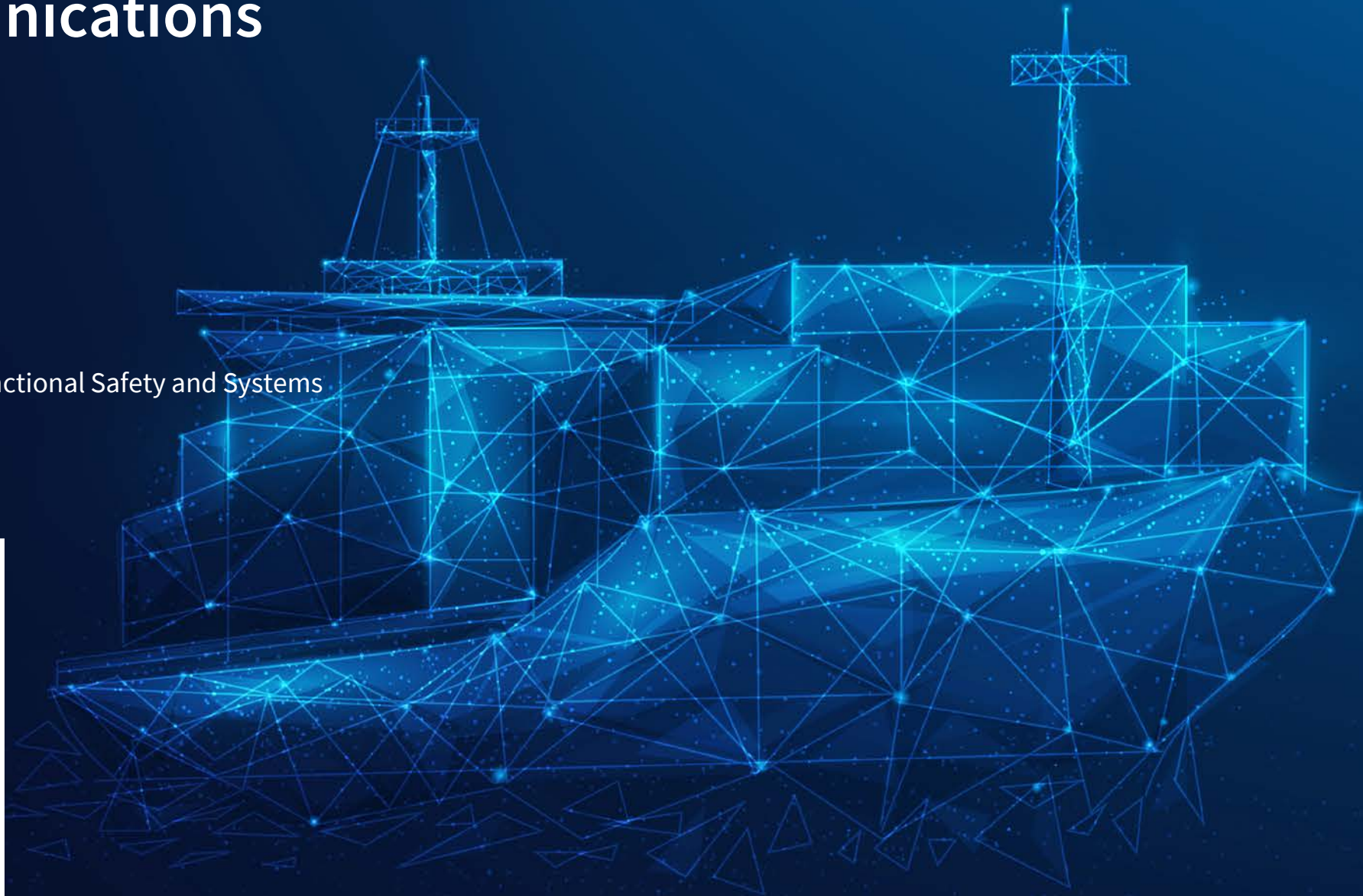


Functional Safety and Communications

Peter Brown – Functional Safety and Systems



Our Members



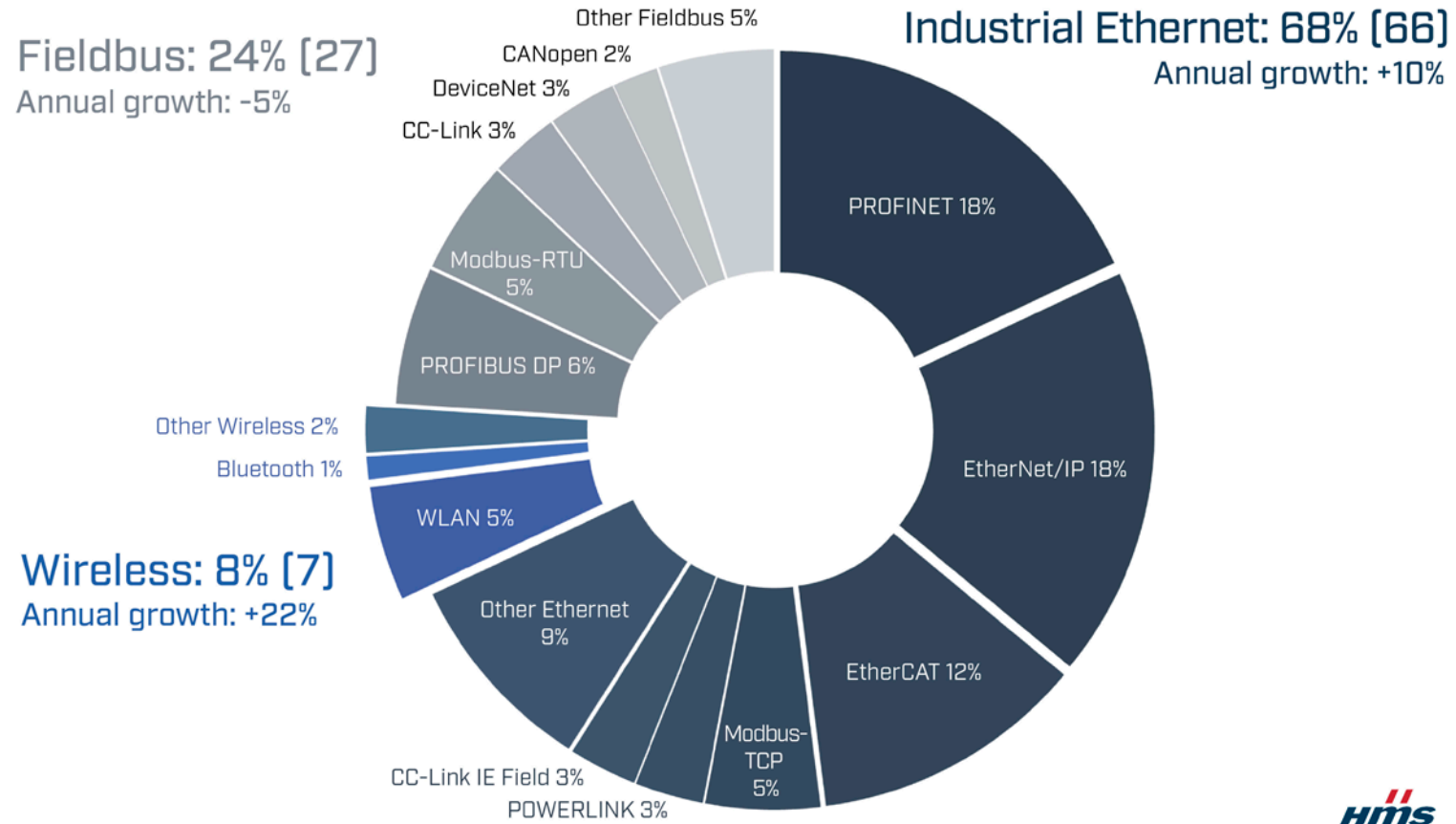
What is (Industrial) “Communications”?

- Data communications.
- “Fieldbus”:
 - PROFIBUS DP, Modbus RTU, CC-Link, DeviceNet, CANopen, ASi, IO-Link, etc.
- Industrial “Networks”:
 - PROFINET, Ethernet/IP, EtherCAT, Modbus-TCP, POWERLINK, CC-Link IE Field, etc.
- “Wireless” Communications:
 - WLAN, Bluetooth, WirelessHART, ISA100, ZigBee, Infrared based, etc.
- Modern Communication Technologies:
 - TSN, APL , SPE, PoE, PoDL, etc.

No longer just a simple cable!

We are not promoting any particular technology or methodology.

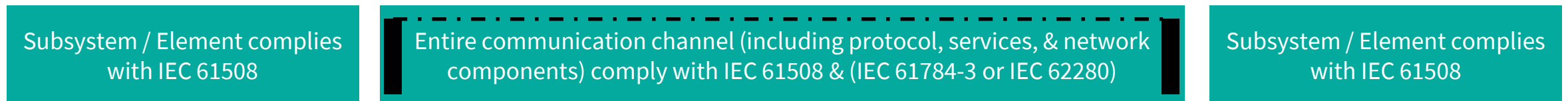
What is (Industrial) “Communications”?



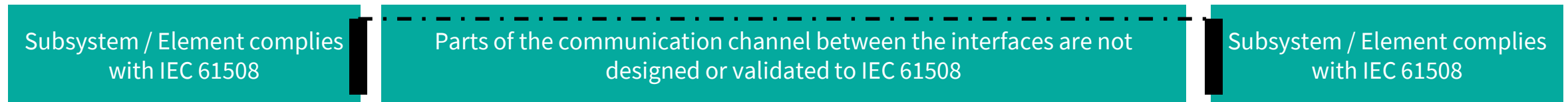
IEC 61508-2:2010 & IEC 61508-3:2010

- 7.4.11 is *Additional requirements for data communications*.
- The failure rate / residual error rate shall be estimated considering **transmission errors, repetitions, deletion, insertion, resequencing, corruption, delay** and **masquerade**.
- Equal to or less than the target failure measure (tolerant).
- Included in the estimation of random failures.
- “Black Channel” / “White Channel” (“Grey Channel”).
- IEC 61508 & (IEC 61784-3 or IEC 62280).
- SRS, safety design specification (SDS), and software safety requirement specification (SSRS).

White Channel:



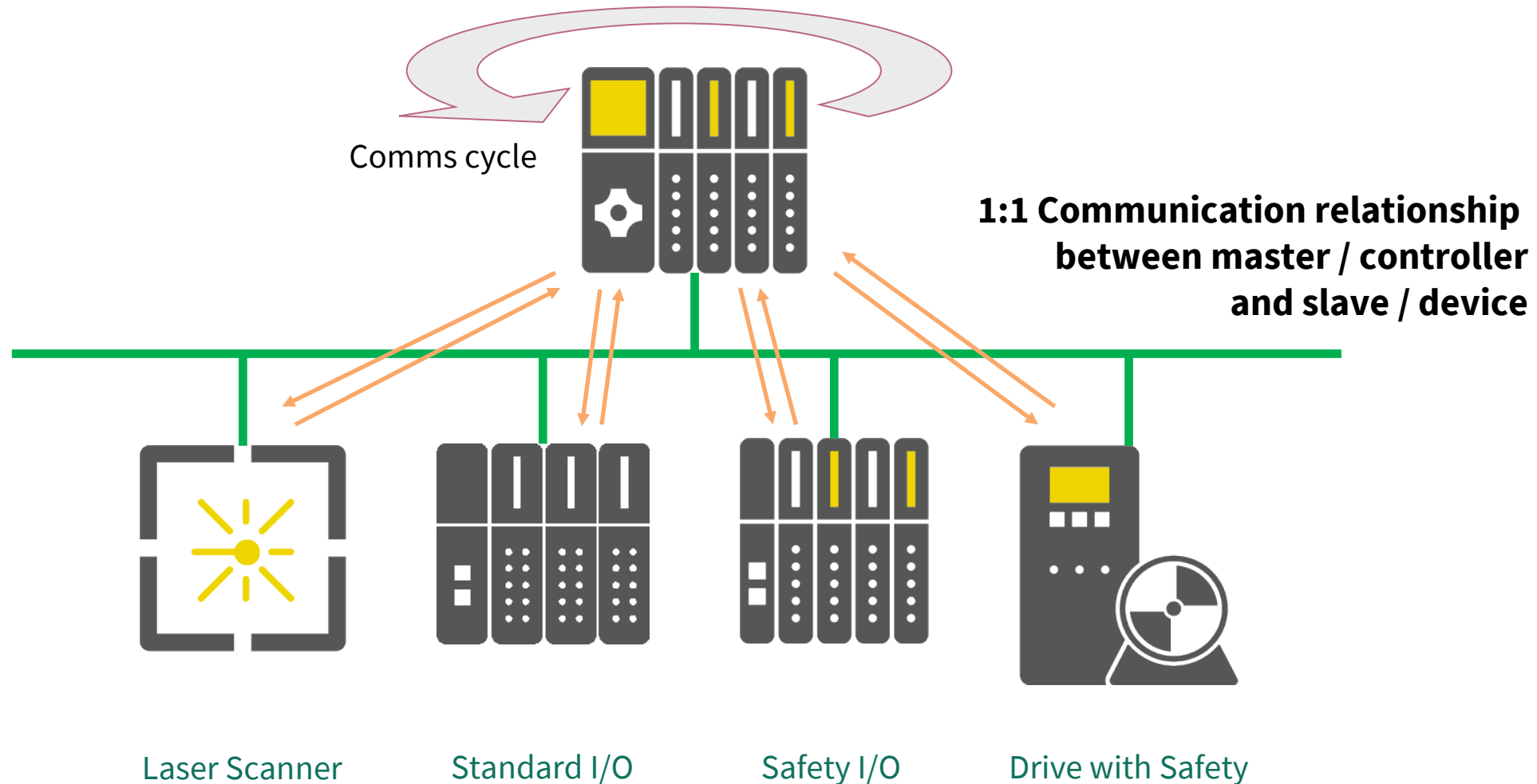
Black Channel:



Interface(s) comply with IEC 61784-3 or IEC 62280 (incl. services / protocols)

Interface(s) comply with IEC 61784-3 or IEC 62280 (incl. services / protocols)

Cyclic Communication, CSMA/CD, CSMA/CA, TSN



Example: PROFIsafe - Checks



	Consecutive Number	Timeout with Receipt	Codename for Sender and Receiver	Data Consistency Check
Repetition	✓			
Deletion	✓	✓		
Insertion	✓	✓	✓	
Resequencing	✓			
Data Corruption				✓
Delay		✓		
Masquerade (standard message mimics failsafe)		✓	✓	✓
Revolving memory failure within switches	✓			

Other Functional Safety Standards

- IEC 61511:2017.
- IEC 62061:2021.
- ISO 13849-1:2023.
- All still require estimation of the dangerous failure rate.
- All still require details in the requirements specifications.
- Use of communications in safety-related systems / safety functions is generally accepted for:
 - Process industry.
 - Machinery sector.
 - Infrastructure projects.
 - Maritime sector.

Industrial Communication Networks – Fieldbus Specifications



- The IEC 61784 series defines several Communication Profile Families (CPF).
- IEC 61784-3 is for “safety”.
- Each CPF specifies a set of protocol specific Communication Profiles (CP) based primarily on the IEC 61158 series, to be used in the design of devices involved in communications.
- Mainly for machinery / manufacturing and process control.
- The IEC 61158 series specifies the generic concept of “fieldbuses” and defines the physical, data link and application protocol types for Fieldbus and Ethernet based networks.
 - Example: IEC 61784-3-3 is for “PROFIsafe” (www.profibus.com).
 - Example: IEC 61784-3-2 is for “CIP Safety” (www.odva.org).
 - Example: IEC 61784-3-12 is for “Safety over EtherCAT”.
 - Example: IEC 61784-3-13 is for “openSAFETY”.

Failure Modes

- For example, revolving memory failure within switches!
- Understand not just your system failsafe state but also your communications failsafe state.
- Competence: learn about your selected communication system.
- Define all your communications failure modes (safe, dangerous, spurious trip frequency).
 - Many “select” a communications system and don’t understand the failure modes.
 - Many neglect to define the details in SRS / SDS / SSRS.
 - Can usually get support from your product manufacturer / supplier.
- Ensure cyber security derived failure modes are included!
- Ensure EMI derived failure modes are included.
- Is the communications system wired only or both wired and wireless?
- Do the “pre-defined” techniques and measures protect for your failure modes?
- Or do you need to define extra techniques and measures (SRS, SDS, SSRS)?

Latest technologies and OSI model




OSI
Open Systems Interconnection

Software

43
66
34
5E
9E
7E
93
ED
9C
9C
6B
E3
B7
A2
A8
2A
1A
34
5D
7A

84 63
CF C3
1B 3E
92 2A
DC F9
51 26
32 0B
AE D1

Hardware



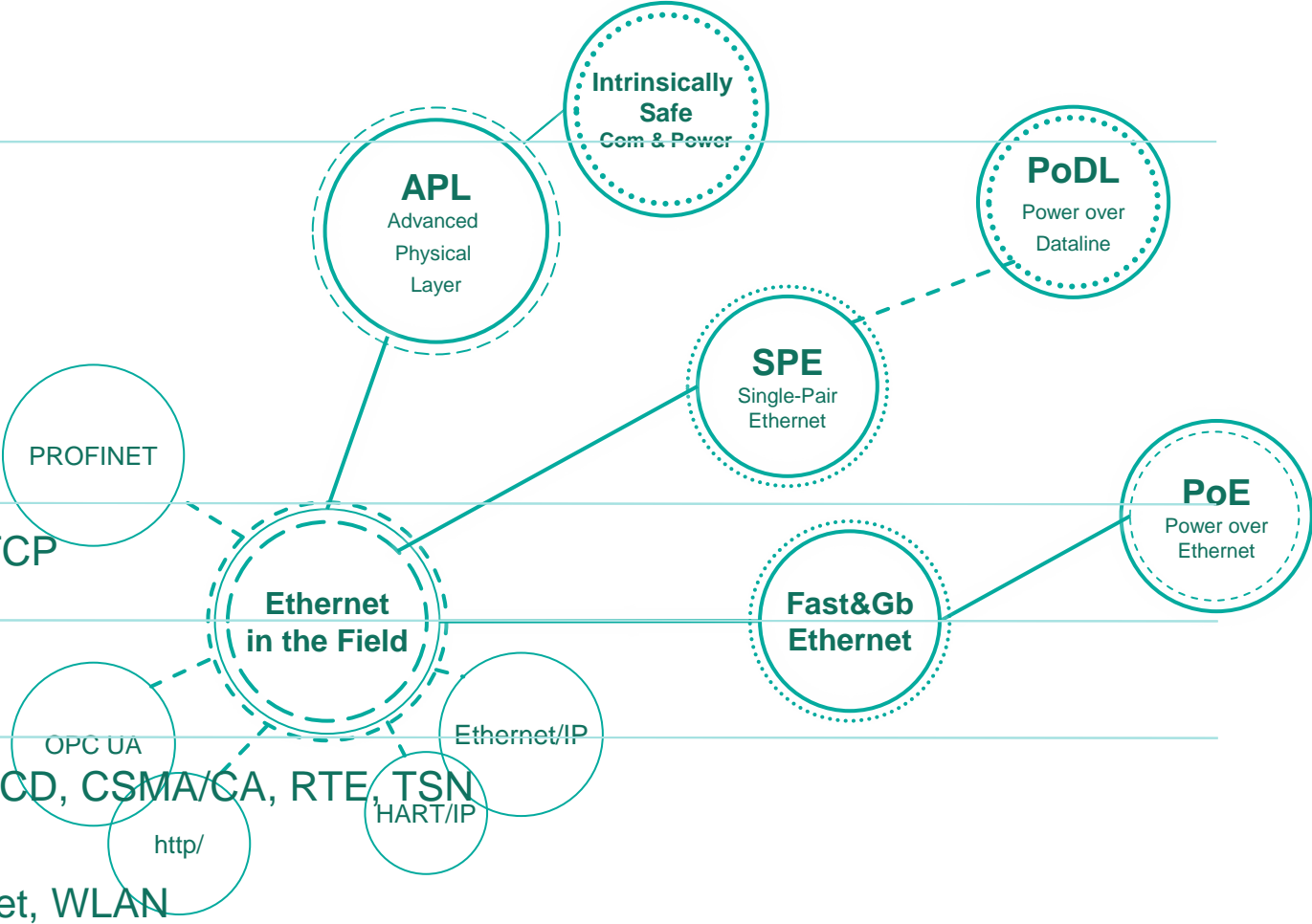
Application
Presentation
Session
Transport
Network
Data Link
Physical

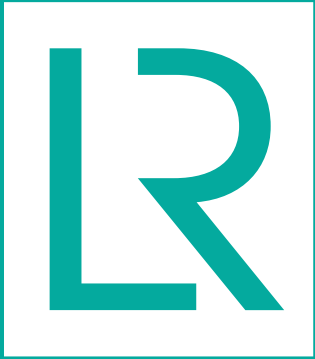
UDP, TCP

IP

CSMA/CD, CSMA/CA, RTE, TSN, HART/IP

Ethernet, WLAN





Thank you

Peter Brown

Functional Safety and Systems

pete.brown@lr.org

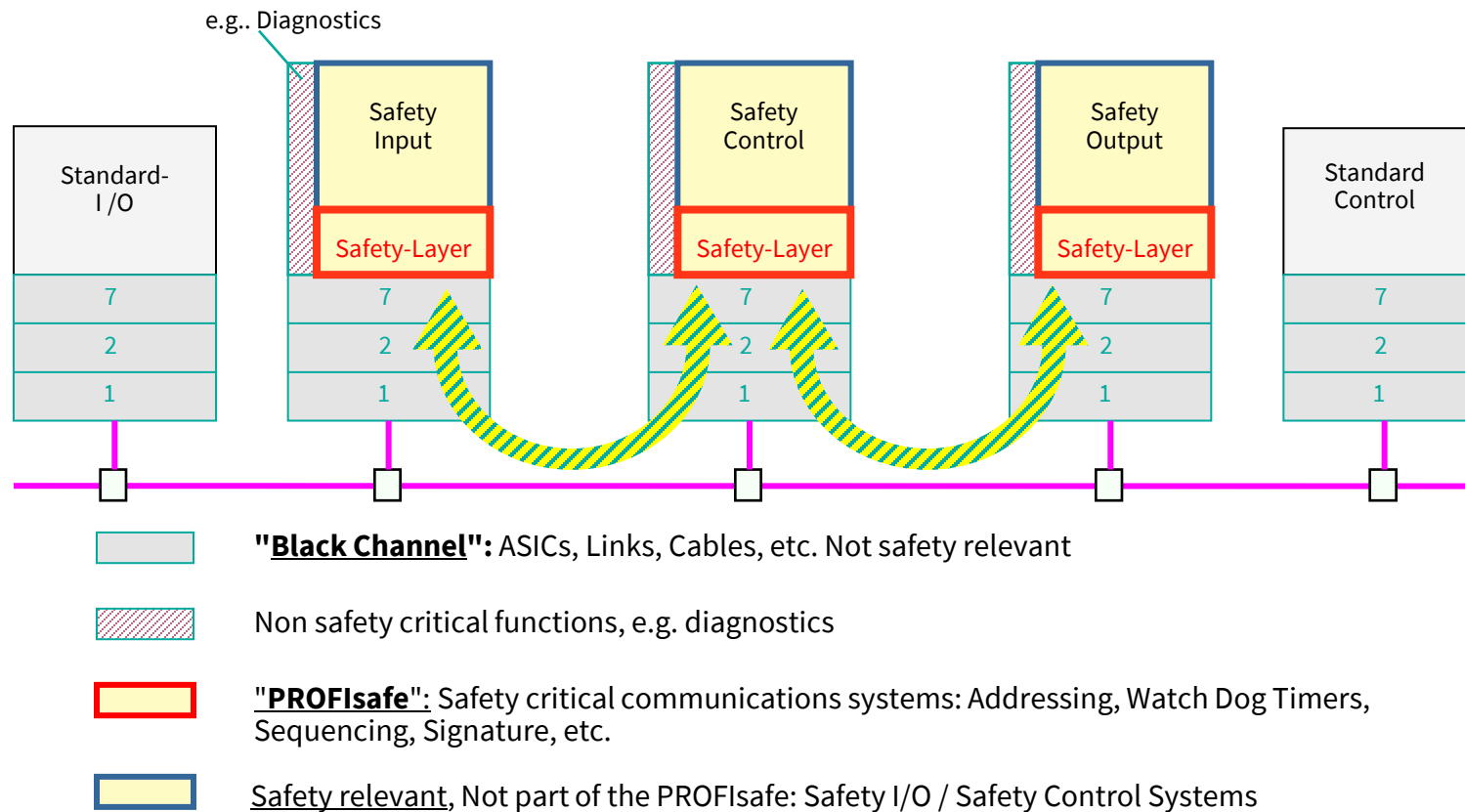
Slot	Start Time	Paper	Workshop	Finish Time
-	16:30	CLOSE - Informal Post Symposium Questions / Discussions		17:30
-	N/A	N/A		N/A

Extra Slides in Case of Questions

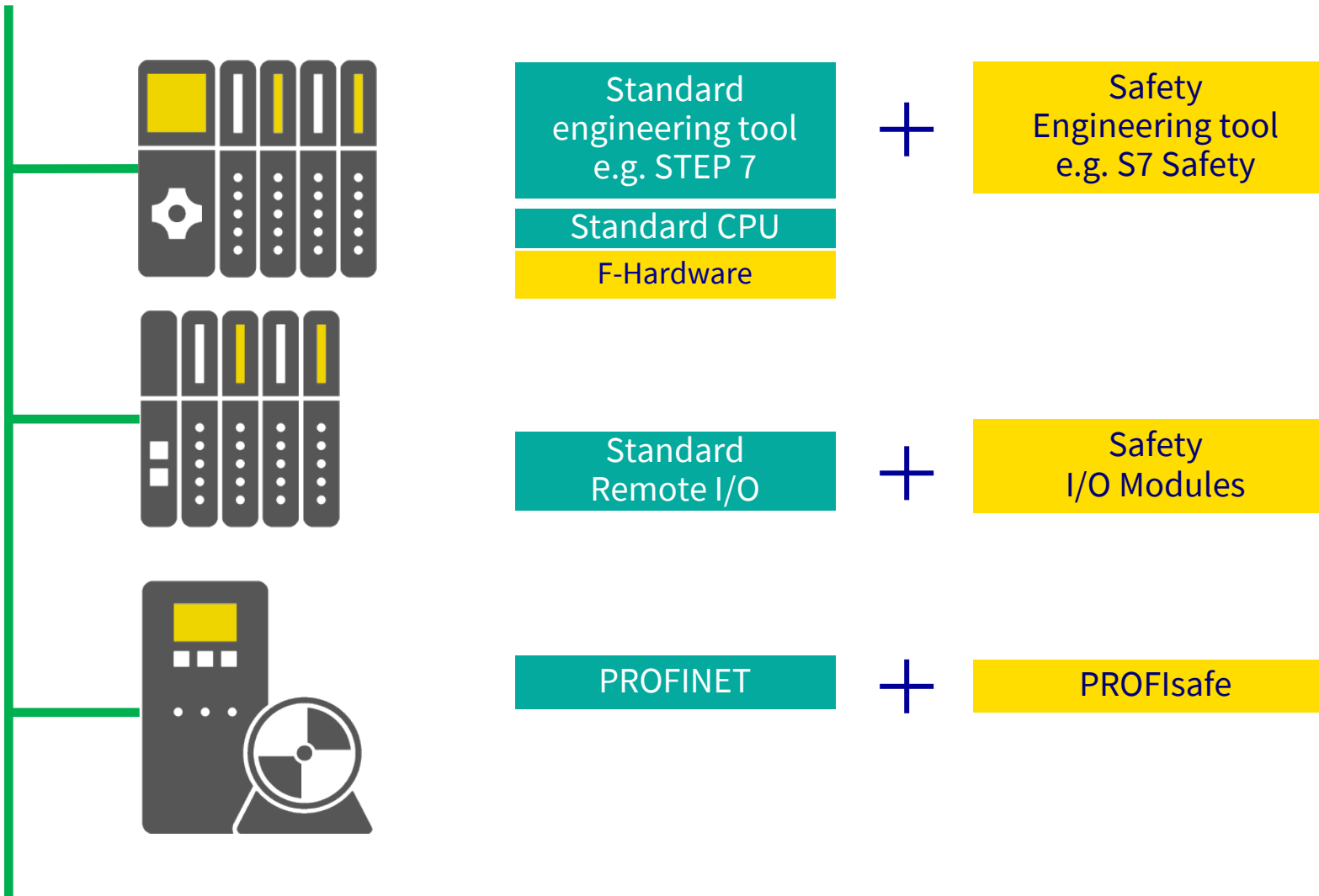
See the slides after this slide.



PROFIsafe – ISO / OSI Model



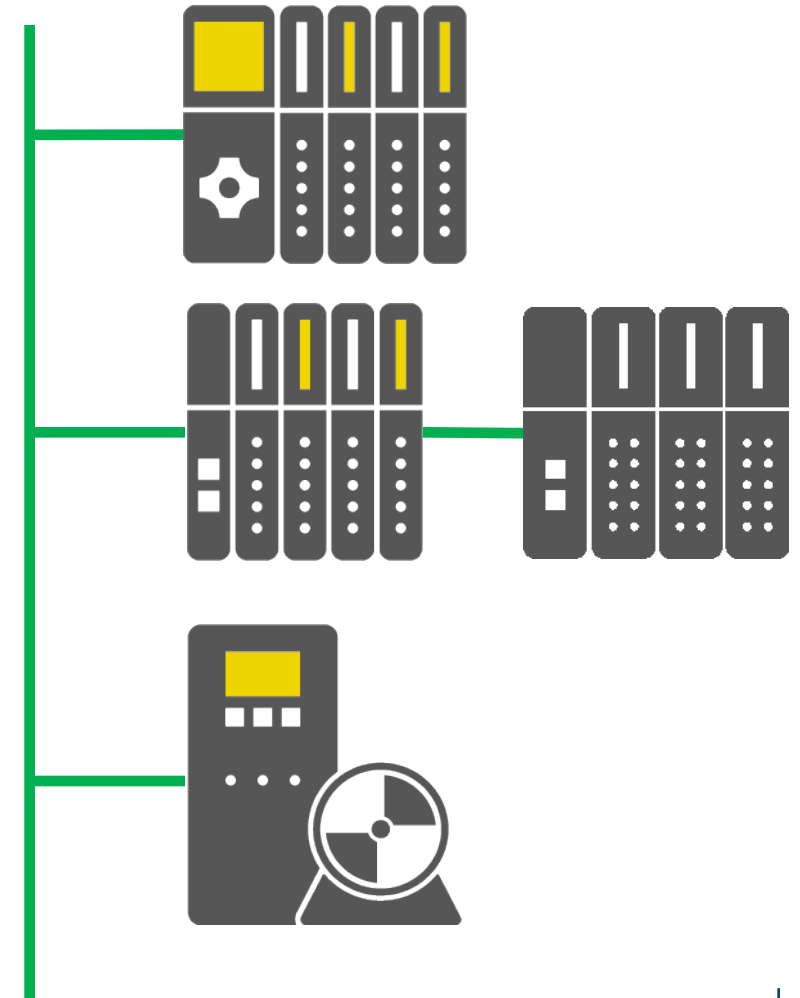
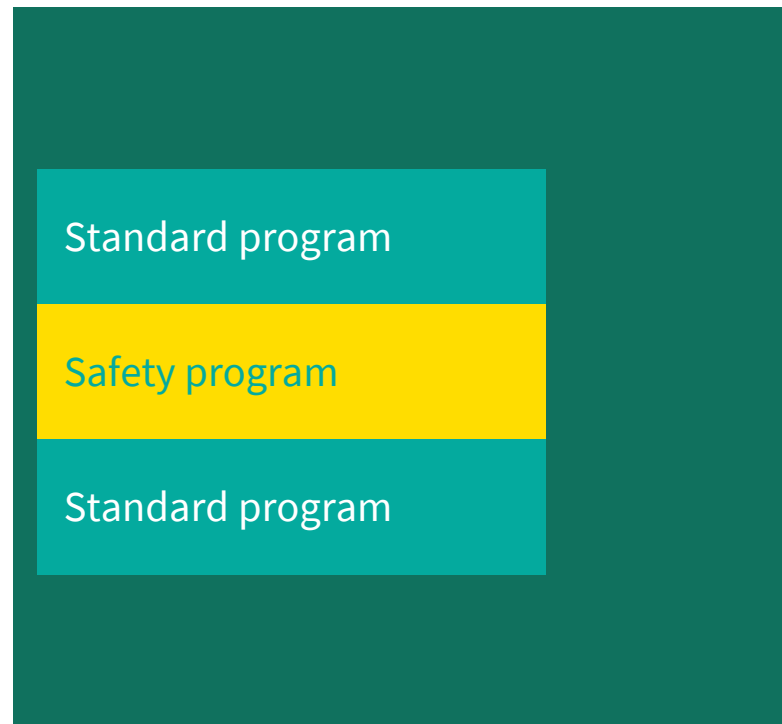
PROFIsafe – Add-on Strategy



PROFIsafe – Application Program



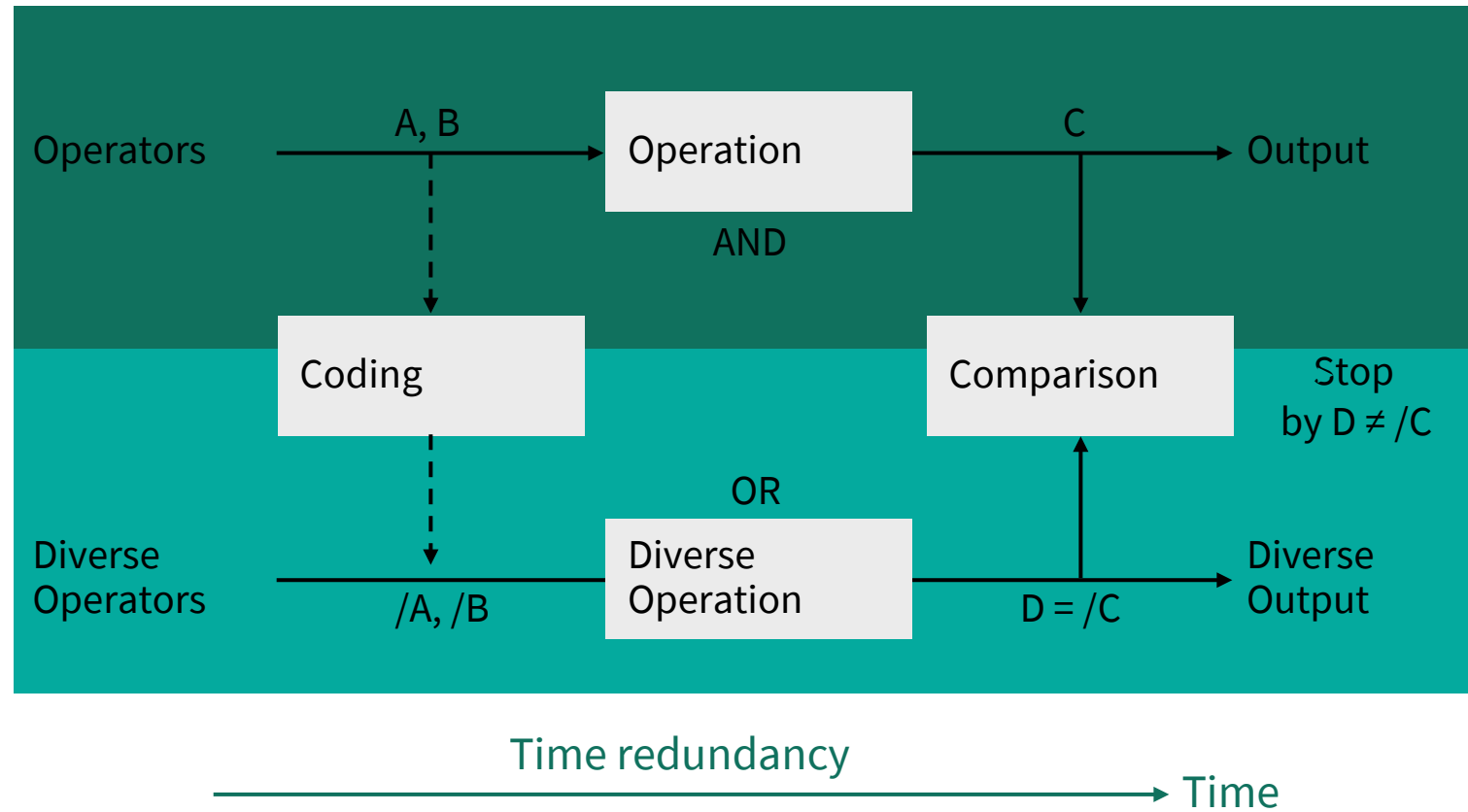
- Coexistence of standard program and safety-related program on one CPU.
- Changes to the standard program have no effect on the integrity of the safety-related program section.



PROFIsafe – Coded Processing



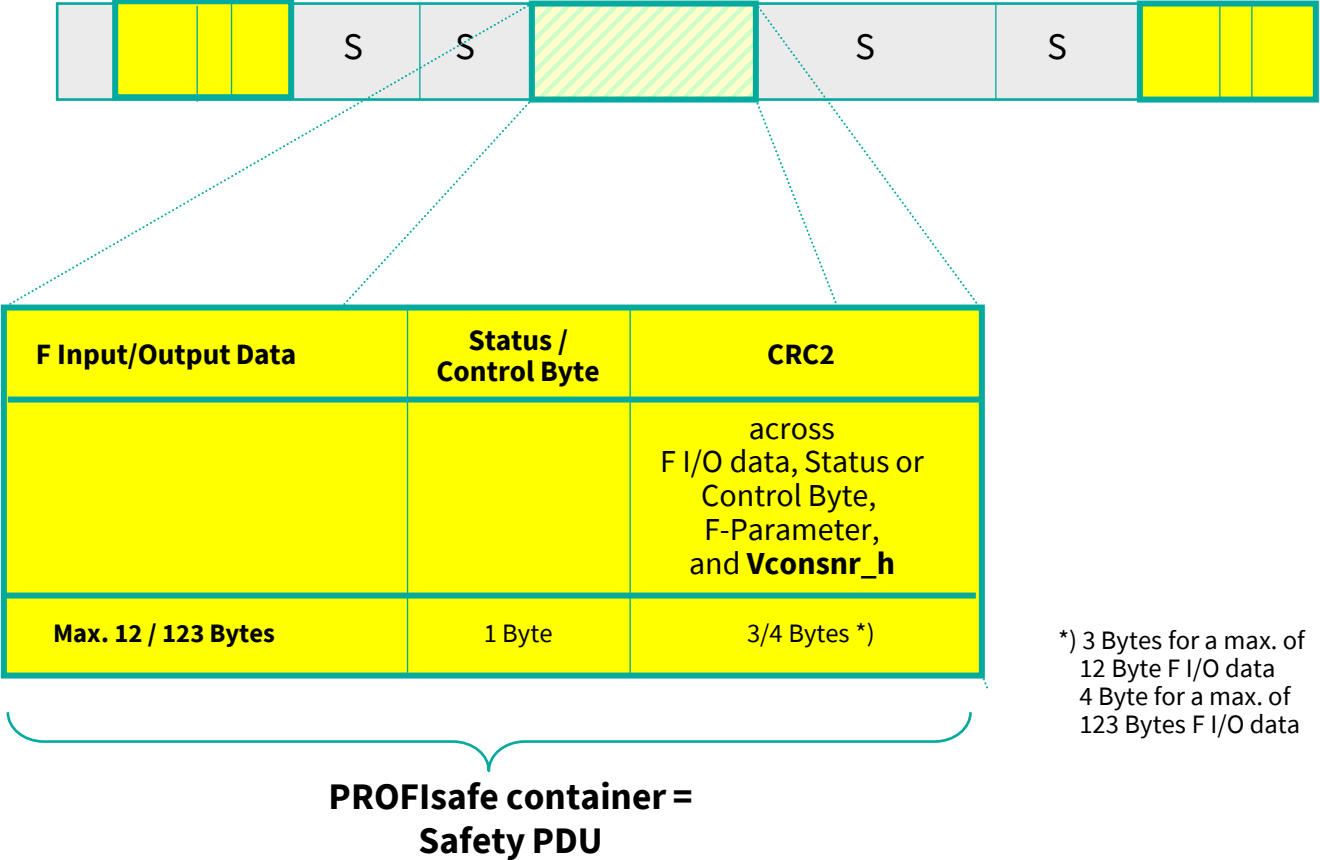
Time redundancy and diversity replace complete redundancy



PROFIsafe – Safety PDU



Standard PROFINET IO messages



*) 3 Bytes for a max. of 12 Byte F I/O data
4 Byte for a max. of 123 Bytes F I/O data