FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE

CONFINDUSTRIA

DAL 1945 IL VALORE DELL'INNOVAZIONE

Dispositivi di comando e controllo

Reti di sicurezza

Reti di Sicurezza

- Consentono di gestire le funzioni di Sicurezza con la stessa tecnologia che è oggi tipica dell'Automazione Standard

  => Soluzione Integrata per Automazione Standard e Safety

- Esistono diversi consorzi con soluzioni e caratteristiche differenti

Reti di Sicurezza

- Soluzioni Standard “tollerano” certi errori
  - La gestione errori che è tipica delle reti Standard non è sufficiente per le applicazioni Safety per es. in SIL3
  - Reti Standard non sono necessariamente insicure ma per le soluzioni Safety sono richieste misure addizionali per raggiungere un livello di copertura più elevato
  - PFD (**P**robability of **F**ailure on **D**emand) insufficiente per le applicazioni di sicurezza
- Soluzioni Safety devono rilevare e gestire gli errori portando il sistema in stato “Sicuro”

Reti di Sicurezza

Protocollo Safety

fornisce misure che garantiscono un alto livello di integrità

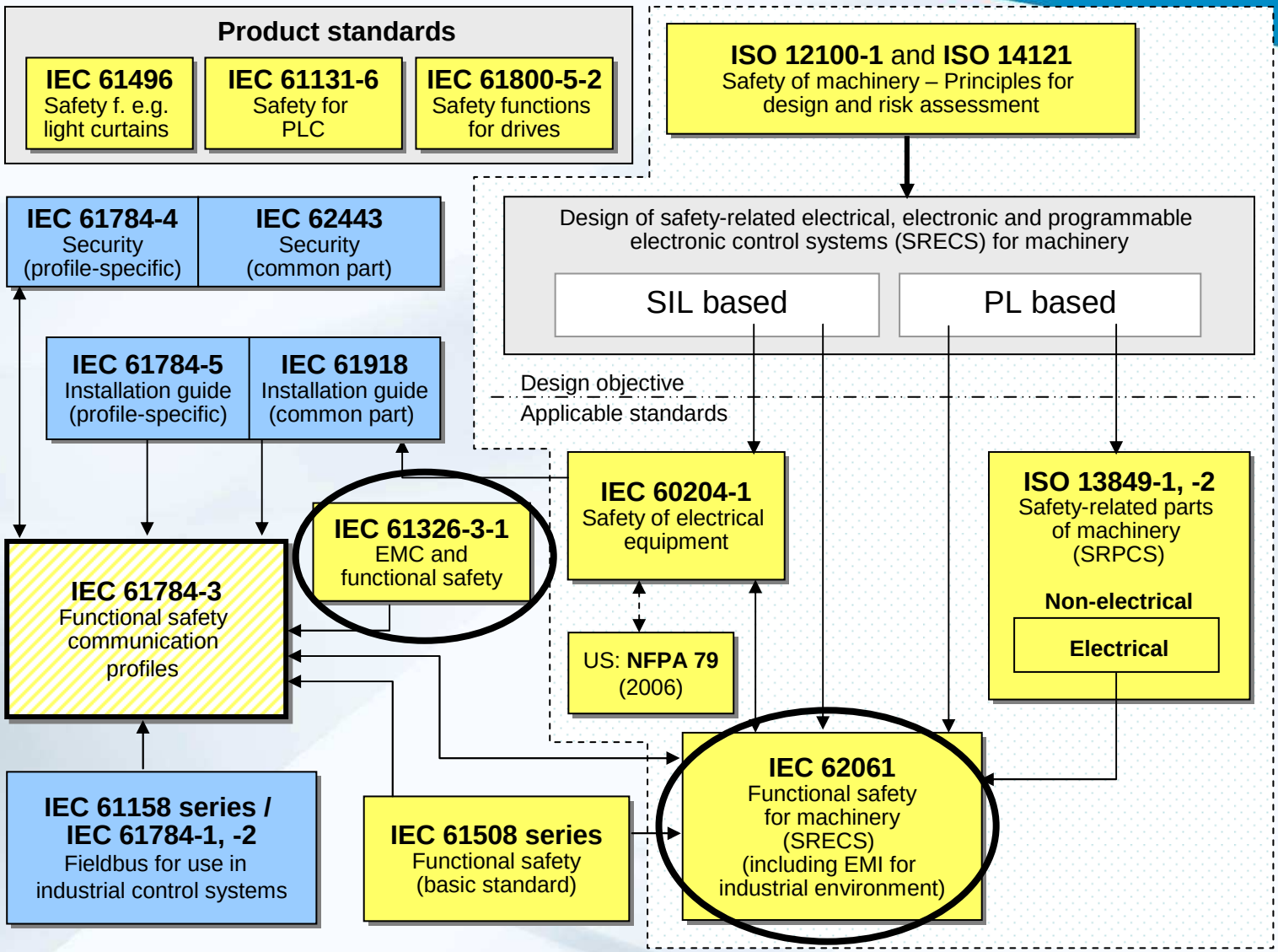
- Opera correttamente con alto livello di Sicurezza

oppure

- Si porta in uno stato ben definito, cioè Sicuro

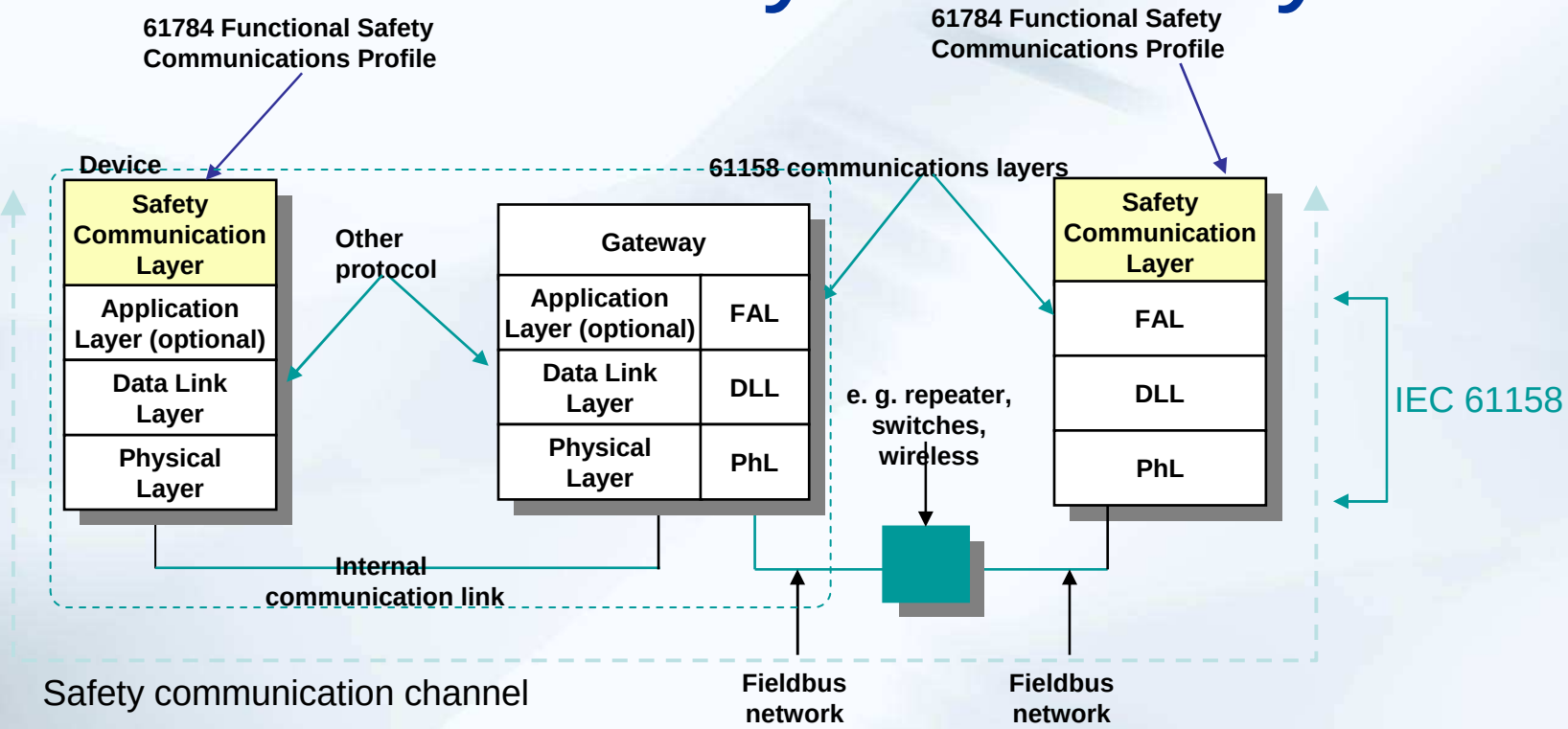
Caratteristiche del Bus di Sicurezza

- Certificazione Safety SIL3 / IEC 61508 e Cat 4 / EN 954-1
- Può essere una soluzione aperta “Multi-vendor” con protocollo di comunicazione indipendente
- Messaggi Standard e Safety sulla stessa rete
- Architettura di rete per accesso alle informazioni standard e safety
- Flessibilità: differenti architetture senza modifiche nella task di controllo
  - Safety e Standard sullo stesso cavo
  - Safety e Standard su cavi separati
  - Possibilità di modifiche successive

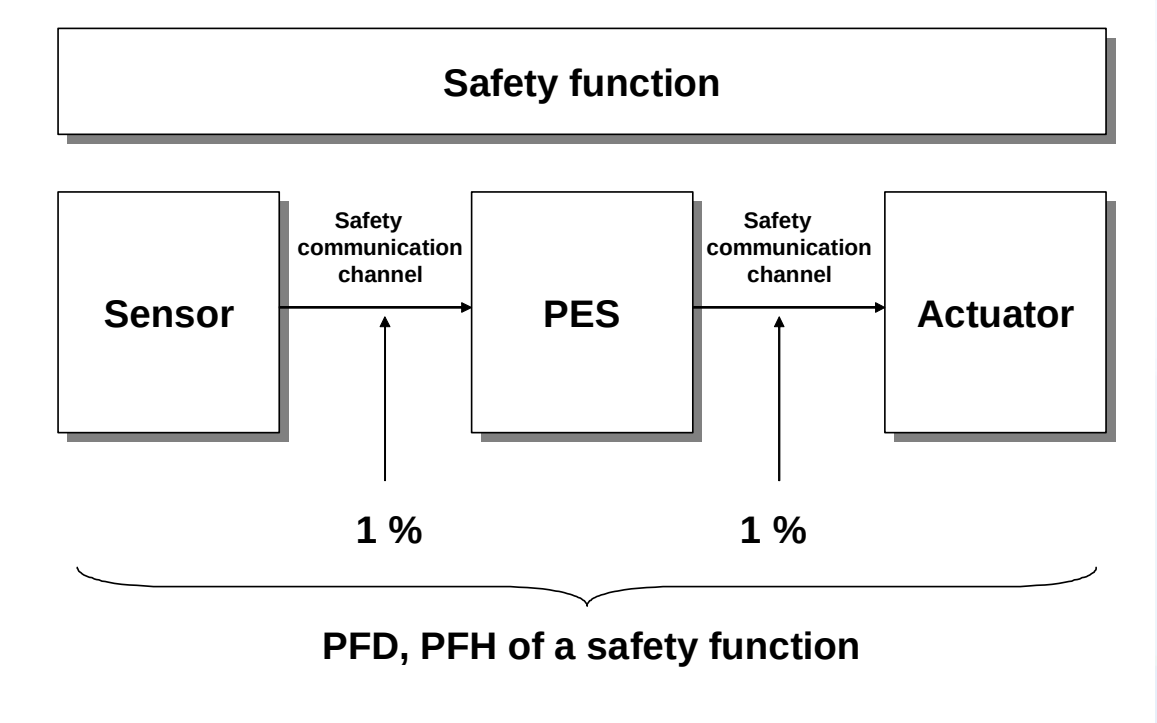


Applicabile alle macchine (altro set di standards per processo)

Functional safety comm. system

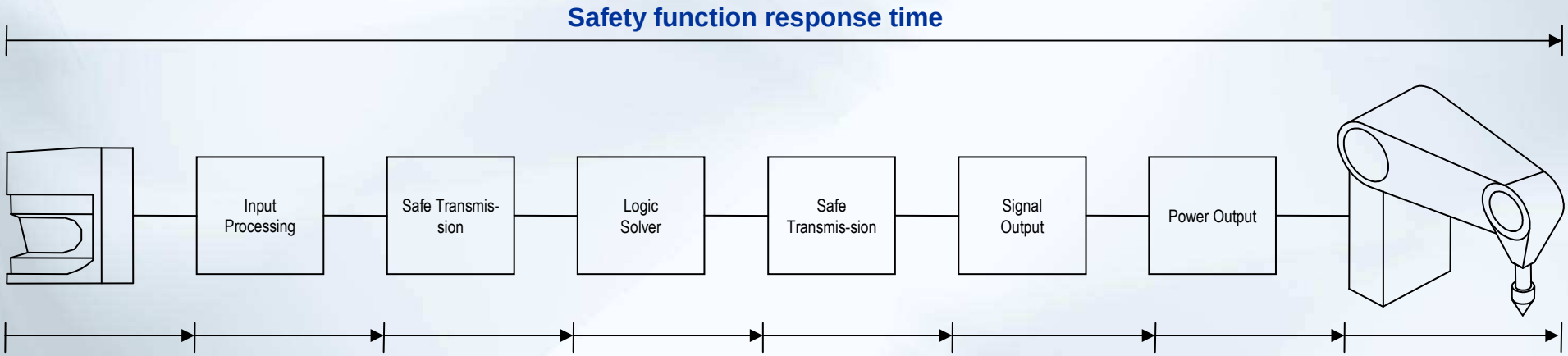


- Functional safety in IEC 61784-3
  - Sono basati su sistemi fieldbus “standard” specificati in IEC 61158
  - Definisce un addizionale “safety communication layer” per realizzare tutte le misure necessarie per implementare la trasmissione dei dati Safety in accordo alla IEC 61508



- Il sistema di comunicazione trasmette dati safety
- Il canale di comunicazione safety non deve consumare più del 1% del massimo PFD o PFH (probability of failure) dell'obiettivo SIL per il quale il profilo di comunicazione della sicurezza funzionale è progettata => funzioni di sicurezza SIL3 devono assicurare che PFH e così il tasso di errore residuo per ora del sistema di comunicazione safety non superi 10^{-9} per ora

Safety function response time

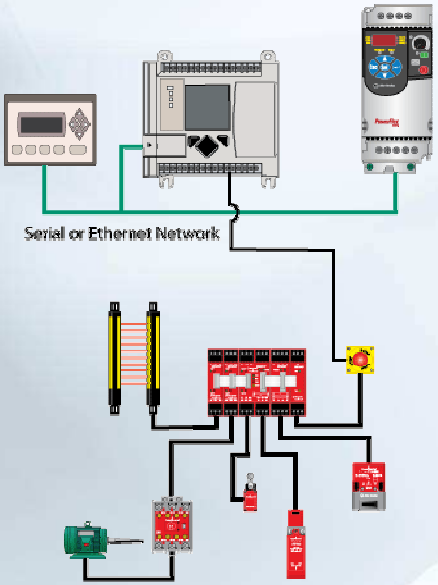


Errori e misure di sicurezza

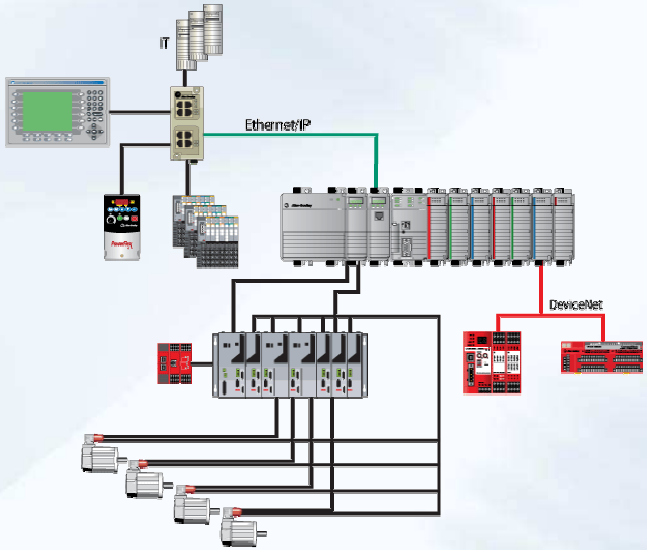
Errori	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption					X	X	only for serial bus	
Unintended repetition	X	X					X	
Incorrect sequence	X	X					X	
Loss	X				X		X	
Unacceptable delay		X	X					
Insertion	X			X	X		X	
Masquerade				X	X			X
Addressing				X				

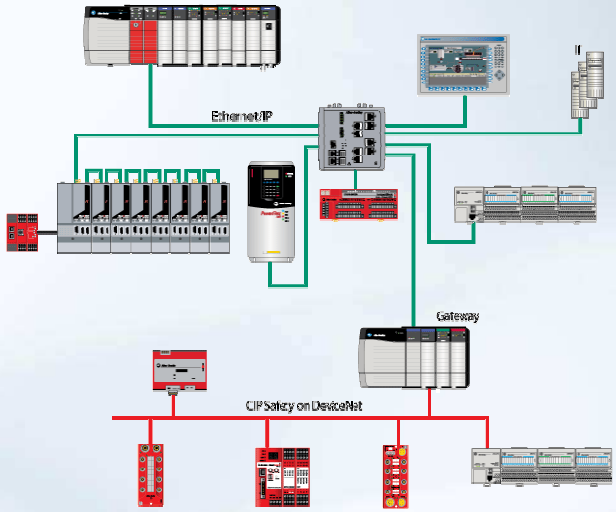
Integrazione della sicurezza

Architettura semplice



Architettura integrata

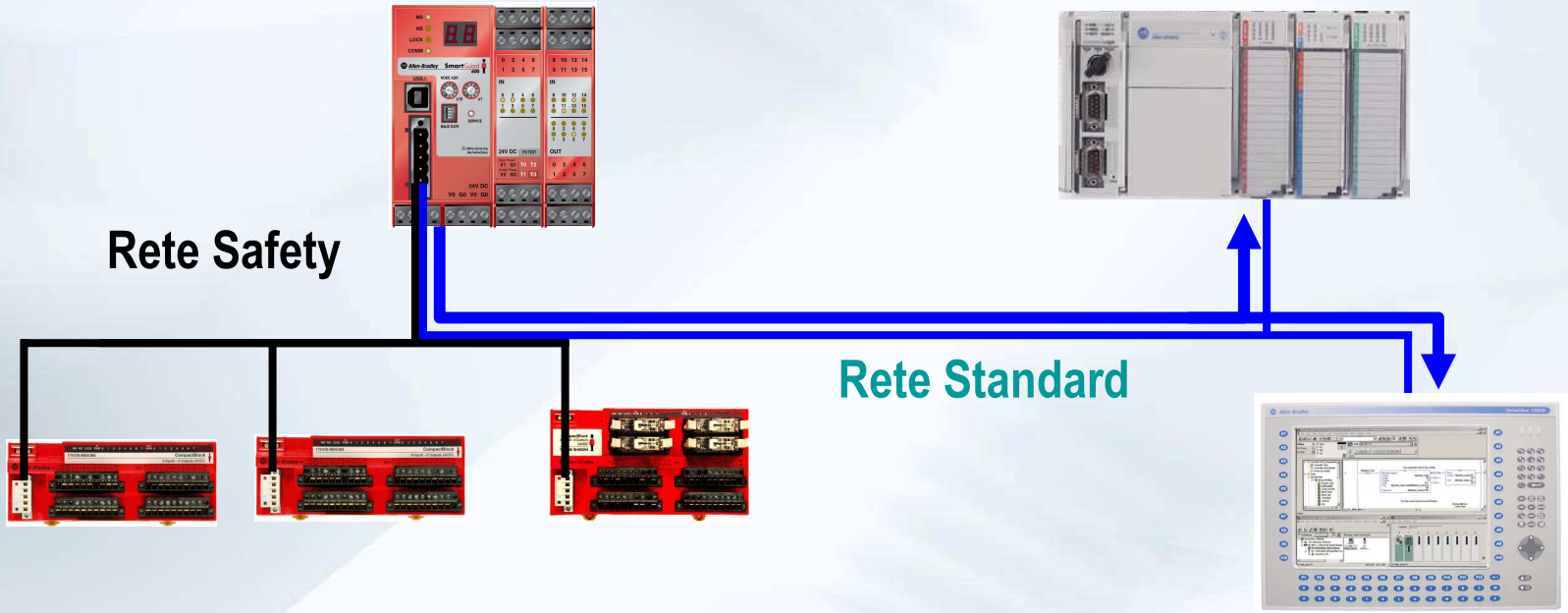




Low ← **Integrazione** → **High**

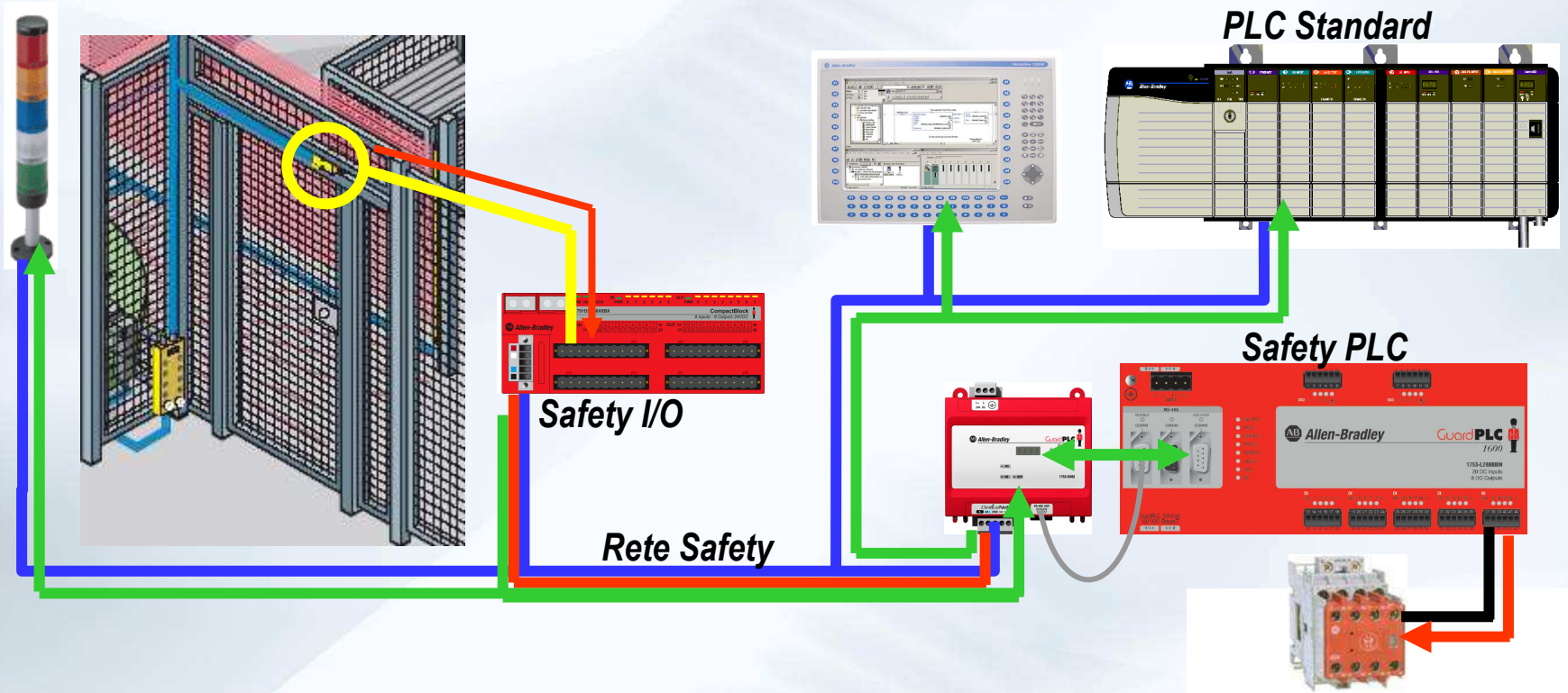
Trasferire lo stato del sistema Safety al resto del sistema

- Sistema di Sicurezza coordinato con il Sistema di controllo standard
- Visualizza lo stato del sistema di sicurezza su HMI per aumentare la diagnostica e migliorare gli interventi di riparazione

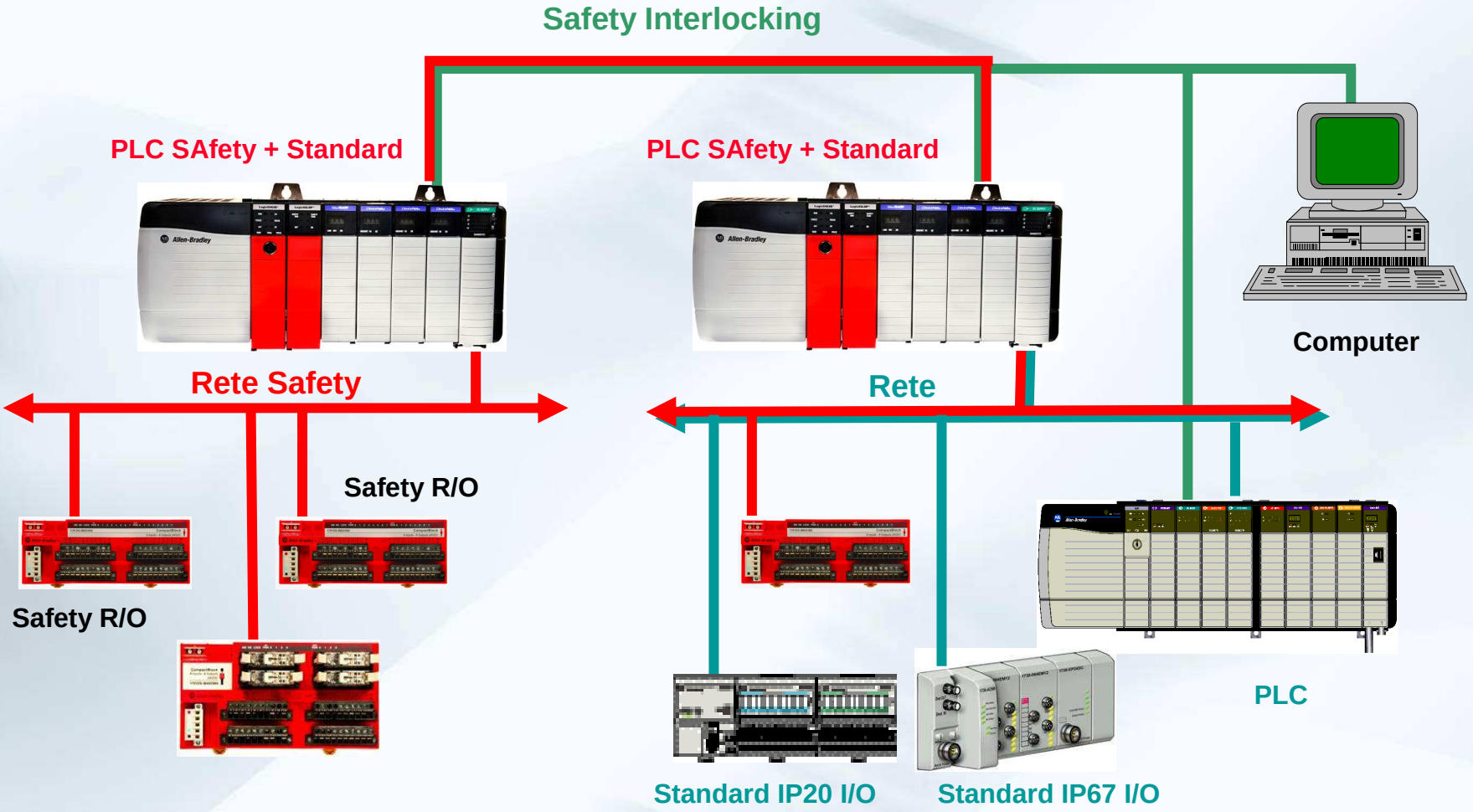


Rende la macchina più produttiva!

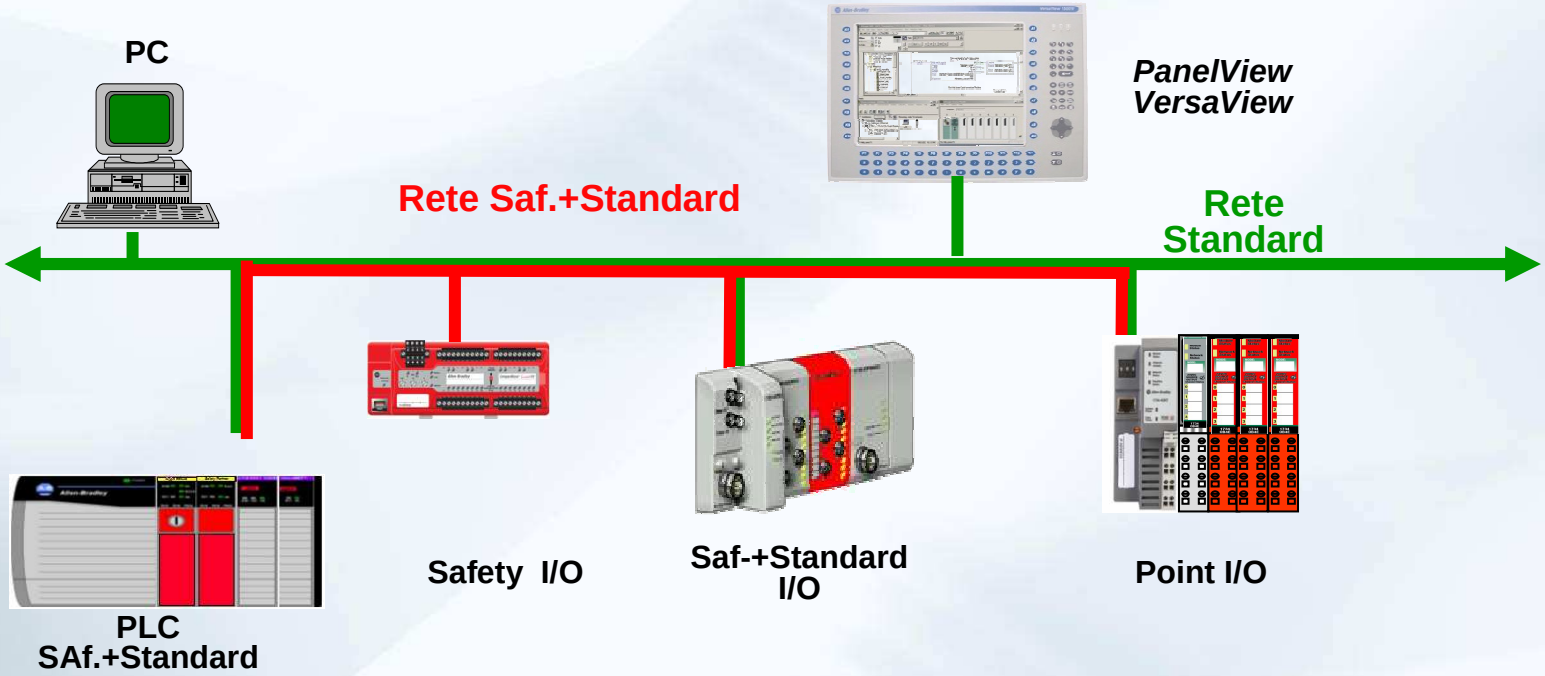
Esempio: Perchè Rete Standard & Safety



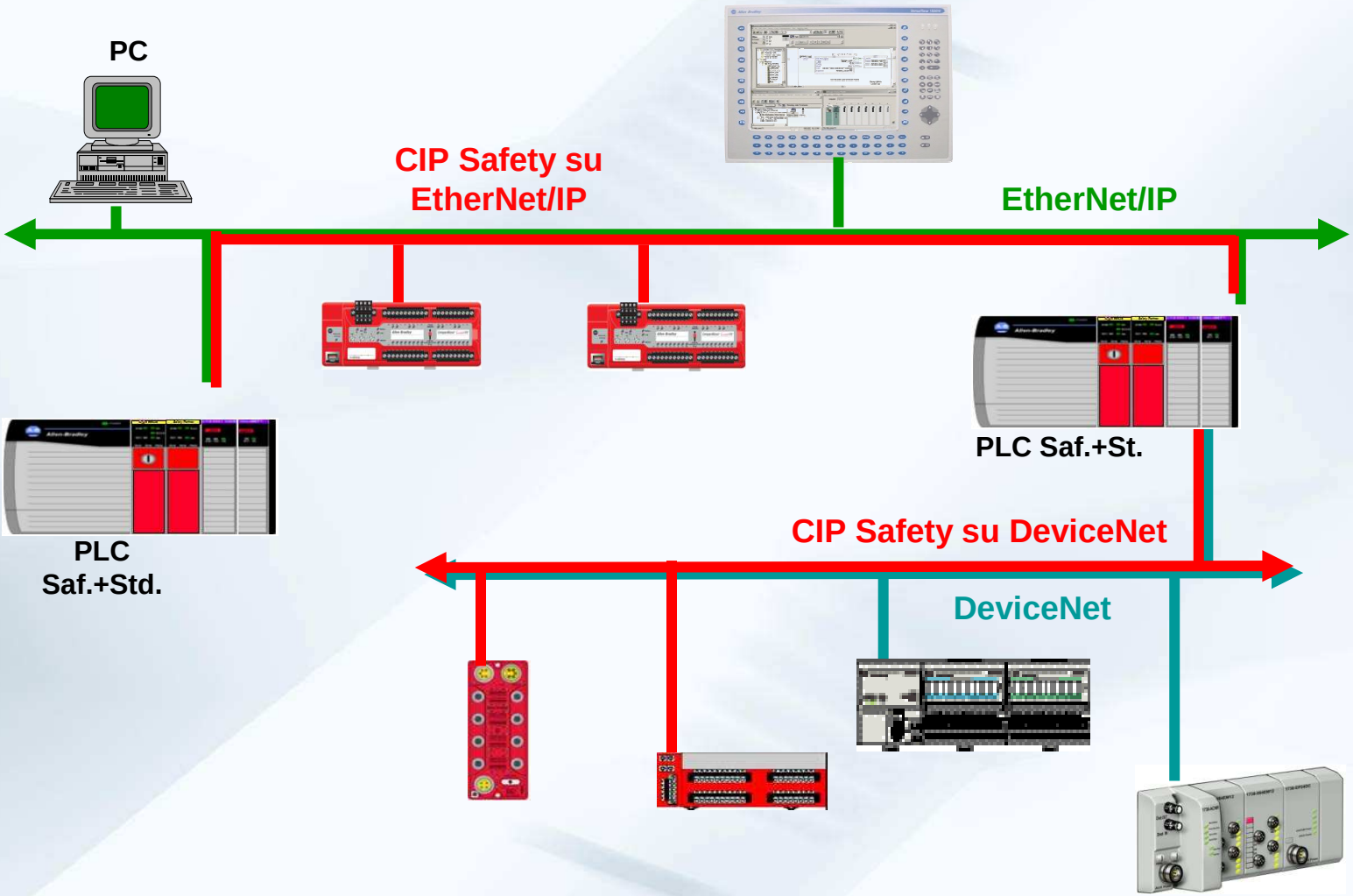
Esempio di Architettura



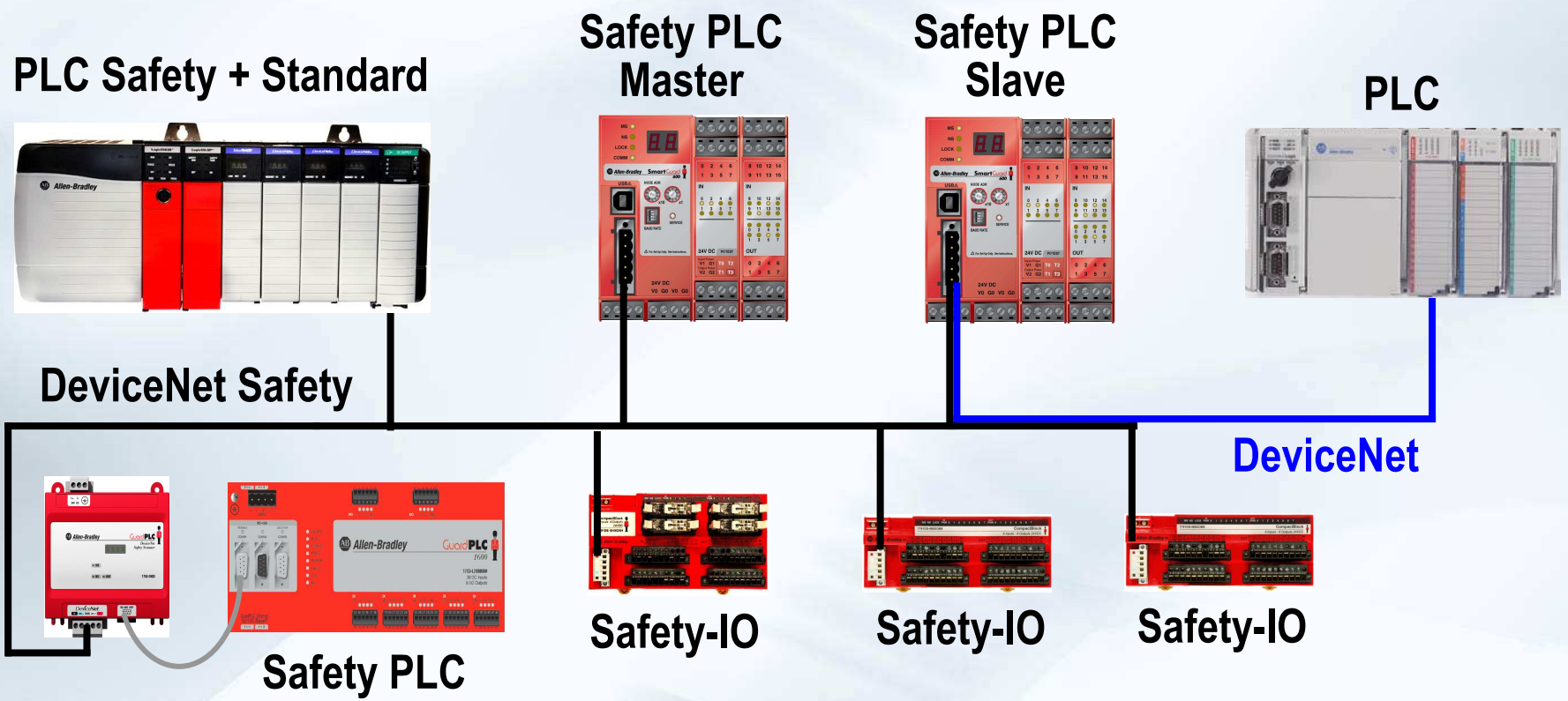
Esempio di Architettura



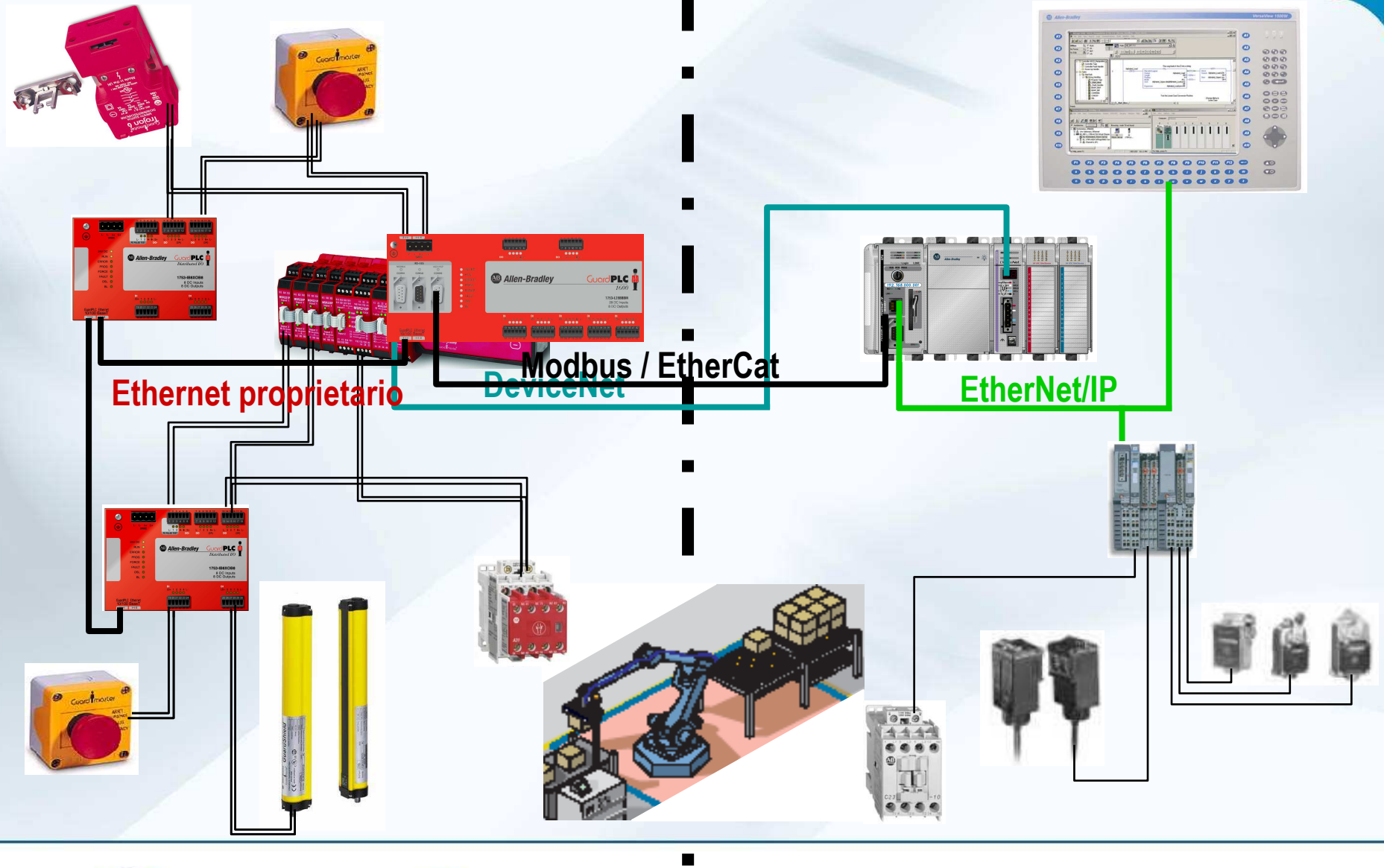
Esempio Architettura



Esempio Architettura



Esempio di Architettura di controllo con 2 o 3 reti separate



Esempio di Architettura di controllo con 2 o 3 reti separate

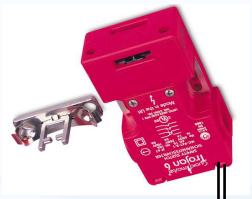
Vantaggi

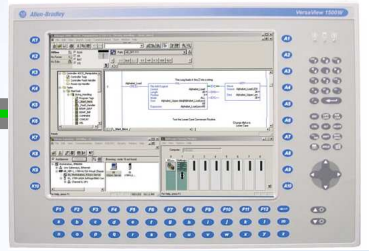
- Comunicazione dello stato del sistema di sicurezza tramite la rete in alternativa al cablaggio
- Sono richiesti meno I/O standard
- Riduzione di cablaggio
  - Minori costi di installazione
  - Più facile manutenzione
  - Maggiore produttività della macchina
  - Più semplice ri-assemblare dopo lo spostamento della macchina

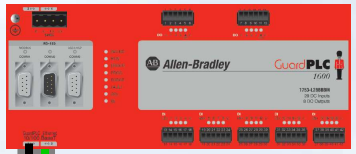
Svantaggi

- 2 o 3 reti separate da gestire
  - Maggiore competenza del personale di manutenzione
  - Maggiori parti di ricambio
- In molti casi la rete di sicurezza è proprietaria e richiede HW dedicato
  - Aumento dei costi di installazione
- Utente deve gestire la sicurezza su una rete

Esempio di Architettura di controllo con 1 rete e 2 protocolli

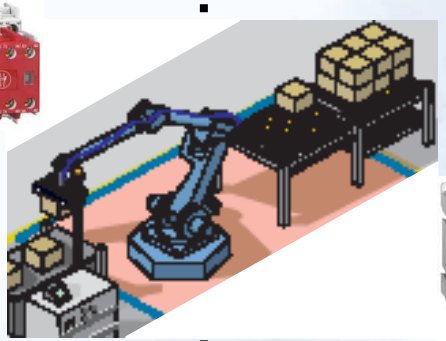






Ethernet proprietario

EtherNet/IP



FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

DAL 1945 IL VALORE DELL'INNOVAZIONE

AssoAutomazione
Associazione Italiana
Automazione e Misura

Esempio di Architettura di controllo con 1 rete e 2 protocolli

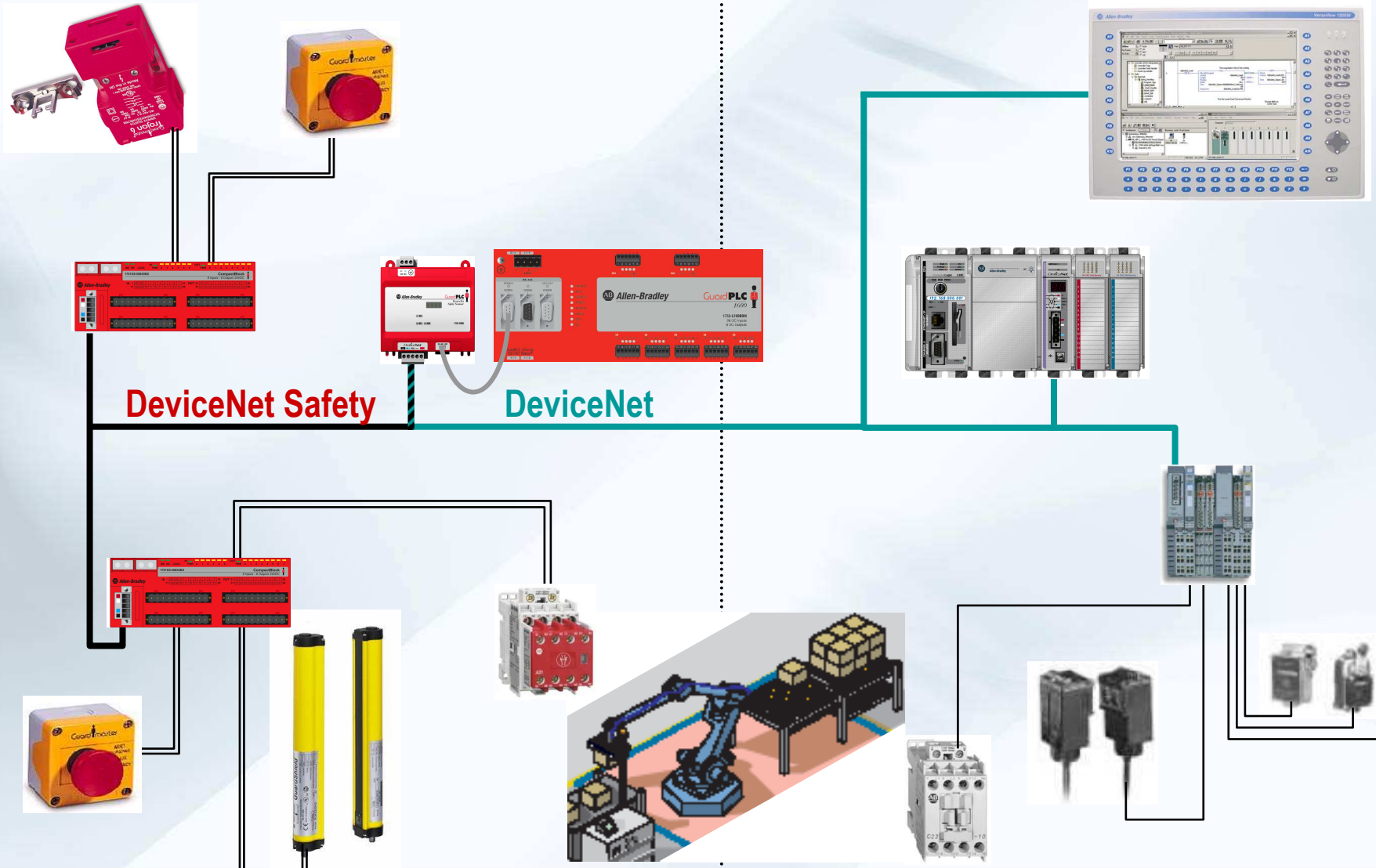
Vantaggi

- Una rete fisica da gestire
  - Poche parti di ricambio necessarie
  - Richiesta minore competenza del personale tecnico
  - Ethernet può utilizzare le infrastrutture del cliente già esistenti

Svantaggi

- Richiede ancora 2 sistemi separati per gestire la diagnostica

Esempio di Architettura di controllo con 1 rete e 1 protocollo



Esempio di Architettura di controllo con 1 rete e 1 protocollo

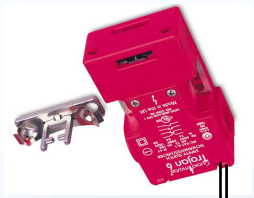
Vantaggi

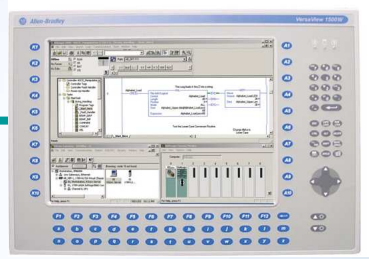
- Una sola rete da gestire
  - Servono solo poche parti di ricambio
  - Richiesta minore competenza da parte dei manutentori
- Un solo sistema di diagnostica
- CIP Safety è un protocollo aperto

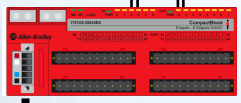
Svantaggi

- Richiede ancora due ambienti di programmazione separati

Esempio di Architettura di controllo con Integrazione totale

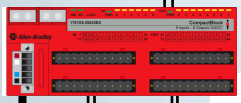


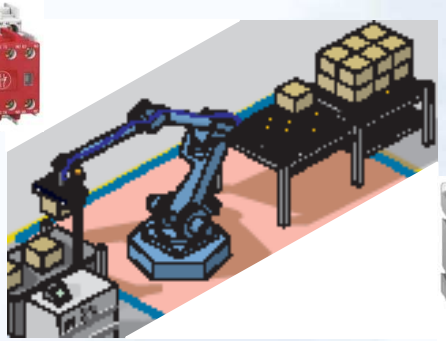




DeviceNet Safety

DeviceNet





ANIE FEDERAZIONE
FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA
DAL 1945 IL VALORE DELL'INNOVAZIONE

AssoAutomazione
Associazione Italiana
Automazione e Misura

Esempio di Architettura di controllo con Integrazione totale

Vantaggi

- Un solo HW per le parti safety e standard
- Un solo ambiente di programmazione
- Minori costi di installazione
- Minore costo di:
  - Training
  - Ricambi
  - Migliora la produttività

Svantaggi

- Perdita di ogni separazione fisica tra I sistemi di controllo safety/standard

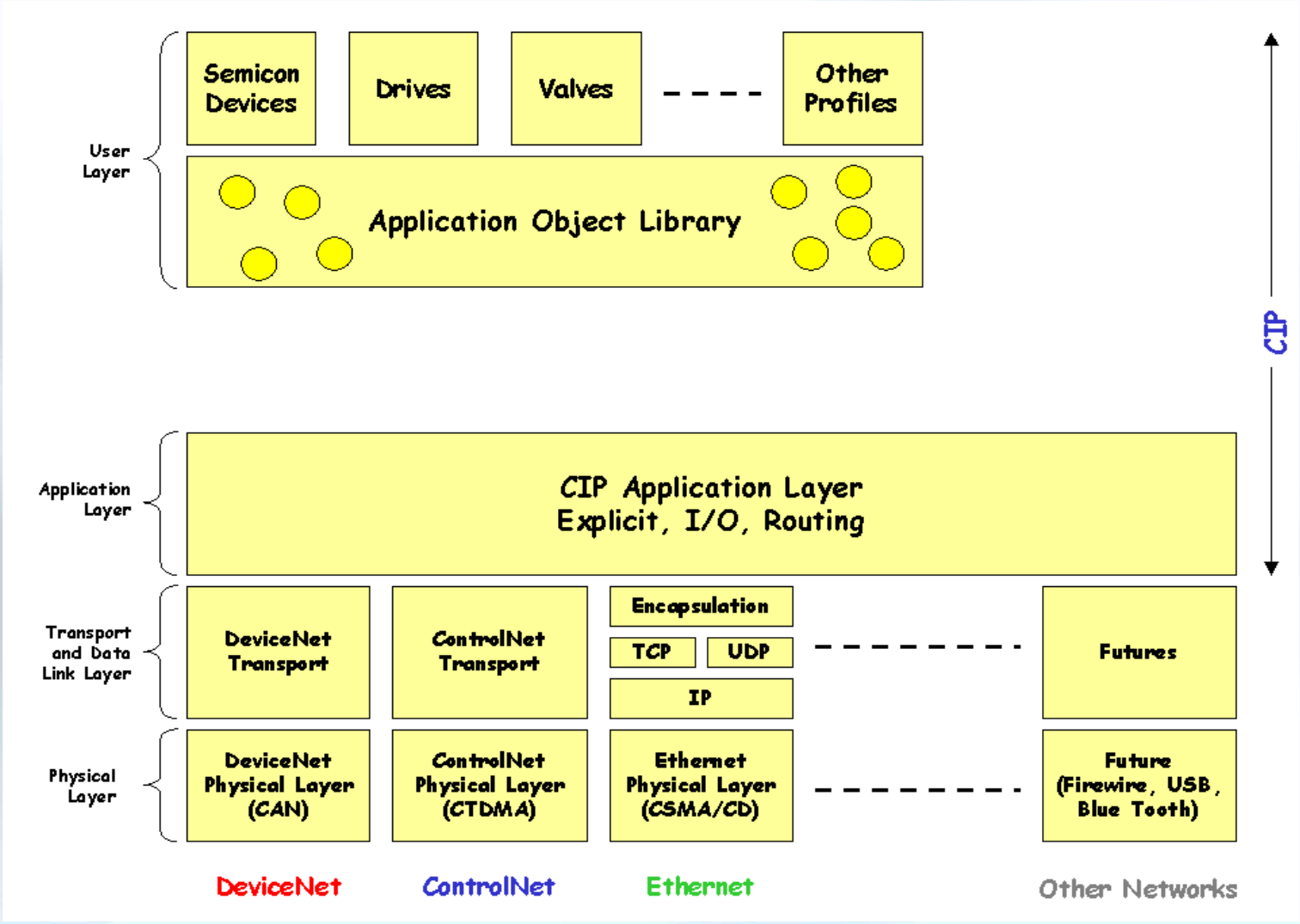
Safety Integrity Levels

Risk & Hazard

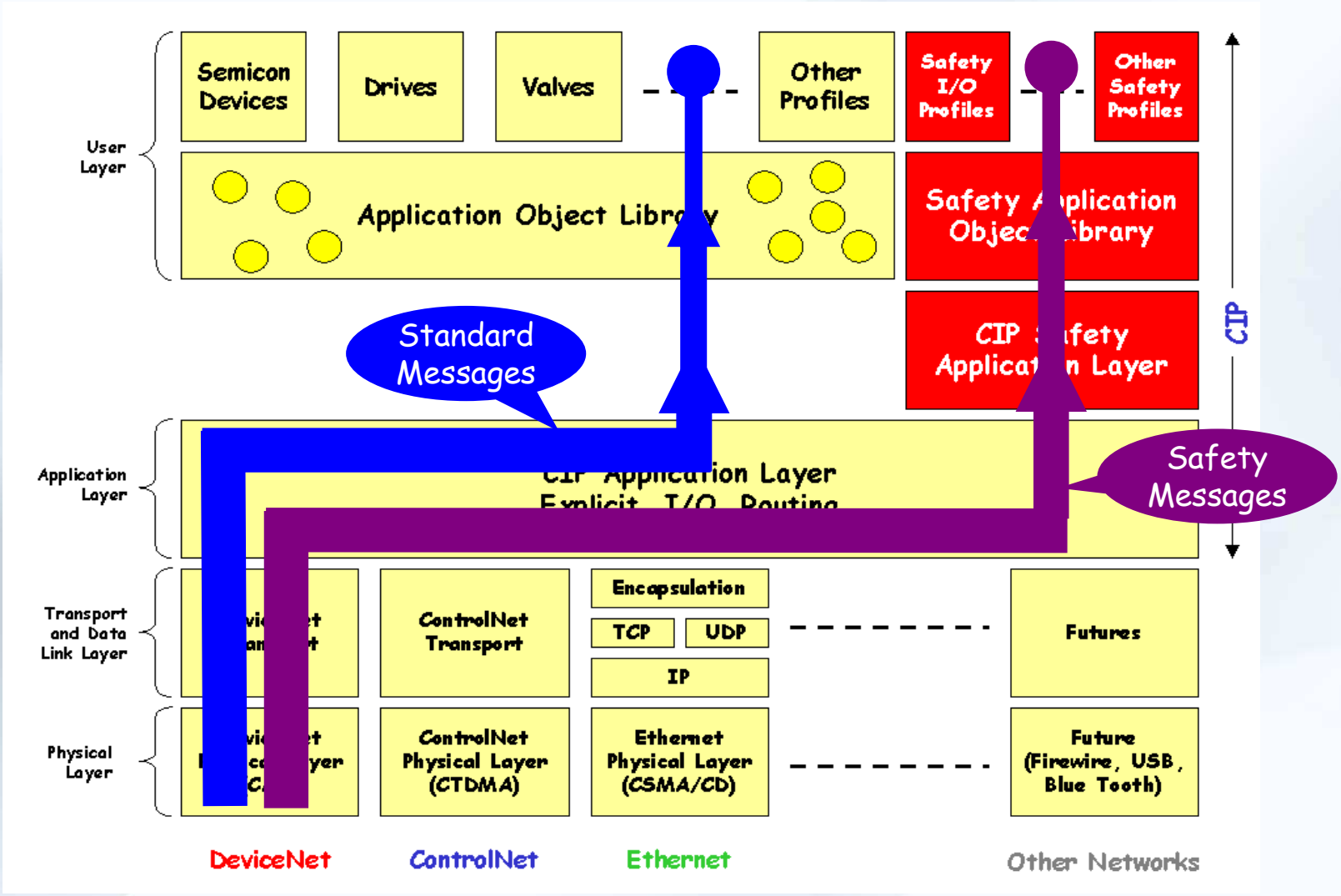
Safety Integrity Level	PFD Probability of failure on demand per year	1/PFD Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

Alcune reti di sicurezza sono certificate SIL3

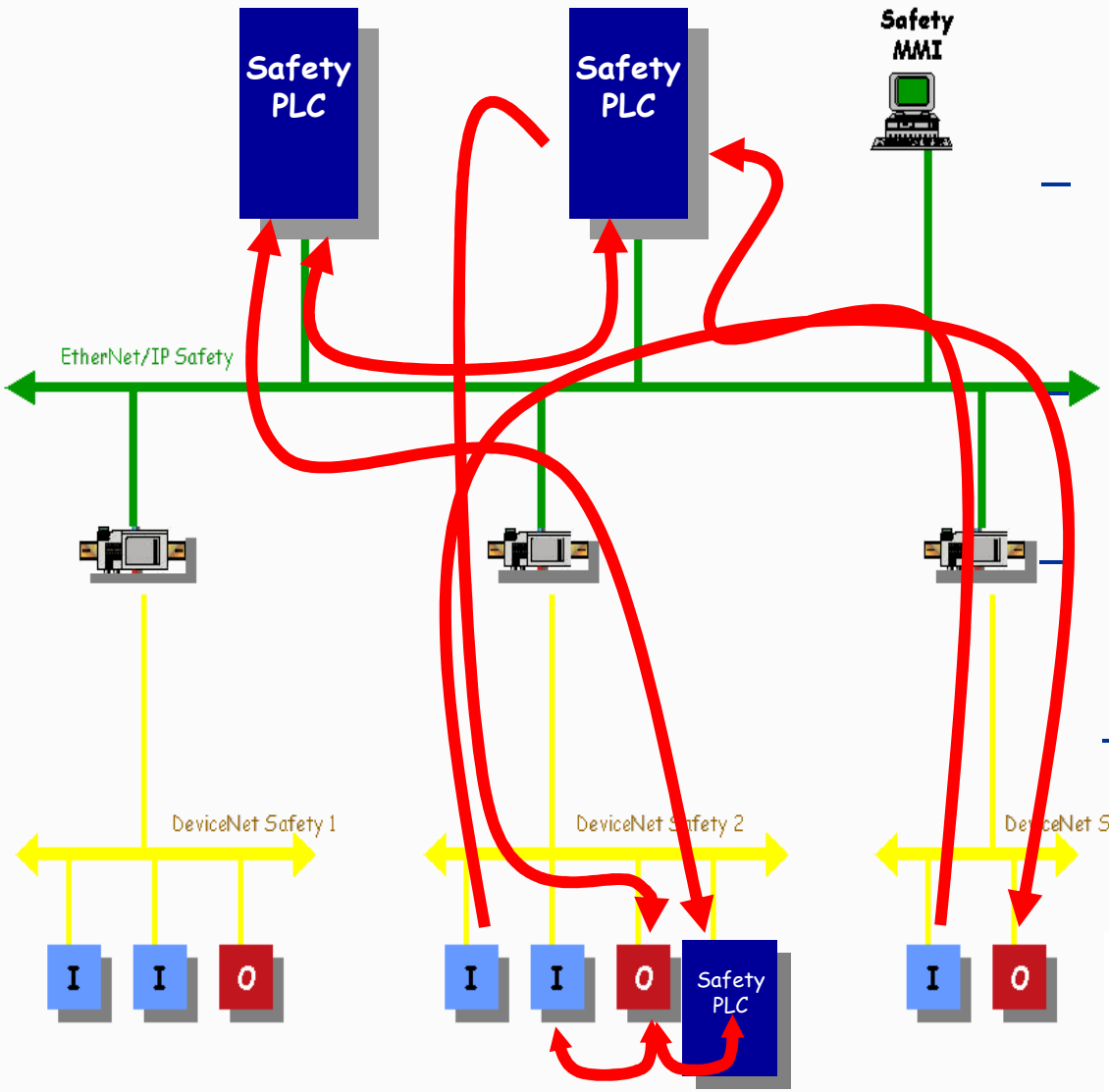
Esempio di rete Standard



Esempio di rete Safety

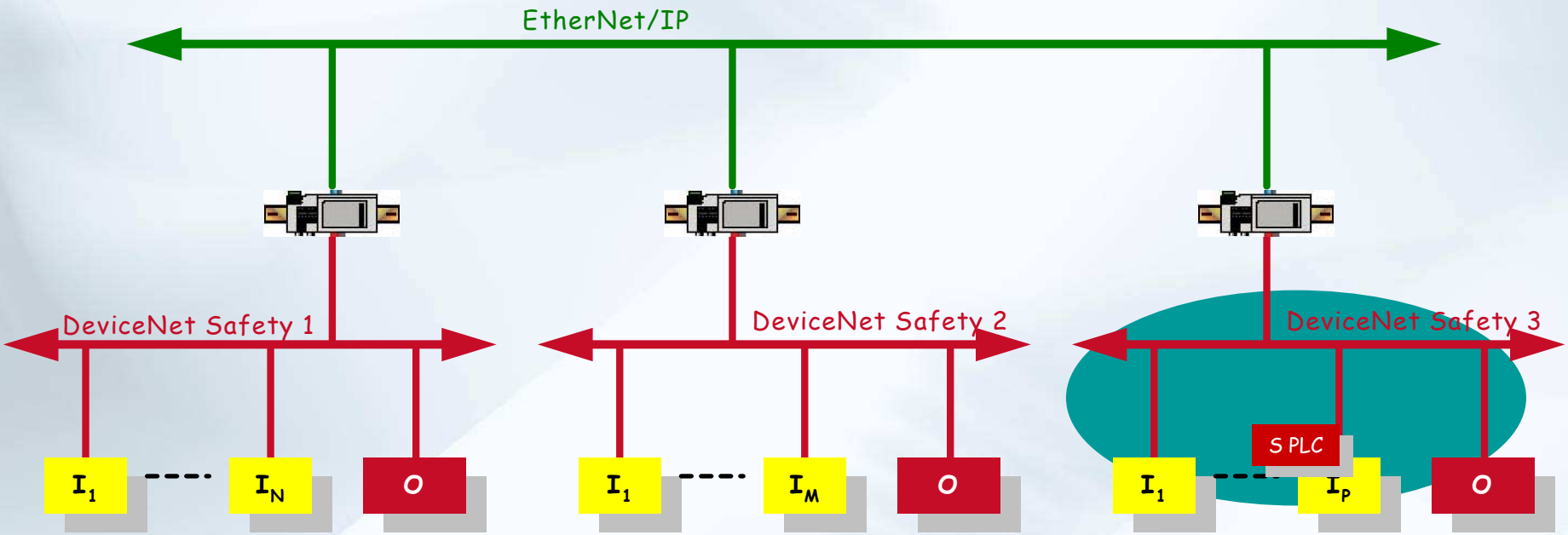


Protocollo Safety: Le possibilità sono senza limiti

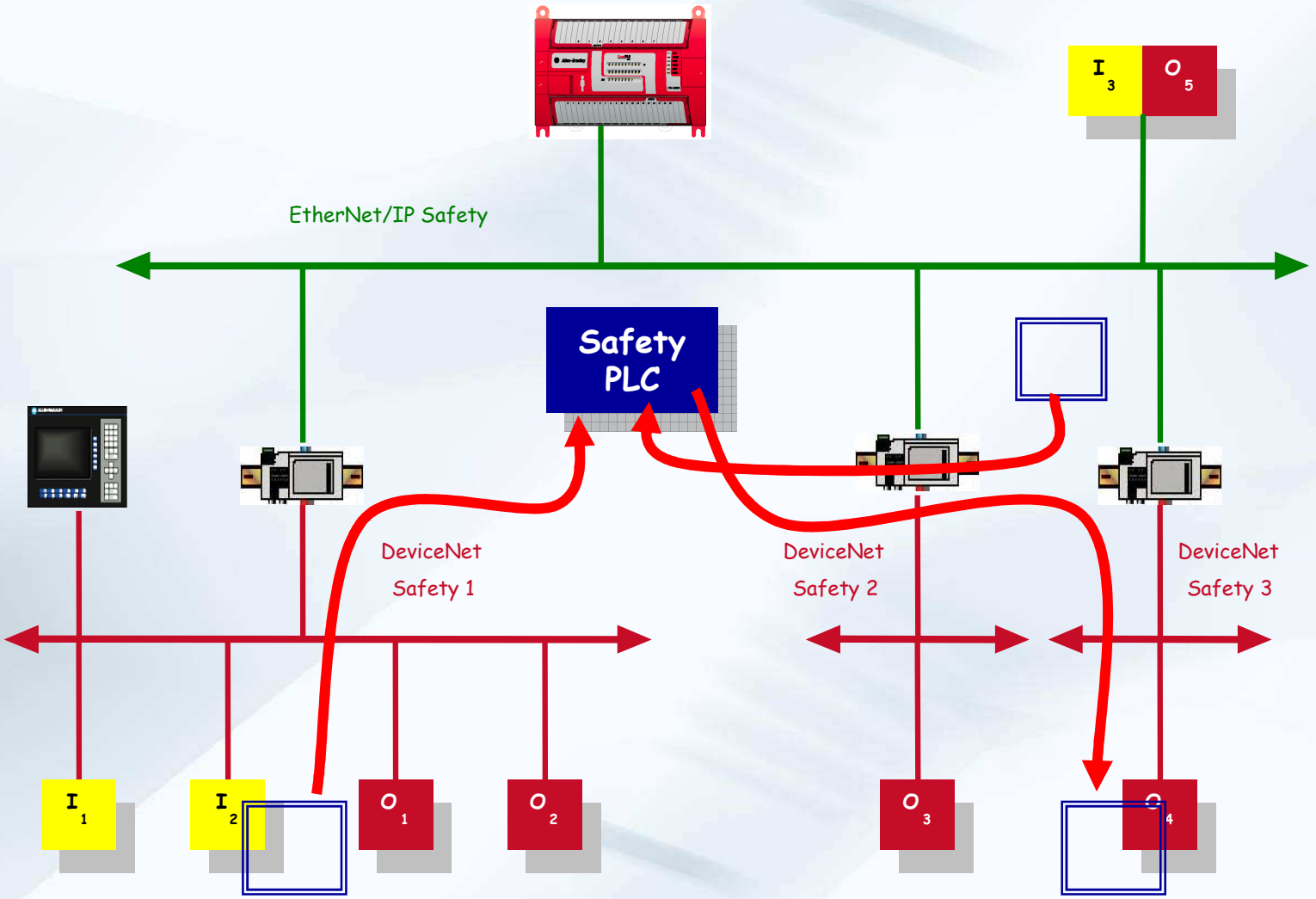


- **Comunicazione tra controllori su singolo collegamento**
- **Comunicazione tra controllori su collegamenti multipli**
- **Peer to peer comunicazione su un singolo collegamento**
- **Peer to peer comunicazione su collegamenti multipli**
- **Peer to peer comunicazione tramite controllore logico**

Esempio: Architettura Multi-Link



Esempio: Architettura Multi-Link



Esempio di certificazione per rete Safety

Certificato TUV Rhineland / Approvato da BGIA

Certificato:

- IEC-61508 (SIL3)
- EN954-1 (Cat 4)

TÜV Rheinland Group

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EL 373.00/06

Prüfgegenstand Product tested	CIP Safety Network protocol and network specification	Zertifikatsinhaber Licence Holder	ODVA 1099 Highland Drive, Suite A USA-Ann Harbor, Michigan 48108 United States of America
Typbezeichnung Type designation	CIP Safety on DeviceNet and CIP Safety on EtherNet/IP	Verwendungs-zweck Intended application	Specification to build CIP Safety devices for DeviceNet and EtherNet/IP
Prüfgrundlagen Codes and standards forming the basis of testing	IEC 61508 part 1 - 7:2000 EN 954-1:1996 GS-ET-26/05.02 "Principle rules for test and certification of bus systems for the transmission of safety relevant messages"		
Prüfungsergebnis Test results	The CIP Safety specification is in compliance with the requirements of the standards above up to and including SIL 3/Cat. 4 and enables vendors to build CIP Safety devices in compliance with these standards.		
Besondere Bedingungen Specific requirements	The design, development and suitability of devices for use in safety related applications has to be approved. The network conformance testing has to be performed for individual devices.		

Der Prüfbericht-Nr.: 968/EL 373.00/06 vom 2006-02-09 ist Bestandteil dieses Zertifikates.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. Es wird ungültig bei jeglicher Änderung der Prüfgrundlagen für den angegebenen Verwendungszweck.

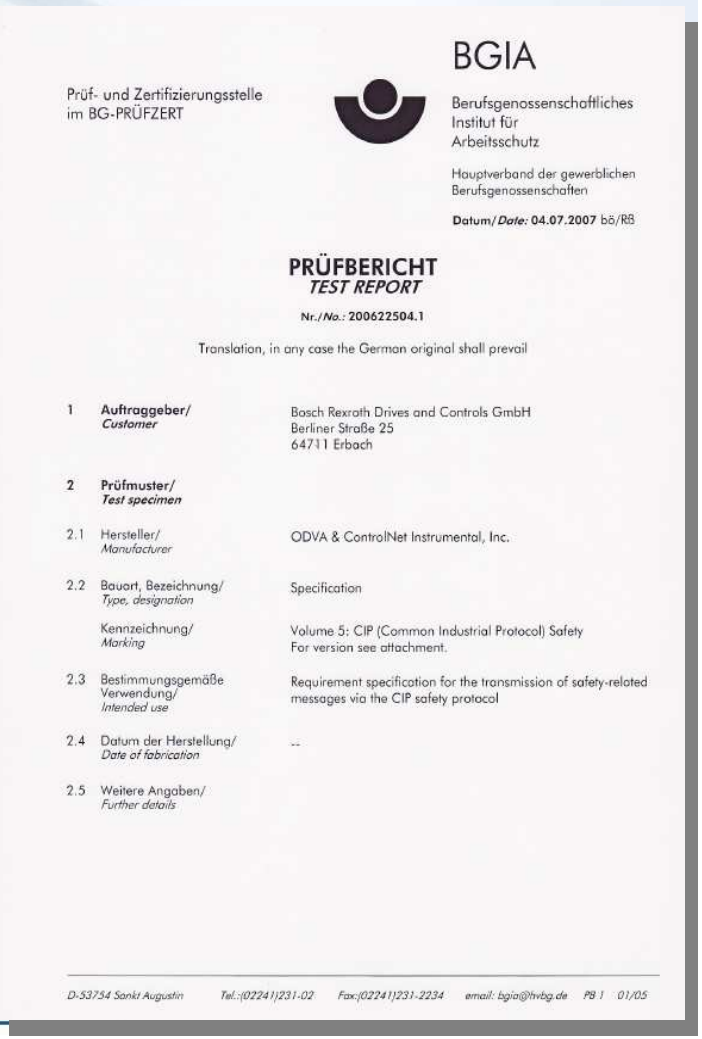
The test report-no.: 968/EL 373.00/06 dated 2006-02-09 is an integral part of this certificate.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

2006-02-09
Datum/Date

Firmenstempel/Company seal

Unterschrift/Signature



BGIA

Prüf- und Zertifizierungsstelle im BG-PRÜFZERT

Berufsgenossenschaftliches Institut für Arbeitsschutz

Hauptverband der gewerblichen Berufsgenossenschaften

Datum/*Date:* 04.07.2007 bö/RB

PRÜFBERICHT
TEST REPORT

Nr./*No.:* 200622504.1

Translation, in any case the German original shall prevail

1	**Auftraggeber/** ***Customer***	Bosch Rexroth Drives and Controls GmbH Berliner Straße 25 64711 Erbach
2	**Prüfmuster/** ***Test specimen***	
2.1	Hersteller/ *Manufacturer*	ODVA & ControlNet Instrumental, Inc.
2.2	Bauart, Bezeichnung/ *Type, designation*	Specification
	Kennzeichnung/ *Marking*	Volume 5: CIP (Common Industrial Protocol) Safety For version see attachment.
2.3	Bestimmungsgemäße Verwendung/ *Intended use*	Requirement specification for the transmission of safety-related messages via the CIP safety protocol
2.4	Datum der Herstellung/ *Date of fabrication*	--
2.5	Weitere Angaben/ *Further details*	

D-53754 Sankt Augustin Tel.:(02241)231-02 Fax:(02241)231-2234 email: bgia@hvbg.de PB 1 01/05

Una soluzione di sicurezza totalmente integrata