Functional Safety - SIL
PLC di sicurezza - Safety Relay

Is it safe?

La "Safety" è necessaria

- Nessun sistema fisico è in grado di garantire un coefficiente di errore pari a zero
- L'errore umano non può essere eliminato
- Nessun progetto software può prevedere e garantire l'esecuzione di operazioni a rischio zero
- L'insorgere di errori improvvisi può causare danni più o meno gravi a terzi o nei confronti dell'ambiente
- Molte corporation considerano i danni ambientali delle *esternalizzazioni* di alcuni costi: il tutto avviene nel rispetto delle normative locali che però cambiano moltissimo da paese a paese

Come indurre la "Safety"

- L'insorgere di incidenti ha portato nel tempo alla necessità di apparecchiature specifiche per la "protezione e salvaguardia" di beni
- Necessità di affiancare ai normali sistemi apparecchiature concepite per ridurre il maggior numero di rischi
- Nascita di standard e di leggi che governino tali apparecchiature (IEC 61508)

Da dove viene

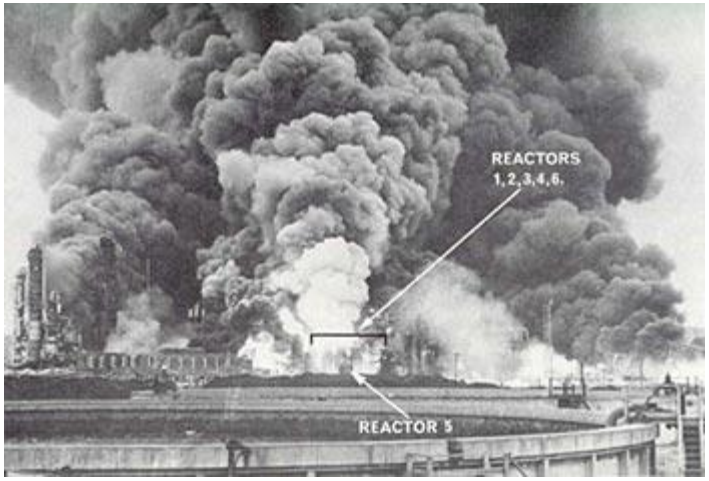
- Inizi 1970
  - Innalzamento processi industriali
  - Finanziamento di enormi impianti e utilizzo di materiali pericolosi
- Inaccettabilità del metodo di studio con pratica per errori
- Necessità di ridurre al massimo le conseguenze dei fallimenti

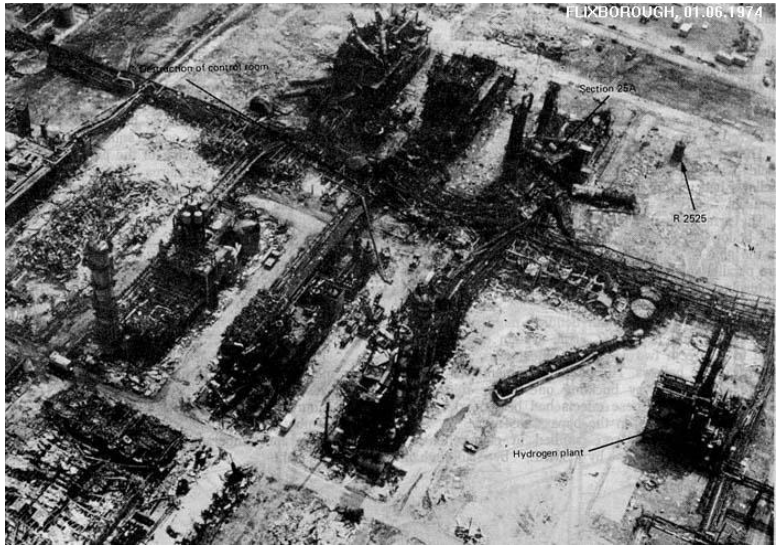
Situazione di sicurezza '70

- La mancanza di una forma di controllo per la regolazione delle attività che avrebbero potuto favorire l'insorgere di fallimenti non era di interesse pubblico

Giugno 1974....FLIXBOROUGH...

28 morti





http://www.hse.gov.uk/comah/sragtech/caseflixboroug74.htm

10 Luglio 1976 SEVESO (Italia)

http://www.eu.int/comm/environment/seveso/index.htm

Nello stabilimento chimico ICMESA una valvola di sicurezza del reattore A-101 esplode provocando la fuoriuscita di alcuni chili di diossina nebulizzata. Casi d'intossicazione si estendono sempre più, i più colpiti sono i bambini. Si da nome ad una malattia finora quasi sconosciuta: la Cloracne

Nasce la direttiva Seveso

- Viene proposta una direttiva sulla limitazione del pericolo di incidenti rilevanti connessi con determinate sostanze pericolose

Le prime regolamentazioni per la sicurezza

- Adozione di metodi di riduzione sulla frequenza di fallimenti in impianti disponibili
- Preoccupazione sui costi di apparecchiature di salvaguardia
- Section 6 of the Health and Safety at Work Act 1974 sostenne la necessità di attuare efficaci sistemi di salvaguardia
- A seguito dell'incidente di Flixborough nacquero:

  -1984 regolazioni CIMAH (Control of Industrial Major Accident Hazards)

  divenne poi nel 1999 la COMAH (Control Of Major Accident Hazzards)

1989

ENVIRONMENT AGENCY

- Nascita di un documento sull'assunzione di sicurezze funzionali delle apparecchiature programmabili

Valutazione Rischi

Rischio

Frequenza x Conseguenza

I rischi sono relativi (http://www.enre.umd.edu/ctrs/ctr04.htm)

- ai Beni
- alle Persone
- alla Collettività
- all'Ambiente

Definizione di safety

- *Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment*

- Allontanamento da un rischio inaccettabile di danni fisici o alla salute, sia direttamente sia indirettamente, associato al danneggiamento di beni proprietari o dell'ambiente

Definizione di Functional Safety

- *Is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs*
- E' la parte della Safety che dipende da sistemi o apparati che operino correttamente in risposta a degli ingressi

- Esempio di Functional Safety:
  - Un dispositivo di protezione contro il surriscaldamento che usi un sensore termico sulle alette di raffreddamento di un motore il quale riduca la alimentazione del motore.
- Non è Functional Safety:
  - Un isolamento particolare che protegga dalle alte temperature

Safety Function

- Funzione che deve essere attuata da un Sistema Strumentale di Sicurezza (SIS) o dagli altri Livelli di Protezione (indipendenti)
- SCOPO:
  - Mantenere o riportare il processo in sicurezza, in relazione ad uno specifico evento pericoloso quando una o più condizioni predeterminate non siano più soddisfatte
- Safety Related System:
  - Sistemi che implementano le Safety Functions
- Safety Integrity:
  - Misura quanto una Safety Function si comporta in maniera adeguata (è un livello)

Malfunzionamenti

- Safety-related
  - Viene usato quando si manifesta l'avvento di errori su attrezzature che non provocano necessariamente errori critici che possano portare a pericolose conseguenza (anche sugli altri oggetti)
- Safety-Critical
  - Viene usato per fenomeni di guasto separati che sono guida a fatali errori che possono portare all'incremento dei rischi e di esporre delle persone.

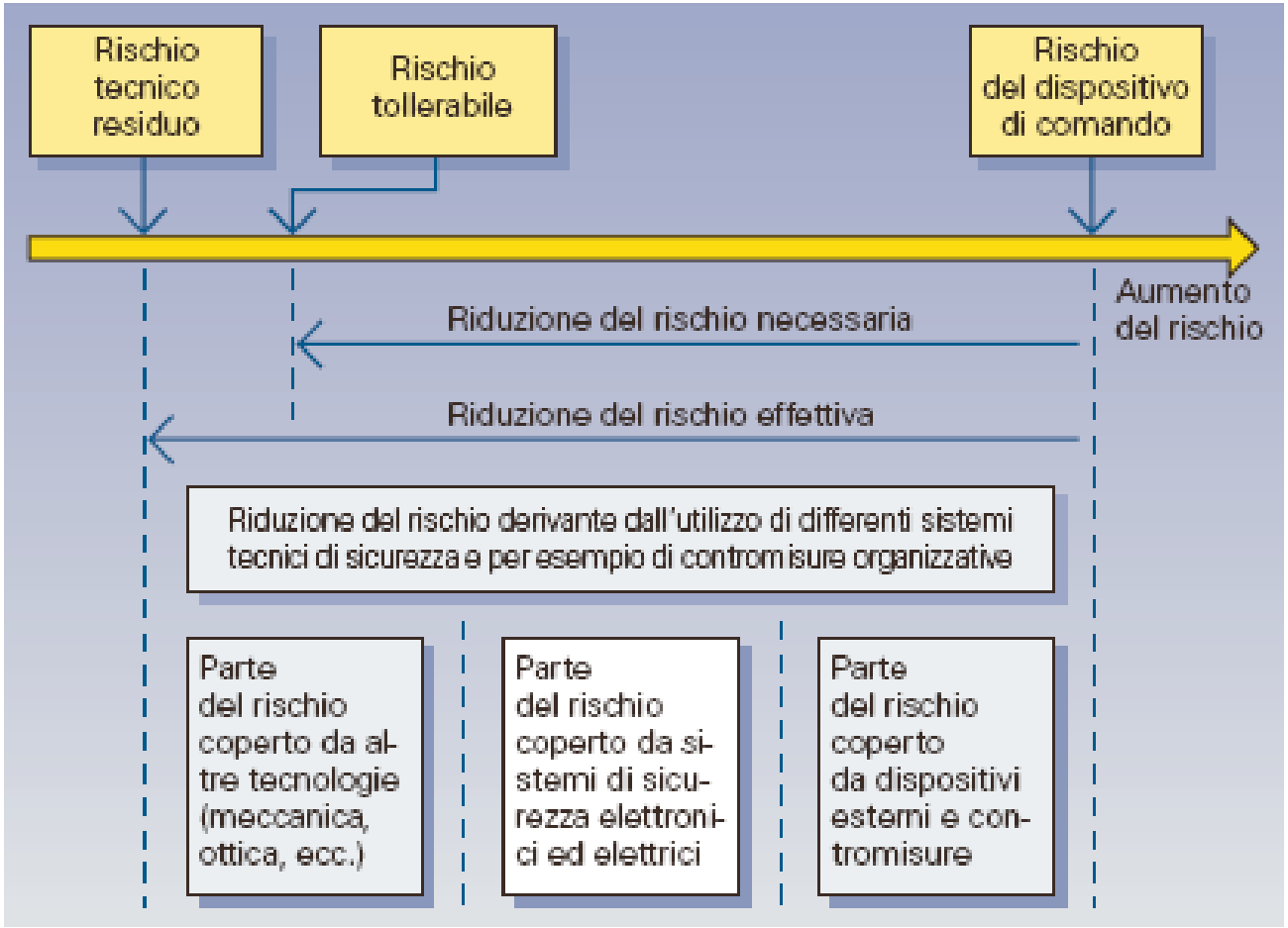
Safety Instrumented System

I sistemi di sicurezza sono costituiti da tre sottosistemi:

- S1: Il sottosistema dei trasmettitori costituito dai rilevatori di campo, ossia dai quei componenti che rilevano e convertono le variabili controllate
- S2: Il sottosistema degli elementi finali costituiti dai dispositivi di blocco veri e propri
- S3:Il sottosistema logico che gestisce le connessioni e lo scambio di informazioni tra le due precedenti tipologie di componenti; esso può essere l'unità PLC.

Fig.1 - Schema generale di un sistema di sicurezza

Riduzione del rischio



Dal momento che risulta impossibile una completa riduzione del rischio sia dal punto di vista tecnico che economico, è allora necessario non solo stabilire il rischio esistente ma anche considerare il rischio tollerabile. Dalla differenza tra i due si ricava quale debba essere l'affidabilità riferita alla sicurezza ("Safety Integrity") delle funzioni di riduzione del rischio.

Per assicurare la Functional Safety

1. Hazard Anlysis
   - ◇ Identifica le minacce analizzando le pericolosità del processo e quali possono essere le safety function implementabili

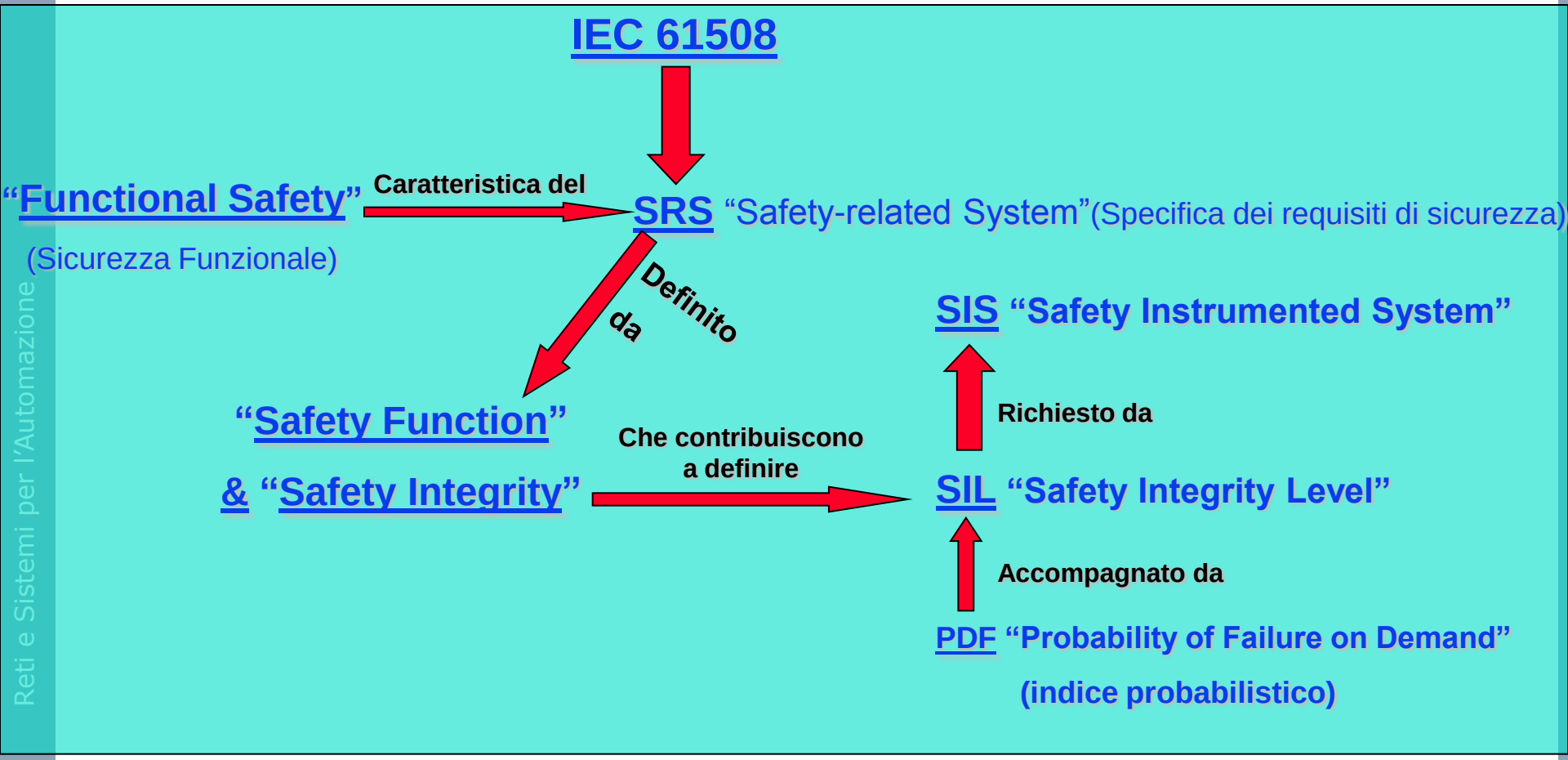
2. Risk Assessment
   - ◇ Quantifica il rischio determinando le performance della safety function da implementare.
   - ◇ Lo scopo è quello di di assicurare una safety integrity sufficiente ad assicurare che nessuno sia esposto a un rischio inaccettabile.
   - ◇ Il livello di safety integrity richiesto sarà proporzionale al possibile danno e alla riduzione di rischio necessaria

Norme di interesse

- A partire dal 1990 il Comitato Tecnico 65 della IEC ha elaborato tre standard internazionali in materia di sicurezza, usando come base di partenza gli standard esistenti in Germania ed altri standard e linee guida a carattere nazionale. I risultati ottenuti sono:

- IEC 61508 "*Functional Safety of Safety-Related System*"
  - pubblicato nel 1998 – 2000 che è uno standard internazionale che fissa l'approccio generale per tutte le attività del Ciclo di Vita della sicurezza per sistemi di tipo E/E/PES (Elettrici/Elettromeccanici/Elettronici Programmabili) utilizzati per eseguire funzioni di sicurezza. Questo standard fornisce un metodo per lo sviluppo della specifica dei requisiti di sicurezza, come pure introduce ed utilizza i livelli di integrità della sicurezza(SIL) e interessa in particolare produttori e fornitori di componenti dei Sistemi di Sicurezza Strumentale.
- IEC 61511 "*Functional Safety instrumented system for the process industry sector*"
  - è stato specificatamente sviluppato come implementazione dello standard IEC 61508 per il Settore di Processo ed è uno standard internazionale che fornisce gli obiettivi ed i requisiti per specificare, progettare, installare, operare e manutere i Sistemi Strumentali di Sicurezza (SIS). Quest'ultimo standard è di particolare interesse per titolari, progettisti, integratori ed utenti dei sistemi di sicurezza strumentale.
- IEC 61131 "Programmable controllers"
  - pubblicata nel 1992

Quadro riassuntivo della 61508



Ciclo di vita della sicurezza

- La IEC 61508 è basata anche sul concetto di Safety Life Cicle, in modo da analizzare in maniera sistematica le differenti fasi di vita di un sistema SRS, da svolgere nell'arco temporale che parte dalla fase di Concezione Generale del Progetto della Sicurezza Funzionale e termina con la dismissione del SIS stesso.

- Il Ciclo di Vita della Sicurezza è usato come base per il raggiungimento della conformità agli standard IEC 61508 e IEC 61511.

Ciclo di vita standard IEC 61508

- Si compone di 12 fasi dove le più importanti sono
  - Concezione generale del progetto
  - Analisi dei rischi
  - Allocazione delle funzioni di sicurezza ai livelli di protezione indipendenti
  - Progettazione del SIS (sistema strumentale di attuazione di funzioni di sicurezza)
  - Test dei componenti HW e SW prima dell'installazione in campo
  - Installazione
  - Manutenzione
  - Modifiche
  - Dismissione

Safety Integrity Level (SIL)

- Le norme relative ai sistemi elettrici ed elettronici suggeriscono di misurare il livello di sicurezza di un sistema attraverso l'indice SIL (Safety Integrated Level)
- Il SIL è una rappresentazione statistica della affidabilità di un sistema quando viene effettuata una richiesta di processo.
- E' utilizzato sia in ANSI/ISA-S84.01 che in IEC 61508.
- Sia ISA che IEC sono d'accordo che esistano 3 livelli: SIL 1,2 e 3.
- IEC aggiunge anche un livello 4 che ISA non prevede.
- Il SIL 4 è il più affidabile sistema che esista.

Divide lo spettro di integrità in un numero discreto di livelli

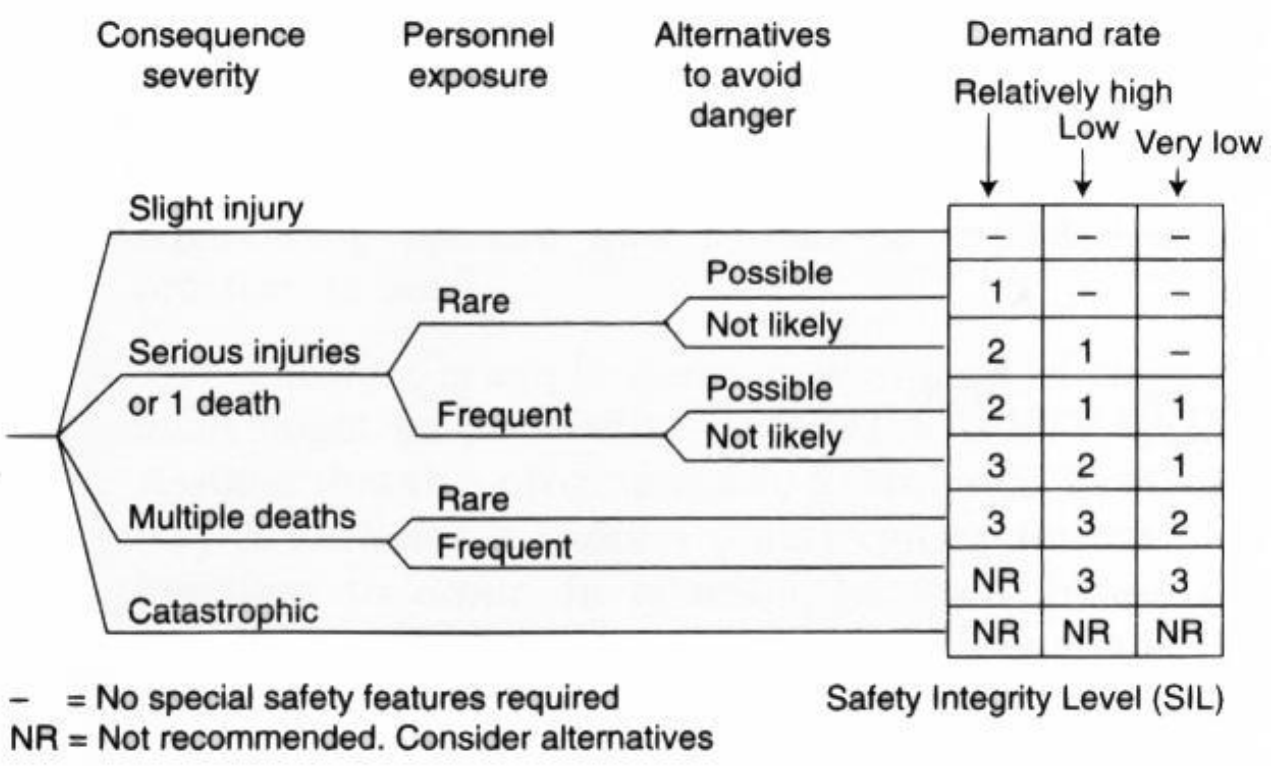
Safety-Integrity Level	Frequenza alta di richiesta (Malfunzionamenti pericolosi/ora)	Frequenza bassa di richiesta (Probabilità di malfunzionamenti su richiesta)
4	>= di 10^{-9} e <10^{-8}	>= di 10^{-5} e< 10^{-4}
3	>= di 10^{-8} e <10^{-7}	>= di 10^{-4} e< 10^{-3}
2	>= di 10^{-7} e <10^{-6}	>= di 10^{-3} e< 10^{-2}
1	>= di 10^{-6} e <10^{-5}	>= di 10^{-2} e< 10^{-1}

- Le richieste di un SIL particolare vengono spesso associate a
  - **SIL1** : Protezione di produzione e proprietà primaria
  - **SIL2** : Protezione di produzione e proprietà secondaria (con possibilità di lesioni fisiche)
  - **SIL3** : Protezione di dipendenti e della comunità
  - **SIL4** : Impatto catastrofico sulla comunità

Grafo dei rischi (SILs)

Per assegnare ad ogni S.I.S. un SIL

L'utilizzo di un grafo dei rischi consente una maggiore velocità e facilità di utilizzo ma sicuramente una minor precisione e vi è la necessità di rendere non ambigui i termini (low, very low etc.)



Certificazione dei livelli SIL di un apparato

- **SIL 1** : assegnato da persone indipendenti rappresenta il livello minimo associato ad un buon progetto pratico, specialmente se l'ISO 9001 è applicato a quel progetto provvedendo che la capacità di sicurezza funzionale sia dimostrata

- **SIL 2** : assegnato da persone indipendenti richiede una buona progettazione su vari livelli, con numerosi controlli (anche ripetuti) e test e non solo secondo lo standard ISO 9001.

- **SIL 3** : assegnato da dipartimenti indipendenti richiede una sofisticata progettazione tecnica, i costi e i tempi hanno una importanza molto importante per i venditori che limitano comunque a 3 il livello del SILs

- **SIL 4** : assegnato da organizzazioni indipendenti, rappresenta il più oneroso dei livelli e richiede una notevole abilità e arte nella progettazione con l'utilizzo di metodi formali, i costi sono notevolmente alti e i requisiti tecnici sono di alto livello e non molto facili da trovare. Il 4 livello viene per una questione di semplificazione di applicabilità suddiviso spesso in più sottogruppi

Dalla 61508 alla 61511

- La IEC 61508 è nata come standard generico, applicabile a tutti i sistemi SRS a prescindere dal relativo campo di impiego per poter ottenere almeno all'inizio uno standard internazionale

- La IEC 61511 è stata sviluppata come evoluzione della IEC 61508 per il settore dell'industria di processo; lo standard riguarda essenzialmente sistemi di sicurezza di strumentazione (SIS), di cui fanno parte sensori, attuatori, logic solver ecc.

- I concetti fondamentali rimangono sempre i Safety Life Cicle ed i Safety Integrity Level (SIL). Lo standard suggerisce che applicazioni che richiedono l'uso di un SIL 4 nell'industria di processo sono rari e andrebbero evitati ove possibile.

I moderni sistemi di Sicurezza

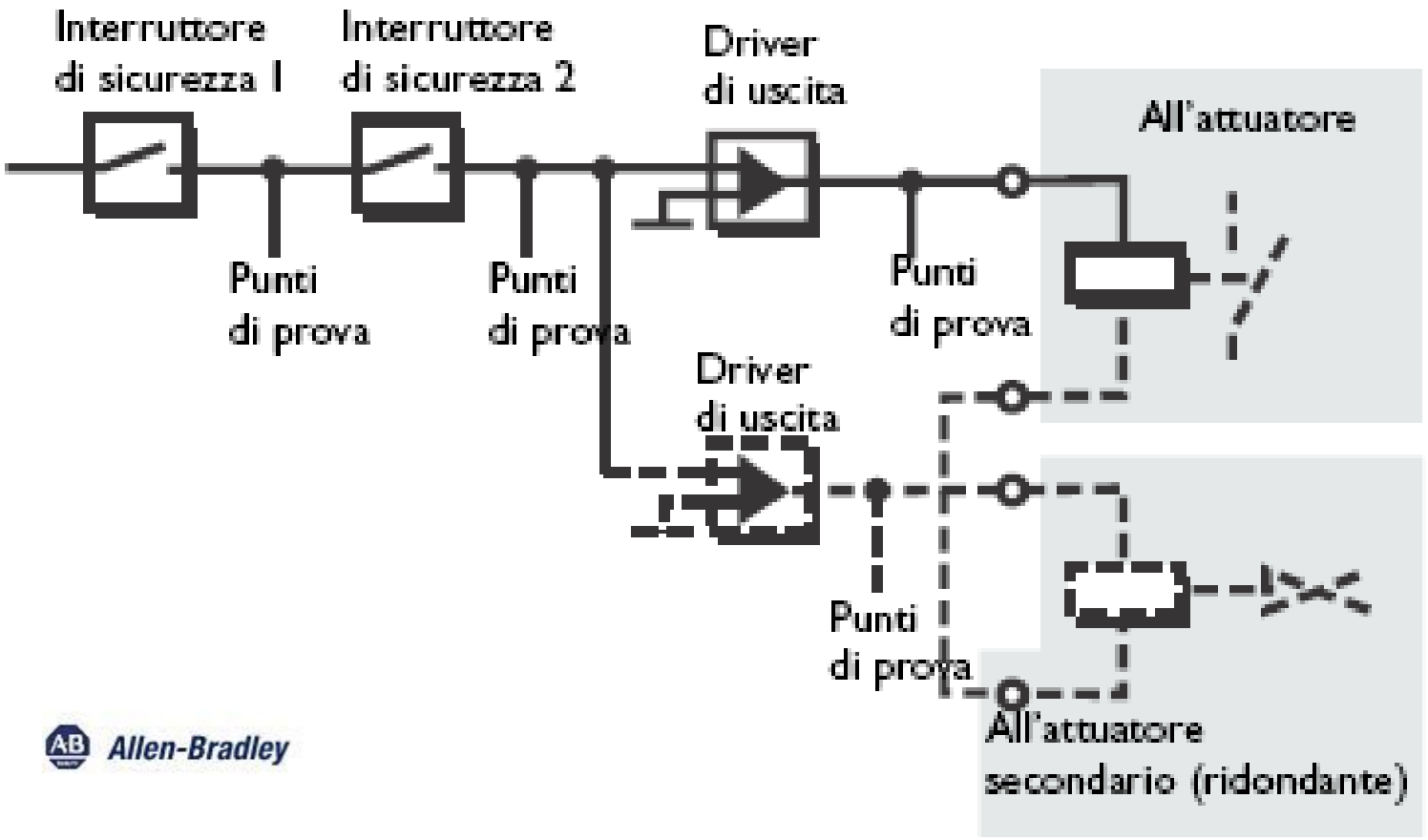
- Passaggio dalla logica a relè ai controllori logici programmabili (PLC)

- Rivoluzione del mercato dei sistemi di controllo macchina con produttività, flessibilità, ed affidabilità estremamente elevati

- Caratteristiche per applicazioni in sistemi con livello di integrità di sicurezza fino a SIL 3 secondo IEC 61508

PROGETTO FUNZIONALE

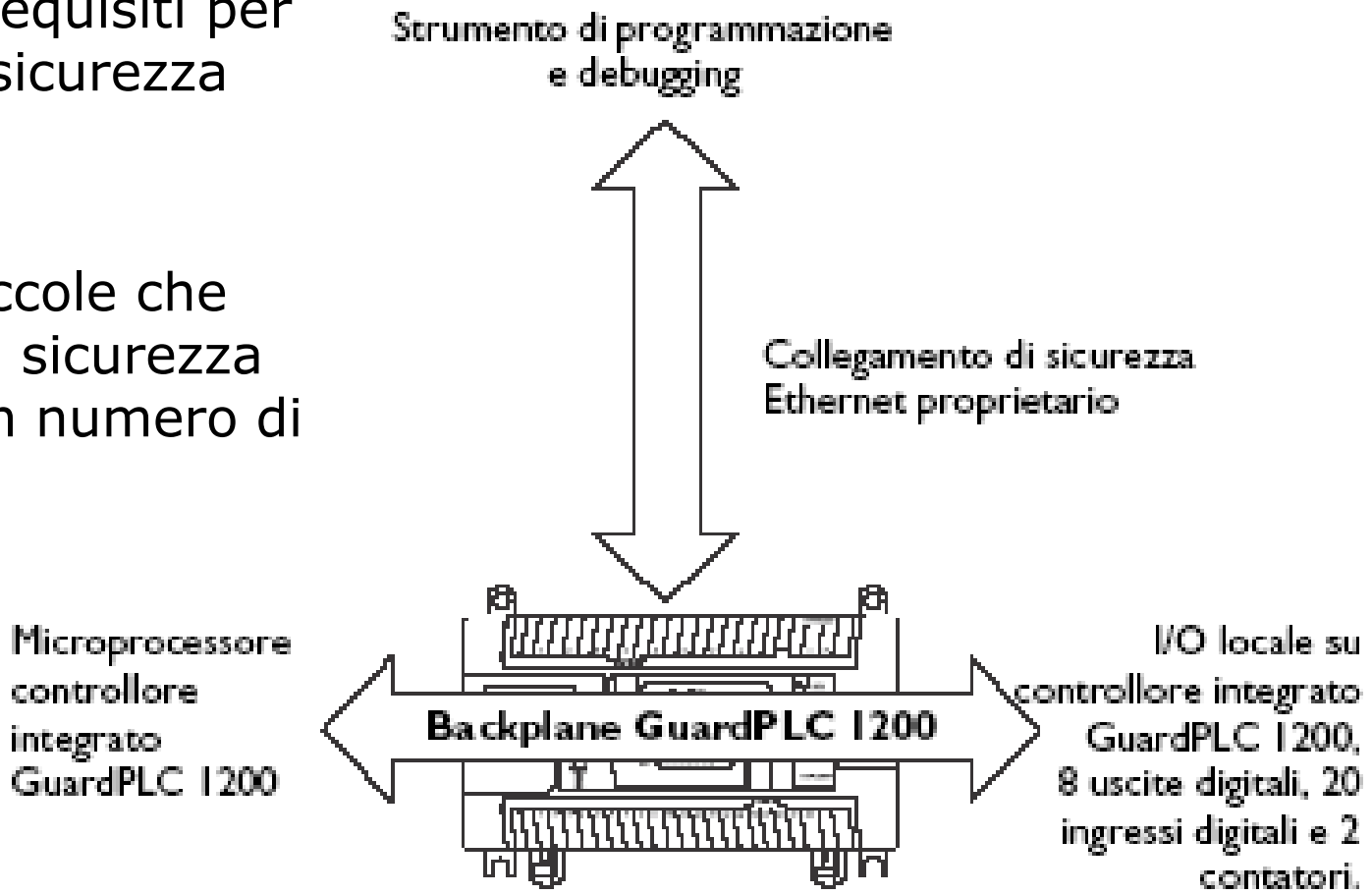
Esempio di struttura di sistema del GuardPLC



GuardPLC 1200

Il GuardPLC 1200 è conforme hai requisiti per un sistema di sicurezza (Sil3)

progettato per applicazioni piccole che richiedono una sicurezza funzionale e un numero di I/O fisso.

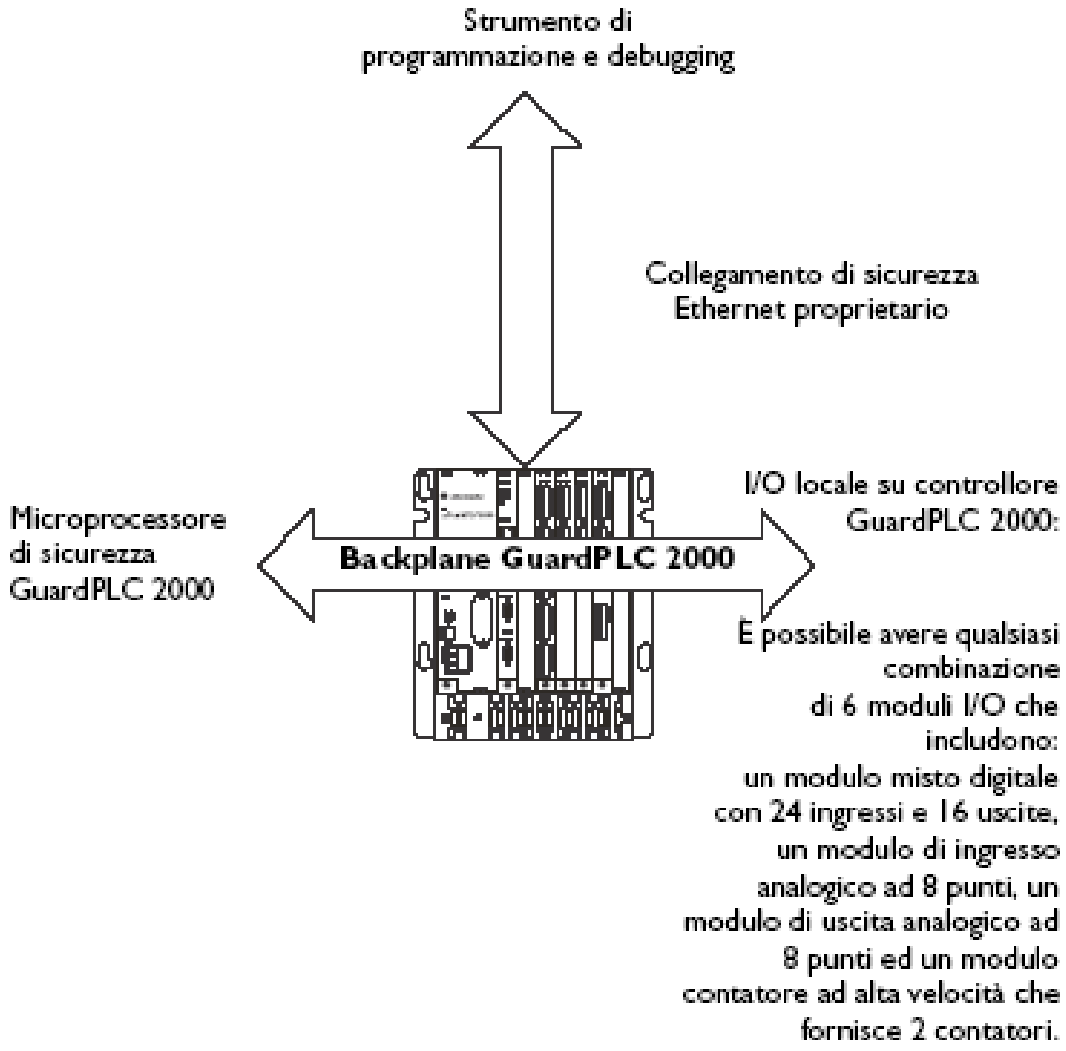


GuardPLC 2000

La CPU GuardPLC2000 ha una porta Ethernet 10/100BaseT per programmazione e configurazione e due porte di interfaccia (9 pin D-shell) per collegamenti seriali

La CPU controlla tutte le funzioni del sistema GuardPLC 2000, nonché la comunicazione verso altri sistemi.

I LED visualizzano le modalità di funzionamento:
esecuzione ed errore per i moduli I/O; esecuzione, errore, arresto, programmazione e forzatura per la CPU.



Programming Software

Studiato e testato appositamente per tutti i sistemi di GuardPLCs permette oltre le normali capacità fornite dai precedenti RSLogic, ha la possibilità di interagire e fornire e-stop controllo luci di segnalazione, stazioni in run con duplice attività, gestione di input ridondanti e pulse test output.

Il nuovo ambiente di sviluppo fornisce inoltre, con la massima flessibilità, con un numero illimitato di tag e di pagine di programmazione la possibilità di effettuare simulazioni offline, la possibilità di monitorare online il programma e di definire librerie in blocchi funzionali di attività e progetti basati sul controllo link

Safety Relay

Apparati progettati per individuare guasti su circuiti di sicurezza: sensori, collegamenti, contatori, ecc… e provvedono a applicare un’azione di scambio come nei normali relè.

MINOTAUR SAFETY-RELAY

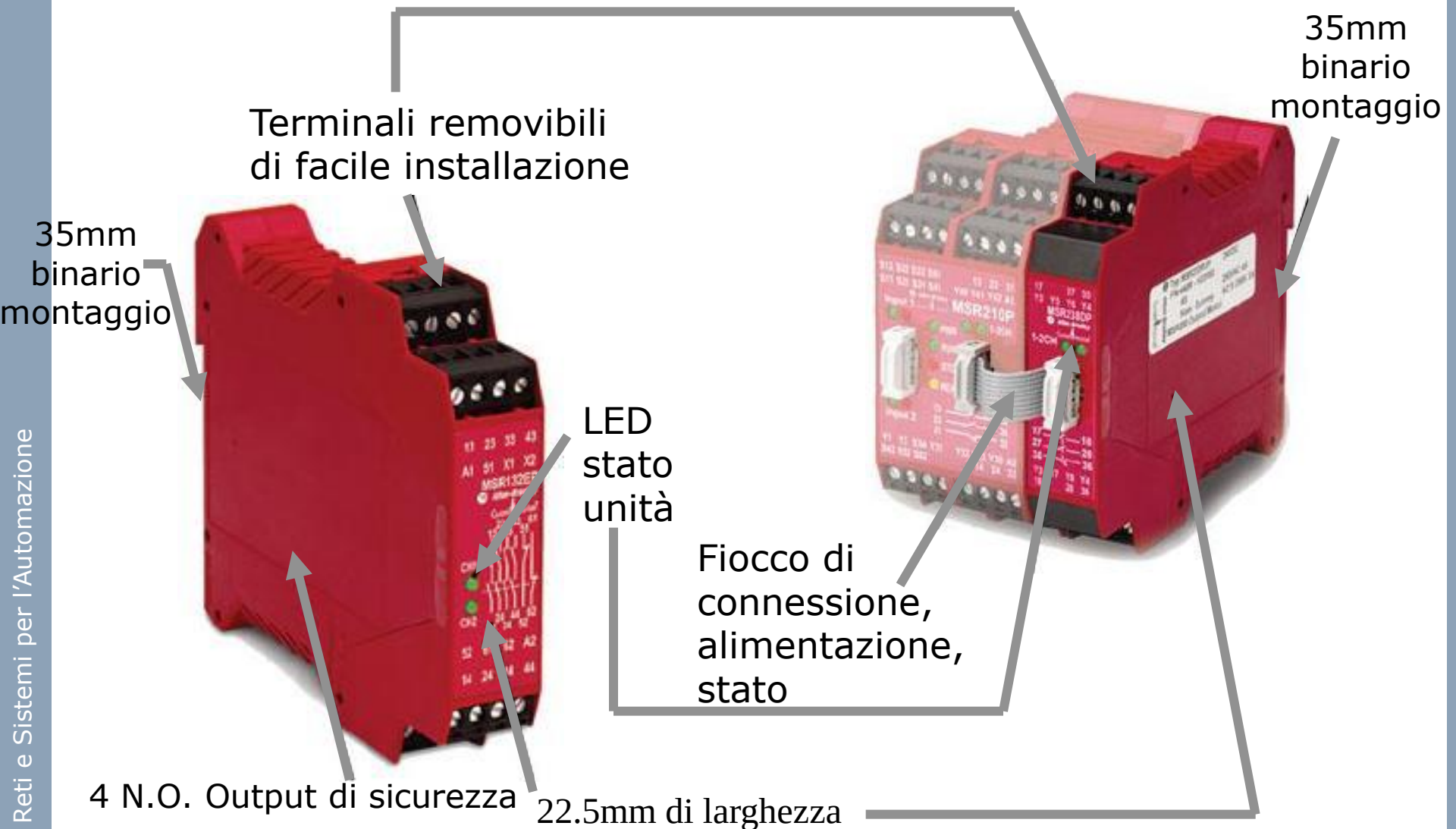
Modulo Diagnostica

Modulo di stato di tutti i moduli connessi

Estensione moduli di sicurezza

Modulo di Base

Modulo di estensione contatti


Terminali removibili
di facile installazione
35mm
binario
montaggio
35mm
binario
montaggio
LED
stato
unità
Fiocco di
connessione,
alimentazione,
stato
4 N.O. Output di sicurezza
2 N.C. Output ausiliari
1 N.C. Output di monitoraggio
22.5mm di larghezza

CU – Control Unit

- La CU è una gamma di prodotti per la sincronizzazione ed unità di arresto motion-control
- Queste sono state sviluppate per integrare con gli interruttori di bloccaggio di sicurezza in uso sulle macchine che sono state riparate o con periodi run-down variabili
- Utilizzando un tempo prestabilito, la gamma del CU offrirà un ritardo sul segnale di apertura della protezione solo quando verrà configurata correttamente con un interruttore di bloccaggio della protezione
- Ciò permette che la protezione rimanga attiva fino a che non venga ripristinato uno stato di sicurezza attivo