Micaela Caserza Magro
Università degli Studi di Genova

La trasmissione dei dati nei sistemi di sicurezza

Facolta' di Ingegneria
Università degli Studi di Genova

Safety: definizione

La **SAFETY** è la protezione contro i **malfunzionamenti** di componenti e sistemi in un impianto

E' necessario considerare i **rischi in modo globale** in modo da garantire **l'affidabilità del servizio** di processo

Le funzioni vitali per la gestione degli impianti sono affidate A sistemi di protezione, controllo, monitoraggio e supervisione :

- distribuiti negli impianti
- dipendono da una rete di comunicazione locale e remota

Gli impianti industriali vengono a dipendere sempre di più dall'**affidabilità** e dalla **sicurezza** dei **sistemi d'automazione** e **dell'infrastruttura di comunicazione**

Un sistema di sicurezza per..

Personale

Macchine

Ambiente

INFORTUNI
MORTE

PERDITA
INVESTIMENTI

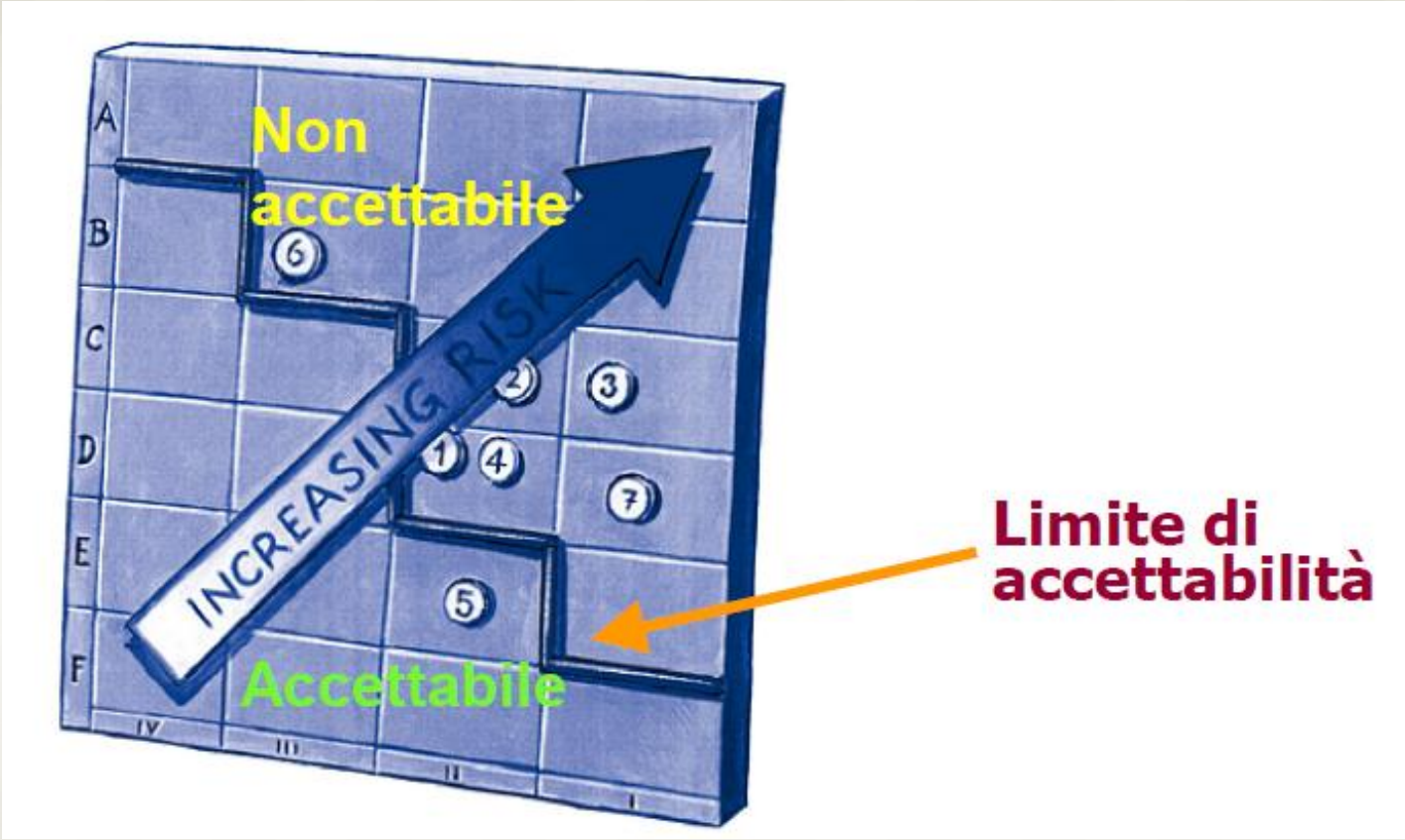
DANNI
AMBIENTALI

Ridurre il RISCHIO

Dove serve la safety?

Protezione macchine	Processo	Trasporti
▪ Nastri ▪ Presse ▪ Macchine di produzione ▪ Controlli	▪ Bruciatori ▪ Industria petrolifera ▪ Chimica ▪ Farmaceutica	▪ Funivie ▪ Ascensori ▪ ...

Profilo di rischio



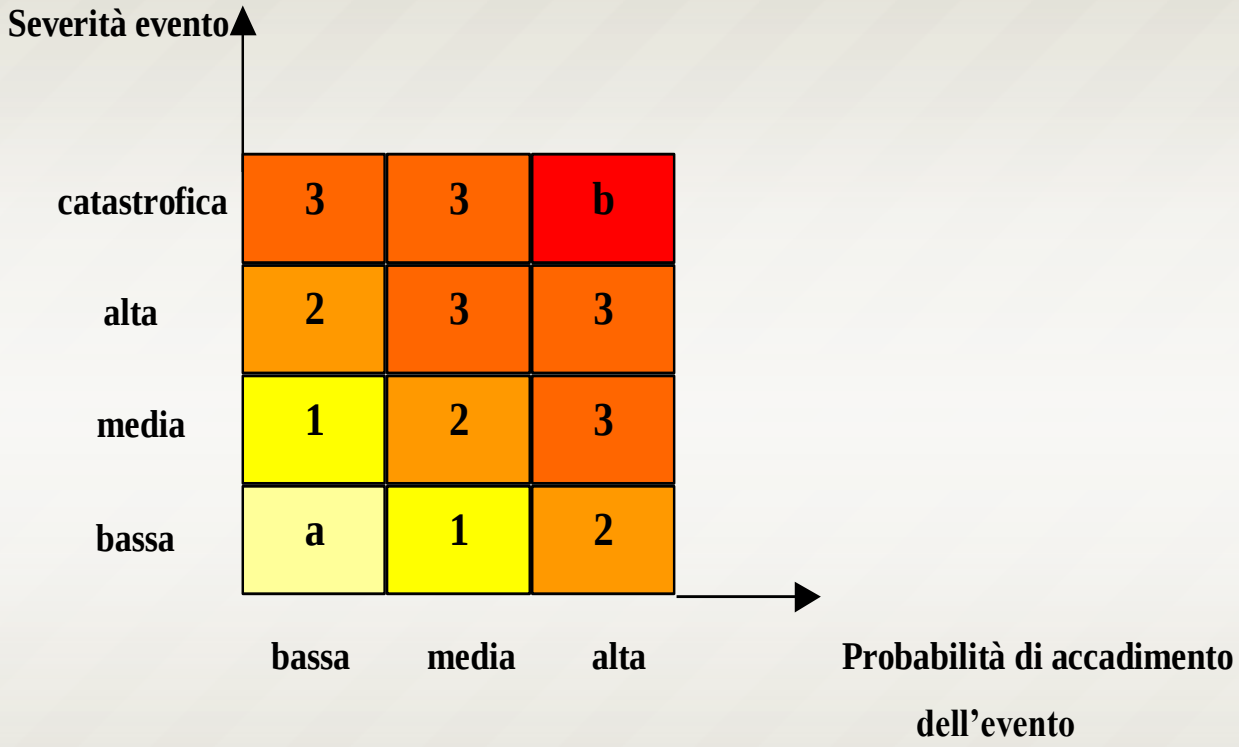
Valutazione rischio in termini di **probabilità** e **severità**

Probability of Failure on Demand PFD

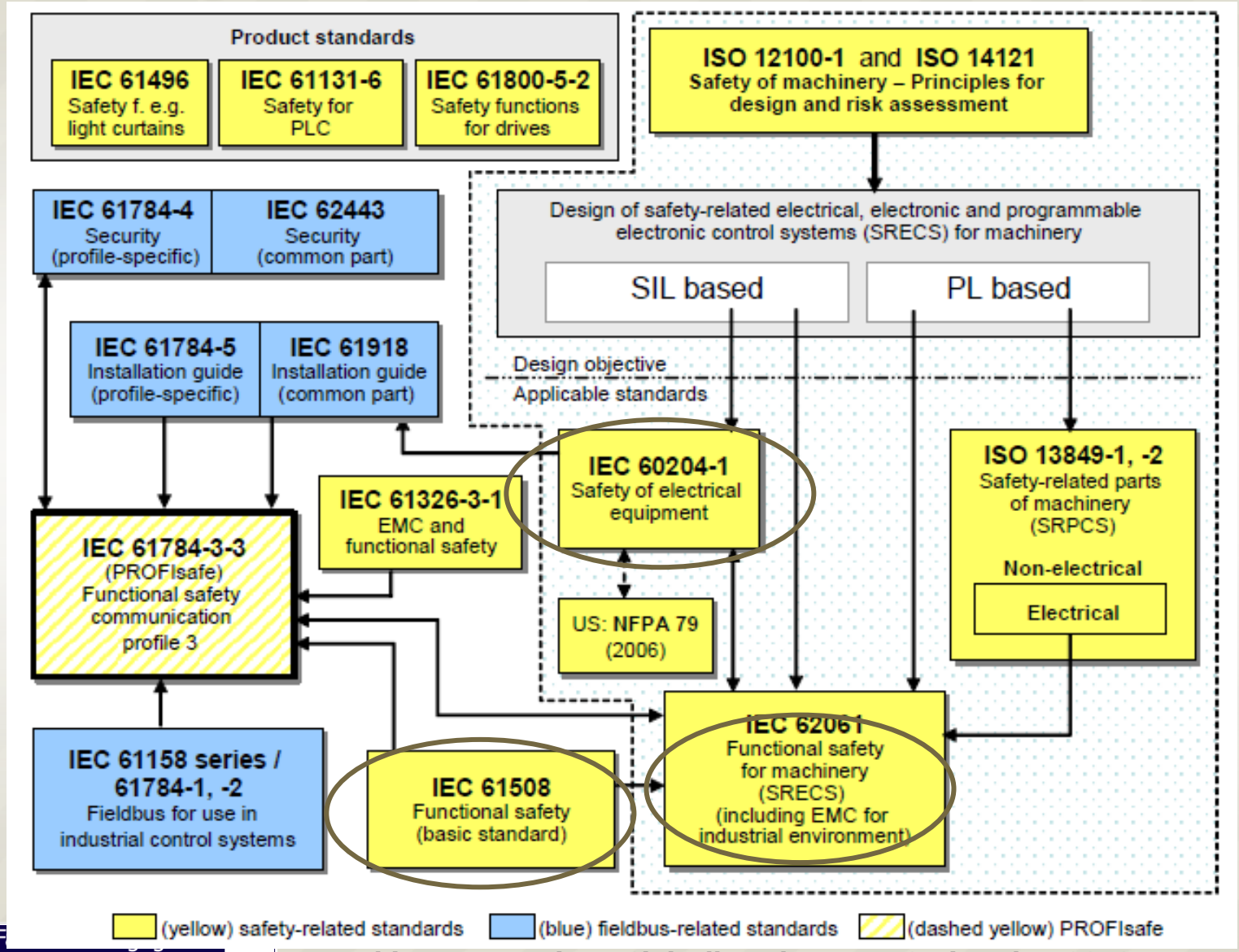
Safety Integrity Level	Low demand mode of operation
1	10^{-2} [PFD $<10^{-1}$
2	10^{-3} [PFD $<10^{-2}$
3	10^{-4} [PFD $<10^{-3}$
4	10^{-5} [PFD $<10^{-4}$

Safety Integrity Level	High demand or continuous mode of operation
1	10^{-6} [PFD $<10^{-5}$
2	10^{-7} [PFD $<10^{-6}$
3	10^{-8} [PFD $<10^{-7}$
4	10^{-9} [PFD $<10^{-8}$

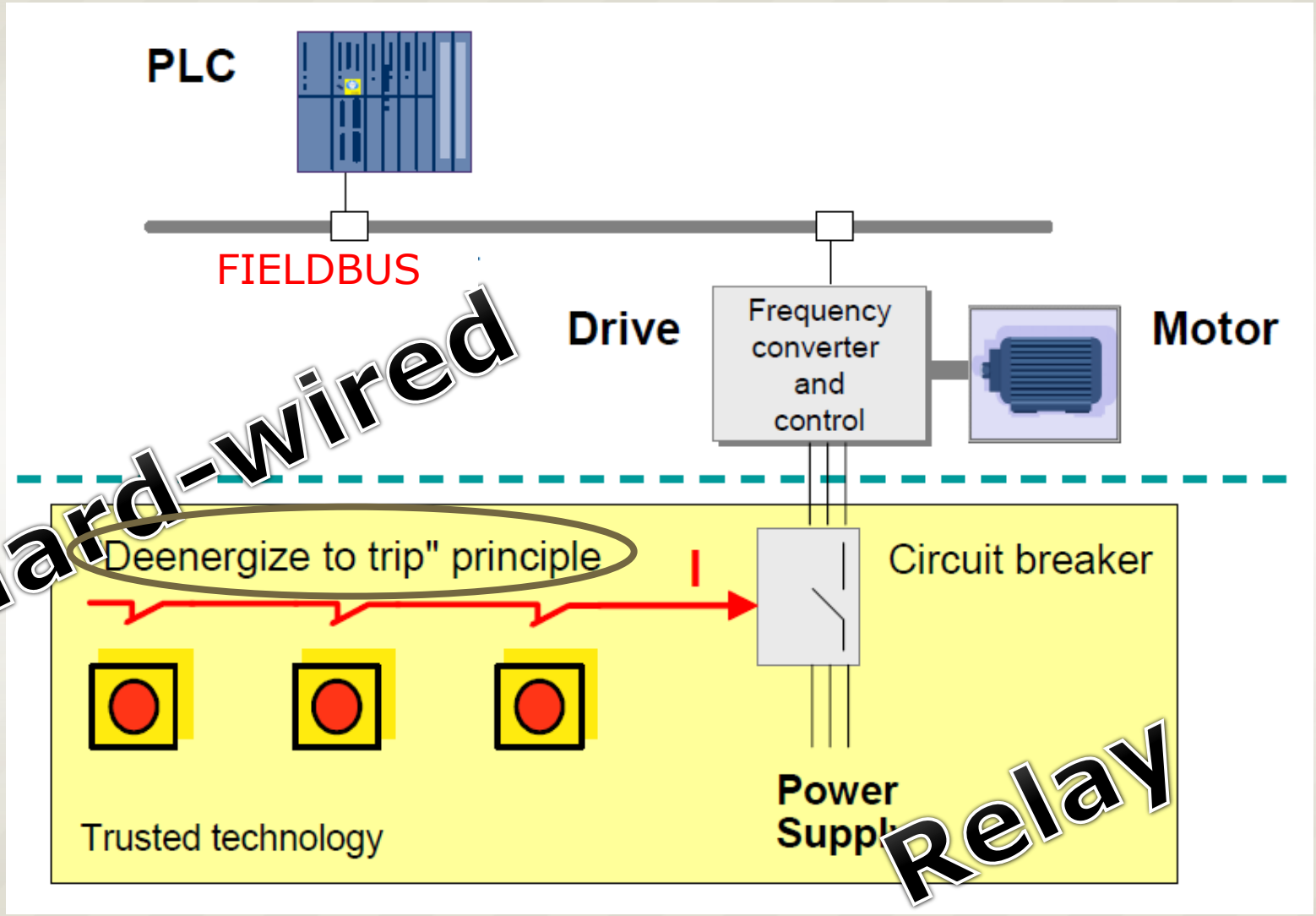
Matrici di rischio



Il panorama normativo



La situazione ieri



L'evoluzione

Prestazioni affidabilistiche

- Micro controllori e software

Meccanismo di riconoscimento errore

Ampie installazioni -> lungo tempo di esercizio

Prestazioni di failure

Modi di guasto

Gli attori in gioco

Sensori o attuatori

- Identici costruttivamente ai convenzionali
- Unica modifica: porta di comunicazione

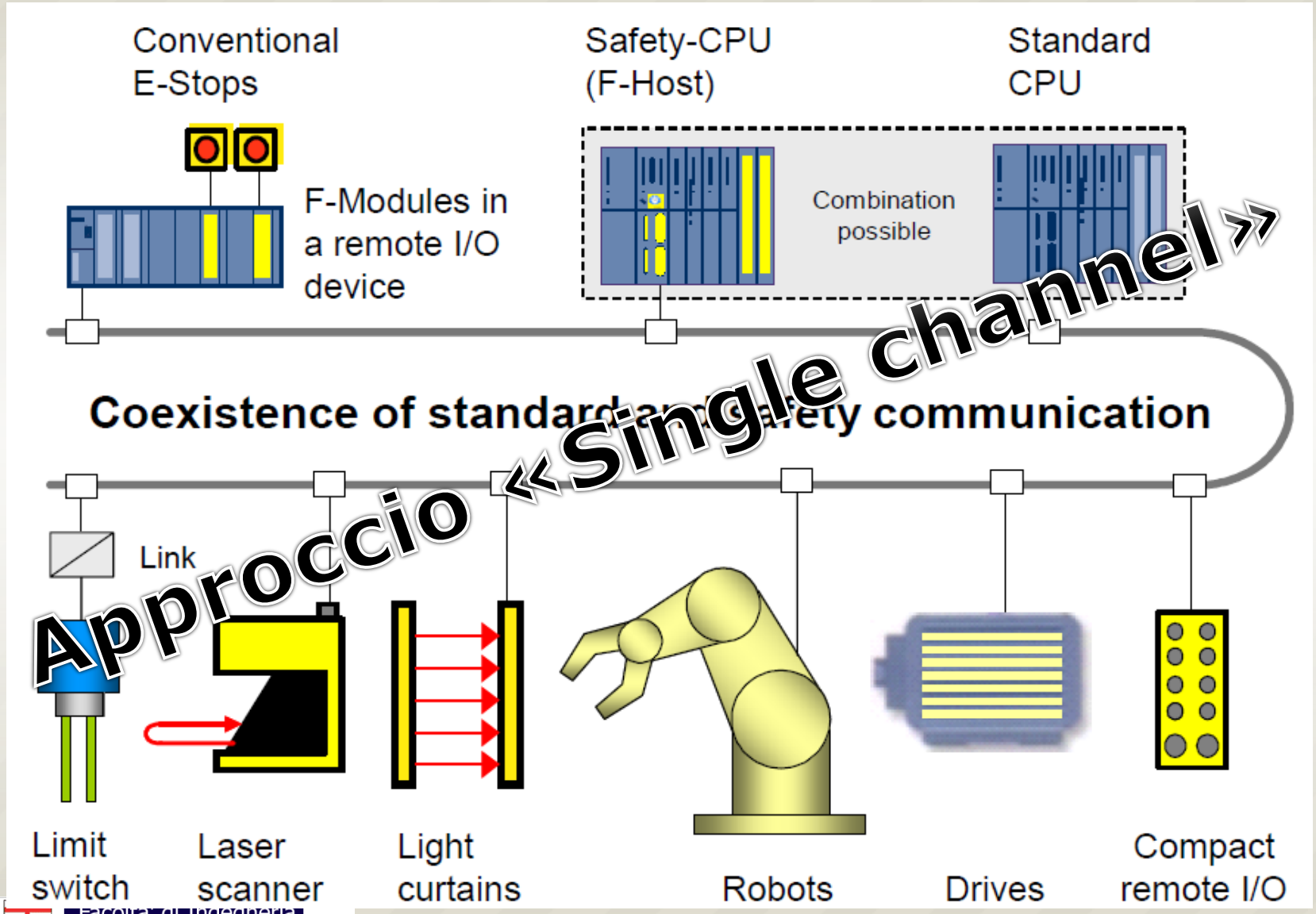
Stack software di comunicazione

- Il software legato alla comunicazione safe viene testato secondo IEC 61508
- Test del PLC di sicurezza con stack software

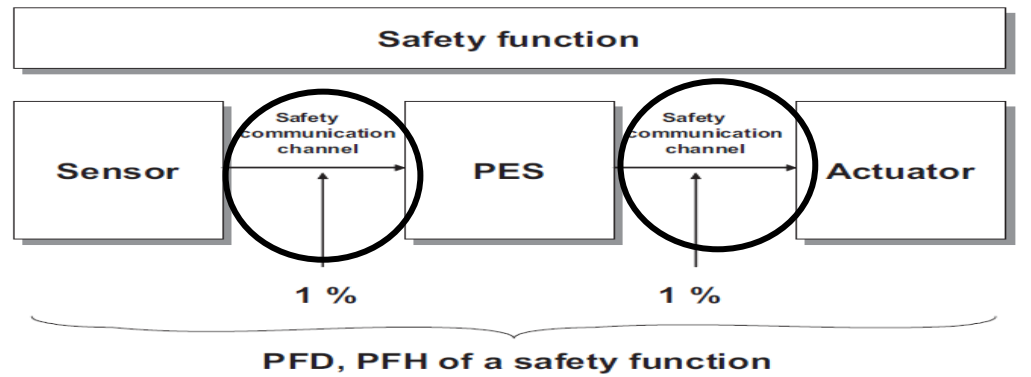
Cosa testare

- Stack software
- Interfaccia di comunicazione

La situazione oggi



La catena di sicurezza



- Sensore
- Programmable Electronic System
- Attuatore
- Canale di comunicazione sicuro

I vantaggi dell'integrazione

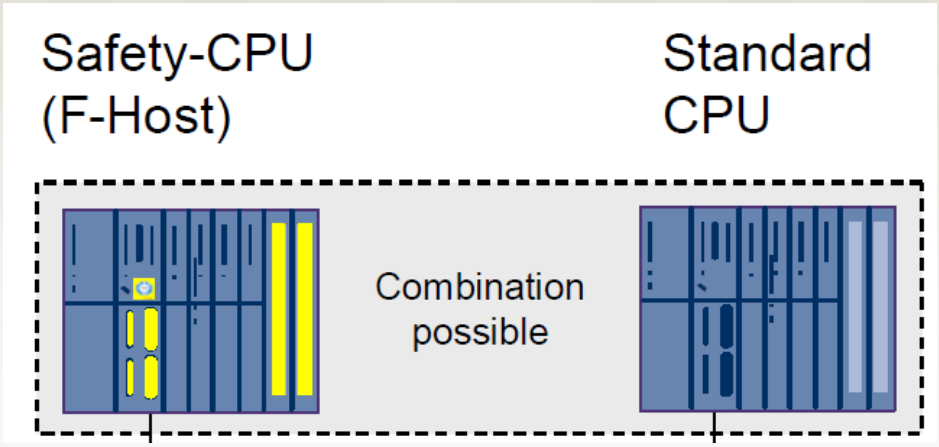
- Riduzione materiali di cablaggio
- Una sola CPU
- Coesistenza di un programma standard e fail-safe
- Unico bus di comunicazione
- Un solo ambiente di programmazione
- Prestazioni in accordo ai limiti IEC 61508
- Possibilità di implementare logiche di safe per rallentare

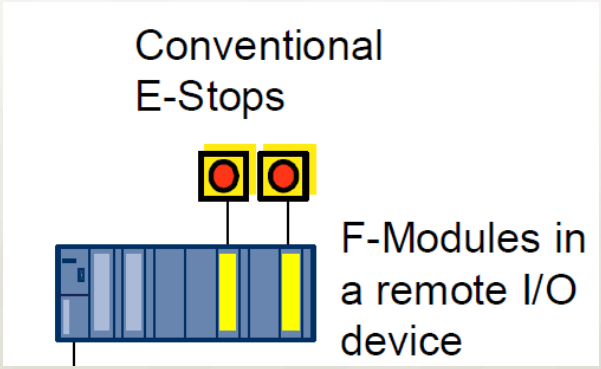
La soluzione: il profilo Safety

Profilo per Fieldbus safety

- È un layer aggiuntivo sopra i protocolli esistenti
- Riduce la probabilità di errore di trasmissione tra un Safe Controller e un Safe Device
- Coesistenza messaggi standard e messaggi di safety sullo stesso mezzo
- Mezzi trasmissivi supportati: rame, fibra ottica, wireless e backplane
- Certificato fino a SIL3, secondo IEC 61508
- Soluzioni commerciali

Profilo safet: elementi HW e SW



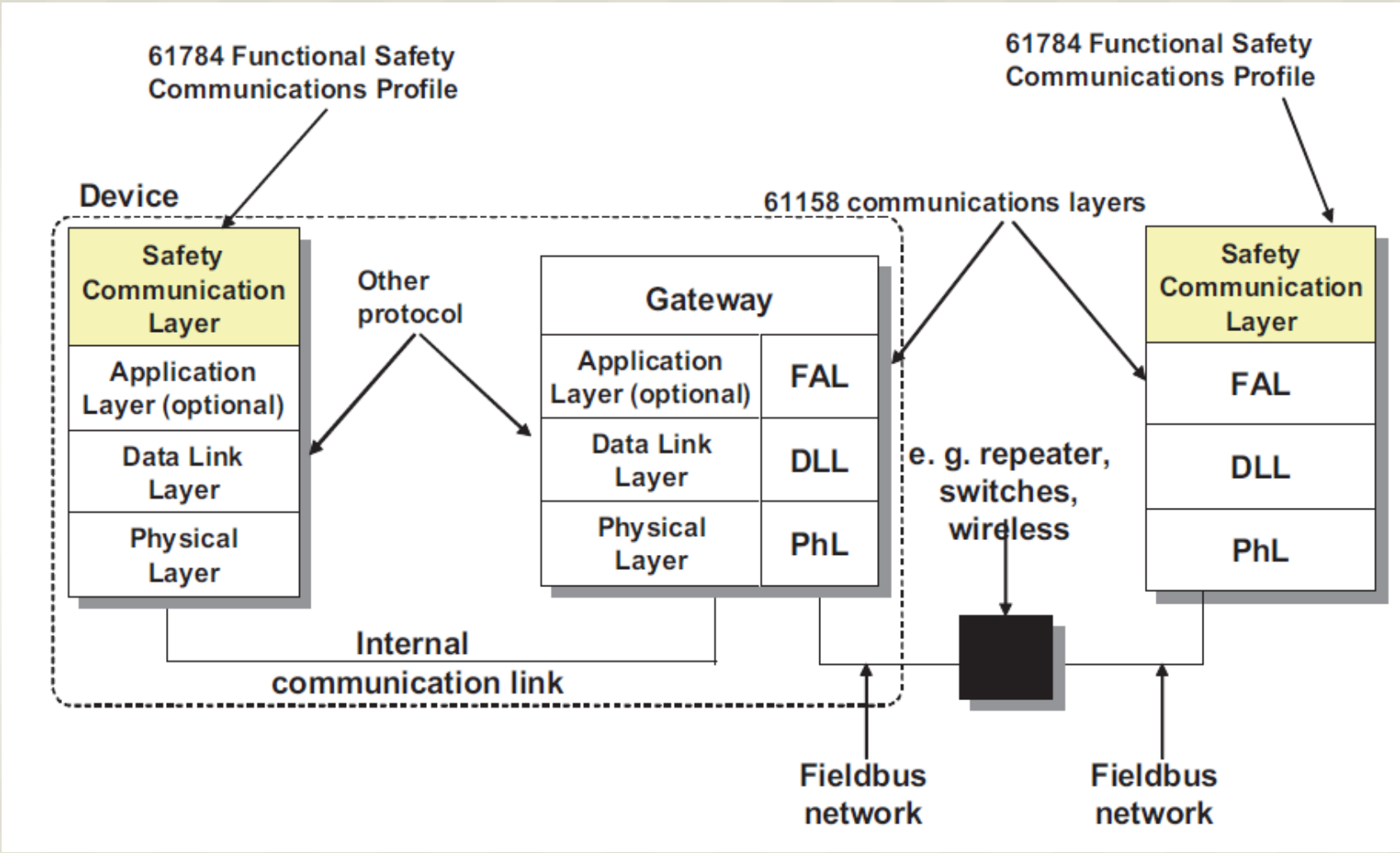


Controller
Safe

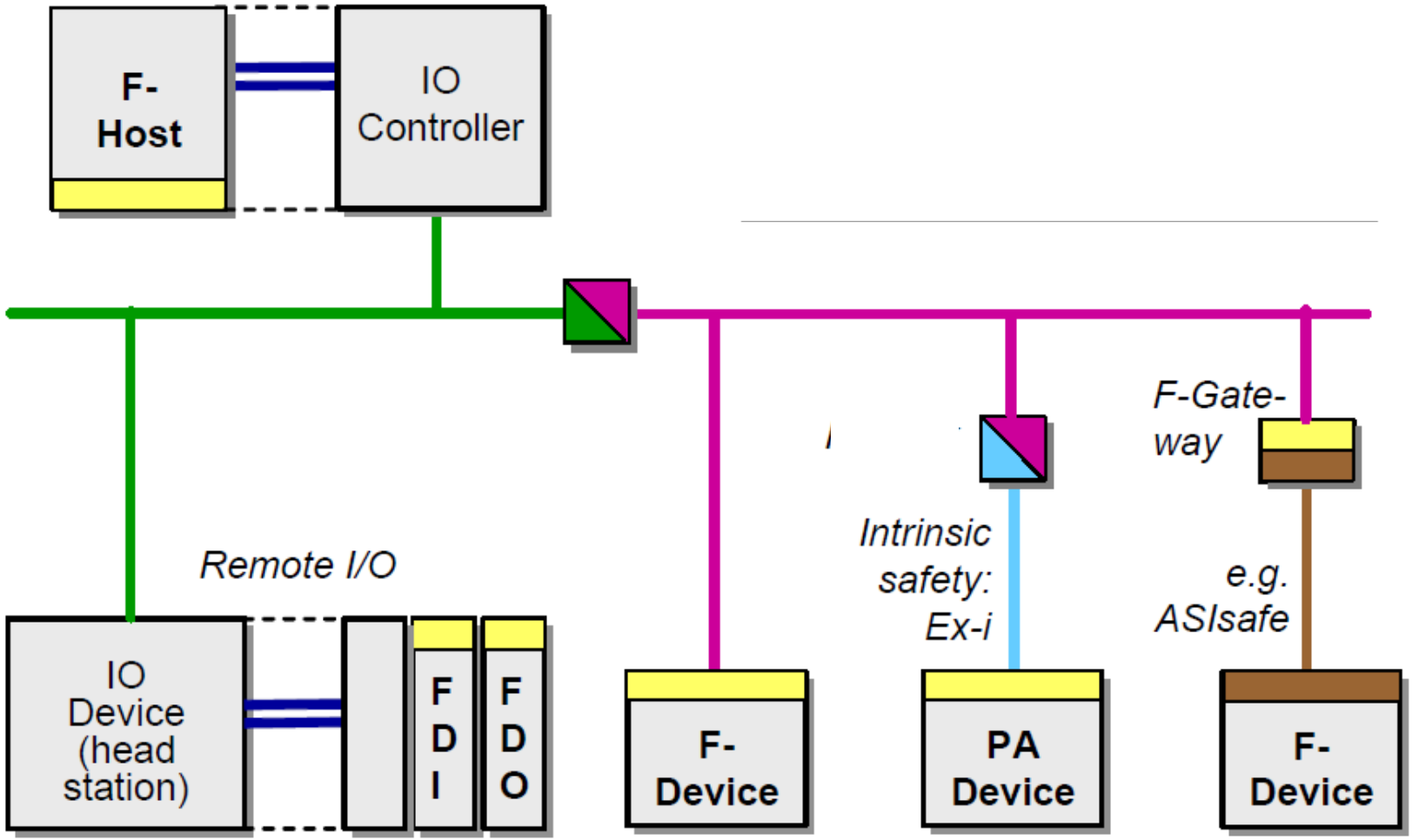
Profilo Safety
stack

Device
Safe

Approccio «Black Channel»

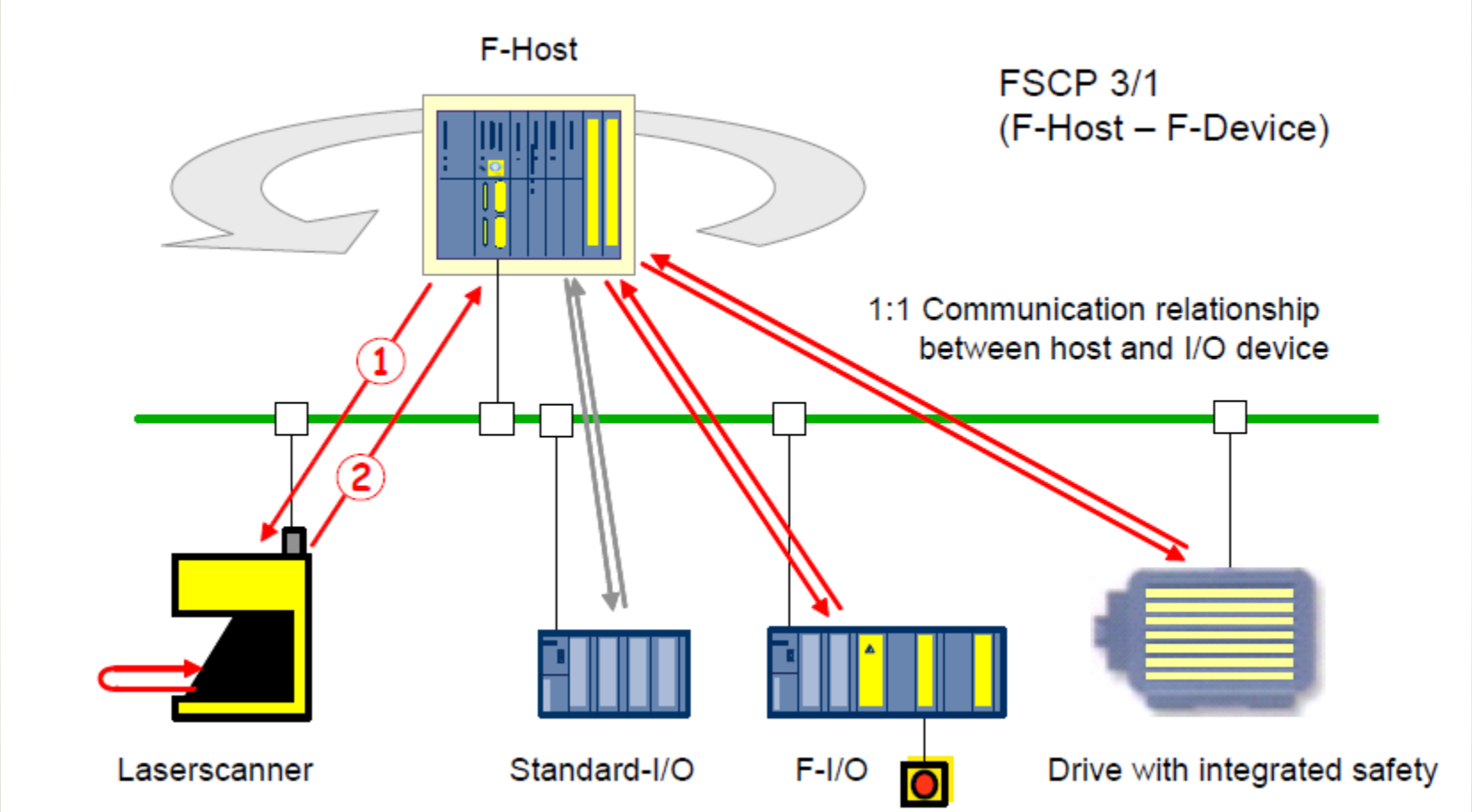


Il percorso della comunicazione



Viene «assicurato» l'intero percorso tra dove il dato viene generato a dove viene usato

La gestione della comunicazione



Alcune funzionalità di fieldbus di safety

Caratteristiche di base

- Comunicazione ciclica: permette di individuare subito un device in fault
- Relazione di comunicazione 1:1, un F-device è preso in carico da un solo F-Host

Componenti di rete

- Esistono diversi componenti trasparenti per il «black channel»: switches, routers, links
- Possono essere collegati solo 100 switch in cascata

Indirizzamento

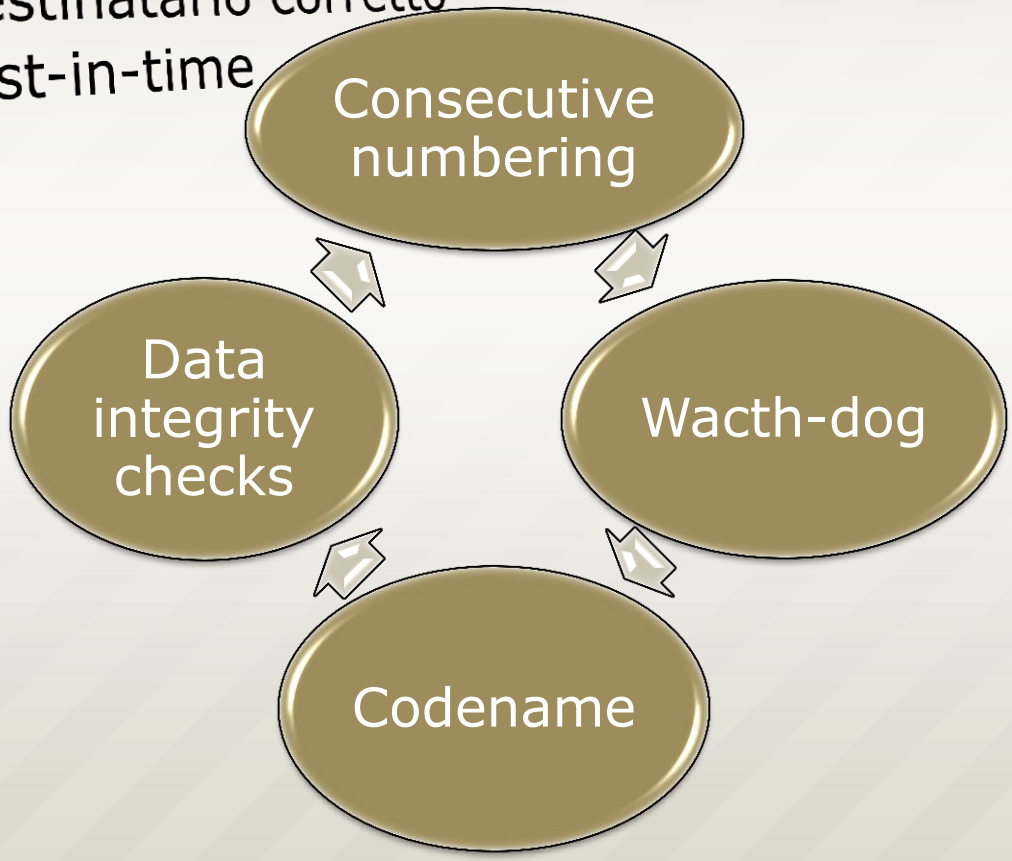
- Ogni dispsoitivo deve avere un indirizzo unico nell'isola safety

Parametri

- I parametri di safety sono inseriti all'interno del file descrittivo
- Vengono assicurati con metodi di CRC ed esistono tool di verifica (CPD)
- I parametri sono funzione della tipologia di device

Fieldbus per safety in a nutshell

- Dati corretti
- Destinatario corretto
- Just-in-time



Errori di trasmissione e rimedi

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption (see 5.3.2)					X	X	Only for serial bus[d]	
Unintended repetition (see 5.3.3)	X	X					X	
Incorrect sequence (see 5.3.4)	X	X					X	
Loss (see 5.3.5)	X				X		X	
Unacceptable delay (see 5.3.6)		X	X [c]					
Insertion (see 5.3.7)	X			X [a,b]	X [a]		X	
Masquerade (see 5.3.8)				X [a]	X [a]			X
Addressing (see 5.3.9)				X				

Errori di trasmissione e rimedi

Sequence number

- Un numero di sequenza è inserito nel messaggio

Time stamp

- Incluso nel messaggio dal mittente. Il messaggio è valido in un certo lasso temporale

Time expectation

- Il ricevitore fa un check tra 2 messaggi consecutivi, se supera un ritardo genera errore

Connection authentication

- Identificativo unico di mittente e ricevente

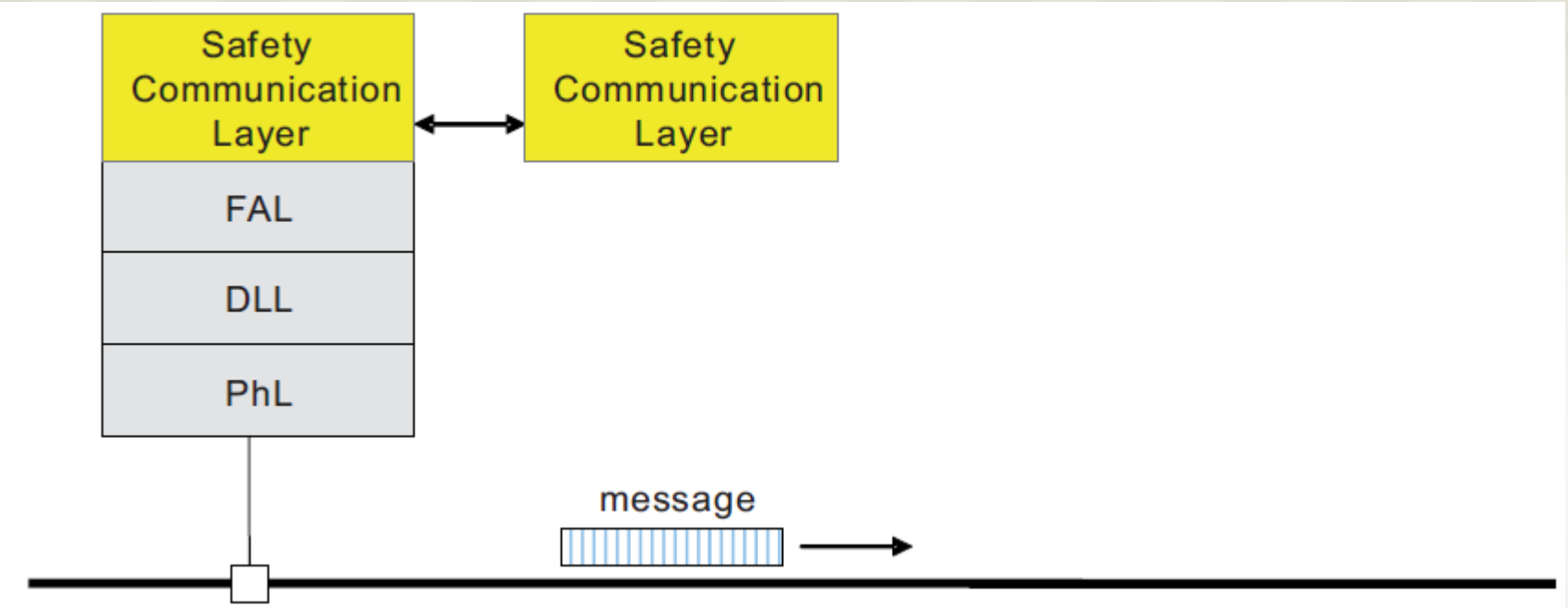
Feedback message

- Generato dal ricevente

Cross checking

- I dati vengono inviati 2 volte

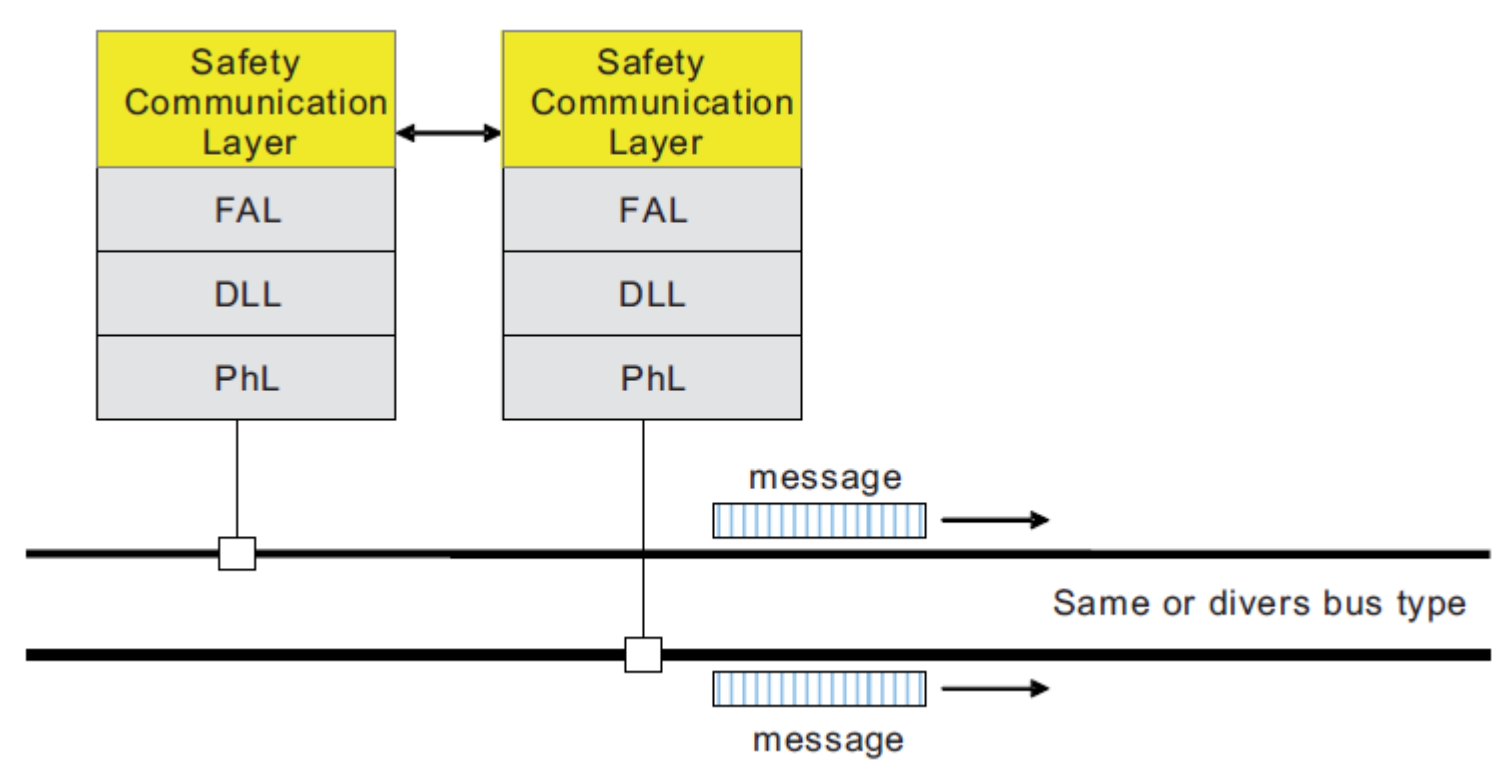
Modello di comunicazione A



Safety check e cross check sui messaggi generati a livello di safety layer

L'implementazione può essere HW o solo SW

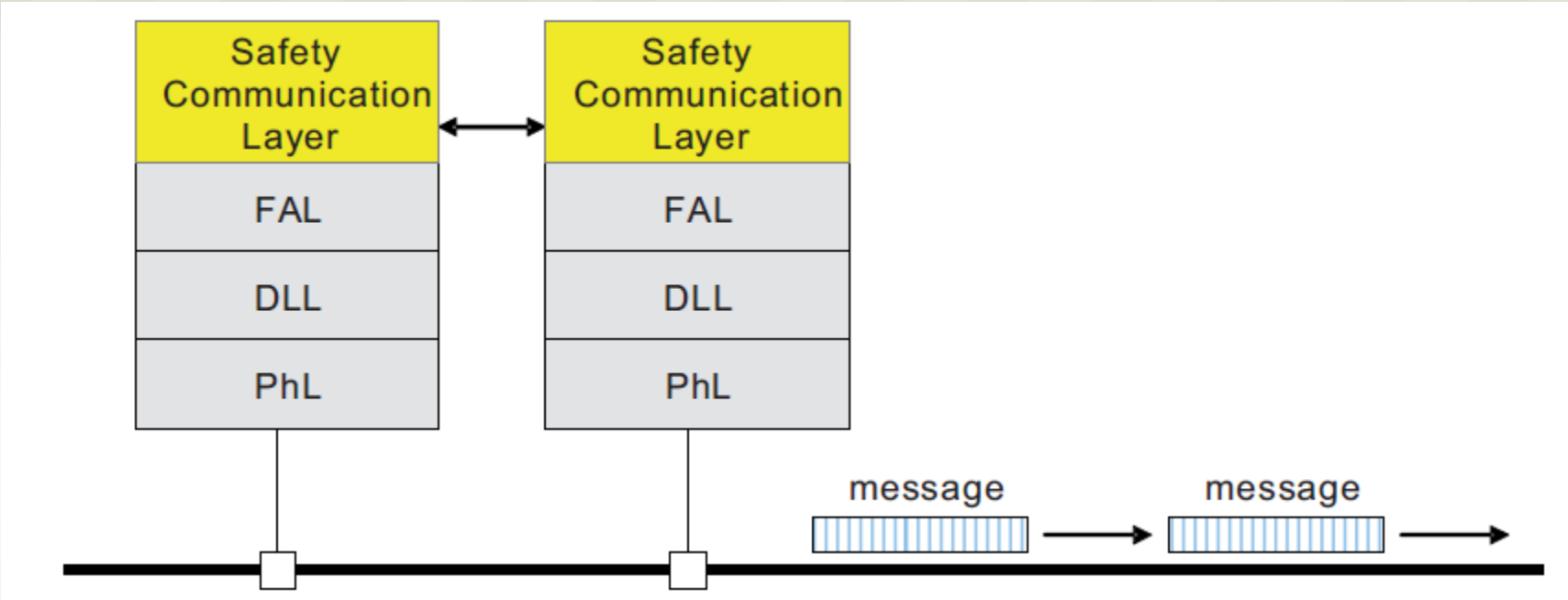
Modello di comunicazione B



Viene tutto raddoppiato, anche il mezzo trasmissivo

Cross check a tutti i livelli del messaggio di sicurezza

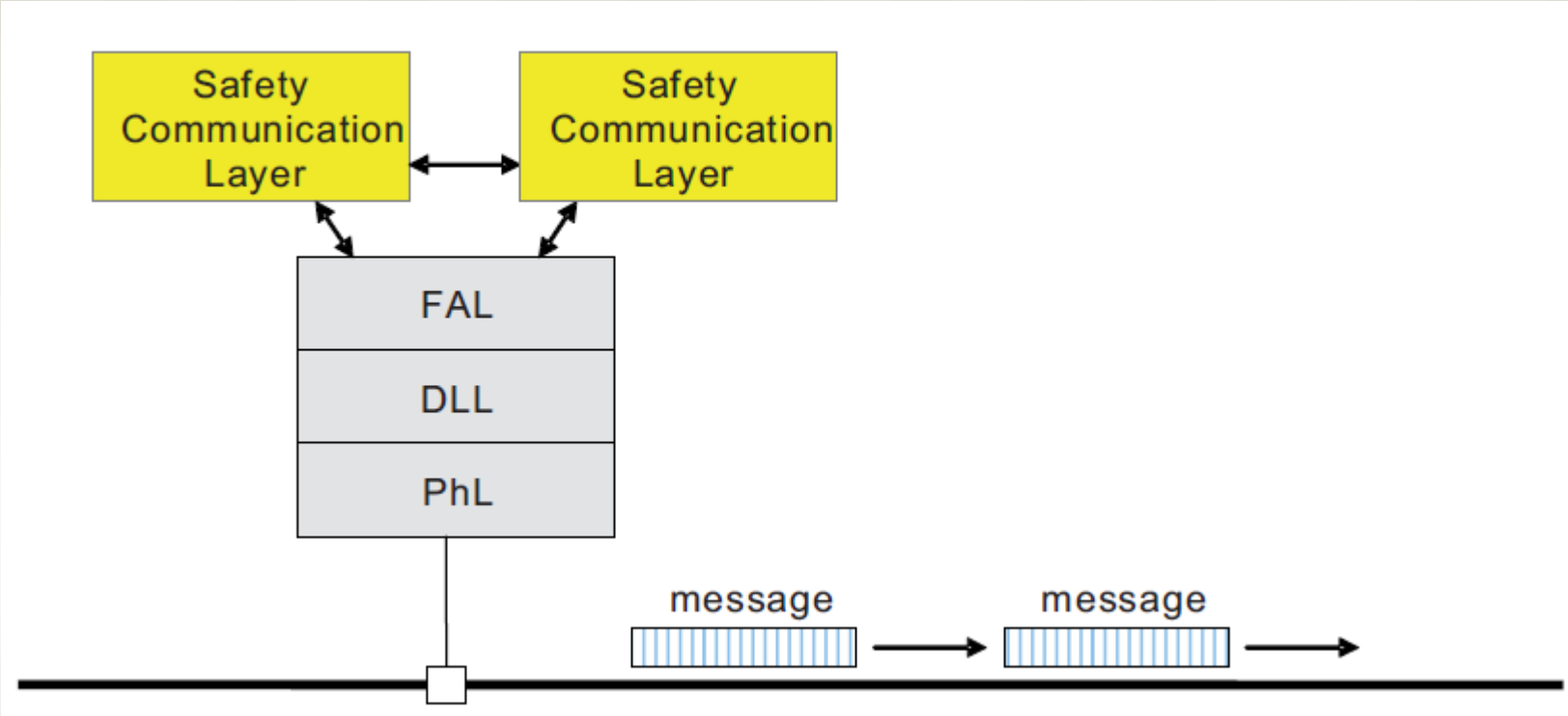
Modello di comunicazione C



Viene tutto raddoppiato, tranne il mezzo trasmissivo

Cross check a tutti i livelli del messaggio di sicurezza

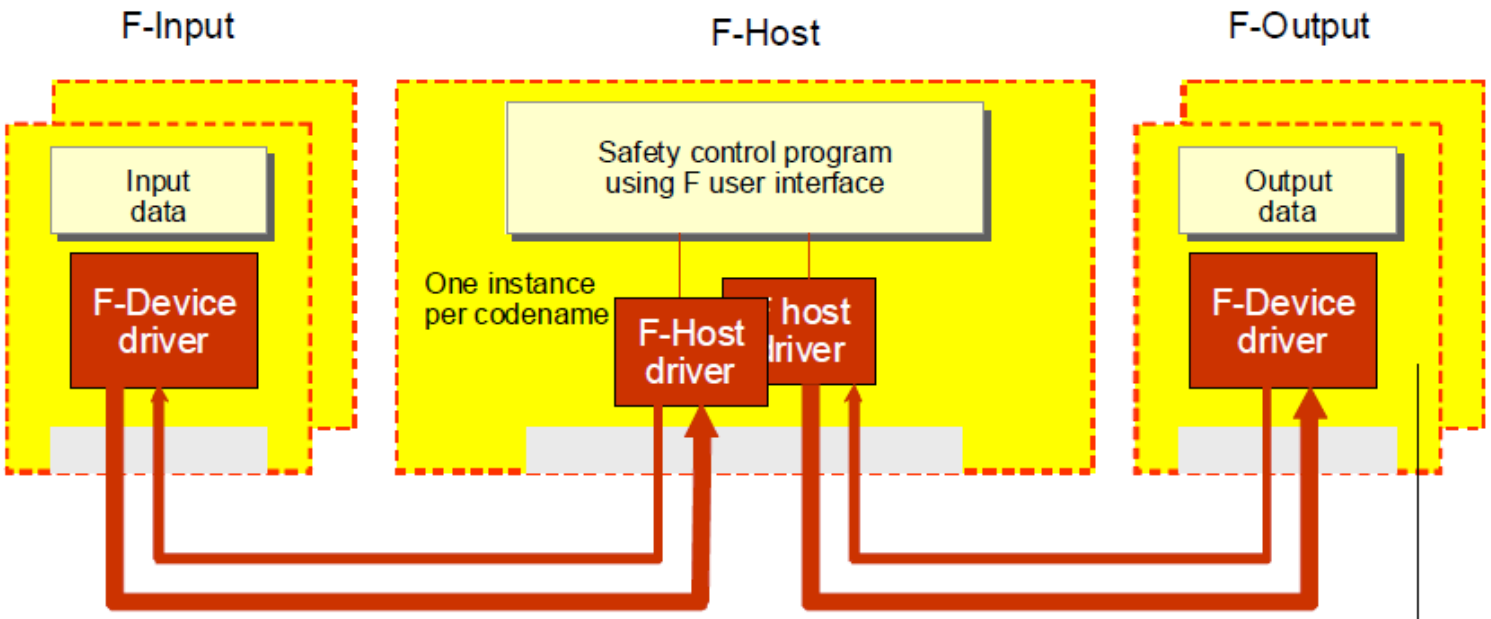
Modello di comunicazione D



Si raddoppia unicamente lo stack di sicurezza e vengono inviati 2 Messaggi di safety

Cross check a tutti i livelli del messaggio di sicurezza

Struttura della comunicazione



F-I/O data + safety code

Safety code

Preconditions for an encapsulated FSCP 3/1 transmission system:

- Authorized access only
- Error detection mechanisms of transmission media not necessarily known and well defined
- Sufficient availability

Additional measures in a device in order to achieve a required SIL. E.g. for SIL3 a second micropro-cessor and compare facilities

Servizi F-Host

F-Host

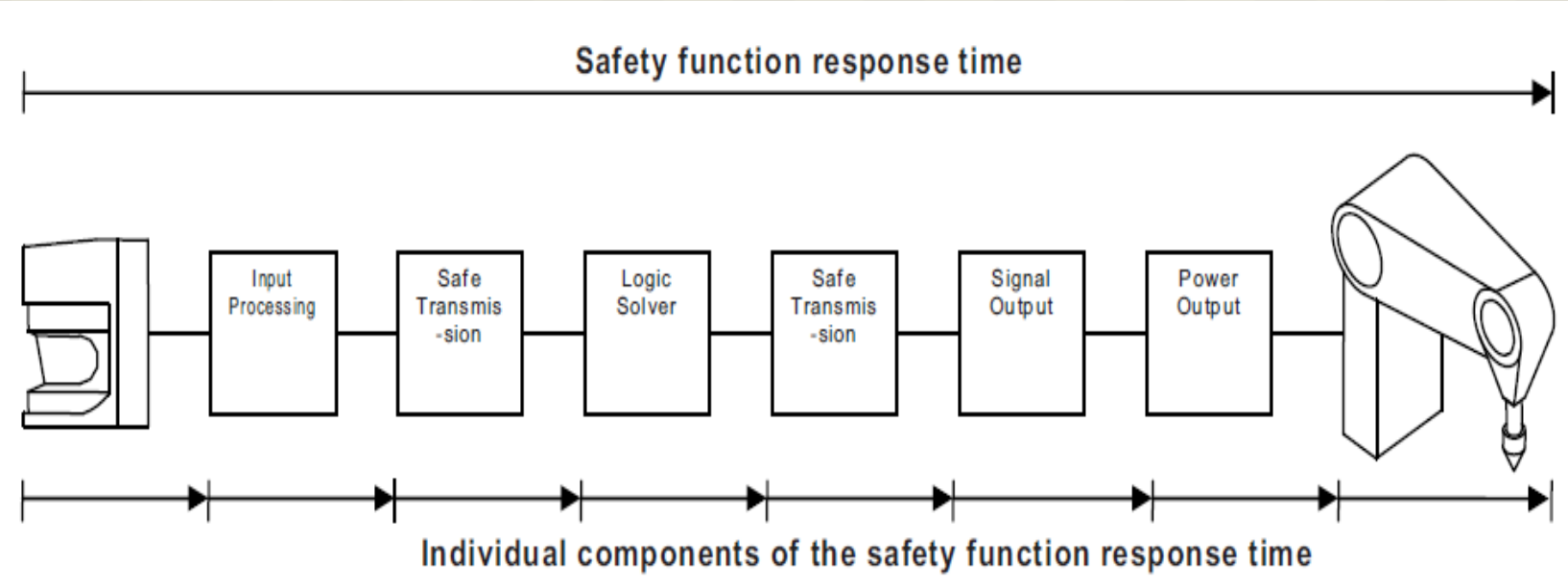
- Durante start-up valori settati a valori fail-safe
- Durante un errore valori settati a valori fail-safe
- Possibilità di attivare safe state che non siano la de-energizzazione, ma un rallentamento
- Un errore di comunicazione dello stack di safety causa il passaggio allo stato di fail-safe

Servizi F-Device

F-Device

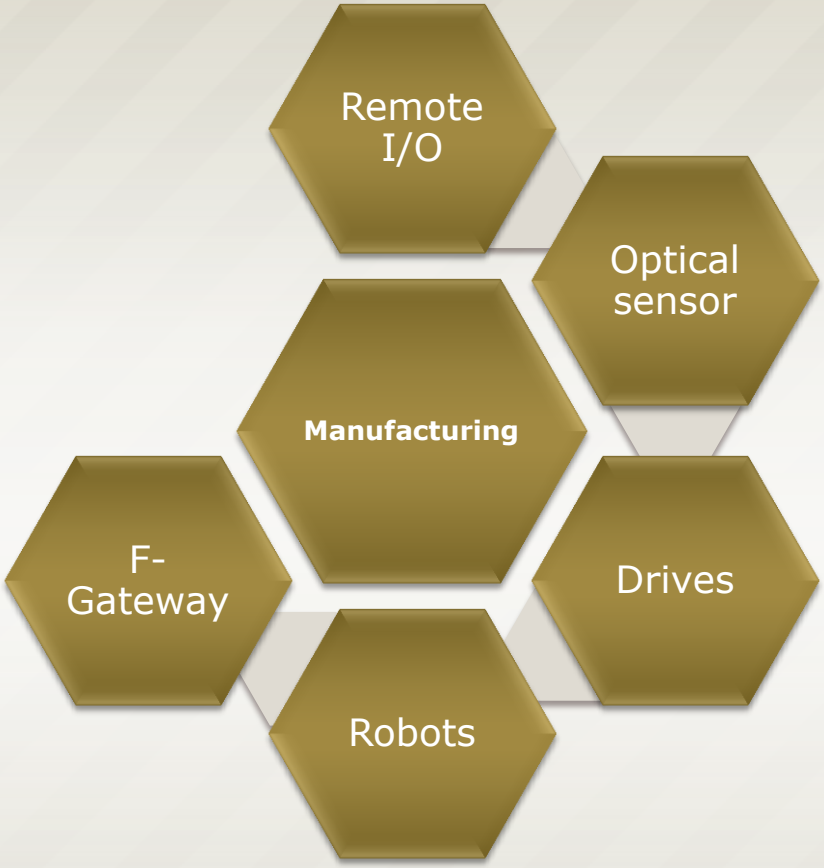
- Possibilità di attivare e riportare valori fail-safe
- Riportare al F-Host i guasti avvenuti sul device
- Configurazione dei parametri legati alla safety durante lo start-up

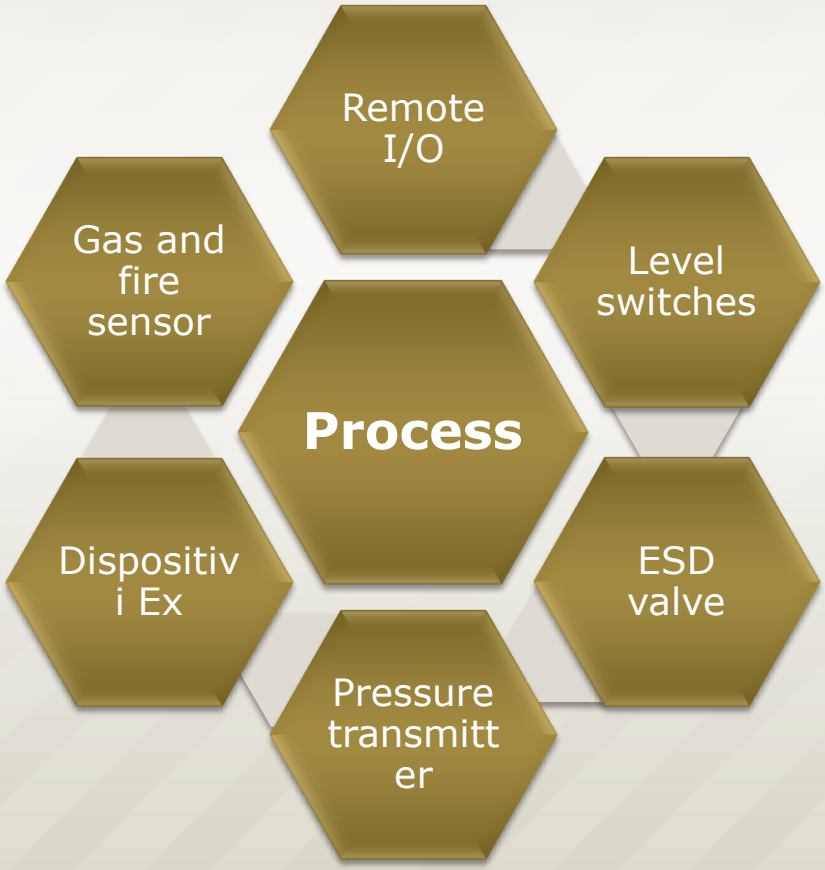
Response time



Permette di calcolare il caso peggiore nel tempo di risposta di una certa funzione di sicurezza.

Famiglie di F-Device





Conclusioni

La sicurezza corre

Anche sul fieldbus