Embedded Networking Solutions

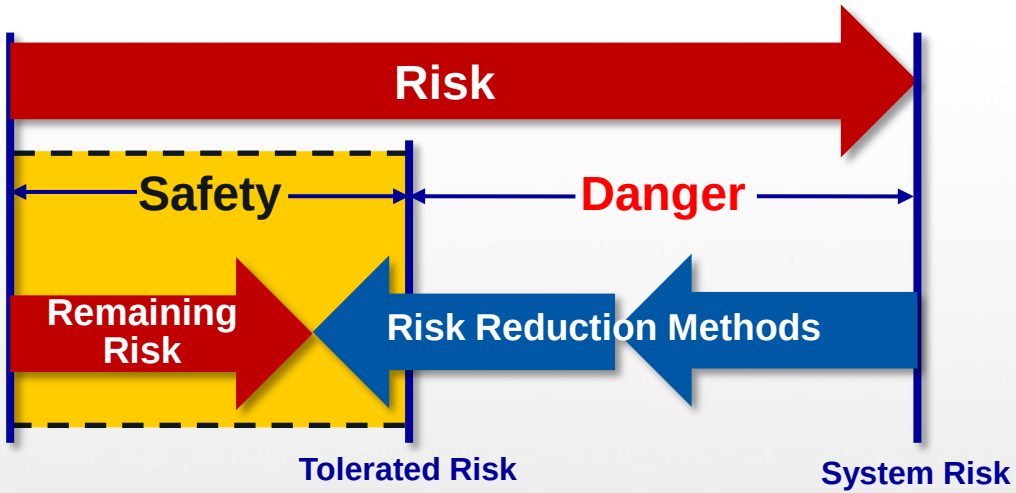
Twincomm

Safety communication over Industrial Ethernet

for embedded systems

Kurt van Buul
Twincomm

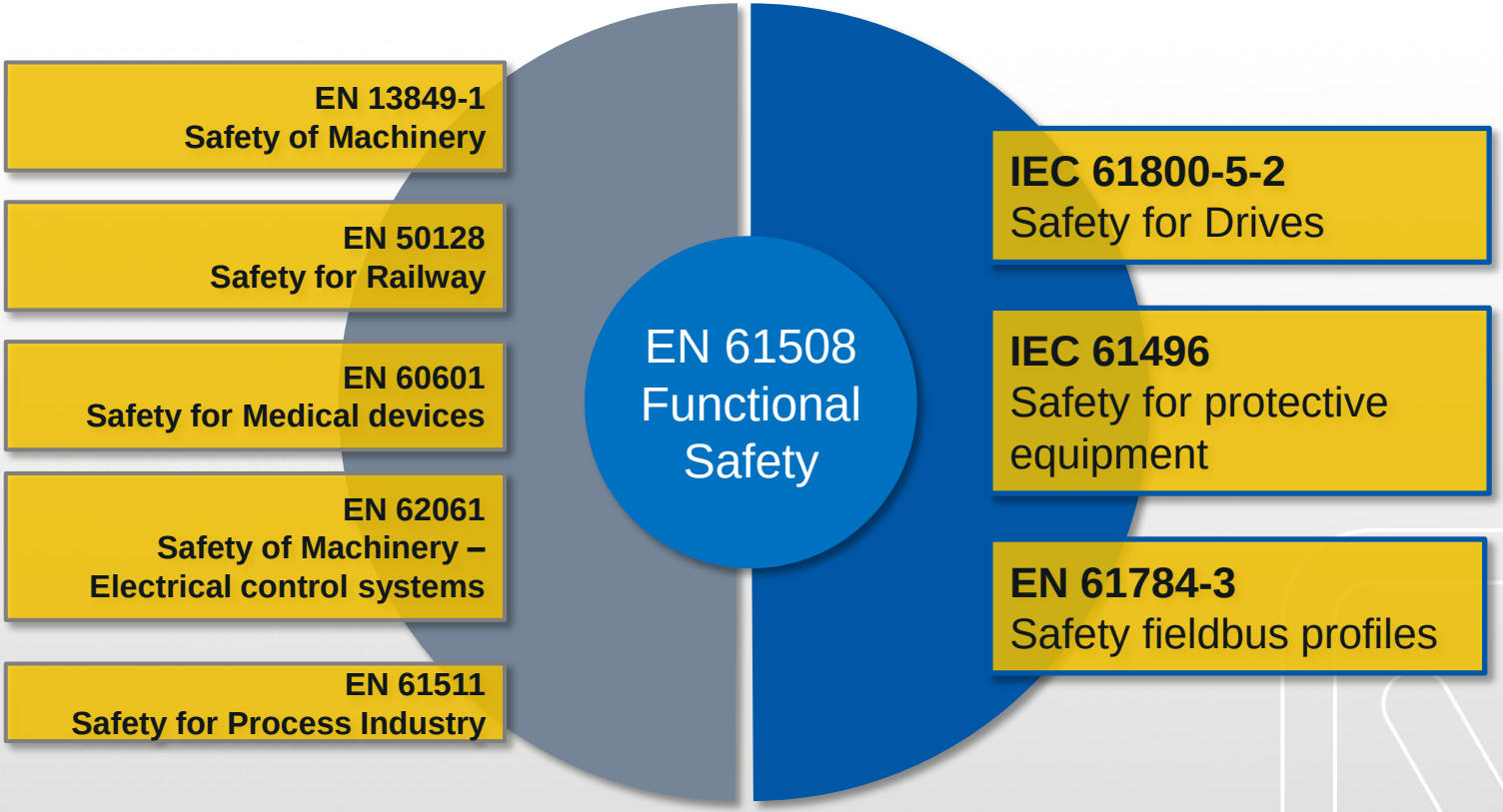
Safety - Some basics



Risk = Chance of a damaging event **x** Expected damage

Safety = Reduction of dangers for people and environment

Safety - Some basics



Safety Integrity Level (SIL) - EN 61508

SIL	Danger failure per hour[1]
1	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-8}$ to $< 10^{-7}$

One failure in ~1100 years

[1] High demand or continuous mode

Safety Integrity Level (SIL) - EN 61508

SIL	Danger failure per hour[1]	Assessment
1	≥ 10^{-6} to < 10^{-5}	Independent Person
2	≥ 10^{-7} to < 10^{-6}	Independent Departement
3	≥ 10^{-8} to < 10^{-7}	Independent Organisation

One failure in ~1100 years

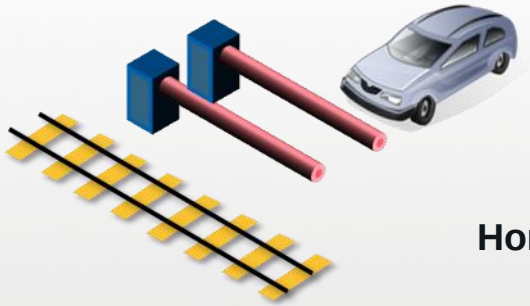
[1] High demand or continuous mode

Safety Lifecycle (EN 61508)

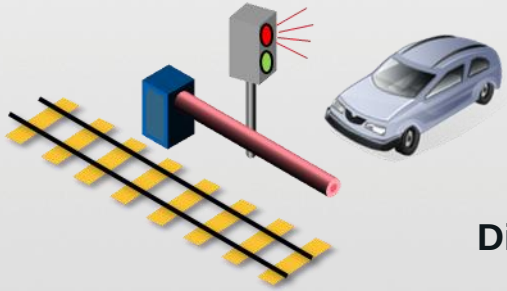
- Concept
- Field of Application
- Danger and Risk analysis
- Overall safety requirements
- Design of
  - overall operation and maintenance
  - overall validation
  - installation and putting into service
- Specification of safety requirements for the safety system
- Installation and putting into service
- Overall validation
- Overall operation, maintenance and repair
- End of life / decommissioning
- Modification and retrofitting

Safety - Some basics

Redundancy

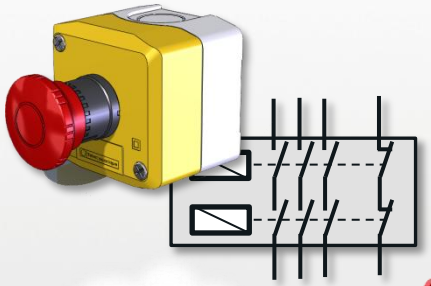


Homogeneous



Divers

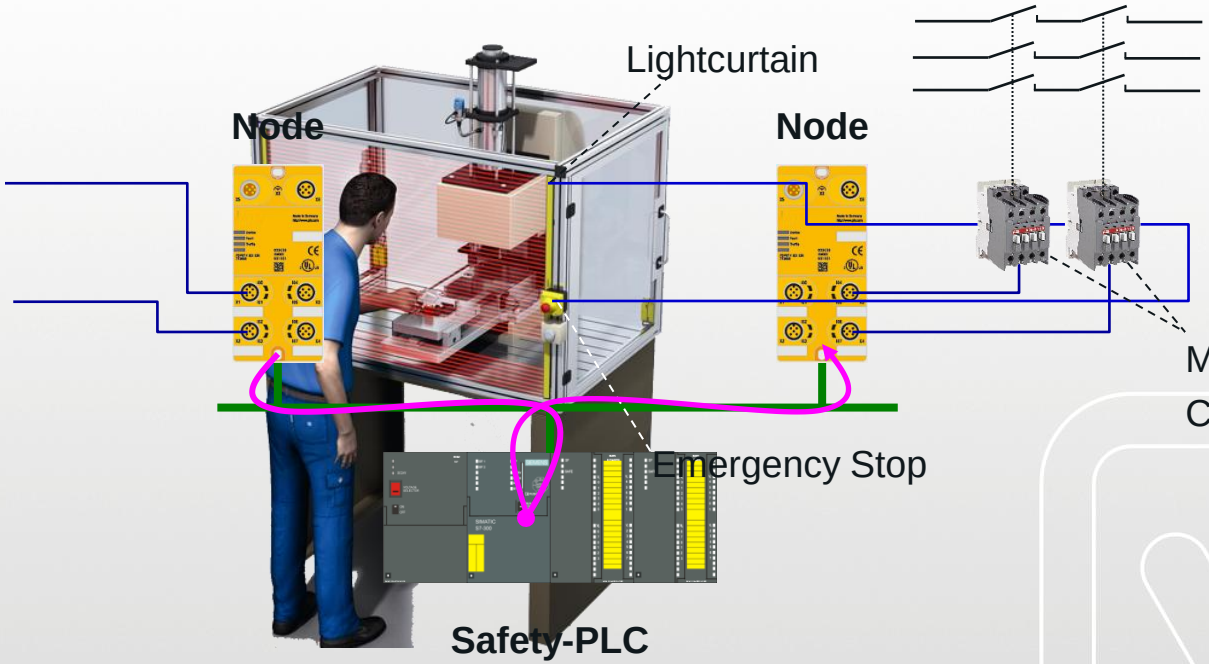
Safe State



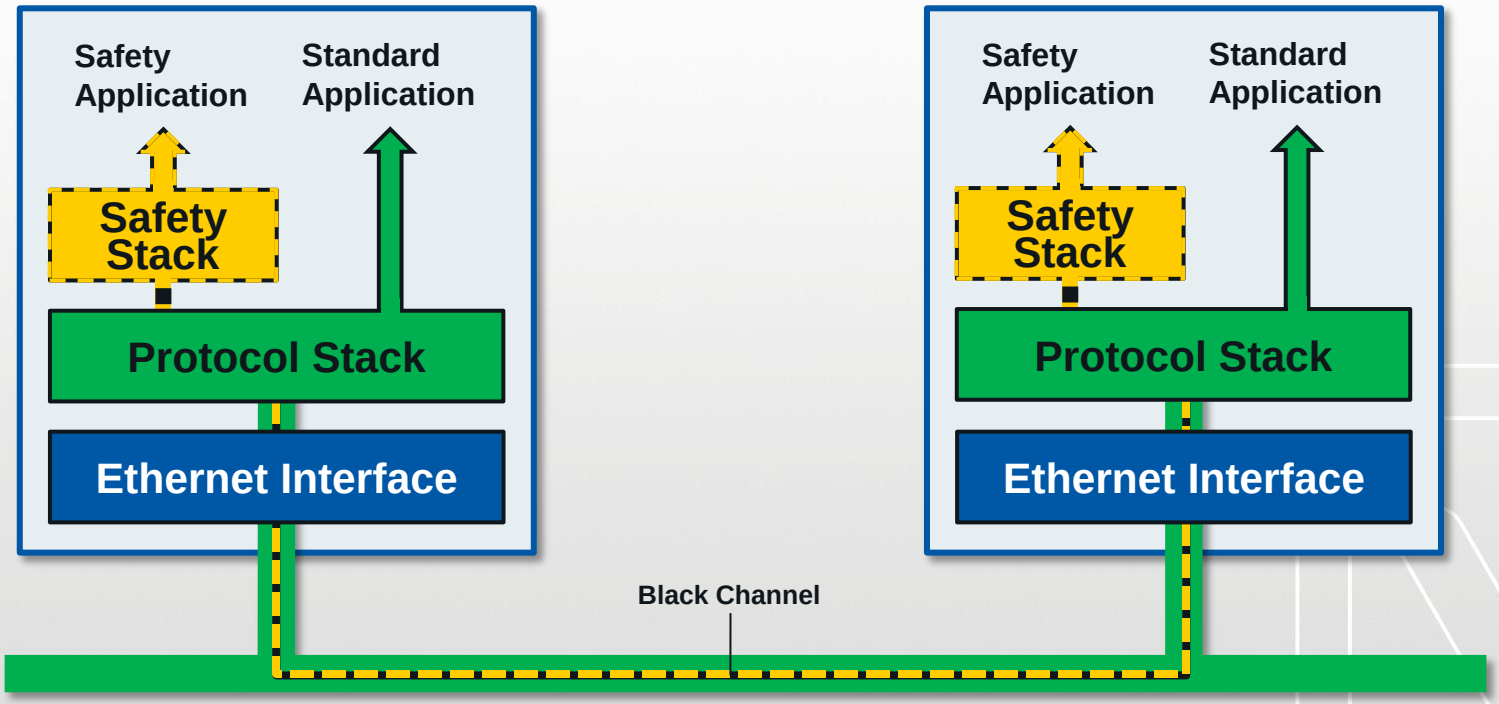
Power interrupt

Safe operation

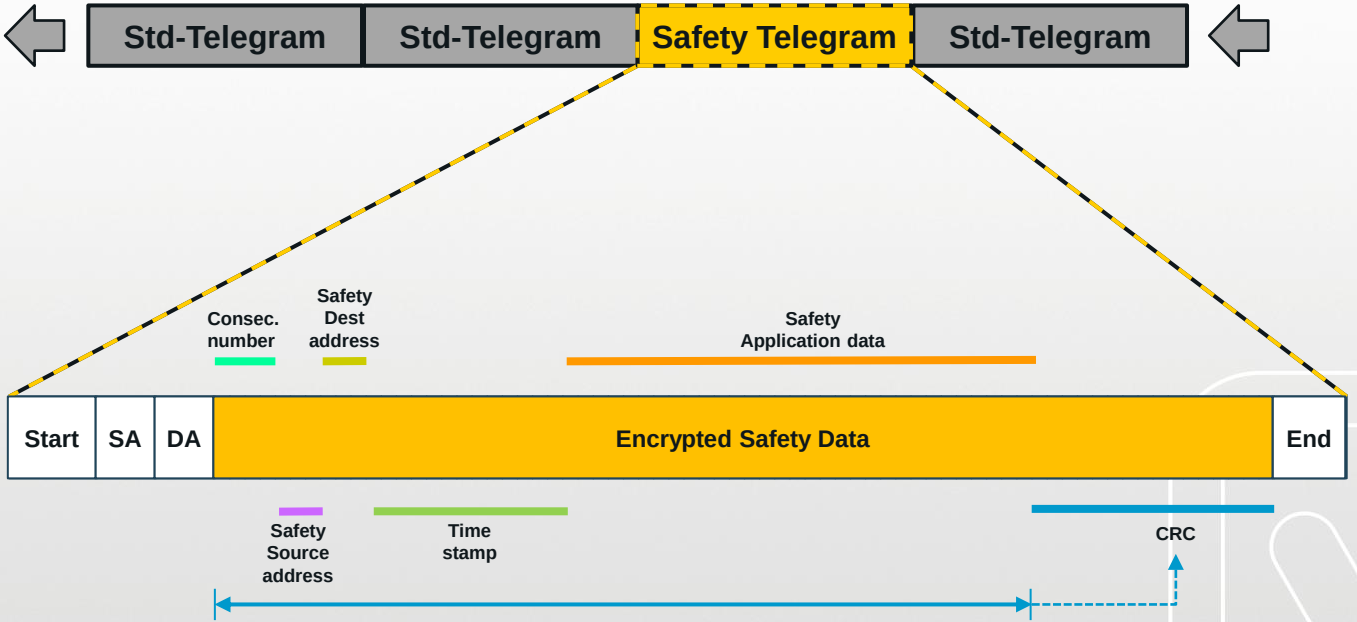
Example


Lightcurtain
Node
Node
Main
Contactors
Emergency Stop
Safety-PLC

Safe communication ≠ Always available



Mixed mode: Safety Telegram between Standard telegrams



Safety communication - Protocols

D&E event 2016

Twincomm

Safety protocols on top of communication protocols

PROFINET®

PROFIBUS®

Safety over EtherCAT®

EtherCAT®

sercos

ControlNet™

DeviceNet™

EtherNet/IP™

CC-Link Safety™

CC-Link

open SAFETY

PROFINET®

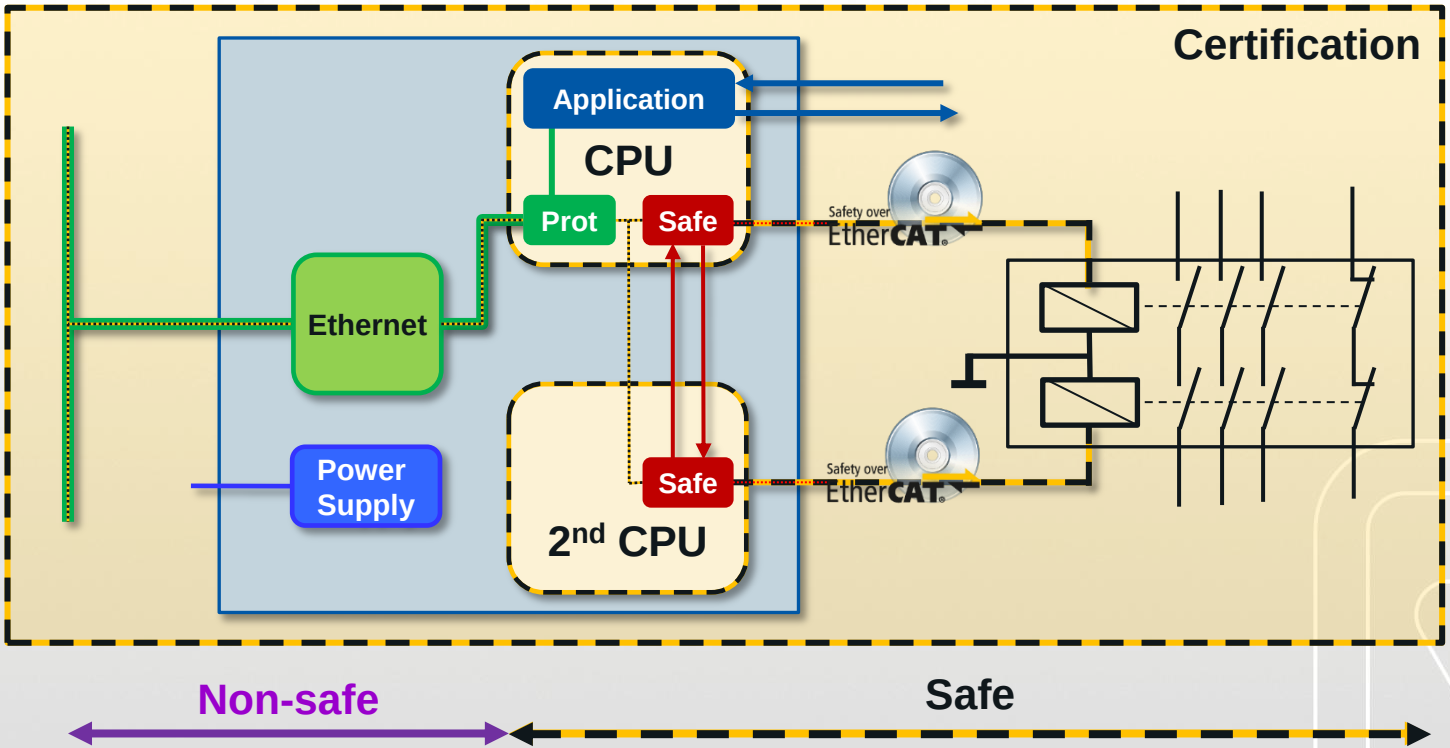
EtherNet/IP™

Modbus

ETHERNET POWERLINK

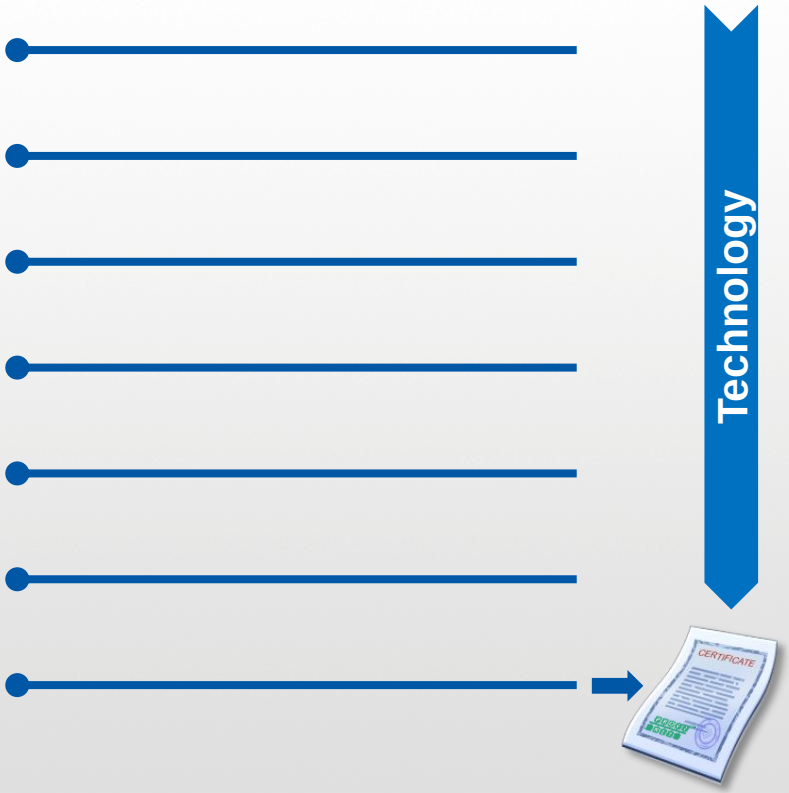
sercos

Safety design

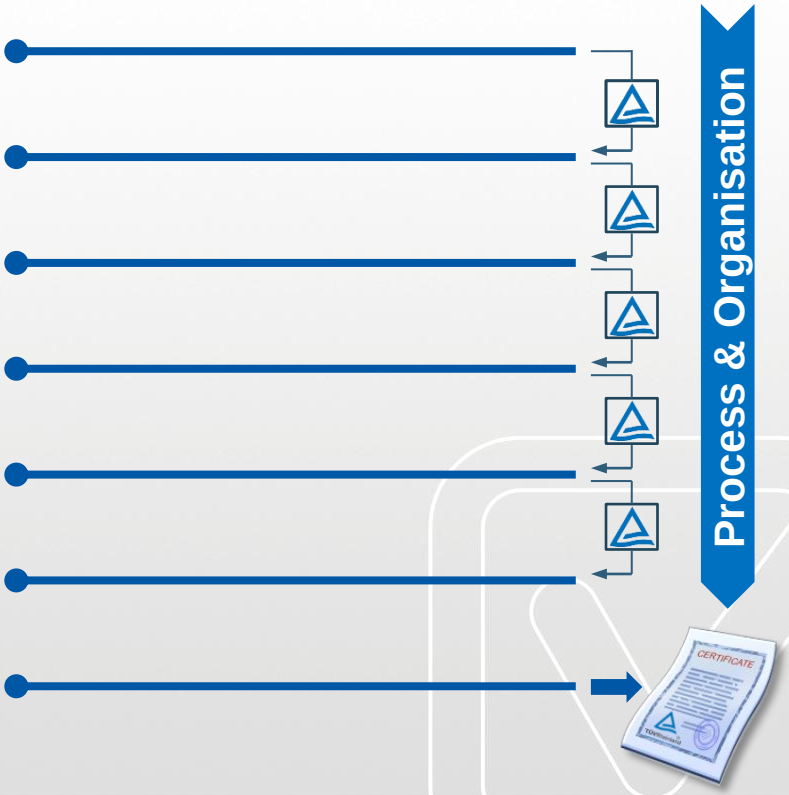


General embedded design-in

Protocol certification



Safety certification



Safety Development Process

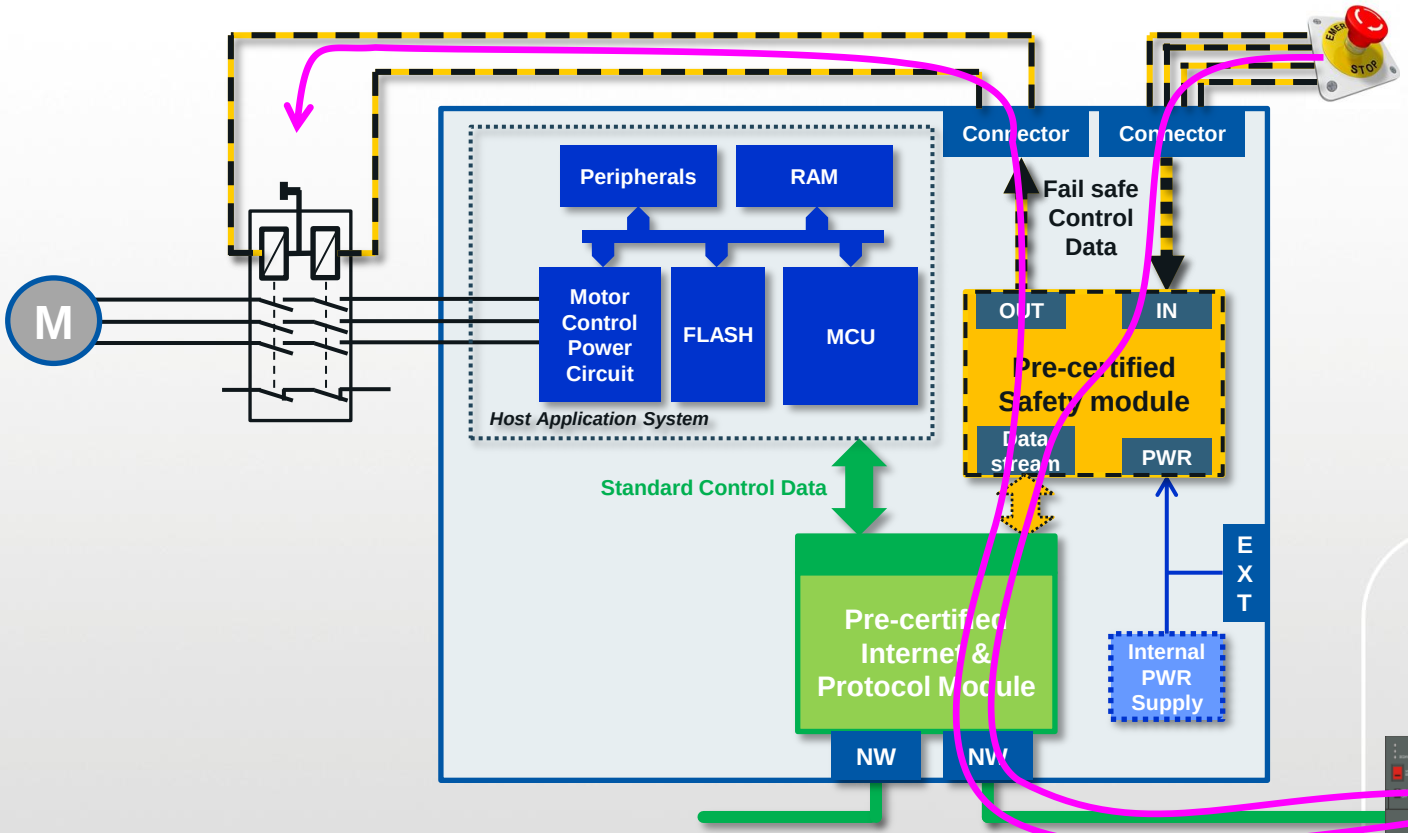
A set of documents describing the safety system and its development is required:

- **Safety Requirement Specification**
- **Functional Safety Management** (FSM) or **Safety Plan** collates all structural and technical activities during the different development phases
  - Responsibilities and competences
  - Communication / information flows
  - Definition of product lifecycle
  - Documentation (In- and Output documents for each lifecycle phase)
  - Planning of methods and techniques to avoid errors
  - Rating of the (achievable) functional safety
  - Dealing with modifications
  - Configuration management

Safety Development Process (cont)

- **Verification and validation plan**
  shows the fulfillment of the goals and requirements that were defined for the different safety lifecycle phases
  - Summary of used methods and techniques (e.g. described by IEC EN 61508-2 and -3)
  - List of used tools (e.g. Compilers, CAD-Systems etc.)
- **Hardware- and Software Design Documents**
  - Tracking of requirements shall be possible
  - Documented Reviews necessary
- **User manual or Safety Manual**
  - User obligations and terms of use
  - Restrictions to the appliance of the safety functions
  - Description of the safety functions and their API

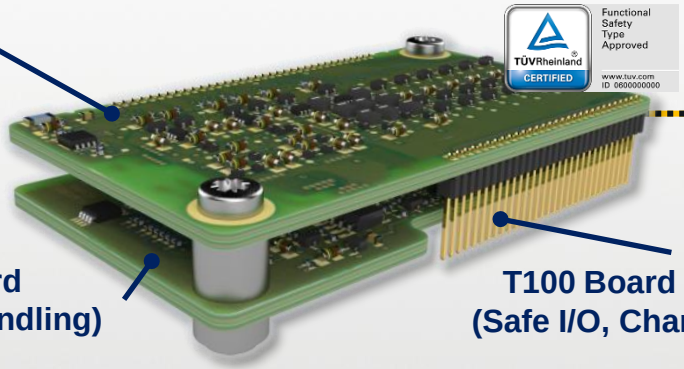
Modular Safety Design-in



Integration & Certification

- **Technical design-in**
  - Power Supply (SELV/PELV): Logic and Safe I/O
  - Environmental operating conditions (EMC, temperature, humidity)
  - Routing of safe I/O signals to external connectors
  - Mechanical dimensions and clearances
  - Electrical connection to non-safe communication controller
  - Shielding and housing to achieve enhanced EMC requirements
- **Functional and technical testing**
- **Adapt/provide *Device Description*-file *& Product Safety Manual***
- **Product Validation**
- **Product Safety Approval e.g. by TÜV**

Example system set-up

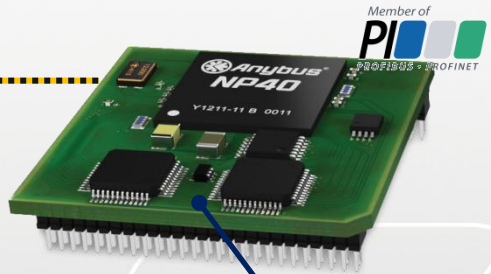


Safe I/O board

Safe CPU board
(safety protocol handling)

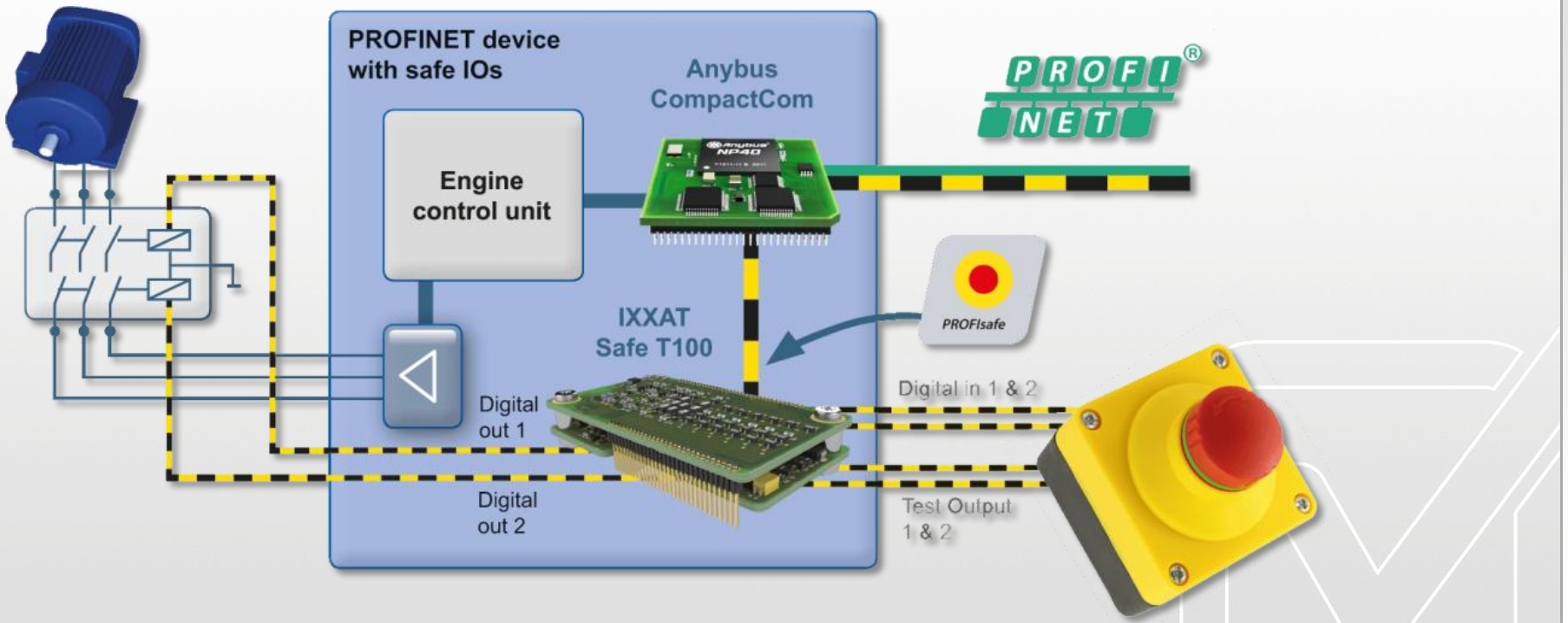
T100 Board connector
(Safe I/O, Channel, Power)

Black Channel



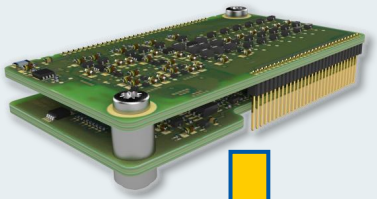
Anybus CompactCom
Industrial Ethernet Module

Example system set-up

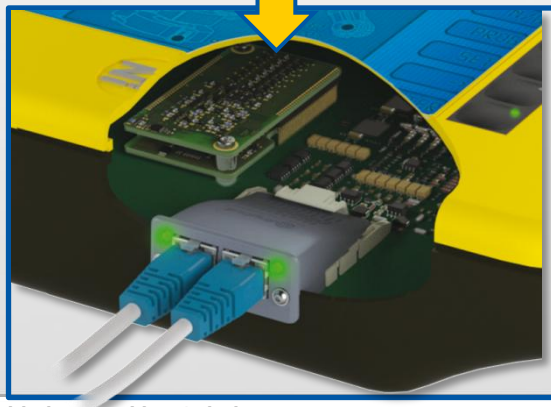


Design-in and Certification Steps

IXXAT Safe T100



Pre-Certified



IXXAT®

Thanks for your attention!

Please visit us at booth 15

Twincomm
de Olieslager 44
5506 EV Veldhoven
the Netherlands

T +31-40-2301.922
E welcome@twincomm.nl
I www.twincomm.nl