono uno stato totalmente deenergizzato come sicuro (es.: impianto a fune fermo);
  - ➢Sistemi protetti che NON ammettono uno stato totalmente deenergizzato come sicuro (es.: propulsione aerea, condizionamento critico, pompe di ricircolo per il raffreddamento del nocciolo di un reattore nucleare).

SICUREZZA FUNZIONALE - 20

- Nei sistemi protetti che ammettono uno stato totalmente deenergizzato come sicuro, un sistema di sicurezza fail-safe può essere sufficiente.
  - ✓ Si tratta di casi in cui la funzione di sicurezza si basa su sensori ed il suo intervento comanda istantaneamente gli attuatori che pongono l'impianto in sicurezza.
- In quelli che non lo ammettono, il raggiungimento della sicurezza deve comprendere la componente di fault-tolerance necessaria a mantenere la continuità di esercizio delle parti necessarie alla sicurezza.
  - ✓ Si tratta di casi in cui gli attuatori devono essere coinvolti continuativamente nel mantenimento della sicurezza.

PARTE 2

EVOLUZIONE NORMATIVA ITALIANA ED EUROPEA SUGLI IMPIANTI ELETTRICI FUNIVIARI

ing. Andrea Fornasa, EEI S.p.A.

ARGOMENTI

- **Evoluzione delle norme** per l'equipaggiamento elettrico delle funivie, dagli anni '80 ad oggi.
- Particolare riguardo alle norme per la "**Sicurezza funzionale**": le funzioni di sicurezza realizzate dal sistema di controllo della funivia.
- Come sono cambiati i "**principi di base**" delle norme per le "Macchine" e per le "Funivie".

MISURE DI SICUREZZA - 1

- Opportune "**misure di sicurezza**" devono ridurre i rischi per la salute delle persone a dei valori che le comunità considerano **oggi** tollerabili.
- L'entità dei "rischi tollerabili" viene stabilita dalle comunità mediante leggi e norme; cambia nel tempo, anche in base alla sensibilità sociale:
- *A parità di condizioni, l'incidente con una funivia è più sentito dell'incidente con un'automobile*.

MISURE DI SICUREZZA - 2

- Le “**misure di sicurezza**” sono le più varie:

- **Scelte progettuali** che prevengono alcuni rischi.

- **Misure tecniche**, per ridurre l’entità di certi rischi senza ricorrere alle azioni di persone.

- **Misure organizzative**: regole di organizzazione e comportamento, informazioni ed altro che guidano le azioni di persone per ridurre dei rischi.

- Esaminerò soprattutto le **misure tecniche**.

MISURE DI SICUREZZA - 3

- Una “misura di sicurezza” deve ridurre l’entità di un rischio dal valore “senza la misura” al valore “con la misura”.
- In qualche modo occorre determinare questi due **valori di entità del rischio**.
- Tanto maggiore è la differenza tra i due valori, tanto maggiore sarà il “**grado di sicurezza**” che la misura di sicurezza deve garantire.

MISURE DI SICUREZZA - 4

- Due esempi minimi:

1 – La misura “A” riduce l’entità di un certo rischio da “Lieve” a “Trascurabile”. Il grado di sicurezza richiesto può essere “**Basso**”.

2 – La misura “B” riduce l’entità di un altro rischio da “Grave” a “Trascurabile”. Il grado di sicurezza richiesto dovrà essere “**Alto**”.

LA PROCEDURA

- La procedura seguita dalle norme non è cambiata:

1 – **Individua i rischi** da ridurre e la loro entità.

2 – **Stabilisci le misure** per ridurre questi rischi.

3 – Stabilisci il loro “**grado di sicurezza richiesto**”.

4 – **Dimostra** di aver realizzato le misure richieste.

5 – **Dimostra** che essa hanno almeno il “grado di sicurezza richiesto”.

LE NORME ELETTRICHE - 1

- Le misure di sicurezza degli equipaggiamenti elettrici delle funivie coprono due aspetti:

  1 - **Sicurezza elettrica**, per ridurre i rischi dovuti all'impiego dell'energia elettrica**.**

  2 – **Sicurezza funiviaria**, per ridurre gli altri rischi, dovuti al funzionamento della funivia.

- Qui analizziamo soprattutto le misure tecniche per la Sicurezza funiviaria, di interesse più generale.

SICUREZZA ELETTRICA - 1

- **CEI 64-8**, **IEC 60364** - *Impianti elettrici degli edifici.*
- **CEI EN 61800-5-1** - *Azionamenti elettrici a velocità variabile - Parte 5-1: Prescrizioni di sicurezza - Sicurezza elettrica, termica ed energetica*.
- In linea generale, i rischi dovuti all'energia elettrica e la loro gravità sono noti, ad esempio:
  Elettrocuzione per contatto diretto ed indiretto
  Ustioni o incendi causati da sovratemperature
  Esplosioni o incendi causati da cortocircuiti.

SICUREZZA ELETTRICA - 2

1 – *Individua i rischi da ridurre e la loro entità*.

- Le norme individuano i rischi ed in pratica anche la loro entità, con poca libertà di interpretazione.

2 – *Stabilisci le misure per ridurre questi rischi*.

- Le norme stabiliscono le misure di sicurezza e ne prescrivono le caratteristiche e prestazioni.

SICUREZZA ELETTRICA - 3

3 – *Stabilisci il "grado di sicurezza richiesto"*.

- A questo scopo, le due norme introducono una regola che incontreremo spesso più avanti:

  "La protezione dai rischi termici e dalle scosse elettriche deve essere mantenuta in condizioni di ***guasto singolo****, oltre che in condizioni normali."*

SICUREZZA ELETTRICA - 4

4 – *Dimostra di aver realizzato le misure di sicurezza*.

5 – *Dimostra che essa hanno almeno il "grado di sicurezza richiesto"*.

- Il Costruttore deve poter dimostrare quanto richiesto mediante i documenti di progetto, accompagnati da calcoli e dai risultati delle prove richieste dalle norme.
- In definitiva, queste norme "elettriche" stabiliscono una procedura molto standardizzata.

PROGETTO NORME UNIFER-CEI

- Progetto di norme UNIFER-CEI per gli impianti elettrici delle funivie monofune (1984 … 1986)
- *Le presenti norme riguardano l'impianto elettrico (1) per **funivie monofune** (1.2.02) **ad attacchi fissi**, in servizio pubblico*, […]
- Mai formalmente emesse, ma utilizzate per comune accordo negli anni '80 e '90, anche per ammorsamenti automatici e funivie bifuni.

UNIFER-CEI - 2

- Classificazione dei circuiti elettrici: di potenza, comando, sicurezza, segnalazione e misura, telecomunicazione.
- Buona trattazione dei comandi di arresto, rallentamento, ripristino, parzializzazione ecc.
- Molta attenzione ai dispositivi di comando di arresto.

UNIFER-CEI - 3

- Buona trattazione degli attuatori della marcia:

- Freni di servizio elettrico e meccanico, freno di emergenza; coordinamento delle loro azioni.

- Azionamento principale (elettrico o termico) ed eventuale azionamento di riserva con motore termico, con batteria e caricabatteria dedicati.

UNIFER-CEI - 4

- Uno o più circuiti elettrici di sicurezza:

- I singoli **relè** di questi circuiti devono esplicare la funzione di sicurezza per **diseccitazione**.

- **Impedire l'avviamento** se non sussistono tutte le condizioni di sicurezza necessarie.

- **Arrestare l'impianto** per l'intervento di un comando manuale […] o automatico di arresto emesso da una delle **protezioni** previste.

UNIFER-CEI - 5

- **Circuiti di sicurezza esterni** (pulsanti di arresto):

a) elevata **affidabilità** di intervento, a ripristino.

b) criterio della **ridondanza** intesa come **duplicazione dei relè** o dispositivi stessi;

c) che i predetti relè siano muniti di **controllo automatico** oppure di **controllo ciclico** che riveli l'eventuale guasto di uno di essi;

- Concetti di *Affidabilità*, *Duplicazione*, *Test.*

UNIFER-CEI - 6

- **Protezioni**: dispositivi di comando automatico che intervengono per determinare l'arresto.
- **Classi delle protezioni** mediante le due frasi:

a) Di tale protezione non si richiede la duplicazione;

b) *Di tale protezione si richiede la* ***duplicazione*** *ed il* ***controllo automatico*** *oppure il* ***controllo ciclico***;

- Definite implicitamente "funzioni di protezione" e "funzioni di sicurezza" delle successive PTS-IE.

UNIFER-CEI - 7

- **Protezioni duplicate**:
  - Coppia massima, in avviamento ed a regime.
  - Relè finali del circuito di sicurezza di linea.
  - Velocità massima: meccanica + elettrica senza duplicazione.
- **Protezioni non duplicate**:

Usura ed apertura del freno di servizio, gradiente di coppia, confronto di velocità motore-argano, chiusura temporizzata del freno di servizio, ecc.

UNIFER-CEI - 8

- **Protezioni con circuiti elettronici:**

- *L'impiego di componenti elettronici nei circuiti con funzioni di sicurezza, è ammesso a condizione che sia garantita una* ***sicurezza non minore*** *di quella richiesta per i componenti elettrici*.

- [Le protezioni di coppia] *devono avere una caratteristica di taratura definita e consentire l'agevole* ***individuazione del valore di taratura*** *richiesto*.

UNIFER-CEI - 9

- **Alcuni limiti della norma:**

- Duplicazione delle batterie e caricabatterie: per l'avviamento del motore di riserva, ma non richiesta per le alimentazioni di sicurezza.
- Comando del freno di emergenza: non richieste duplicazioni (elettrovalvole, catene finali), né di evitare le urgenze contemporanee, né l'intervento per mancata decelerazione.
- Focus sui relè, quasi nulla sull'elettronica.

PRIMI AMMORSAMENTI

- Nei primi impianti ad ammorsamento automatico (Folgarida, Pinzolo, Etna) per anticollisione e prova morse si usavano **circuiti ad elettronica semplice**, un po' analogica ed un po' digitale.
- I risultati francamente erano **scarsi**, nonostante l'impegno e la fantasia inventiva dei progettisti:

  - Rampa di decelerazione con due o tre sezioni

  - Prova morse con sensori di forza On/Off

ELETTRONICA COMPLESSA

- L’elettronica complessa è entrata negli impianti funiviari nel corso degli anni ’80, spinta dalla sua evoluzione e dalla complessità dei nuovi impianti.
- **1982**: primo impiego di microprocessori per funzioni di sicurezza (Unità di Controllo).
- **1987-1989**: «balzo in avanti», conquista delle Unità di Elaborazione e delle Unità di Controllo.
- **1989-2004**: le norme funiviarie fissano le regole.

LOGICHE STATICHE - 1

- **Circolare D.G. n° 159/89** (ottobre 1989):

  Sistemi a logica statica programmabile

Inizia con classificazioni (con qualche incertezza):

- **Sensori** (interruttori di fine corsa e prossimità)
- **Unità funzionali** (controlli di corrente, velocità ..)
- **Unità di controllo**: comandi di marcia e arresto
- **Unità di visualizzazione** ed interazione.

LOGICHE STATICHE - 2

1. Ogni sistema di controllo delle funzioni legate all'attività di un impianto funicolare aereo o terrestre deve comprendere **due sottosistemi indipendenti a logica statica programmabile** (**canali A e B**), affiancati da un terzo sottosistema di tipo tradizionale **a logica cablata** (**canale C**).
2. I tre sottosistemi suddetti devono far capo ad un dispositivo […] destinato ad assolvere solo funzioni di segnalazione.

LOGICHE STATICHE - 3

- **Caratteristiche dei Sottosistemi a logica statica**:

- Completamente indipendenti e realizzati con dispositivi totalmente distinti,
- alimentati da due separate linee elettriche a 24 V c.c. provenienti da due distinte batterie di accumulatori,
- ciascuna provvista del proprio gruppo di ricarica in tampone.

LOGICHE STATICHE - 4

- **Caratteristiche dei Sottosistemi a logica statica**:

- Completamente separati dagli altri circuiti elettrici dell'impianto e galvanicamente isolati dal campo ,
- gli enti periferici (sensori ed unità funzionali), anche se duplicati devono inviare i propri segnali, in parallelo, ad ambedue i sottosistemi.

LOGICHE STATICHE - 5

- **Forte accento sulle funzioni di autodiagnosi**:

- Test periodici delle memorie EPROM.
- Ciclo di lavoro ripetuto entro 40 ms, test della durata con dispositivo Watch-Dog esterno.
- Relè finali di tipo “dinamico” (relè modulati).
- Test per verificare che i Sottosistemi comandino azioni coerenti, usando contatti dei relè finali.

LOGICHE STATICHE - 6

- **Forte accento sulle funzioni di test**:

- Test di attivazione: vitalità dei microprocessori, validità dei dati memorizzati su EPROM.
- Test dei segnali di ingresso, annullati e verificati all'inizio di ogni ciclo di lavoro.
- Test continuo delle memorie RAM.
- Test di avviamento: annullamento dei segnali ON/OFF e simulazione di misure (velocità, ecc.).

LOGICHE STATICHE - 7

- **Programma di Base e Programma Applicativo**:

- il primo programma, non modificabile, caratterizza le modalità di funzionamento del sottosistema;
- il secondo, variabile da impianto ad impianto, comprende le regole decisionali impiegate dal sottosistema.

LOGICHE STATICHE - 8

- Completa e dettagliata documentazione dei sottosistemi (hardware e software), esaminata e conservata dal Ministero.
- Anche senza fare riferimento ad altre norme sulla Sicurezza funzionale, le regole adottate hanno dimostrato negli anni la loro validità.

LOGICA CABLATA

- **Sottosistema a logica cablata (Canale C)**:

- *"deve comunque ricevere informazioni vitali ai fini della sicurezza del servizio"*.
- Deve riassumere i consensi di quasi tutti i "dispositivi di sicurezza".
- Qualche "toppa" per tener conto delle diverse soluzioni EEI – BMB, con lunghe discussioni.

FUNIVIE E MACCHINE

- I regolamenti e le norme tecniche delle "*Funivie*" e delle "*Macchine*" sono diversi.
- *Funivie* e *Macchine* hanno in comune molti rischi ed esigenze di sicurezza.
- Dagli anni '90, le disposizioni per le *Macchine* hanno avuto una evoluzione più rapida.
- Le disposizioni per le *Funivie* si stanno avvicinando a quelle delle *Macchine.*

VARIETA' DELLE MACCHINE

- Negli anni '90, leggi e norme hanno ampliato il campo da "Macchine industriali" a "Macchine" .
- *Oggi una "Macchina" va dal frullatore di casa al sezionale di cartiera, con più di 50 motori*.
- Le norme non possono più stabilire a priori tutti i rischi, le misure tecniche ed il grado di sicurezza.
- Leggi e norme cominciano ad affidare molte di queste attività ai Progettisti e Costruttori.

DIRETTIVA “MACCHINE”

- Direttiva **2006/42/CE** … relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione).
- D.Lgs. 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.
- **Guida all’applicazione della direttiva** “macchine” 2006/42/CE – 2° edizione (Commissione europea, Imprese ed Industria – giugno 2010).

DIRETTIVA “FUNIVIE”

- Direttiva **2000/9/CE** del Parlamento europeo e del Consiglio, del 20 marzo 2000, relativa agli impianti a fune adibiti al trasporto di persone.
- D. Lgs 12 giugno 2003, n. 210 "Attuazione della direttiva 2000/9/CE in materia di impianti a fune adibiti al trasporto di persone e relativo sistema sanzionatorio“.
- **Guida per l’applicazione della direttiva** 2000/9/CE … relativa agli impianti a fune adibiti al trasporto di persone (Commissione europea, Imprese ed Industria).

ANALISI DI SICUREZZA

- Direttiva Funivie, art. 4: il progetto deve essere sottoposto alla **Analisi di sicurezza** definita nell'allegato III.
- L'Analisi di sicurezza dà luogo alla **Relazione di sicurezza**, che specifica:
- - Misure previste per affrontare i rischi
- - Elenco dei componenti di sicurezza.

ATTORI COINVOLTI

- Guida alla direttiva: l'Analisi di sicurezza è dedicata ad un singolo impianto, coinvolge il Committente che la promuove ed i Costruttori.
- La relazione di sicurezza è intesa a far riconoscere e accettare, dal complesso dei partecipanti alla realizzazione dell'impianto, le disposizioni stabilite per far fronte ai rischi suscettibili di manifestarsi [requisiti essenziali, all. II punto 2.2]

VALUTAZIONE DEI RISCHI

- L’ Analisi di sicurezza della direttiva Funivie è la Valutazione dei rischi della direttiva Macchine.
- Per la Valutazione dei rischi, le future versioni di norme “EN Funivie” faranno riferimento alla norma “EN Macchine”, o meglio “EN generale”.
- Esempio: EN 12929-1, art. 4.3.2: richiamata per i dispositivi di protezione in zone di circolazione e lavoro che presentano dei rischi.

UNI EN ISO 12100 - 1

- Dal 30/11/2013, la sola norma utile per la Valutazione dei rischi e l'Analisi di sicurezza è:

  UNI EN ISO 12100: 2010-11 – Sicurezza del macchinario – Principi generali di progettazione – Valutazione del rischio e riduzione del rischio.

- E' stata eliminata una selva di vecchie norme:

  EN 292, EN 1050, EN 14121, EN 12100-1 e -2, etc.

UNI EN ISO 12100 - 2

- La norme EN 12100 è classificata di “tipo A”, cioè ha validità generale e guida la redazione di norme di “tipo B” e “tipo C” per gli impieghi specifici.
- “*This International Standard is also intended to be used as a basis for the preparation of type-B or type-C safety standards. It does not deal with risk and/or damage to domestic animals, property or the environment*.”

UNI EN 954-1 - 1

UNI EN 954-1: 1998 - Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Principi generali per la progettazione.

- La norma ha risposto a queste esigenze, relative alle misure tecniche per la riduzione dei rischi :

3 – Stabilisci il loro "**grado di sicurezza richiesto**".

5 – **Dimostra** che essa hanno almeno il "grado di sicurezza richiesto".

UNI EN 954-1 - 2

- **Dalla parte dell'Utilizzatore**:

L'Utilizzatore di un dispositivo deve specificare:

- quale funzione deve svolgere,

- il grado di sicurezza richiesto.

La EN 954-1 definisce il grado di sicurezza con 5 "**Categorie di sicurezza**": B, 1, 2, 3, 4

Il grafo dei rischi della EN 954-1 aiuta a determinare il grado di sicurezza richiesto.

UNI EN 954-1 - 3

S - gravità del danno

S1 lesione leggera (normalmente reversibile).
S2 lesione grave (normalmente irreversibile) o morte della persona.

F - frequenza / durata di esposizione al rischio

F1 da rara a abbastanza frequente e/o tempo di esposizione corto.

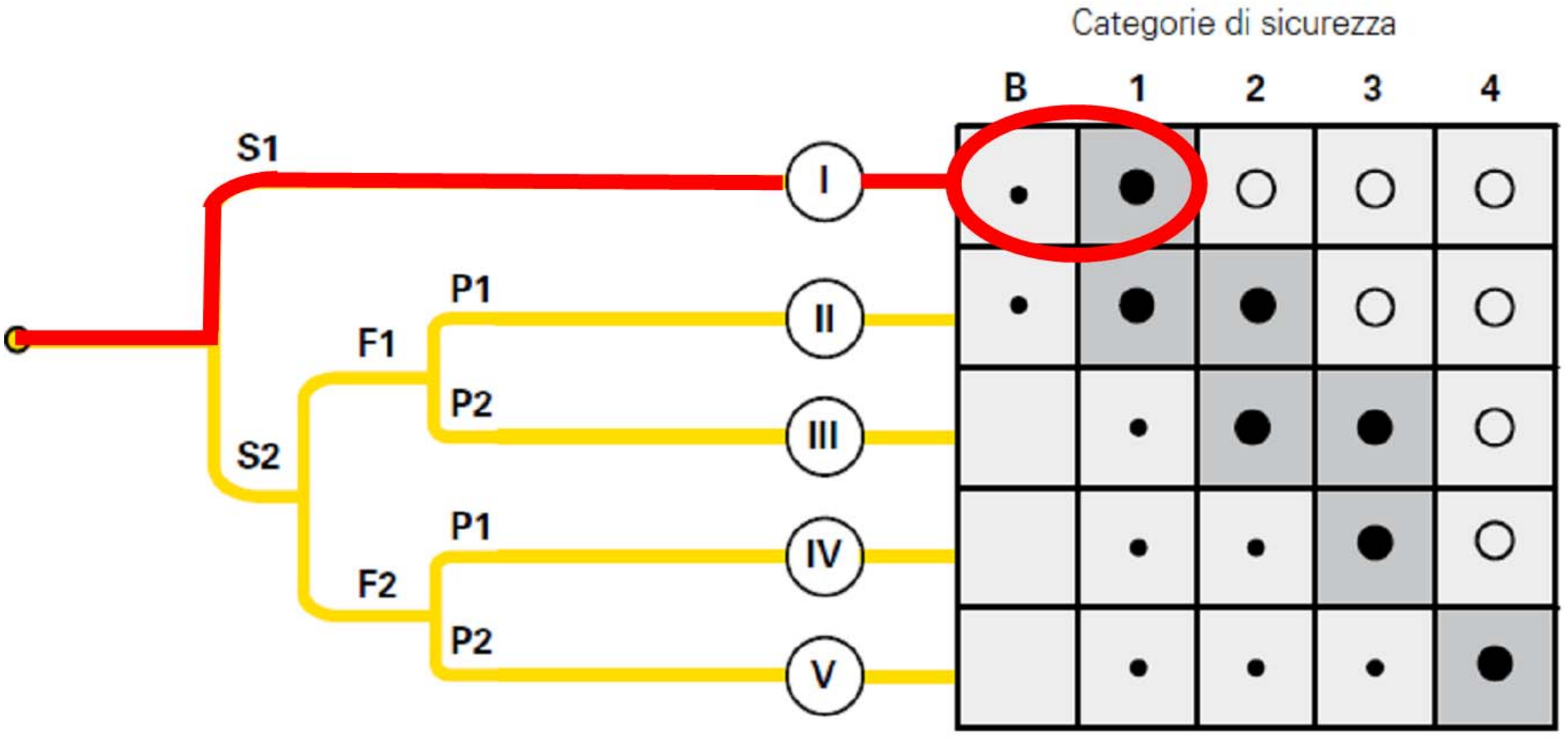
F2 da frequente a continua e/o tempo di esposizione lungo.

P - possibilità di evitare il pericolo

P1 possibile in particolari condizioni (fuga o intervento di terze persone).

P2 quasi impossibile (il fenomeno si manifesta rapidamente).

EN 954-1 – GRAFO RISCHI



UNI EN 954-1 - 5

- Presupposti: quando il dispositivo è stato provato, ha svolto regolarmente le sue funzioni; in seguito non è stato modificato, e non sono cambiate le condizioni di impiego al suo esterno.
- Conseguenza: se ha cessato di funzionare, deve aver subito dei guasti, anche in tempi diversi.
- Il più pericoloso è il guasto latente: oggi non influisce, ma domani potrebbe contribuire al fallimento del dispositivo.

UNI EN 954-1 - 6

- **Dalla parte del Costruttore del dispositivo:**

La EN 954-1 stabilisce per ogni Categoria:

1. Quanti guasti deve poter tollerare: la necessità di tollerare un guasto implica l'impiego di dispositivi duplicati.
2. Le prestazioni delle funzioni di autodiagnosi nello scoprire i guasti latenti: ciò determina la frequenza e capacità di scoperta dei test.

EN 13243 – FUNIVIE - 1

- La norma EN 13243 per le funivie usa un metodo molto simile alla EN 954-1.
- Qualifica il grado di sicurezza in 4 “**classi di requisiti**”, da **AK1** ad **AK4.**
- Questa analisi è sufficiente per i dispositivi semplici, di tipo A.
- Per i dispositivi con elettronica complessa (tipo B), fa anche riferimento alla norma **EN 61508**.

EN 13243 – FUNIVIE - 2

AK (Requirements class) prEN 13243	SIL[a] (Safety Integrity Level) EN 61508	Category[a] EN 954-1	Brief description
1	0	B	Control system according to the state of the art
2	1	1/2	Safety-proven components and principles / testing
3	2	3	Redundancy with partial fault recognition, in accordance with the state of the art
4	3	4	Self-monitoring
-	4	-	Not meaningful for machinery protection
[a] From BIA report «Categories of safety related commands according to EN 954-1», 6/97			

PTS-IE ITALIANE - 1

- Le PTS-IE sono state concepite dal ’92 al ’94, in parallelo alle norme europee EN del CEN.
- Solo “**risistemazione delle norme in vigore**”:

- integrare le UNIFER-CEI e la Circolare 159/89,
- inquadrare lo stato dell’arte delle realizzazioni.

- Non si conoscevano gli indirizzi della EN 61508, ancora nelle mani di esperti di altri settori.

PTS-IE ITALIANE - 2

- Una “**Norma**” ed un “**Libro di testo**”: formulare i principi di base, dare le prescrizioni, spiegarne i motivi e le modalità di applicazione.
- Imposizione di architetture abbastanza rigide, basate sulle realizzazioni EEI e BMB dell’epoca.
- Principi di **duplicazione e test**, come nella 954-1, con due sole categorie: **funzioni di protezione** e **funzioni di sicurezza**, con i relativi dispositivi.

PTS-IE ITALIANE - 3

- **Dispositivo di protezione**:

- Non è richiesta la duplicazione

- Test all'avviamento e test in bianco

EN 954-1 – **Categoria 2**: Un guasto può portare alla momentanea perdita della funzione di sicurezza.

Il guasto viene rilevato all'esecuzione del test prima dell'inizio del successivo ciclo di lavoro della macchina.

PTS-IE ITALIANE - 4

- **Dispositivo di sicurezza**:

- E’ richiesta la duplicazione

- Test all’avviamento, test in bianco, altri test

EN 954-1 – **Categoria 3**: Un singolo guasto non deve portare alla perdita della funzione di sicurezza.

Quando possibile il singolo guasto deve essere rilevato.

PTS-IE ITALIANE - 5

- **Guasto latente – § 1.3.7**:

Ogni guasto che compaia dopo l'ultimo test o prova, e che non si renda immediatamente manifesto attraverso un comando d'arresto o una segnalazione d'allarme.

- **Prescrizione**: i test devono eliminare tutti i guasti latenti che potrebbero portare a guasti pericolosi.
- **Rischio accettato:** due guasti latenti nell'ambito di uno stesso dispositivo di sicurezza.

PTS-IE ITALIANE - 6

Conviene iniziare la lettura da questi capitoli:

- **Nota del gruppo di lavoro - Principi ispiratori**, alla fine del documento. Introduce e giustifica i postulati ed i principi adottati.
- **2.1.1**: Livello di sicurezza in relazione alle condizioni di esercizio.
- **2.1.38**: Parzializzazioni ed esclusioni.
- **2.1.39**: Misure organizzative per condizioni di esercizio limitate.

PTS-IE ITALIANE - 7

Fig. 1 - OPERAZIONI FONDAMENTALI DEL SISTEMA DI SORVEGLIANZA

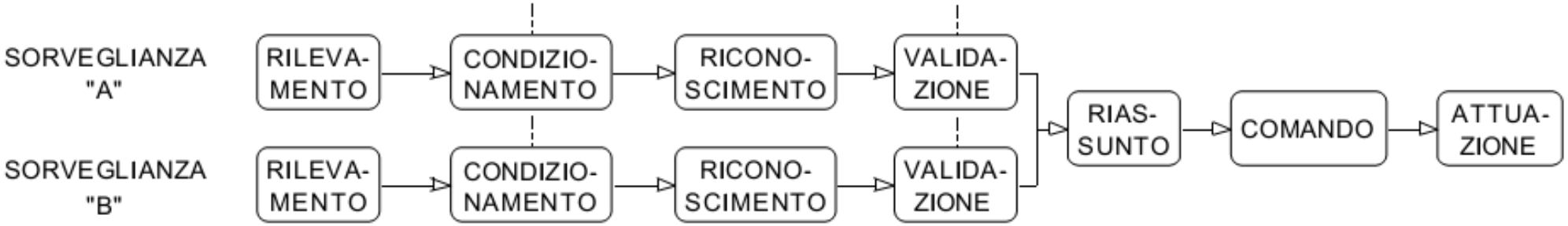
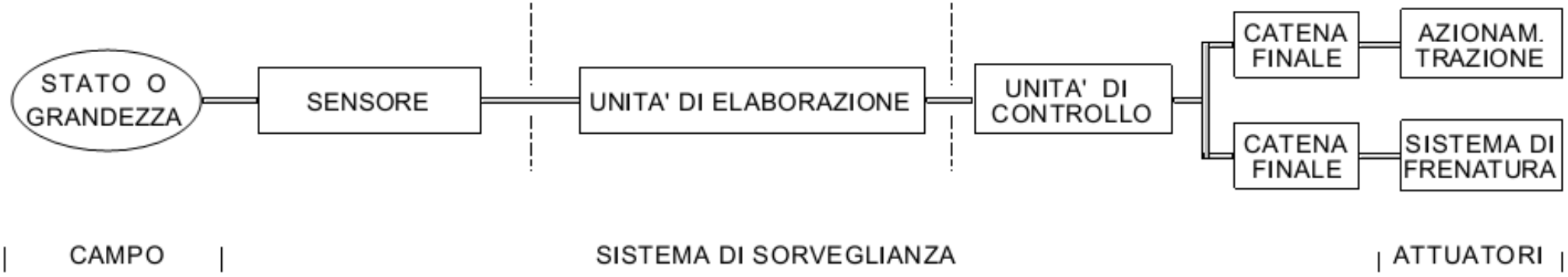


Fig. 2 - ELEMENTI DEL SISTEMA DI SORVEGLIANZA



PTS-IE ITALIANE - 8

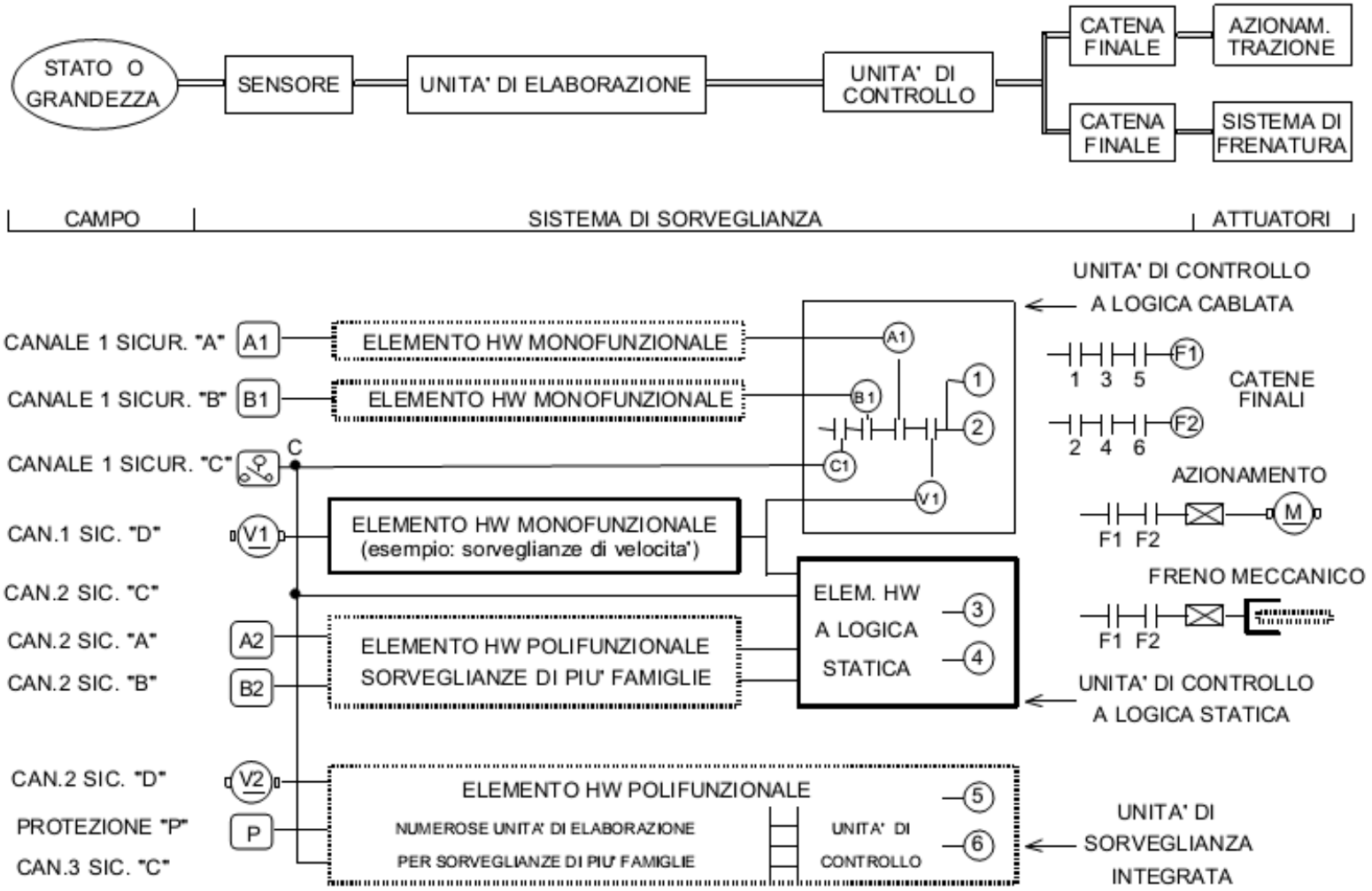
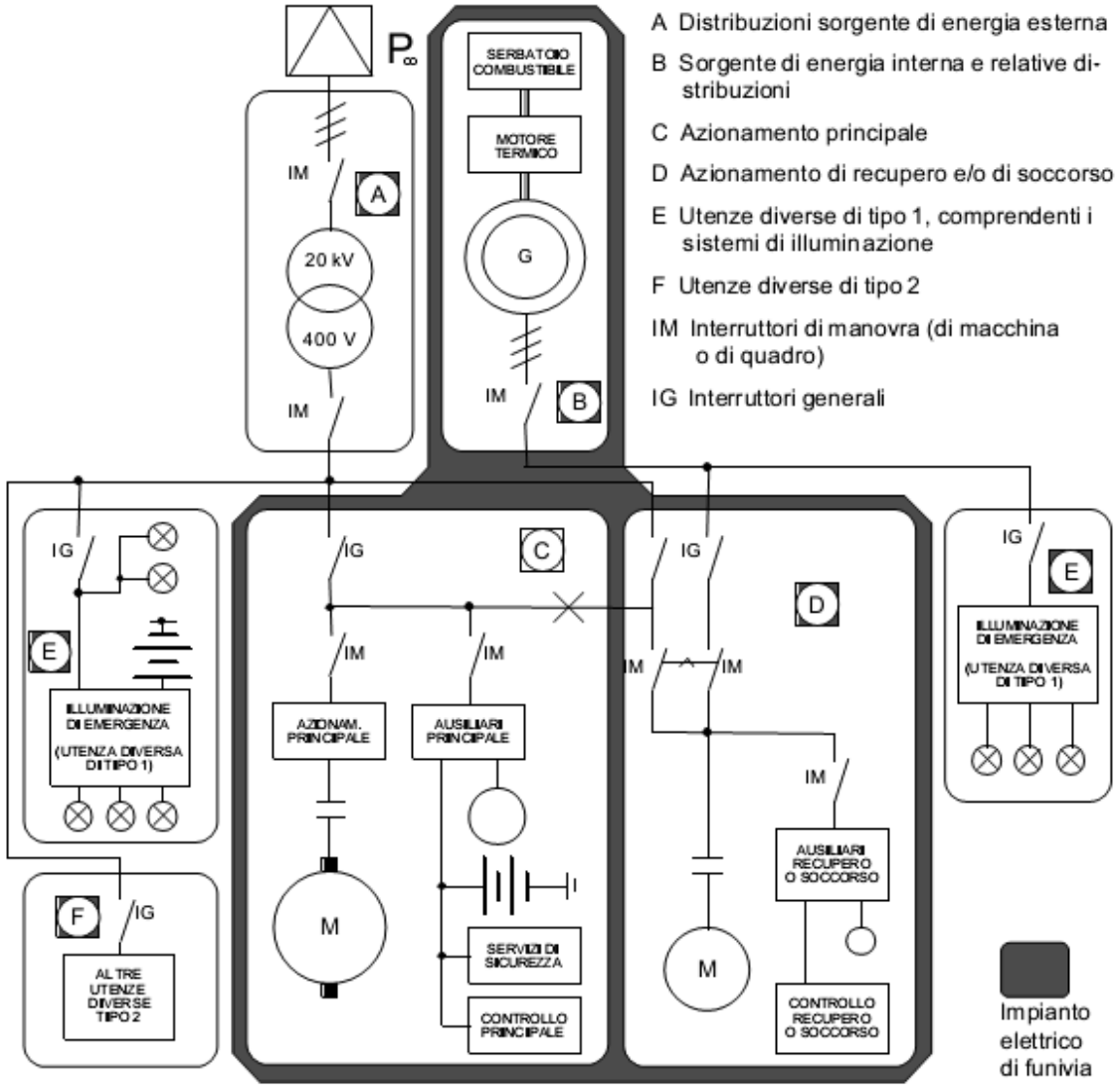


Fig. 5 - SISTEMA CON DUE UNITA' DI CONTROLLO A LOGICA STATICA ED UNA A LOGICA CABLATA

PTS-IE ITALIANE - 9



NORME EN FUNIVIE

- Le norme armonizzate di “Sicurezza Funiviaria” per gli impianti elettrici delle funivie sono:

  UNI EN 13223: 2007 (2004) Requisiti di sicurezza per gli impianti a fune progettati per il trasporto di persone - Argani ed altri dispositivi meccanici.

  UNI EN 13243: 2007 (2004) Requisiti di sicurezza per gli impianti a fune progettati per il trasporto di persone - Apparecchiature elettriche ad esclusione di quelle per gli argani. [*NdR: la più importante, in fase di aggiornamento*]

AGGIORNAMENTI

- La nuova versione della **EN 13243** farà riferimento a due norme più aggiornate rispetto alla EN 954-1:

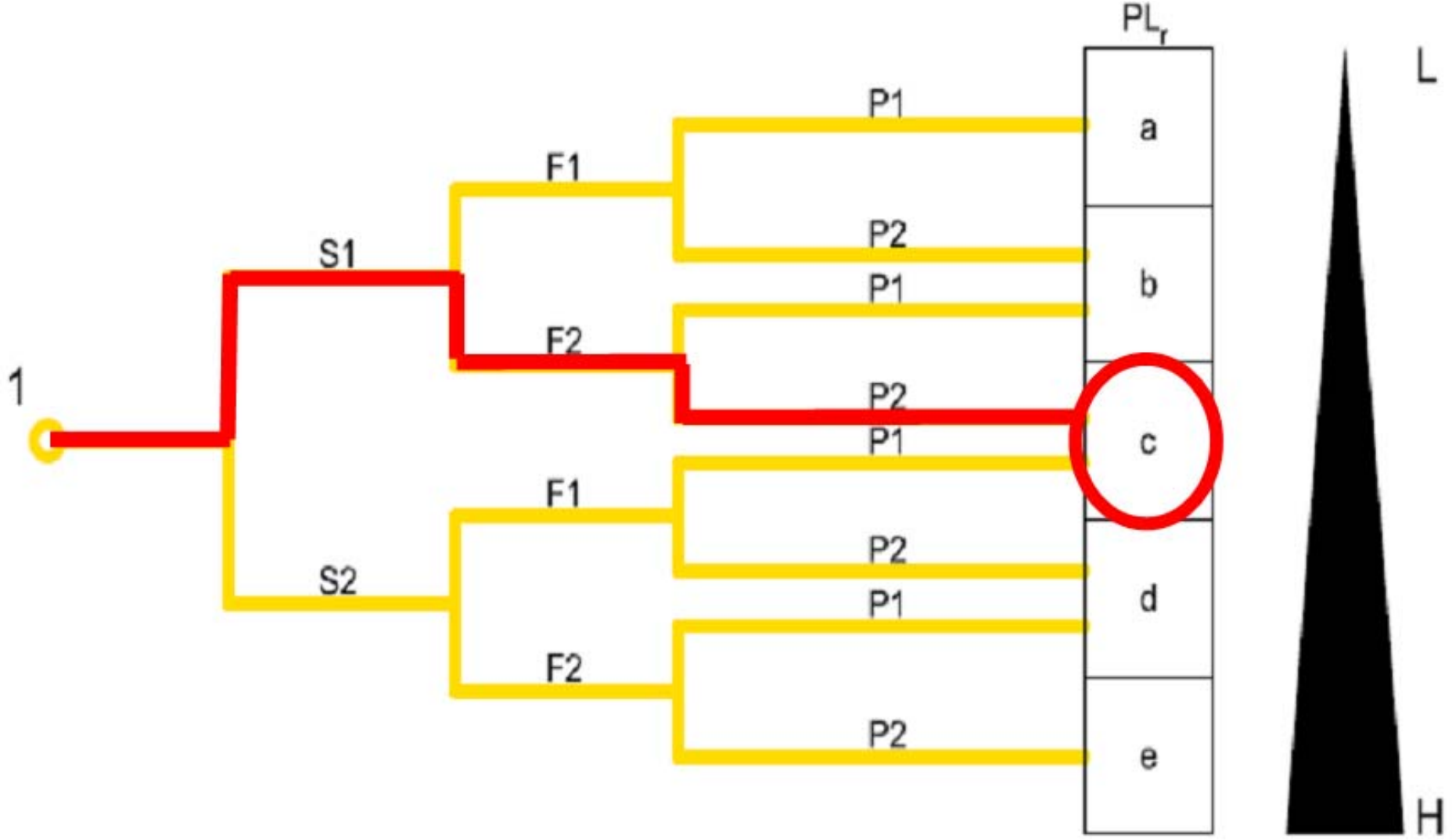
  UNI EN 13849 (-1 -2): Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione (Parte 2: Validazione).

  CEI EN 61508 (-1…-7): Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza.

EN 13849 - 1

- La EN 13849 è una versione aggiornata della EN 954-1, è adatta a dispositivi di controllo “semplici” come circuiti a relè o elettronici semplici.
- Utilizza una “tabella di valutazione del rischio” per determinare il “Performance Level” necessario per la riduzione del rischio.
- Il Performance Level (PL) va dal minimo “**a**” fino al massimo “**e**”.

EN 13849 – GRAFO RISCHI



ESEMPIO DI GRAFO

Inizio stima	→	Gravità del danno possibile a persone	→	Grado di esposizione all'evento pericoloso	→	Possibilità di evitare o ridurre il danno temuto	→	PL= Livello di Prestazione
----→	→	**S1** = <u>Lesione reversibile</u> (ad es. scottatura, contusione, ferita guaribile)	→	**F1** = la persona è esposta di tanto in tanto e per un tempo breve	→	**P1**=L'evento è lento, si può evitare il danno	→	**a**
					→	**P2= L'evento è rapido, non si può evitare**	→	**b**
			→	**F2 = la persona è esposta di frequente o per un tempo lungo**	→	**P1**=L'evento è lento, si può evitare il danno	→	**b**
					→	**P2= L'evento è rapido, non si può evitare**	→	**c**
	→	**S2** = <u>**Lesione irreversibile**</u> (ad es. perdita di dita, ferita con danni permanenti)	→	**F1** = la persona è esposta di tanto in tanto e per un tempo breve	→	**P1**=L'evento è lento, si può evitare il danno	→	**c**
					→	**P2= L'evento è rapido, non si può evitare**	→	**d**
			→	**F2 = la persona è esposta di frequente o per un tempo lungo**	→	**P1**=L'evento è lento, si può evitare il danno	→	**d**
					→	**P2= L'evento è rapido, non si può evitare**	→	**e**

ESEMPIO DI USO

- L'operatore entra di tanto in tanto in una zona dove può essere colpito da uno **schizzo di liquido caldo**.
- Lo schizzo può provocare una scottatura guaribile (Gravità **S1**), l'operatore entra nella zona qualche volta al giorno e ci resta pochi minuti (Esposizione **F1**), ma non è in grado di evitare uno schizzo eventuale (Possibilità **P2**).
- Un dispositivo impiegato per ridurre il rischio legato a questo evento deve avere Livello di Prestazione "**b**".

DIFFERENZE DEL GRAFO

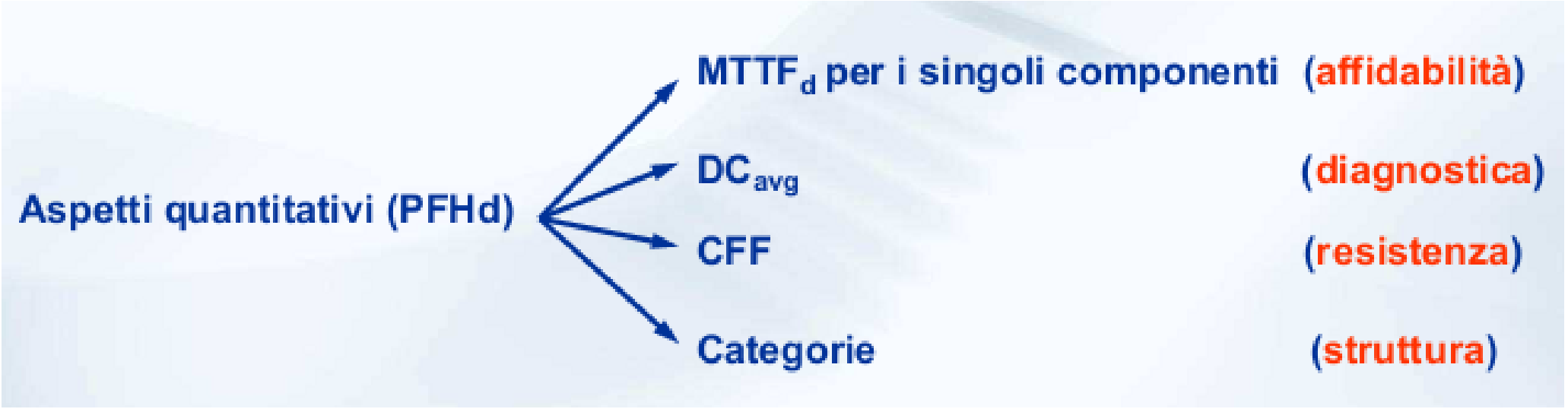
- **Alcune differenze rispetto alla EN 954-1**:

- Un rischio di infortunio leggero (danno non permanente) non porta più necessariamente ad un basso livello di sicurezza (categoria B o 1).

- Se l'esposizione è frequente e difficilmente evitabile, viene considerato pari ad un rischio di infortunio serio assai infrequente ed evitabile.

COSA CAMBIA

- **Per l'Utilizzatore non cambia molto**, perché deve solo stabilire il Performance Level richiesto (PLr).
- **Per il Costruttore, cambia molto**: oltre ad aspetti qualitativi deve determinare dei <u>valori numerici</u>.



MTTF, DC, CFF

MTTFd = Stabilisce la durata media di funzionamento, espressa in anni, di un singolo canale del sistema di controllo di sicurezza prima che capiti un guasto casuale potenzialmente pericoloso (e non un guasto generico).

DC = copertura diagnostica *(indica quanto il sistema sia efficiente nel rilevare un proprio eventuale malfunzionamento per tempo).*

Rappresenta il rapporto fra il tasso di guasti pericolosi rilevati λdd *(dd = dangerous detected)*, e il tasso di tutti i guasti pericolosi possibili λd (*d=dangerous*) rilevati e non rilevati.

CCF = Guasti dovuti a cause comuni *(grado di indipendenza di funzionamento dei canali di un sistema ridondante)*

EVOLUZIONE

- Nel 1980 gli esperti di sicurezza funzionale studiavano due mondi completamente separati:
- **Macchine Industriali**, ed impianti analoghi
- **Nucleare e Petrolchimico**: sistemi di controllo molto più complessi, rischio di catastrofi.
- Per molti anni i due gruppi normatori hanno seguito vie diverse, con poche interazioni.

EN 954-1

- La EN 954-1 negli anni ’80 era la norma di base «Sicurezza funzionale» per le Macchine industriali.
- Sistemi di controllo con circuiti elettromeccanici (pulsanti, relè, microinterruttori) e circuiti elettronici «semplici», spesso progettati ad hoc.
- PLC e microprocessori erano «**ospiti poco graditi**» nei circuiti per la sicurezza funzionale.

PRINCIPI DI BASE

- Principi di sicurezza da buon senso ed esperienza:

- Usa componenti affidabili.

- Fa in modo che un guasto non metta fuori uso una funzione relativa alla sicurezza.

- Fa in modo che un guasto non rimanga nascosto.

- Per applicare questi principi non era necessario misurare, calcolare o stimare valori numerici.

REGOLE APPLICATIVE

- Le regole per l'applicazione di questi principi erano basate su **assunti o soluzioni condivise**:

- Un circuito elettromeccanico è più affidabile di un circuito elettronico, peggio se programmabile.

- Usa due dispositivi indipendenti, ed evita i guasti di modo comune che possono bloccare entrambi.

- Verifica il loro funzionamento con controlli di parità, funzioni di autodiagnosi e test periodici.

REGOLE APPLICATIVE

- Sono sani e solidi principi, validi ancora oggi.
- Le norme funiviarie hanno seguito questa strada fino a dieci anni fa: UNIFER-CEI, PTS-IE in Italia; norme funiviarie di altri Paesi.
- La **direttiva** accoglie questi principi in Allegato III, **Analisi di sicurezza**; i dispositivi di sicurezza:

  - siano in grado di reagire ad un primo guasto

  - siano ridondati e sorvegliati, *oppure siano* ….

LE STRADE CONVERGONO

- *oppure siano tali che le **probabilità di cedimento** possano essere **valutate**.*

- Questa frase mostra l'avvicinamento alla strada normativa del Nucleare e Petrolchimico.
- Quando gli impianti ed i processi superano una certa complessità, i circuiti semplici non bastano: diventa necessario ricorrere all'elettronica digitale con i suoi programmi firmware e software.

NORMA EN 61508

EN 61508 (-1…-7): 2011 - Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza.

- Questa Norma tratta quegli aspetti di carattere generale da considerare quando sistemi eletttrici/elettronici/ elettronici programmabili (E/E/EP) sono impiegati per svolgere funzioni di sicurezza. Uno degli obiettivi principali di questa norma è di facilitare lo sviluppo di norme internazionali di prodotto e di applicazione settoriale da parte dei comitati tecnici.

COSA CAMBIA

- ***Per le Macchine, dalla 61508 è stata ricavata:***

  CEI EN 62061 *- Sicurezza del macchinario - Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza* (+ Errata Corrige ed Amendment A1).

  CEI CLC/TR 62061-1 *-Guida all'applicazione delle Norme ISO 13849-1 ed IEC 62061 nella progettazione di sistemi di controllo relativi alla sicurezza per macchinari.*

  ANIE-Assoautomazione *– Le nuove norme armonizzate EN ISO 13849-1 e EN 62061 [NdR: consiglio la lettura]*

COSA CAMBIA

- **Per l'Utilizzatore, non cambia molto**: al posto del valore PLr, ora dovrà assegnare il valore **SIL**:

Consequences	Severity (Se)	Class (Cl)					Frequency and duration (Fr)		Probability of hazardous event (Pr)		Avoidance (Av)	
		3–4	5–7	8–10	11–13	14–15						
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 hour	5	Very high	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 hour – ≤ 1 day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	> 1 day – ≤ 2 weeks	4	Possible	3	Im-possible	5
Reversible, first aid	1				OM	SIL 1	> 2 weeks – ≤ 1 year	3	Rarely	2	Possible	3
							> 1 year	2	Negligible	1	Likely	1

Classe Cl = Fr + Pr + Av

OM = Raccomandato l'uso di altre misure

COSA CAMBIA

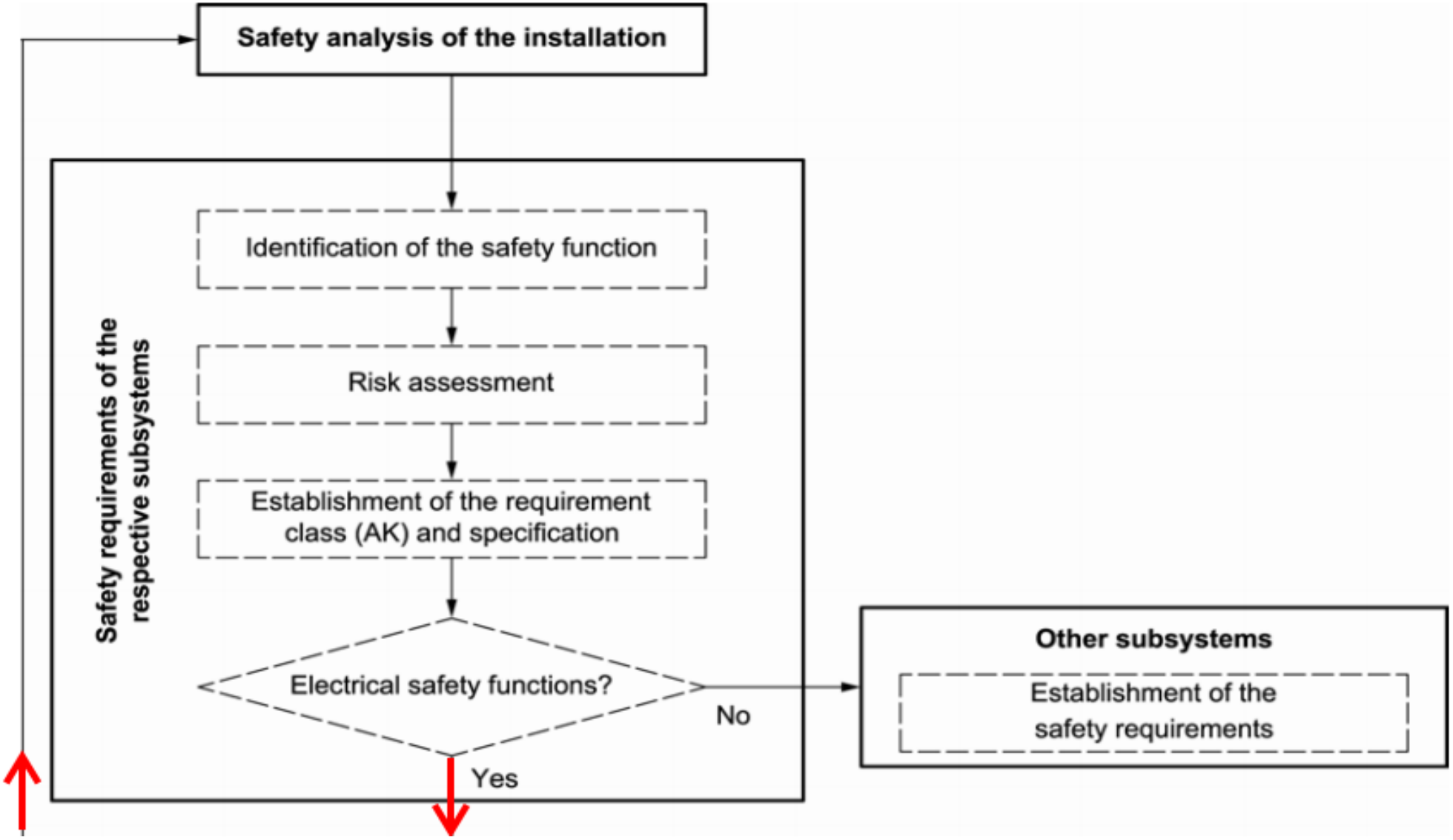
- **Per il Costruttore cambia molto**: deve calcolare la Probabilità che avvenga un guasto pericoloso in un'ora (**PHFd**); in base ad essa dichiara il SIL.

Safety integrity level	Probability of a dangerous failure per hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

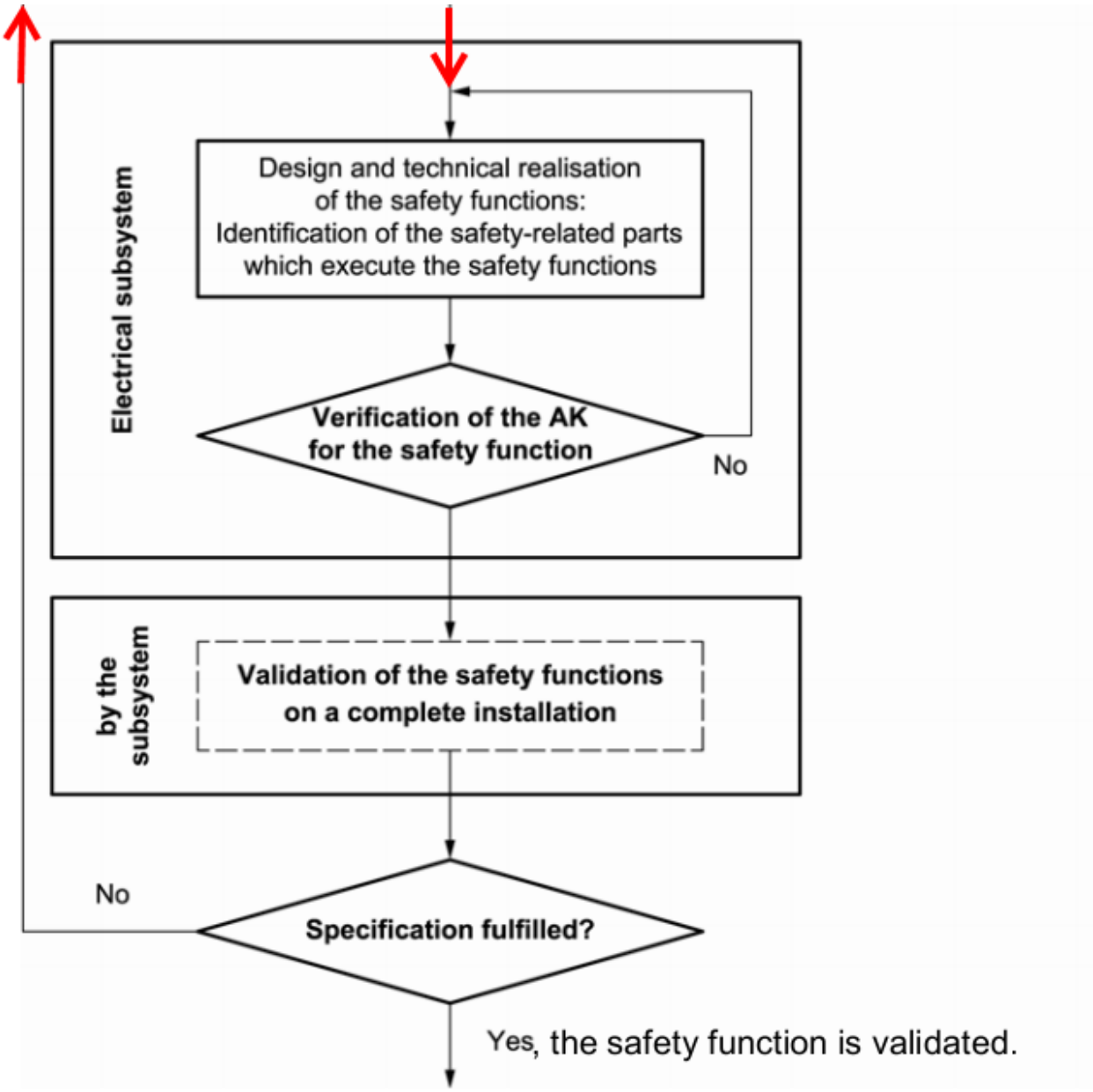
LA FUTURA EN 13243

- La norma EN 13243 è in corso di revisione, e dovrebbe recepire molti dei nuovi indirizzi:
- - Analisi dei rischi
- - Sistemi di controllo ad elettronica complessa
- - Armonizzazione delle classi AK con PL e SIL

PER L'UTILIZZATORE



PER IL COSTRUTTORE

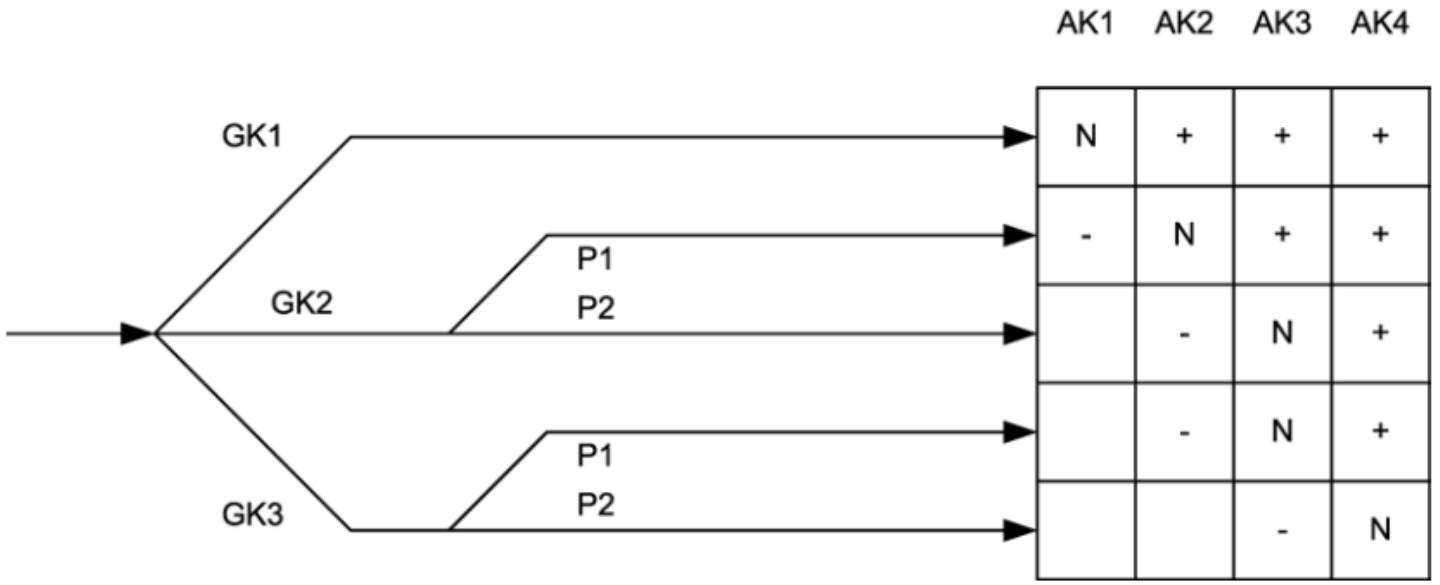


NUOVE TABELLE

Level of fault detection (FG)	
Designation	Area
None	FG < 60 %
Low	60 % ≤ FG < 90 %
Medium	90 % ≤ FG < 99 %
High	99 % ≤ FG
NOTE In the case of electrical safety devices which are made up of several parts, a mean value of the FG shall be used. For examples, in accordance with Annex D.	

$MTTF_d$	
Designation for each channel	Area for each channel
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years
NOTE The restriction of the $MTTF_d$ value of each channel up to a maximum of 100 years refers to the individual channel which executes the safety function.	

IL GRAFO DELLE CLASSI AK



Parameter GK (hazard category):

GK1 = no personal hazard

GK2 = slight (usually reversible) injuries to persons

GK3 = serious (usually irreversible) injuries, death of persons

Parameter P (possibility of avoiding the hazard):

P1 = possible under specific conditions (P1 only applicable in exceptional cases)

P2 = scarcely possible

CORRISPONDENZA AK-PL-SIL

PL → Performance level EN ISO 13849-1	AK Requirement class EN 13243	← SIL Safety integrity level EN 61508	Brief description of the requirement classes in accordance with EN 13243
a/b	1	- /1	control systems according to the state of the art
c/d	2	1	safety-proven components and principles/testing
d[1]	3	2	redundancy with partial fault recognition, in accordance with the state of the art
e	4	3	self-monitoring
NOTE Single-channel components (Cat. 2 in accordance with EN ISO 13849-1) of type B in accordance with 4.2.3.1 may not be used alone for safety functions greater than AK2.			

PROGETTO E VALIDAZIONE

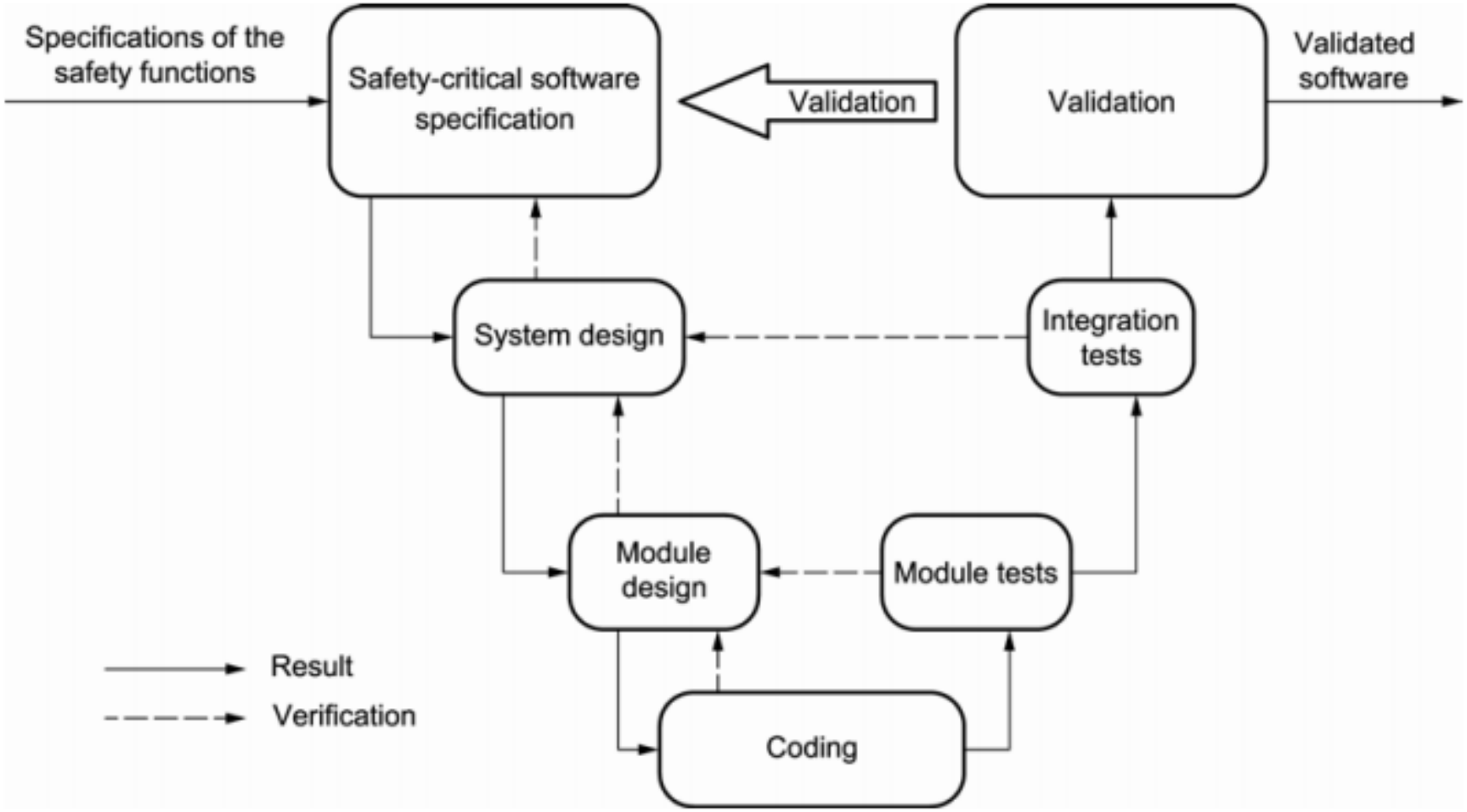
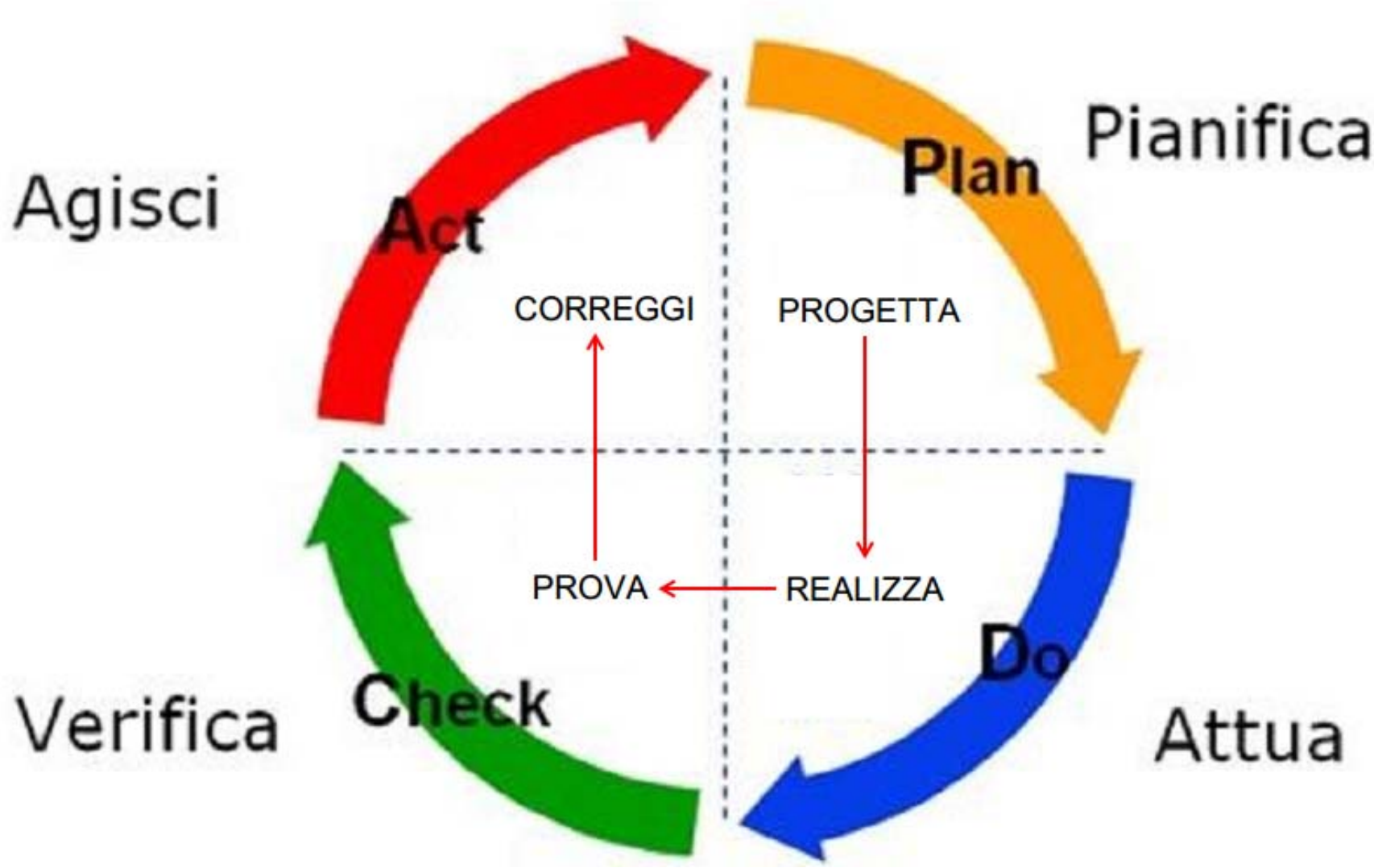


Figure 3 – Simplified V-model of the software life cycle

CICLO DI DEMING



PARTE 3

LA REGOLAMENTAZIONE EUROPEA ATTUALE - DIRETTIVA E NORME

ing. Gabriele Cappello, NIDEC ASI S.p.A.

DIRETTIVA EUROPEA - 1

- DIRETTIVA 2000/9/CE - PUNTI PRINCIPALI
  - Definisce i **COMPONENTI DI SICUREZZA** come quei componenti il cui guasto comporta un rischio per la sicurezza delle persone.
  - Definisce i **SOTTOSISTEMI**, elencandoli in All. I (ad es.: Sottosistema 5: Dispositivi elettrotecnici).
  - Individua l'**INFRASTRUTTURA**, in pratica come tutto quanto non rientra nei sottosistemi (opere civili, ecc.).
  - Impone che i progetti di impianto siano sottoposti ad un'**ANALISI DI SICUREZZA** da cui risulti una relazione sulle misure previste per mitigare i rischi, contenente l'elenco dei componenti di sicurezza e dei sottosistemi interessati.

DIRETTIVA EUROPEA - 2

- Impone che componenti, sottosistemi ed infrastrut-tura rispondano ai Requisiti Essenziali di Sicurezza (RES) applicabili, indicati in All. II.
- Ispira i RES a principi di sicurezza conformi a quelli dettati dalle norme sulla sicurezza funzionale.
- Impone la valutazione di conformità dei componenti (All. V) e dei sottosistemi (All. VII) mediante azione di parte terza, cioè certificazione da parte di un Organismo notificato accreditato per la direttiva.

DIRETTIVA EUROPEA - 3

- La Direttiva, in quanto tale,:
  - ➢costituisce un provvedimento comunitario a carattere generale; la sua adozione è obbligatoria, ma necessita di un atto di recepimento da parte dello Stato membro (D.Lgs. 12/06/2003, n. 210, per l'Italia);
  - ➢è «sostenuta» da un corpus normativo emesso dal CEN di standard europei che sono **norme armonizzate**, e quindi offrono presunzione di conformità ai RES della direttiva quando siano rispettate.
  - ➢ è in corso di revisione e diventerà un Regolamento, cioè un atto di legge europeo che non richiederà provvedimenti di adozione.

CERTIFICAZIONE - 1

- Aspetti generali della certificazione:
  - ➢L'organismo notificato svolge l'attività di valutazione esaminando la concezione dell'impianto in tutti i punti salienti del diagramma di verifica e validazione (specifiche di progetto, realizzazione HW e SW, test di modulo e di integrazione, prove in campo).
  - ➢L'organismo notificato approva i documenti sottoposti, determinando l'esistenza di due «pacchetti di documentazione», uno privato e l'altro pubblico, che delimitano i confini del sistema che viene certificato.

CERTIFICAZIONE - 2

- Aspetti essenziali della documentazione:
  - ➢Quella «privata» rimane riservata (specifiche, ecc.);
  - ➢Quella «pubblica» è riferita allo specifico impianto, ed è consegnata al committente e/o all'autorità tecnica competente nello Stato membro; comprende (ad es.):
    - ✓ Certificati di conformità, Condizioni d'uso dei componenti di sicurezza, Elenco della documentazione tecnica di sottosistema, Manuale di uso e manutenzione;
    - ✓ Matrice delle funzioni di sicurezza richieste e dei relativi AK, Elenco dei sensori ed attuatori, Schemi elettrici, Procedura di test, elenco parametri e checksum.

CERTIFICAZIONE - 3

- Aspetti particolari della certificazione:
  - ➢Il sistema che viene certificato è «rigido», nel senso che tutto quanto riguarda la sicurezza viene vincolato e dunque non è modificabile da impianto a impianto.
  - ➢Per certificare in «modulo H» (cioè in garanzia di qualità totale e non su esemplare unico), è necessario prevedere a priori tutte le varianti opzionali o le combinazioni lecite di elementi certificati.
    - ✓ Ciò porta allo sviluppo di schemi elettrici generalizzati con circuiti safety-related vincolanti, e ad uno spettro di combinazioni di software identificato da check-sum determinate in sede certificativa, pure vincolanti.

CERTIFICAZIONE - 4

- Diversificazioni fra vari Organismi notificati:
  - ➢Si osserva una significativa differenza di approccio nella certificazione del sottosistema 5 da un O.N. all'altro; ad es., c'è chi considera l'apparecchiatura elettrica come un unico componente di sicurezza, e chi preferisce ripartirla in più componenti, in funzione dell'applicazione (ad es. freni, tenditrice, argano, ecc.).
  - ➢Si osserva anche una rilevante differenza nei metodi e nelle esigenze da parte di diversi O.N., ad es. in tema di documenti richiesti, entità dei test in campo, ecc..
    - ✓ Si ritiene che questa mancanza di uniformità costituisca un significativo punto debole del sistema di certificazione.

NORME EUROPEE - 1

- Le principali norme CEN inerenti gli impianti elettrici funiviari sono:
  - ➢EN 13243 : 2004 (Concerne tutte le parti dell'impianto elettrico funiviario ad esclusione degli azionamenti);
  - ➢EN 13223 : 2004 (Concerne tutte le parti dei sistemi di azionamento, incluse le componenti meccaniche).
    - ✓ A differenza delle P.T.S.-I.E.F.A.T. italiane, che sono estremamente dettagliate, le norme CEN forniscono prevalentemente imposizioni di carattere generale.
    - ✓ Entrambe sono state revisionate ed è attesa l'emissione delle edizioni 2015.

NORME EUROPEE - 2

- PRINCIPI DI SICUREZZA DELLA NORMA EN 13243:
  - ➢Sono definiti gli scenari pericolosi di natura elettrica.
    - ✓ Ad es.: corto circuito attivo, guasto a terra, interruzione, caduta di tensione, condizioni ambientali come EMI, ecc..
  - ➢Sono definite tre categorie di pericolo in funzione del danno alle persone per fallimento della missione:
    - ✓ 1 - nessun danno alle persone,
    - ✓ 2 - lesioni reversibili,
    - ✓ 3 - lesioni irreversibili o morte.

NORME EUROPEE - 3

- E’ introdotta una distinzione affidabilistica, di tipo qualitativo, fra i componenti elettrici:
  - ✓ A – Componenti aventi comportamento al guasto e in avaria ben noti, nonché tassi di guasto conosciuti;
  - ✓ B – Componenti di tipo non-A (sostanzialmente: i sistemi elettronici programmabili e il relativo software).
- Sono definite quattro Classi di requisiti per la determinazione del livello di sicurezza richiesto ed ottenuto dalle funzioni (dette da tutti «AK» dal tedesco Anforderungsklasse), essenzialmente riconducibili alle caratteristiche principali seguenti.

NORME EUROPEE - 4

- CLASSE DI REQUISITI 1 (AK 1):
  - ➢CIRCUITI ALLO STATO DELL'ARTE.

  - ➢AK 1 ↔ sufficienza di canale singolo senza test.
    - ✓ Un guasto può condurre alla perdita della funzione;
    - ✓ un guasto può non essere rilevato prima della prima chiamata della funzione di sicurezza perduta;
    - ✓ più guasti latenti possono accumularsi prima che uno di essi venga rilevato.

NORME EUROPEE - 5

- CLASSE DI REQUISITI 2 (AK 2): come AK 1 e inoltre:
  - ➢CIRCUITI BASATI SU PRINCIPI DI SICUREZZA CONSOLIDATI, COMPONENTI DI COMPROVATA AFFIDABILITÀ, GUASTI RILEVATI MEDIANTE TEST PERIODICI, AUTOMATICI O MANUALI.
  - ➢AK 2 ↔ sufficienza di canale singolo con test.
    - ✓ Un guasto può condurre alla perdita della funzione;
    - ✓ un guasto viene rilevato dal test ma può non essere rilevato prima della prima chiamata della funzione di sicurezza perduta;
    - ✓ un cumulo di guasti latenti è possibile ma poco probabile.

NORME EUROPEE - 6

- CLASSE DI REQUISITI 3 (AK 3): come AK 2 e inoltre:
  - ➢AL PRIMO GUASTO LA FUNZIONE DI SICUREZZA SI CONSERVA E IL GUASTO È RILEVATO AL PRIMO TEST.
  - ➢AK 3 ↔ doppio canale con test «frequente».
    - ✓ il primo guasto non è pericoloso;
    - ✓ il primo guasto può non essere rilevato alla chiamata della funzione;
    - ✓ un secondo guasto prima del successivo test può condurre alla perdita della funzione;
    - ✓ il test non passa finché è presente qualche guasto.

NORME EUROPEE - 7

- CLASSE DI REQUISITI 4 (AK 4): come AK 3 e inoltre:
  - ➢Possibilmente il primo guasto o pone l'impianto in sicurezza oppure è rilevato non oltre la prima chiamata della funzione di sicurezza;
  - ➢altrimenti, o al secondo guasto la funzione si conserva, oppure un secondo guasto può essere escluso per l'alta probabilità di rilevare il primo entro poco tempo.

  - ➢AK 4 ↔ doppio canale con test continuo.
    - ✓ il primo guasto non è pericoloso;
    - ✓ il secondo guasto è escluso oppure non è pericoloso.

NORME EUROPEE - 8

- REQUISITI REALIZZATIVI DEI CIRCUITI:
  - ➢Tutti i componenti devono rispettare i requisiti della classe AK richiesta per la funzione di sicurezza in cui sono applicati;
  - ➢quelli di tipo B (incluso il loro SW) devono inoltre:
    - ✓ essere usati in modo da poter dimostrare che la struttura del circuito risultante, le connessioni e le interazioni fra componenti soddisfino gli obiettivi di sicurezza della classe di sicurezza richiesta, OPPURE
    - ✓ essere certificati per l'applicazione alla classe richiesta.

NORME EUROPEE - 9

- ALTRE CLAUSOLE IMPORTANTI:
  - ➢Il guasto singolo include quelli da esso conseguenti.
  - ➢Non è necessario considerare l'accadimento simultaneo di due guasti casuali indipendenti nella stessa funzione di sicurezza (esclusione di guasto).
  - ➢I guasti pericolosi devono essere rilevati con una DC coerente con la classe di sicurezza richiesta.
  - ➢Di regola, la classe di requisito richiesta per una funzione di sicurezza consegue dalla categoria di pericolo (di norma ritenuto scarsamente evitabile).

NORME EUROPEE - 10

- ALTRE CLAUSOLE IMPORTANTI:
  - ➢Le specifiche di sicurezza derivano dall'analisi di sicurezza; esiste un allegato che esemplifica l'assegnazione delle classi AK, ma è informativo.
  - ➢Un allegato normativo esprime i requisiti informativi minimi che l'HMI (supervisore) deve presentare; si tratta di informazioni basiche, che per gli standard italiani è abbastanza ovvio presentare.
  - ➢Non viene trattato il registratore di eventi.

NORME EUROPEE - 11

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢La norma EN 13243 (:2015 ?) non cambia molto nella sostanza, ma recepisce alcuni aspetti affidabilistici della UNI EN ISO 13849-1 per il riconoscimento della classe di requisiti raggiunta dai circuiti di sicurezza.
    - ✓ Anziché modificare radicalmente le definizioni delle AK, o rinunciarvi addirittura a favore dei PL, si è optato per acquisire, solo parzialmente, alcuni concetti e strumenti utilizzati per la determinazione del PL raggiunto.
    - ✓ La parte relativa al valore di MTTFd è rimasta al livello di «raccomandazione», non vincolante.

NORME EUROPEE - 12

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢Il nuovo art. 4.1.3.1 specifica che:
    - ✓ i requisiti per l'eliminazione dei pericoli o la riduzione dei rischi deve provenire dall'analisi di sicurezza;
    - ✓ le specifiche delle funzioni di sicurezza ed i livelli di sicurezza richiesti (classi AK) devono essere stabiliti dal responsabile del sottosistema da cui ha avuto origine il pericolo per l'intero sistema.
  - ➢Il nuovo art. 4.1.3.4 introduce un diagramma di flusso che descrive il processo di riduzione del rischio, in modo simile a quello della norma UNI EN ISO 13849-1.

NORME EUROPEE - 13

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢ Introduzione del concetto di copertura diagnostica:
    - ✓ Tabella 1 – Livello di rilevamento dei guasti:

Table 1 – Level of fault detection

Level of fault detection (FG)	
Designation	Area
None	FG < 60 %
Low	60 % ≤ FG < 90 %
Medium	90 % ≤ FG < 99 %
High	99 % ≤ FG
NOTE In the case of electrical safety devices which are made up of several parts, a mean value of the FG shall be used. For examples, in accordance with Annex D.	

NORME EUROPEE - 14

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢Introduzione del concetto di affidabilità dei componenti ai fini della sicurezza:
    - ✓ Tabella 2 – Tempo medio al guasto pericoloso:

Table 2 – Average time until the dangerous failure ($MTTF_d$)

$MTTF_d$	
Designation for each channel	Area for each channel
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years
NOTE The restriction of the $MTTF_d$ value of each channel up to a maximum of 100 years refers to the individual channel which executes the safety function.	

NORME EUROPEE - 15

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢Modifiche alle definizioni delle classi di requisiti (AK):
    - ✓ **Le definizioni di ciascun AK continuano a contenere tutti i requisiti esistenti nella prima edizione** (2004).
    - ✓ Per AK 1 ed AK 2, è richiesto – a livello di raccomandazione – un valore di MTTFd almeno «inferiore» fra i tre tabulati.
    - ✓ Per AK 2, è prescritto un livello di copertura diagnostica almeno «inferiore» fra i tre tabulati.
    - ✓ Per AK 3, è prescritto un livello di copertura diagnostica almeno «medio» fra i tre tabulati.
    - ✓ Per AK 3, è richiesto – a livello di raccomandazione – un valore di MTTFd almeno «medio» fra i tre tabulati.

NORME EUROPEE - 16

- ✓ Per AK 3, viene specificato che, qualora la realizzazione del circuito di sicurezza (o di una sua parte) avvenga con architettura a canale singolo (non ridondato), allora il livello di copertura diagnostica dev'essere quello «alto» (il maggiore fra i tre tabulati).
- ✓ Per AK 4, è prescritto un livello di copertura diagnostica «alto» (il maggiore fra i tre tabulati).
- ✓ Per AK 4, sono inoltre prescritte misure appropriate contro guasti derivanti da combinazioni di cause.
- ✓ Per AK 4, è richiesto – a livello di raccomandazione – un valore di MTTFd «alto» (il maggiore fra i tre tabulati).

NORME EUROPEE - 17

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢ Esplicitazione del ciclo di vita del **software applicativo**:
    - ✓ Sono adottati i concetti della UNI EN ISO 13849-1.
    - ✓ Per tutte le classi AK, le misure di base sono obbligatorie (sviluppo secondo diagramma V&V, documentazione di progetto, specifiche, programmazione strutturata e modulare, test funzionali, gestione delle modifiche).
    - ✓ Per le classi AK 3 e AK 4, sono specificate in dettaglio diverse misure addizionali, rivolte ad ottenere una chiara comprensibilità del codice e a limitare la possibilità di errori di programmazione non diagnosticabili facilmente.
    - ✓ Sono trattati in dettaglio la parametrizzazione del software e il metodo di trascrizione dei parametri dal supervisore.

NORME EUROPEE - 18

- EVOLUZIONE DELLA NORMA EN 13243:
  - ➢ Quali difficoltà applicative ci si aspettano?
    - ✓ Se la progettazione avveniva anche prima secondo un diagramma di V&V, non ci sono modificazioni sostanziali nella documentazione, se non qualche dettaglio in più.
    - ✓ Dovranno essere dimostrati i valori di copertura diagnostica raggiunti (obbligatorio), e quelli di MTTFd dei componenti (raccomandato); ciò coinvolge, oltre all'elettronica di calcolo (es. PLC), anche i sensori e gli attuatori.
    - ✓ In All. B (informativo), nella tabella di corrispondenza fra PL, AK e SIL, una nota vieta di usare canali singoli con componenti di tipo B per funzioni AK 3 e AK 4.