SIEMENS

Understanding IWLAN – even allowing for Safety

Which bits really matter?

Why is 802.11 suitable for automation tasks?

PROFIBUS - PROFINET user conference 2010

Celebrating 20 Years of PROFIBUS

What advantages does IWLAN bring to the automation world?

SIEMENS

Many reasons for WLAN

- **WLAN frees** Profibus and PROFInet **from cables**
- **bridging of distances** without cables
  - e.g. between buildings
  - across obstacles (streets, rivers, lakes)
- **maintenance-free,** e.g. compare to slip rings
- **higher data rates** than other wireless systems
- WLAN makes **data transmission with mobile machines/devices**

But

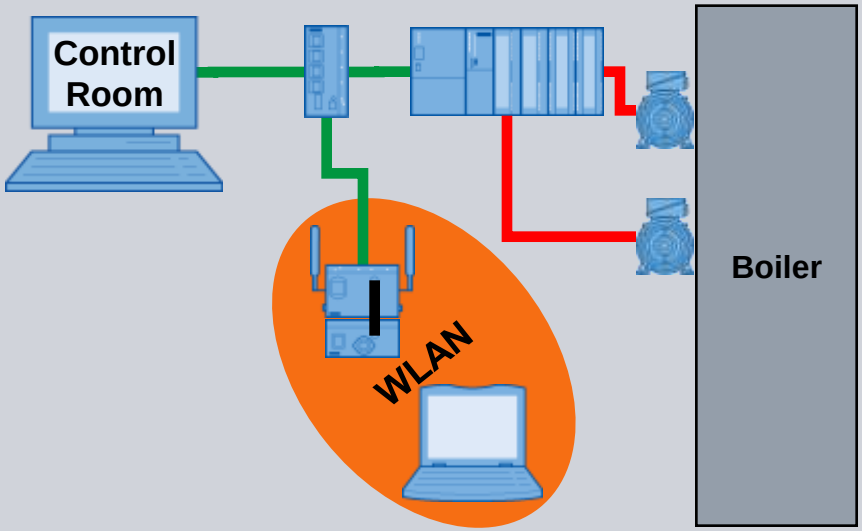
- A **permanently installed cable** will have a higher availability than WLAN!
- WLAN technology is **slightly different**….e.g. CSMA/CA and positive acknowledgement
- **WLAN channels are limited**

Example 1:
Wireless Access to Control Room

SIEMENS

Requirements

- Innovate plant maintenance of sensors and actuators (maintenance with one person/ commissioning)



Ethernet
Control
Power

Example 1:
Wireless Access to Control Room

SIEMENS

Why does the Access Point "understand" the laptop?

The Access Point (AP) and laptop…..

- have been set to the same **wireless standard**
- chat on the same **frequency**
- use the **network name**
- encrypt the messages with the same "secret code"

Example 1:
IEEE 802.11 WLAN Standards (PHY)

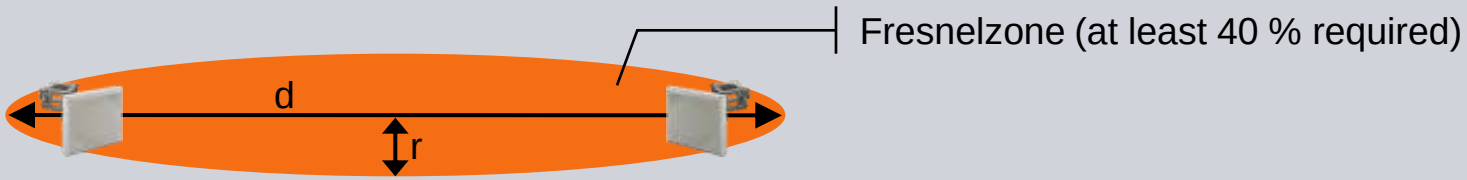
SIEMENS

	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a	IEEE 802.11h	IEEE 802.11n
Frequency Range	2.4 GHz	2.4 GHz	5 GHz	5 GHz	2.4 GHz/ 5 GHz
Range (depends on antenna and env.)	Indoor: 30 m Outdoor: 140 m	Indoor: 30 m Outdoor: 140 m	Indoor: 30 m Outdoor: 120 m	Indoor: 30 m Outdoor: 120 m	Indoor: 70 m Outdoor: 250 m
TX Power (On The Example In EU)	Indoor and outdoor: 20 dBm	Indoor and outdoor: 20 dBm	Indoor: 23 dBm	Indoor and outdoor: 23 dBm/ 30 dBm	Indoor and outdoor: 23 dBm/ 30 dBm
Non Overlapping Channels	3	3	4	8 + 11	2,4 GHz: 3 5 GHz: 8 + 11
Gross Data Rate	11 MBit/s	54 MBit/s	54 MBit/s	54 MBit/s	600 MBit/s
Specifics (On The Example In EU)	because of DSSS-modulation robust			DFS mandatory, up to Ch 64 only indoor	DFS mandatory at 5 GHz

Example 1:
Physical Properties of the Frequency Ranges

SIEMENS

	2.4 GHz				5 GHz			
Use in Networks	- common ➔ often already occupied				+ less common - outdoor only with DFS			
Use In Devices	+ very common				- less common			
Free Space Loss At Different Frequencies („Resistance“ Of The Air)	**1 m**	2 m	10 m	100 m	**1 m**	2 m	10 m	100 m
	40 dB +	46 dB	60 dB	80 dB	**47 dB** -	53 dB	67 dB	87 dB
Fresnelzone (r) At Different Distances (d)	10 m	100 m	1000 m		10 m	100 m	1000 m	
	0.55 m -	1.75 m	5.55 m		0.38 m +	1.19 m	3.75 m	



Example 1:
Network name and Security

SIEMENS

The **SSID** (**S**ervice **S**et **Id**entifier)……..

- is the **name** of a wireless network
- can be **defined freely** (e.g. „bh_1“)
- must be set on the **AP and the wireless client**
- It can have a length limits e.g. up to **32 characters**

Radio waves are able to **propagate across borders of rooms or buildings**

→ Therefore it is necessary to **limit the access to WLAN (authentication)** and to **encrypt the exchanged data**

Tip: To be compatible with devices from multiple manufacturers be careful with characters within the SSID.

Example 1:
Security in Terms of WLAN

SIEMENS

Authentication

- **authentication protects a WLAN** against undesired access
- possible methods of authentication
  - open system (no authentication takes place)
  - shared Key
  - **WPA-PSK +** (encryption with TKIP or AES; **Passphrase**)
  - **WPA2-PSK + +** (encryption with AES (def.) or TKIP; **Passphrase**)
  - WPA and WPA2 can be used with **authentication servers** e.g. RADIUS, but this is uncommon in industrial environments

WPA2-PSK is the preferred authentication method!

Example 1:
Authentication and Encryption

SIEMENS

Encryption

- **encryption protects** the data of a network
- existing encryption methods
  - **WEP** (**weak encryption**, should be avoided)
  - **TKIP +** (**good encryption**, uses changing keys)
  - **AES + +** (**very good encryption**, better than TKIP)

AES is the preferred encryption method

Example 1:
Example Settings for WLAN:

SIEMENS

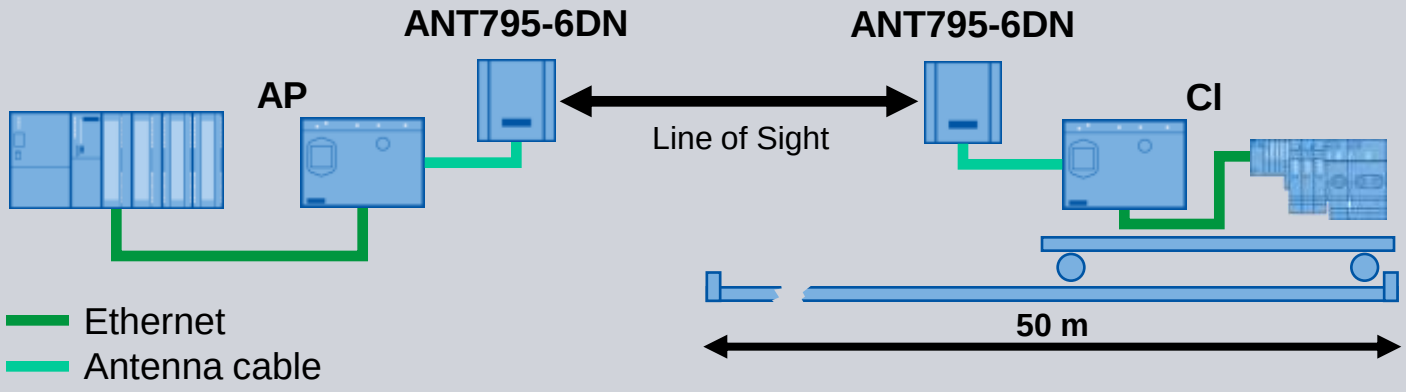
Access point	Laptop/ PG
▪ IP-addresses ▪ Country code ▪ Enable Interface ▪ SSID: bh_1 (for instance) ▪ Mode: 5 GHz, 802.11a ▪ Channel 36 ▪ Antenna: ANT795-4MR ▪ Admin-Password ▪ Auth. type: WPA2-PSK ▪ Cipher: AUTO ▪ Passphrase	▪ WLAN at 5 GHz ▪ search for WLAN ▪ Passphrase

Example 2:
Automatic Guided Vehicle with PN IO

SIEMENS

Requirements

- Wireless communication to automatic guided vehicles
- PN IO between CPU and remote I/O
- PI IO update time 64 ms
- length of the track: 50 m



Example 2:
What are the Antennas for?

SIEMENS

To bridge the 50 m distance reliably for PN IO!

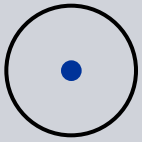
- check internal/supplied antennas and compare to external antenna options
- for Profinet IO a **reliable WLAN connection** is necessary
- **omnidirectional antennas** can bridge up to 30 m (e.g. ANT795-4MS ➔ “rabbit ears”)
- antennas with **directional characteristics** are better suited for this example
- they **concentrate** the radio waves while **sending AND receiving**
  - ➔ **longer range**
  - ➔ **less interferences** because of and for other WLANs

Example 2:
About the mentioned Antenna Types

SIEMENS

Different Antenna Types:

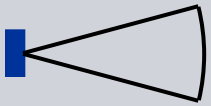
- **omnidirectional Antennas**
  (e.g. ANT795-4MS – “rabbit ears”)



(horizontal pattern bird's-eye view)

- send and receive the signal in/ from radius of 360°

- **directional Antennas** (e.g. ANT795-6DN)



(horizontal pattern bird's-eye view)

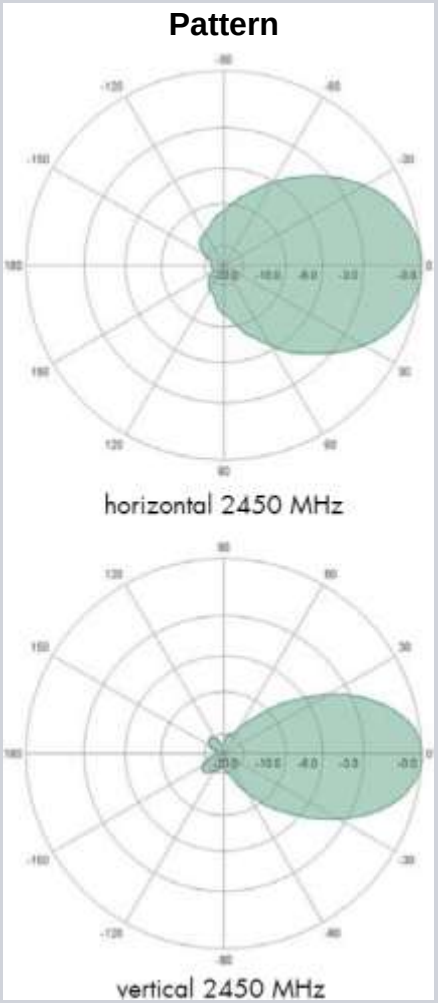
  - send and receive the signal in/ from a sector with a specific angle (here 55 °)
  - have a **gain** like a speaking tube but NO amplification
  - they only **concentrate the signal** in a **small lobe** – when **sending AND receiving**

Example 2:
Example Directional Antenna

SIEMENS

Directional Antenna:

- e.g. ANT795-6DN
- Frequency range: 2.4 GHz and 5.6 GHz
- Gain: 9 dBi
- 3 dB beam width: 75°/ 55°



Example 2:
Reliable WLAN by Thorough Planning

SIEMENS

Why Radio Field Planning?

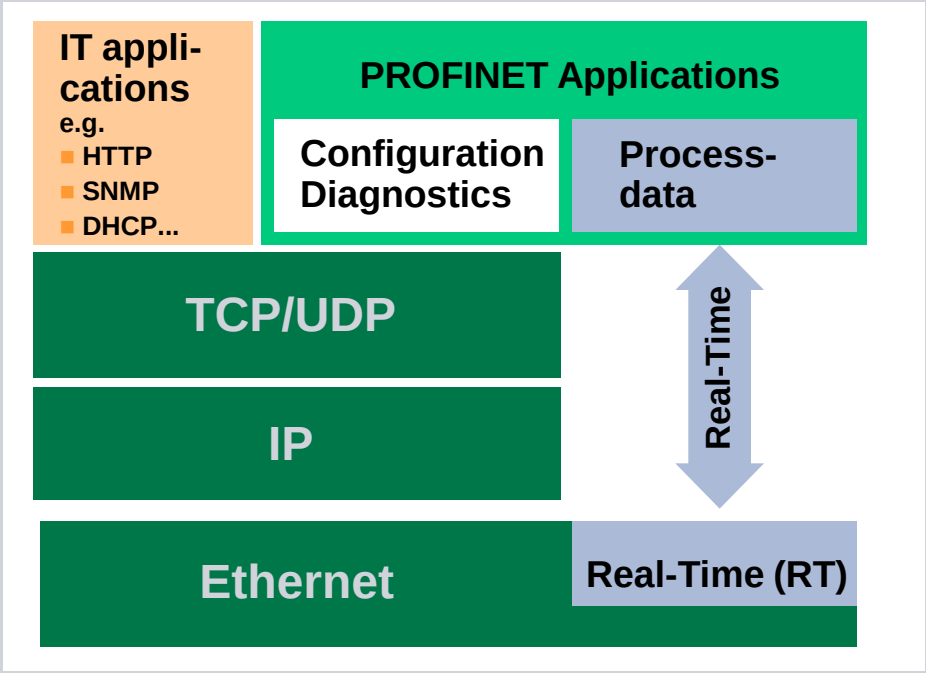
- a thorough planning of the WLAN…….
  - guarantees a **fast and on time commissioning** of the application
  - **saves recofiguring** and modification of the original setup
  - achieves **customer satisfaction**!

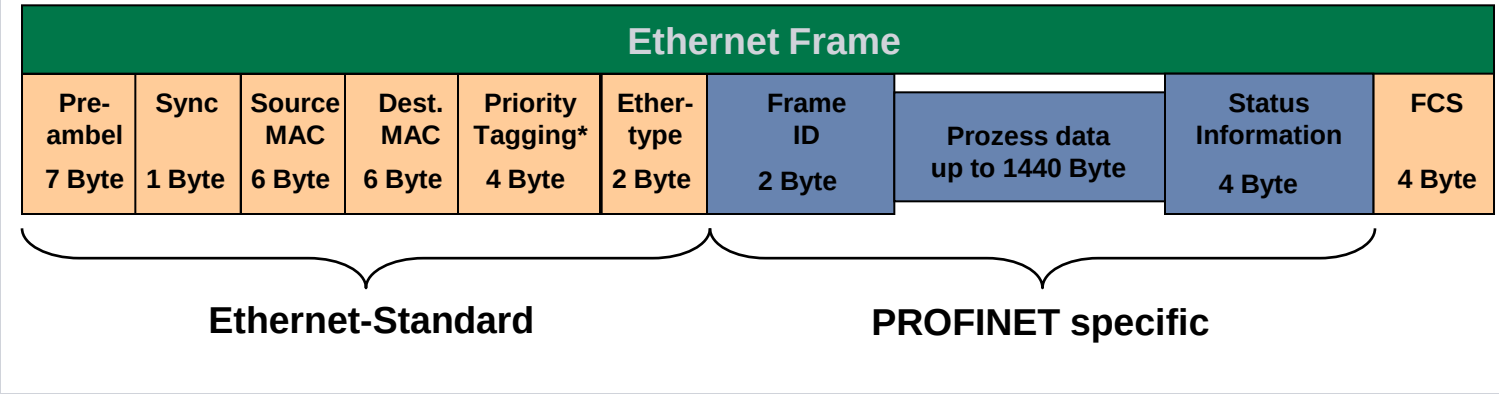
Parts of a Radio field Planning for WLAN

- Site survey
  - spectrum analysis (Network analysis is not enough!)
  - define mounting points for APs and antennas
  - considers distances, obstacles, radio-properties
- Simulation packages (e.g. SINEMA E) and proof of concept re performance and post commissioning comparison

Example 2:
Structure of PROFINET Stack & Telegrams

SIEMENS





Example 2:
WLAN and Profinet IO

SIEMENS

What special requirements has PN IO for WLAN?

- Profinet IO works with **cyclic data communication**
- **3 retries** (default) = bus fault (BF)
- ➔ **the WLAN connection must be reliable!**

“Domestic” WLAN could, however, be used for PN IO – under following conditions:

- No roaming for the Ethernet Client Module (ECM)
- The PN IO update time >= **32 ms**
- **max. of four** WLAN Clients for each AP

PROFIBUS - PROFINET user conference 2010
Celebrating 20 Years of PROFIBUS

Example 2:
MAC Mode setting

SIEMENS

The ECMs can be set to the following MAC modes:

- **Auto find ‘Adopt MAC’**

ECM adopts MAC address from first frame to pass

- **Set 'Adopt MAC' manually**

MAC address can be edited manually

- **Adopt own MAC**

ECM uses its own MAC address

- **Layer 2 Tunnel**

ECM uses its own MAC address **but also the MAC addresses of the end devices** that are connected to the ECM

Example 2:
Example Settings for WLAN:

SIEMENS

Access Point

- Basic settings (IP-Address, SSID ..)
- Mode: 5 GHz, 802.11a
- Antenna Type: ANT795-6DN
- Antenna cable length: 1 m
- Antenna mode: Antenna A
- Auth. type: WPA2-PSK with Passphrase
- Transmit Power Control: - 6 dB

Ethernet Client Module

- Basic settings (IP-Address, SSID ..)
- Mode: 5 GHz, 802.11a
- Antenna Type: ANT795-6DN
- Antenna cable length: 1 m
- Antenna mode: Antenna A
- Auth. type: WPA2-PSK with Passphrase
- Transmit Power Control: - 6 dB
- MAC mode: Auto find 'Adopt MAC'
- Background scan mode: Scan if idle
- Background scan ch. select: Enable
- Background scan channels: 36

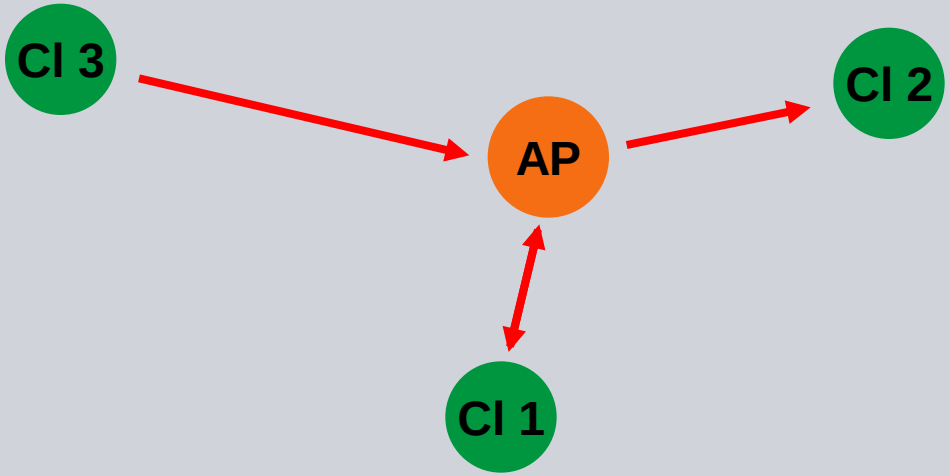
Example 3:
Multiple PN devices behind a WLAN Client

SIEMENS

“Domestic WLAN” ⇔ Real-time WLAN

“Domestic WLAN” – technical details

- In a “Domestic WLAN”, **each device transmits** (AP and clients) as soon as **data is pending** and the **channel is free** (“distributed coordination”)
- “Domestic WLAN” is therefore also known as **DCF** (**d**istributed **c**oordination **f**unction)



Example 3:
“Domestic WLAN” ⇔ Real-time WLAN

SIEMENS

“Real-time WLAN” – technical details

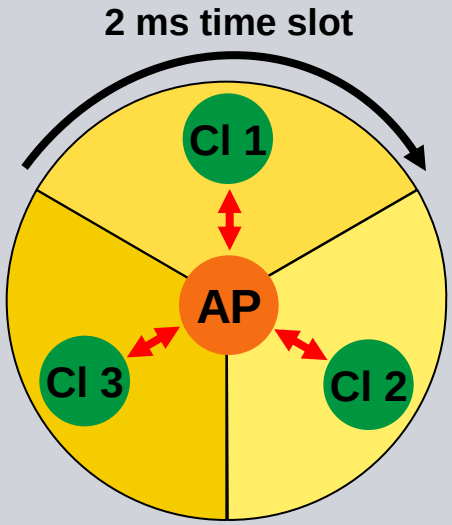
- In real-time WLAN, **the access point coordinates radio traffic**
- Real-time WLAN is therefore also known as **iPCF** (**i**ndustrial **p**oint **c**oordination **f**unction)
- The AP assigns each client a 2 ms time slot
- Now **the AP transmits data** to client 1
- **Client 1 receives this** and **answers in turn with its data**
- This process is known as **“polling”**

Note: “Real-time” doesn’t mean “immediately” but “at a pre-determinable time” i.e. deterministic

Example 3:
“Domestic WLAN” ⇔ Real-time WLAN

SIEMENS

“Real-time WLAN” – what actually happens



The AP determines the polling sequence and it cannot be influenced!

Example 3:
Example Settings for WLAN:

SIEMENS

Access Point

- Basic settings (IP address, SSID ..)
- System name: AP x
- Mode: 5 GHz, 802.11a
- Transmit power: 0 dB
- Antenna Type: RCoax leaky wave c..
- Antenna cable length: 1 m
- Antenna mode: Antenna A
- Public key 1: [16 ASCII symbols]
- Auth. type: Open System
- Encryption: enable
- iPCF enabled: enable
- Strong AES-CCM encryption: enable
- PNIO support enabled: enable
- PNIO Cycle: 64 ms
- Antenna pattern: Leaky/Directional ...

Ethernet Client module

- Basic settings (IP address, SSID ..)
- System name: Cl x
- Mode: 5 GHz, 802.11a
- MAC mode: Layer 2 Tunnel
- Transmit power: -6 dB
- Antenna Type: ANT793-4MN
- Antenna cable length: 1 m
- Antenna mode: Antenna A
- Background scan ch. select: Enable
- Background scan channels: 36 40 44
- Public key 1: [16 ASCII symbols]
- Auth. type: Open System
- Encryption: enable
- iPCF enabled: enable
- Strong AES-CCM encryption: enable

PROFIsafe
When used with Profibus or PROFInet

SIEMENS

PROFIsafe is a profile for Profibus or PROFInet

- PROFIsafe uses the same ASIC as a “standard” unit but needs safety applied at the firmware/software level.
- The diagnostics for PROFIsafe are the same as for Profibus or PROFInet (whichever you are using).
- The installation rules/guidelines for PROFIsafe are the same as for Profibus or PROFInet (whichever you are using).
- PROFIsafe uses a lot of the same principles of configuration & programming that are used in the “standard” world.

PROFIsafe
WLAN with functional safety?

SIEMENS

As mentioned previously a permanently installed cable will have better availability than a WLAN.

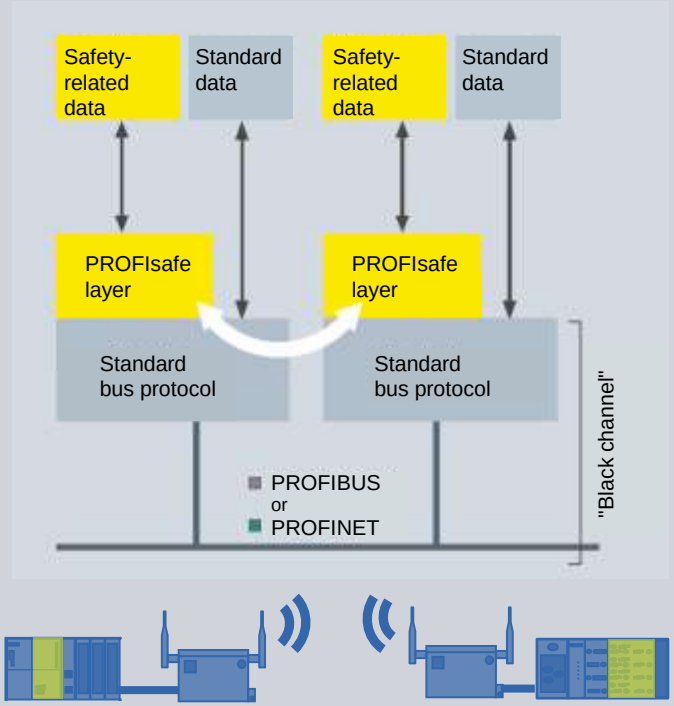
What should I consider when I need to use WLAN for a safety application?

- Always **cable if you can**. Look at WLAN if cabling isn't an option.
- Can be used for **up to SIL 3/PL e** (IEC 61508/62061/61511 & ISO 13849)
- Does the **availability** of WLAN suit the safety application? Number of retries?
- Does WLAN suit your **reaction time** for the safety application?

PROFIsafe
Failsafe communication via PROFIsafe

SIEMENS

- First communications standard developed in accordance with safety standard IEC 61508 with more than 840,000 PROFIsafe nodes implemented in over 85,000 systems
- Developed to IEC 61784-3-3, PROFIsafe is the international standard
- PROFIsafe handles potential faults (e.g. invalid addresses, delays, data loss) by means of
  - Serial numbering
  - Time monitoring
  - Authenticity monitoring
  - Additional CRC backup
- Evaluated by BGIA and TÜV



PROFIsafe supports standard and failsafe communication via one physical bus

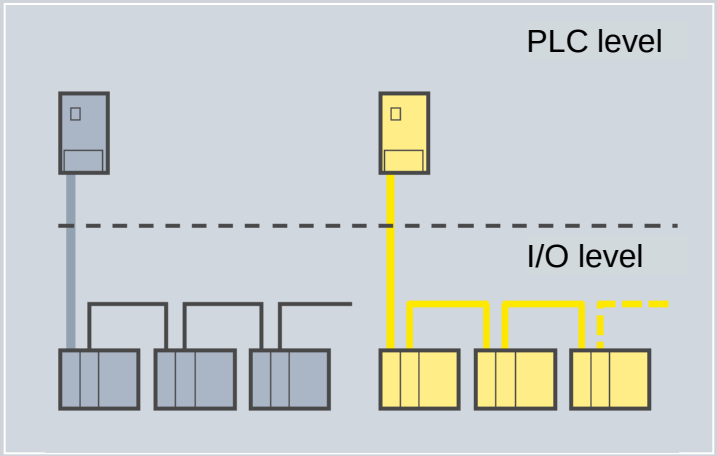
SIEMENS

Overview: Possible Errors and detection mechanism

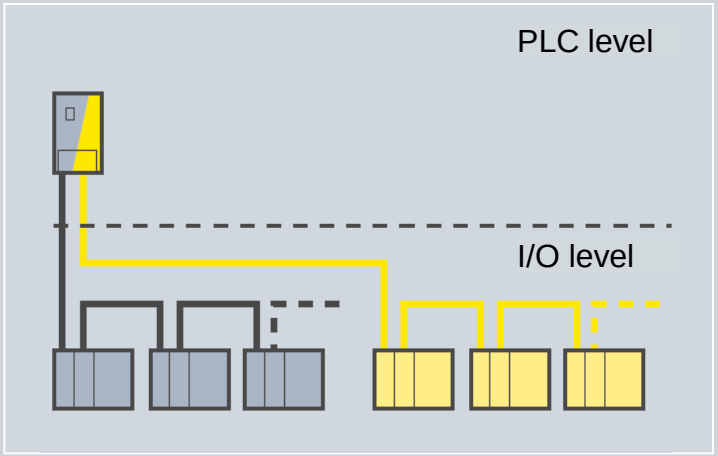
Remedy: / Failure type:	Consecutive Number	Time Out with Receipt	Codename for Sender and Receiver	Data Consistency Check
Repetition	✓			
Deletion	✓	✓		
Insertion	✓	✓	✓	
Resequencing	✓			
Data Corruption				✓
Delay		✓		
Masquerade (standard message mimics failsafe)		✓	✓	✓
Revolving memory failure within switches	✓			

PROFIsafe
High flexibility for applications

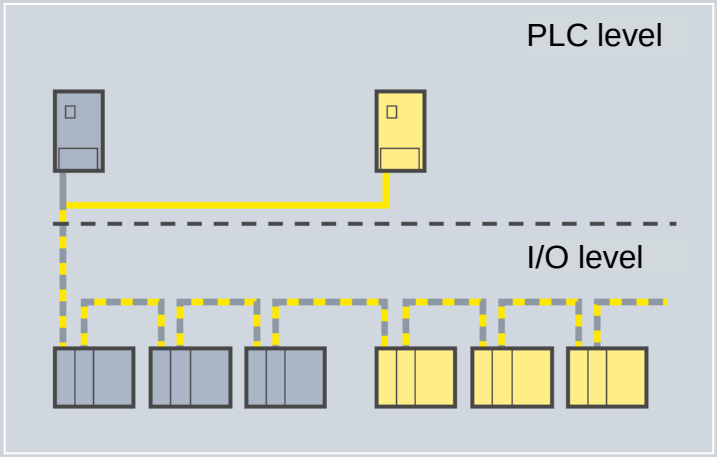
SIEMENS



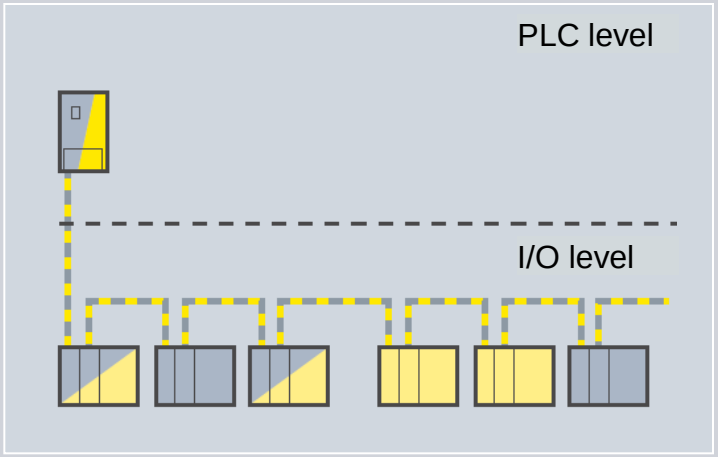
Separation of PLC, I/O and bus



One PLC, but separation of I/O and bus



One bus, but separation of PLC and I/O



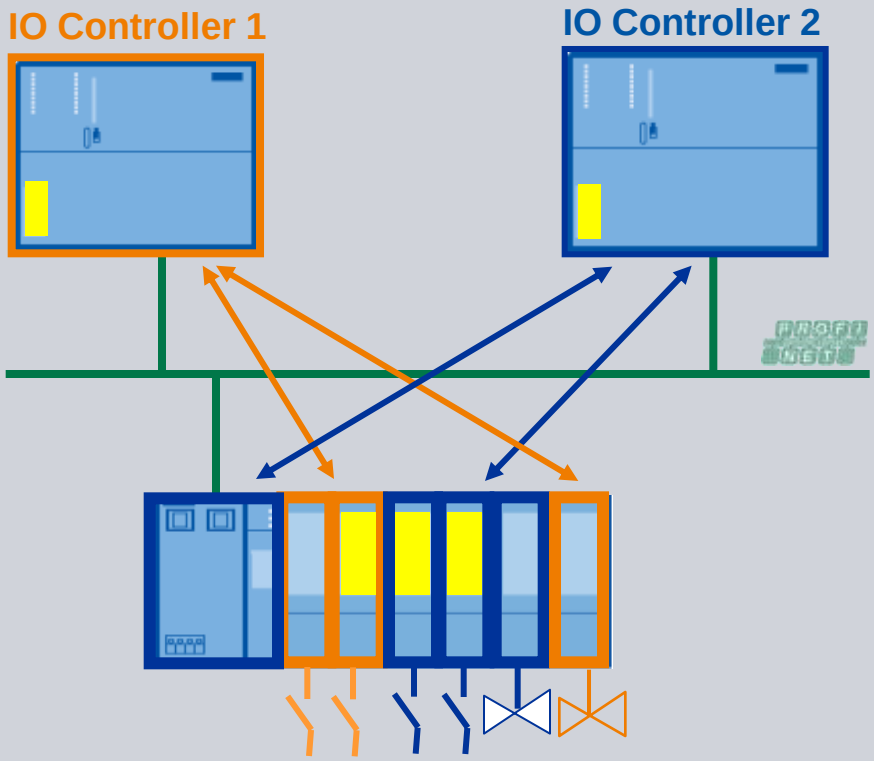
One PLC, one bus and mixed I/O

PROFIsafe
PROFInet “Shared Device”

SIEMENS

Access to one device from several controllers

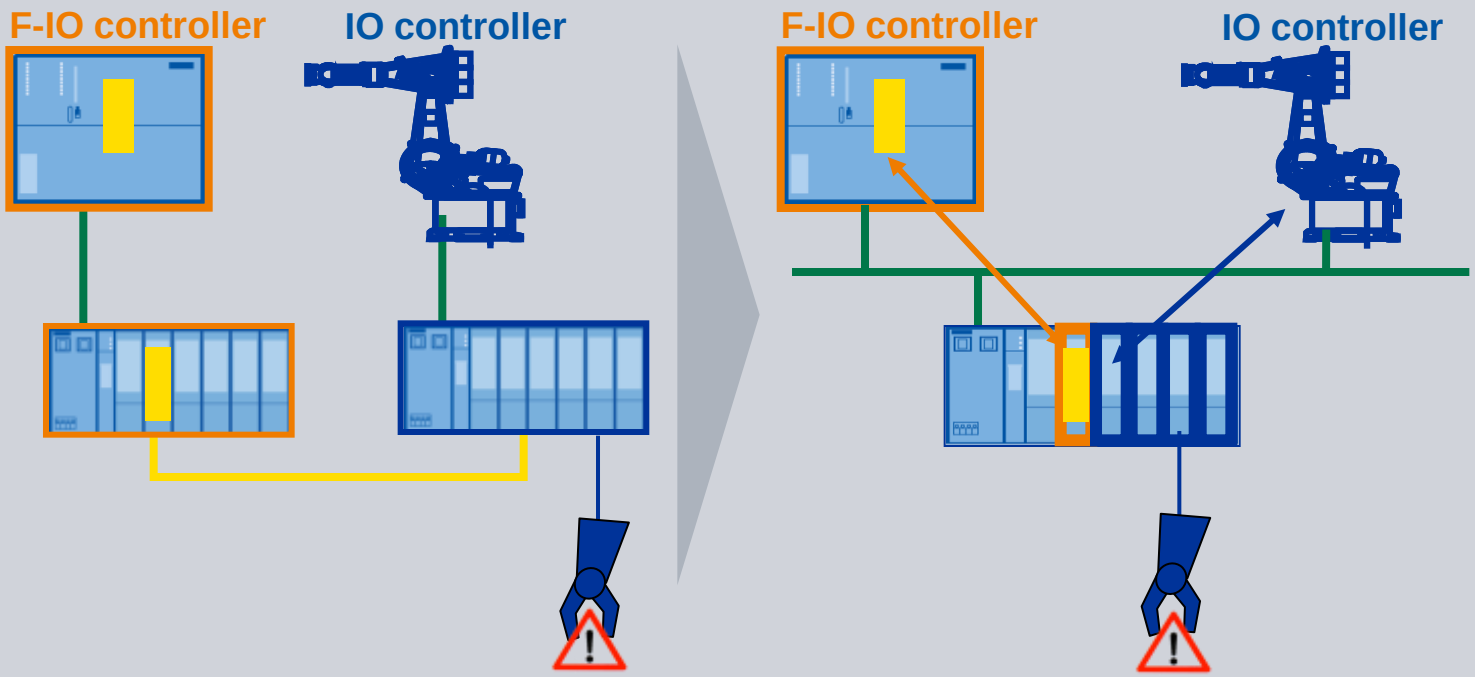
- Flexible assignment of channels and modules to different controllers
- For inputs and outputs



PROFIBUS - PROFINET user conference 2010
Celebrating 20 Years of PROFIBUS

PROFIsafe
“Shared Device” and F-shutdown

SIEMENS



F-shutdown

- Less cabling
- Lower hardware overhead
- Simpler engineering

SIEMENS

Thank you for your attention!

Peter Brown
HelpDesk Team Leader
Functional Safety Professional
Siemens IA&DT

Phone: +44 161 446 - 5545

Any Questions?

PROFIsafe