



# **Permanent Network Monitoring, dalla progettazione alla prevenzione dei guasti**

*Micaela Caserza Magro*  
*Alberto Sibono*

# Introduzione – Argomenti trattati



**1**    **Industria 4.0**

**2**    **Come funziona tecnicamente la  
comunicazione di rete?**

**3**    **PROFIBUS & PROFINET International (PI)**

**4**    **Ciclo di vita della diagnostica di rete**

**5**    **Network troubleshooting**

**6**    **Permanent Network Monitoring**

# INDUSTRY 4.0

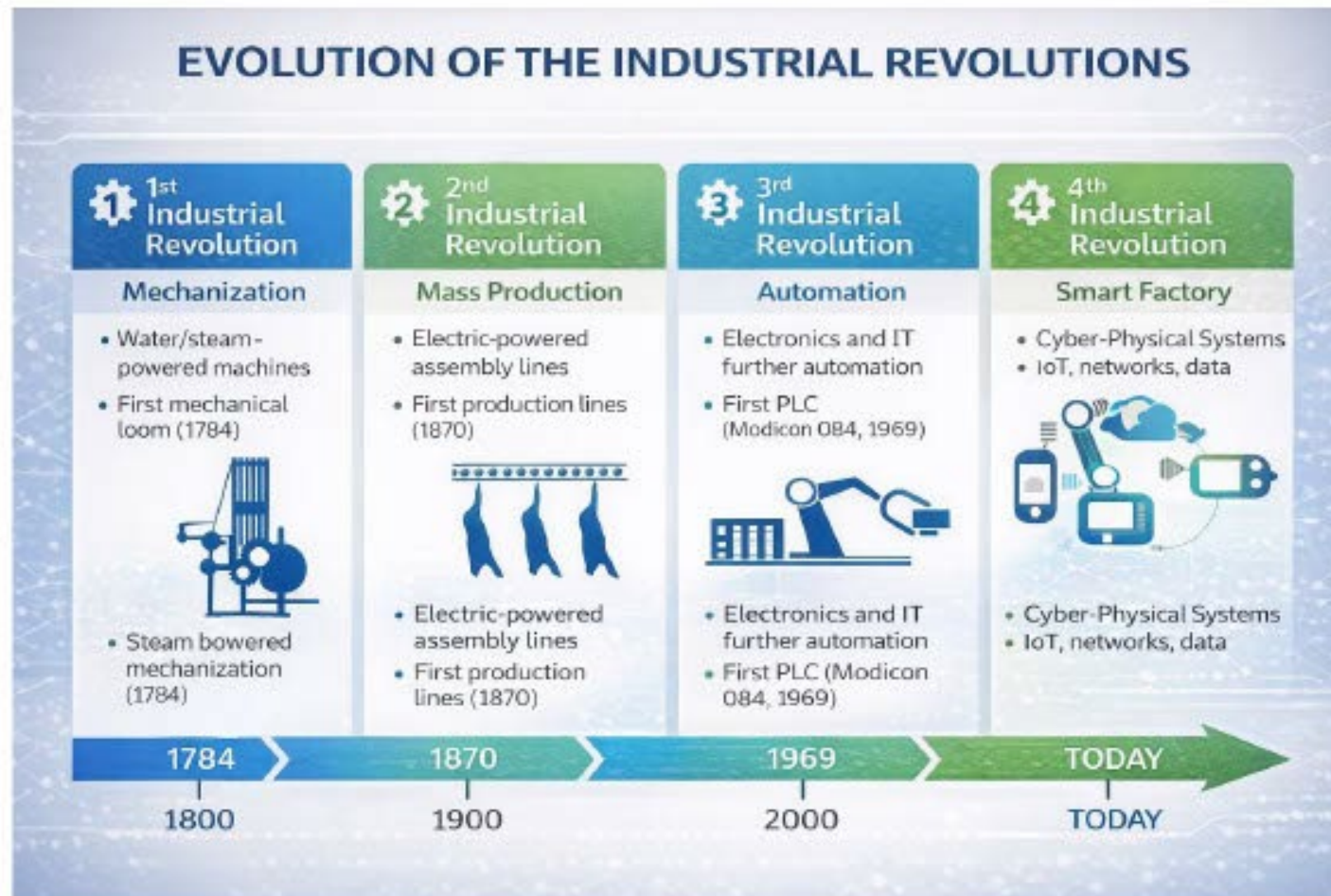


## Industria 4.0



1	Industria 4.0
2	Come funziona tecnicamente la comunicazione di rete?
3	PROFIBUS & PROFINET International (PI)
4	Ciclo di vita della diagnostica di rete

# Industry 4.0: la storia



# Industry 4.0: ma cosa intendiamo?



La **fabbrica digitale e connessa**, dove:

- macchine
- sistemi informatici
- sensori
- operatori
- sono interconnessi tramite reti industriali e sistemi IT.

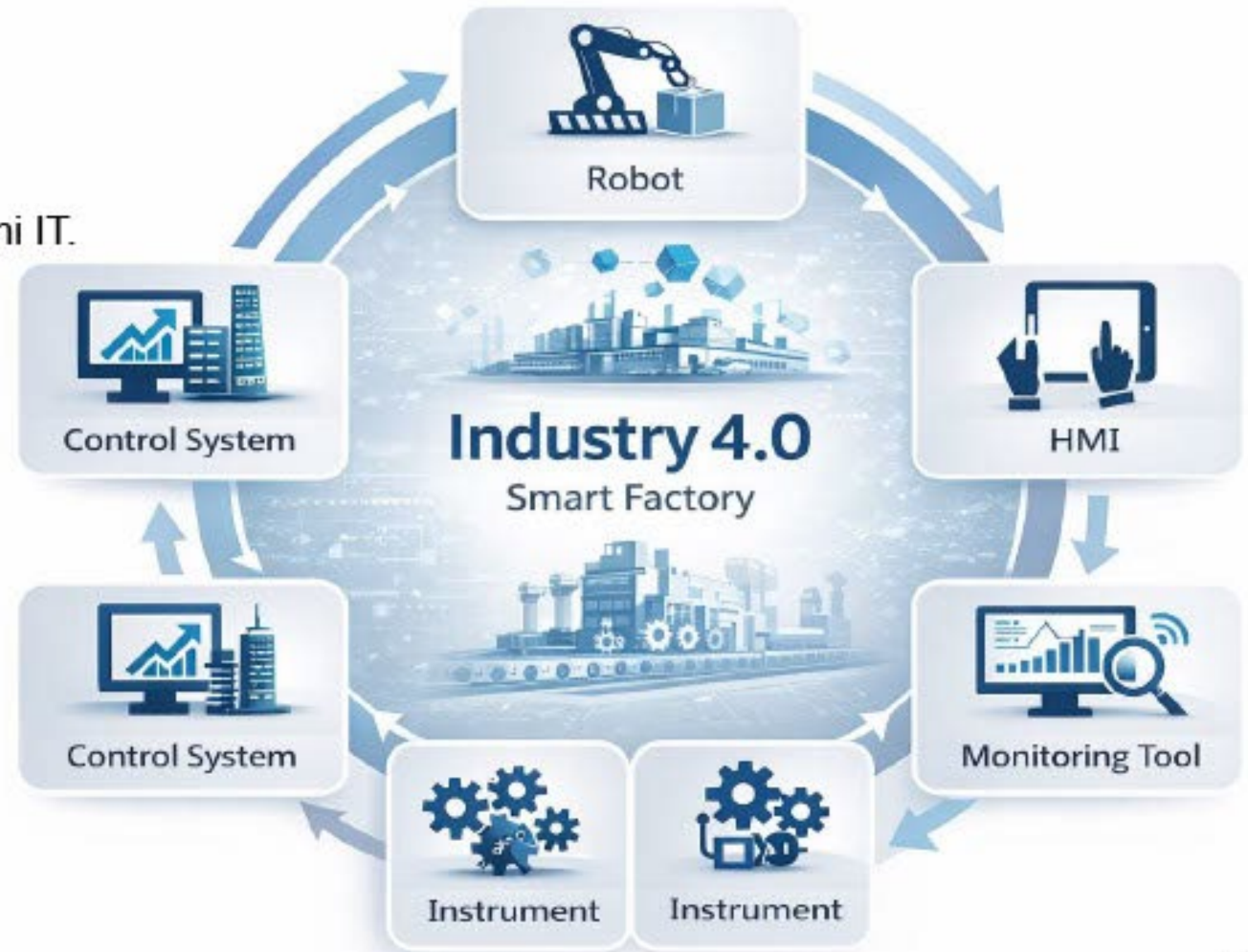
I componenti attorno alla **Smart Factory**

## 1. Robot

Robot industriali utilizzati per:

- assemblaggio
- manipolazione
- automazione dei processi

Sono controllati da sistemi di automazione e comunicano tramite **reti industriali**.



# Industry 4.0: ma cosa intendiamo?



## 2. HMI (Human Machine Interface)

Interfaccia uomo-macchina.

Serve per:

- visualizzare lo stato della macchina
- comandare impianti
- visualizzare allarmi e dati

Esempi:

- pannelli operatore
- SCADA
- sistemi di supervisione.

## 4. Monitoring tool

Strumenti di monitoraggio che analizzano:

- prestazioni macchina
- stato della rete
- efficienza impianto
- anomalie

Qui rientrano ad esempio:

- sistemi di diagnostica
- analisi dati
- condition monitoring.

## 3. Sensor

Sensori che misurano grandezze fisiche:

- temperatura
- pressione
- posizione
- vibrazioni

Sono fondamentali per raccogliere **dati dal processo produttivo**.

## 5. Instrument

Strumenti industriali e dispositivi di campo:

- attuatori
- valvole
- strumenti di misura
- controllori locali.

# Industry 4.0: ma cosa intendiamo?



## 6. Control System

Sistema di controllo dell'impianto.

Esempi:

- PLC
- DCS
- sistemi di automazione

Il PLC riceve dati dai sensori e controlla attuatori e macchine.

**Industry 4.0 nasce dall'integrazione di tutti questi elementi:**

```
Sensori
↓
PLC / sistemi di controllo
↓
Robot e macchine
↓
HMI e supervisione
↓
Sistemi di monitoraggio e analisi dati
```

Tutto collegato tramite **reti industriali (Ethernet industriale, PROFINET, ecc.)**.

# Blocchi funzionali di industria 4.0



## 1. MES & Production Profile (OEE)

### Gestione della produzione.

Serve per:

- raccogliere dati dalle macchine
- monitorare la produzione
- calcolare l'OEE (**Overall Equipment Effectiveness**)

OEE misura:

- disponibilità macchina
- prestazioni
- qualità.

Serve per capire **quanto è efficiente una linea produttiva.**



# Blocchi funzionali di industria 4.0



## 2. Production Testing Equipment

Questa parte riguarda i **sistemi di test e controllo qualità automatico**.

Include:

- Machine Vision (telecamere industriali)
- schede I/O
- piattaforme di calcolo
- controllori.
- Servono per:
  - verificare i prodotti
  - controllare i processi
  - identificare difetti.

## 3. Factory Environmental Monitoring

Qui si monitorano **le condizioni dell'impianto**:

- consumo elettrico
- energia
- acque industriali
- ambiente di fabbrica.

Serve per:

- **efficienza energetica**
- sostenibilità
- controllo dei costi.

# Blocchi funzionali di industria 4.0



## 4. Predictive Maintenance

Questa è una delle parti più importanti dell'Industria 4.0.

Significa **manutenzione predittiva**.

I sensori raccolgono dati su:

- vibrazioni
- temperatura
- stato macchina
- prestazioni.

Con questi dati si possono:

- prevedere guasti
- programmare manutenzione
- evitare fermi impianto.

## 5. Machine Automation

Qui troviamo l'automazione industriale vera e propria:

- robot industriali
- AGV (veicoli autonomi)
- macchine automatiche.

Questi sistemi sono controllati da:

- PLC
- controllori
- reti industriali.

# Blocchi funzionali di industria 4.0



Industry 4.0 nasce dall'integrazione di cinque livelli:

Macchine e robot



Sensori e dispositivi di campo



Raccolta dati tramite rete



Sistemi di analisi e monitoraggio



Ottimizzazione della produzione

In altre parole: **la fabbrica diventa una rete di dati.**



# Comunicazione diretta



1	Industria 4.0
2	<b>Come funziona tecnicamente la comunicazione di rete?</b>
3	PROFIBUS & PROFINET International (PI)
4	Ciclo di vita della diagnostica di rete

# Come funziona tecnicamente la comunicazione di rete?



Nella sezione precedente abbiamo visto come nella fabbrica Industry 4.0 tutti i dispositivi siano interconnessi tramite rete.

Ma questa comunicazione non avviene in modo casuale: segue un modello strutturato chiamato **modello ISO-OSI**, che descrive i diversi livelli della comunicazione.

**La comunicazione di rete non è un unico blocco, ma una pila di livelli**

**Pila OSI e problemi di rete possono avvenire a livelli diversi.**

Livello	Problema
Fisico	cavo danneggiato
Data link	errori Ethernet
Rete	configurazione IP
Trasporto	perdita pacchetti
Applicazione	errore PROFINET

# Come funziona tecnicamente la comunicazione di rete?



## 1. Dati affidabili

La fabbrica digitale funziona solo se i dati sono:

- corretti
- completi
- non corrotti
- disponibili

Esempi di problemi se i dati non sono affidabili:

- errori nei telegrammi
- pacchetti persi
- dati incoerenti nei sistemi MES o SCADA

Questo è fondamentale per:

- controllo processo
- manutenzione predittiva
- analisi produzione.



# Come funziona tecnicamente la comunicazione di rete?



## 2. Infrastruttura di rete

Serve una **rete industriale adeguata** che permetta la comunicazione tra:

- PLC
- robot
- sensori
- sistemi SCADA
- sistemi MES
- sistemi IT

Questa infrastruttura include:

- switch industriali
- cablaggio Ethernet
- reti PROFINET / Ethernet IP
- segmentazione della rete.

Se la rete è progettata male:

- si generano congestioni
- ritardi
- errori di comunicazione.

## 3. Servizi del sistema di comunicazione

Sono i **servizi software e protocolli** che permettono la **comunicazione** tra i dispositivi.

Esempi:

- protocolli industriali (PROFINET, Modbus TCP)
- servizi di diagnostica
- sincronizzazione
- gestione della rete.

Questi servizi operano nei **livelli superiori del modello OSI**.

# Come funziona tecnicamente la comunicazione di rete?



## 4. Tempistiche per il trasferimento dati

In ambito industriale il tempo di comunicazione è fondamentale.

La rete deve garantire:

- **latenza bassa**
- **tempi deterministici**
- **sincronizzazione**

Ad esempio:

- cicli PROFINET in tempo reale
- comunicazione PLC ↔ I/O.
- Se la rete è lenta o instabile:
- il controllo macchina può fallire.

## 5. Il modello OSI rappresenta la **struttura della comunicazione**:

Livello	Funzione
Applicazione	protocolli industriali
Trasporto	TCP / UDP
Rete	IP
Data Link	Ethernet
Fisico	cavi, fibra

# Come funziona tecnicamente la comunicazione di rete?



- Nella slide precedente abbiamo visto che la comunicazione nelle reti industriali segue il modello ISO-OSI e richiede infrastrutture di rete affidabili e tempi di comunicazione deterministici.
- Nella pratica queste comunicazioni sono implementate attraverso diversi protocolli di **Industrial Ethernet**, come PROFINET, EtherCAT o Ethernet/IP.

Tecnologia	Descrizione	Standard
Industrial Ethernet	Standard industriale basato sulla tecnologia Ethernet	IEEE 802.3
PROFINET	Principale protocollo Industrial Ethernet per l'automazione industriale	IEC 61158/IEC 61784
EtherCAT	Protocollo di comunicazione ad alte prestazioni per Ethernet deterministico	IEC 61158
EtherNet/IP	Standard di comunicazione industriale basato su TCP/IP e UDP/IP su Ethernet	IEC 61784-1
POWERLINK	Protocollo realtime deterministico open source basato su Ethernet	IEC 61508
SERCOS	Standard internazionale per comunicazioni realtime basato su Ethernet	IEC 61491/IEC 61158/IEC 61784/IEC 61508
Industrial Wireless LAN	Comunicazione industriale wireless basata sullo standard Wi-Fi	IEEE 802.11

# Come funziona tecnicamente la comunicazione di rete?



La distribuzione (quota di mercato / diffusione) dei principali protocolli Industrial Ethernet è come segue:

Protocollo	Quota
Ethernet/IP	30%
PROFINET	28%
Modbus TCP	22%
POWERLINK	11%
EtherCAT	4%
Altri	5%

Oggi l'**automazione industriale utilizza principalmente Industrial Ethernet** e in particolare tre protocolli dominano il mercato:

1. **Ethernet/IP**
2. **PROFINET**
3. **Modbus TCP**

insieme coprono circa **80% delle reti industriali**.



# Comunicazione diretta



1	Industria 4.0
2	Come funziona tecnicamente la comunicazione di rete?
3	<b>PROFIBUS &amp; PROFINET International (PI)</b>
4	Ciclo di vita della diagnostica di rete

# PROFIBUS & PROFINET International (PI)



- Abbiamo visto che il modello OSI ci descrive come funziona una comunicazione di rete a livello teorico. Nelle reti industriali questa architettura viene implementata attraverso protocolli specifici come PROFIBUS, PROFINET, EtherCAT o Ethernet/IP.
- Nei sistemi di automazione troviamo solitamente due grandi famiglie di tecnologie: i fieldbus tradizionali, come PROFIBUS basati su RS-485, e le reti Industrial Ethernet più moderne, come PROFINET.

## 1. PROFIBUS

- è un **fieldbus tradizionale**
- usa come mezzo fisico **RS-485**
- quindi:
  - **PROFIBUS → RS-485**
  - caratteristiche:
    - comunicazione seriale
    - velocità limitata
    - molto usato negli anni 90-2000

Pila OSI



| implementata da



Protocolli industriali



| PROFIBUS → RS485

| PROFINET → Ethernet

| EtherCAT

| Ethernet/IP

# PROFIBUS & PROFINET International (PI)



## 2. PROFINET

- è l'evoluzione moderna
- usa **Ethernet industriale**

quindi:

**PROFINET → Ethernet**

caratteristiche:

- comunicazione Ethernet
- velocità molto più alta
- base dell'**Industria 4.0**

Fieldbus

├─ PROFIBUS → RS485 (rete seriale)

└─ PROFINET → Ethernet (rete moderna)

**Le reti industriali sono passate da bus seriali (Fieldbus) a Ethernet industriale.**



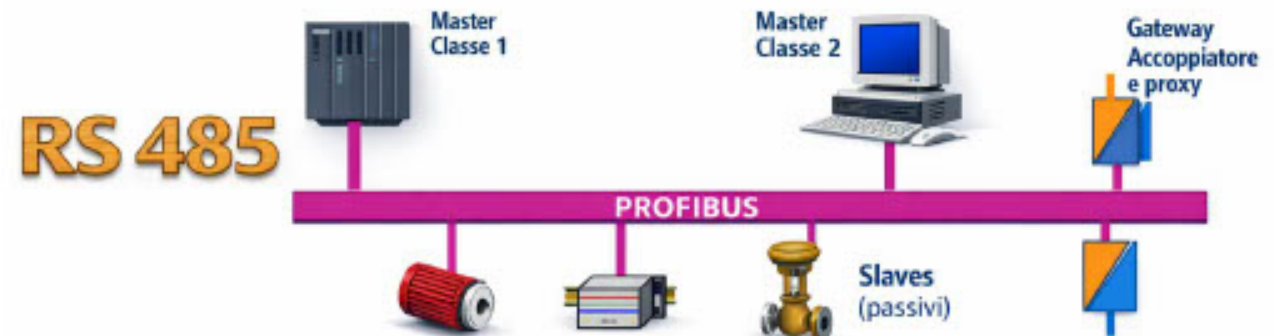
# Architettura PROFIBUS

In una rete PROFIBUS abbiamo normalmente un master principale, tipicamente il PLC, che controlla ciclicamente gli slave. Gli slave sono dispositivi di campo come sensori, attuatori o moduli I/O che rispondono alle richieste del master. La comunicazione avviene su un bus seriale RS-485.

Punti importanti da sottolineare:

- **Master class 1** → PLC
- **Master class 2** → tool di diagnostica
- **Slave** → sensori e attuatori
- **Gateway** → collegamento ad altre reti

Master Classe 1	Master Classe 2	Slave	Slave	Gateway/Accoppiatore
<ul style="list-style-type: none"><li>✓ Controllo principale</li><li>✓ Scambio ciclico con gli slaves</li><li>✓ Scambio aciclico con gli slaves</li><li>✓ Comunicazione prioritaria</li><li>✓ es: PLC / scheda di comunicazione</li></ul>	<ul style="list-style-type: none"><li>✓ Tool di configurazione</li><li>✓ Scambi aciclici</li><li>✓ Comunicazione non prioritaria</li><li>✓ es: DTM / EDD</li></ul>	<ul style="list-style-type: none"><li>✓ Equipements d'acquisizione</li><li>✓ Equipements d'attuazione</li></ul>	<ul style="list-style-type: none"><li>✓ Equipements d'attuazione</li><li>✓ Comunicazione su iniziativa del master</li></ul>	<ul style="list-style-type: none"><li>✓ Nessun ruolo attivo nella rete</li><li>✓ Connessioni verso altre reti superiori</li><li>✓ Connessioni verso il livello campo/sensori</li></ul>



# Categorie di errori in PROFIBUS



Ora introduciamo **la diagnosi basata sui livelli OSI**.

I problemi di comunicazione possono nascere in **livelli diversi**.

## 1. Livello fisico

- Problemi legati al bus o al cablaggio.
- Sintomi:
  - ✓ il device **non comunica**
  - ✓ la comunicazione **cade periodicamente**

## 2. Livello applicazione

- Problemi logici o software.
- Sintomi:
  - ✓ dati non validi
  - ✓ errori di configurazione
  - ✓ problemi sugli I/O
- Transizione:
  - ✓ Nella pratica industriale, però, la maggior parte dei problemi PROFIBUS non nasce dal protocollo ma dal livello fisico della rete.

### Livello Fisico

- Il device **NON** comunica più
- Il device perde periodicamente la comunicazione

### Livello Applicazione

- Dati non validi (calibrazione o bug)
- Diagnostica del device (problemi sugli I/O)

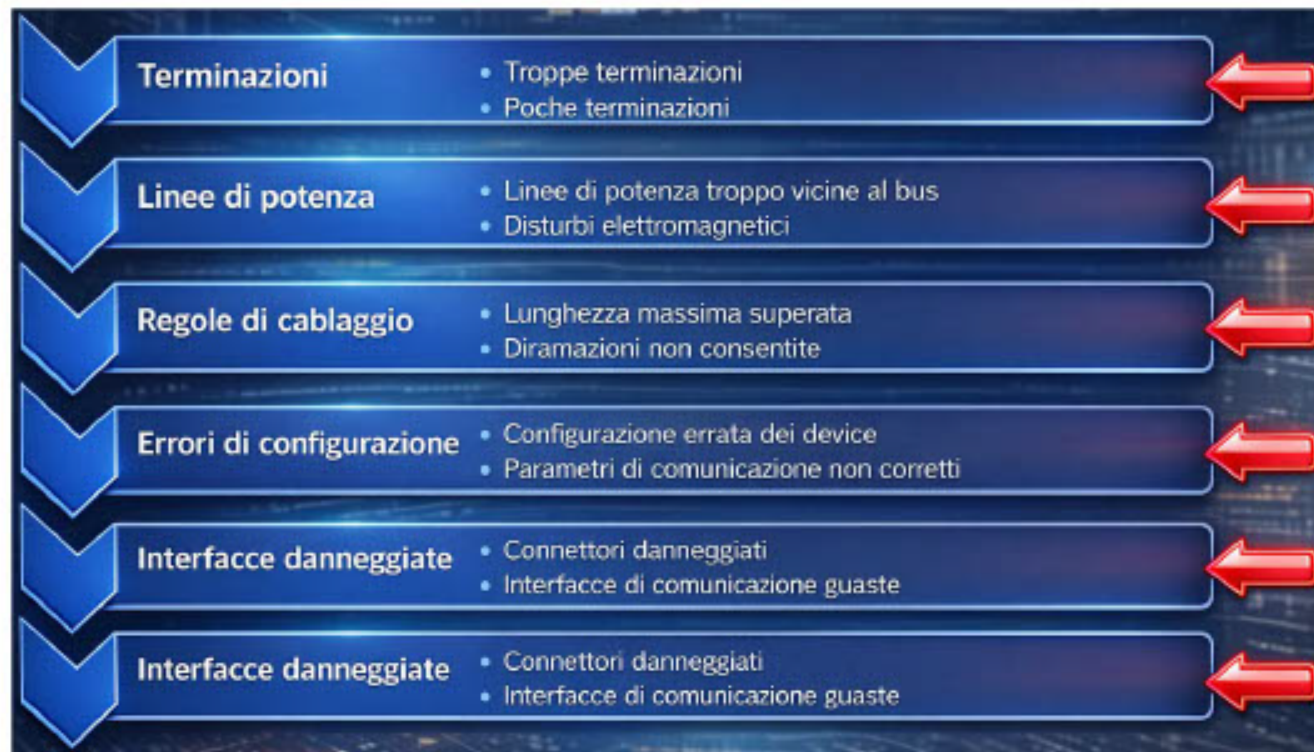
# PROFIBUS - Troubleshooting reale



La maggior parte dei guasti PROFIBUS deriva da **problemi di installazione**.

Cause tipiche:

- 1. Terminazioni**
  - troppe terminazioni
  - terminazioni mancanti
- 2. Disturbi elettromagnetici**
  - linee di potenza vicine al bus
  - interferenze EMC
- 3. Regole di cablaggio**
  - lunghezza massima superata
  - diramazioni non consentite
- 4. Configurazione**
  - parametri sbagliati
  - indirizzi duplicati
- 5. Interfacce**
  - connettori danneggiati
  - schede di comunicazione guaste



I guasti possono essere classificati per livello OSI, **ma nella pratica la maggior parte dei problemi deriva dal livello fisico della rete, cioè da cablaggio, terminazioni e interferenze.**

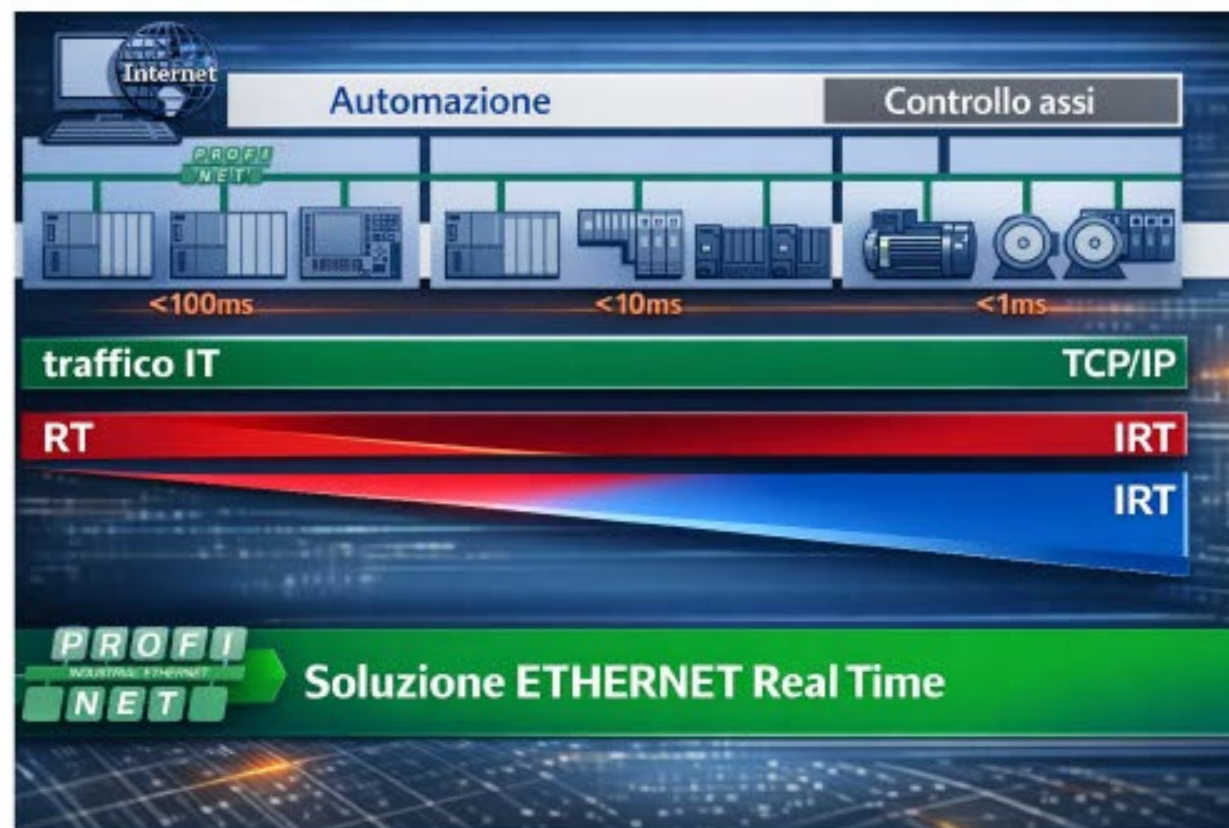
# PROFINET



- Storicamente l'automazione industriale utilizzava fieldbus come PROFIBUS basati su comunicazione seriale RS-485.
- **Con l'evoluzione dell'Industry 4.0** e la crescente integrazione con i sistemi IT si è passati a soluzioni basate su Ethernet industriale come PROFINET.

Fieldbus tradizionali  
↓  
Industrial Ethernet  
↓  
PROFINET

Utilizzare Ethernet nelle reti industriali introduce nuovi vantaggi **ma anche nuove sfide legate alla gestione del traffico e ai requisiti di tempo reale.**



# PROFINET



PROFINET permette di gestire **diversi tipi di traffico sulla stessa rete Ethernet**.

Tre livelli principali:

- 1. Traffico IT**
  - basato su **TCP/IP**
  - comunicazione normale
  - tempi tipici <100 ms
- 2. Real Time (RT)**
  - comunicazione per automazione
  - tempi <10 ms
- 3. Isochronous Real Time (IRT)**
  - comunicazione deterministica
  - controllo motion
  - tempi <1 ms

## Specifiche PROFINET



PROFIBUS & PROFINET International (PI)  
Germany

- ✓ Definiscono e mantengono lo standard PROFINET
- ✓ Responsabili della certificazione dei dispositivi
- ✓ Gestiscono l'ecosistema globale PROFINET



PROFINET utilizza la stessa infrastruttura Ethernet **ma assegna priorità diverse ai diversi tipi di traffico per garantire il tempo reale richiesto dall'automazione industriale**.

Anche con queste tecnologie avanzate, **nella pratica industriale possono comunque verificarsi problemi di comunicazione**.

# PROFINET - Diagnostica reale



## 1. Problemi di rete (livello fisico / infrastruttura)

- cavi danneggiati
- disturbi EMC
- errori di cablaggio
- Tipicamente causano:
- perdita di pacchetti
- instabilità della comunicazione
- device che spariscono dalla rete

## 2. Problemi di configurazione

- indirizzi IP duplicati
- parametri errati
- dispositivi non configurati
- Tipicamente causano:
- impossibilità di comunicare
- device non raggiungibili
- errori di sistema

### Problemi di rete

- Cavi danneggiati
- Disturbi EMC
- Errori di cablaggio

### Problemi di configurazione

- Indirizzi duplicati
- Porta non aperta
- Indirizzi non assegnati

Proprio per individuare rapidamente questi problemi nelle reti industriali moderne **diventa fondamentale utilizzare strumenti di diagnosi e monitoraggio della rete.**



# Ciclo di vita della diagnostica di rete

## 1 Pianificazione

- Definizione requisiti di rete
- Safety e Security
- Parametri di qualità

## 2 Progettazione

- Architettura di rete
- Dimensionamento
- Verifica prestazioni

## 3 Validazione

- Test prestazioni
- Verifica tempi di ciclo
- Verifica cablaggio

## 4 Messa in servizio

- Installazione e cablaggio
- Configurazione dispositivi
- Verifica comunicazione

## 5 Esercizio

- Rete operativa
- Funzionamento continuo
- Controllo stato rete

## 6 Troubleshooting

- Diagnostica di rete
- Identificazione guasti
- Analisi traffico

## 7 Monitoraggio continuo

- Monitoraggio prestazioni rete
- Statistiche e allarmi
- Manutenzione predittiva

1

Industria 4.0

2

Come funziona tecnicamente la comunicazione di rete?

3

PROFIBUS & PROFINET International (PI)

4

Ciclo di vita della diagnostica di rete

# Ciclo di vita della diagnostica di rete



# 6

## Network Troubleshooting

- ✓ Diagnostica di rete
- ✓ Identificazione guasti
- ✓ Analisi traffico



# Network troubleshooting



5	Network troubleshooting
6	Permanent Network Monitoring

# Che tipo di diagnosi posso fare su una rete?



- Quando si verifica un **guasto** su una rete industriale, non esiste un unico modo per fare diagnosi.
- In realtà possiamo utilizzare **diversi livelli di diagnostica**, che ci permettono di analizzare il problema in modo progressivo.
- L'idea fondamentale è che **non tutte le diagnosi hanno la stessa profondità**.
- Spesso si parte da verifiche molto semplici e veloci, e solo se necessario si passa ad analisi più approfondite.
  1. Per esempio, la prima cosa che un tecnico fa sul campo è spesso una **verifica visiva**: controllare i LED dei dispositivi, degli switch o dei moduli di I/O per capire se c'è un errore evidente.
  2. Se questo non è sufficiente, si passa a **test di connettività**, ad esempio verificando se i dispositivi sono raggiungibili sulla rete.
  3. Successivamente possiamo analizzare **la diagnostica fornita direttamente dai dispositivi**, che spesso indicano lo stato di funzionamento o eventuali fault.
  4. Se il problema non è ancora chiaro, si può entrare in un livello più avanzato, come **l'analisi del traffico di rete**, osservando i pacchetti che vengono scambiati tra i dispositivi.
  5. Infine, nei casi più complessi, può essere necessario verificare **la parte fisica della rete**, ad esempio controllando i cavi, le terminazioni o eventuali problemi di cablaggio.



# Dispositivo di diagnostica per reti PROFINET



## 4 analisi del traffico



PNMA II – PROFINET Monitoring and Analysis (della società Indu-Sol)

1. PNMA II non è un protocol analyzer ma un "Network Performance Monitor"
2. A cosa serve
  - È uno strumento hardware di analisi della rete usato per:
    - ✓ Monitorare il traffico PROFINET
    - ✓ Analizzare qualità della comunicazione
    - ✓ Individuare problemi di rete
3. Funzioni principali
  - Registrazione dei telegrammi PROFINET
  - Analisi del carico di rete
  - Rilevazione di jitter e ritardi
  - Diagnostica di errori di comunicazione
  - Monitoraggio continuo della rete



# Architettura PNMA II in reti PROFINET



## 1. Livello 1 — Rete PROFINET

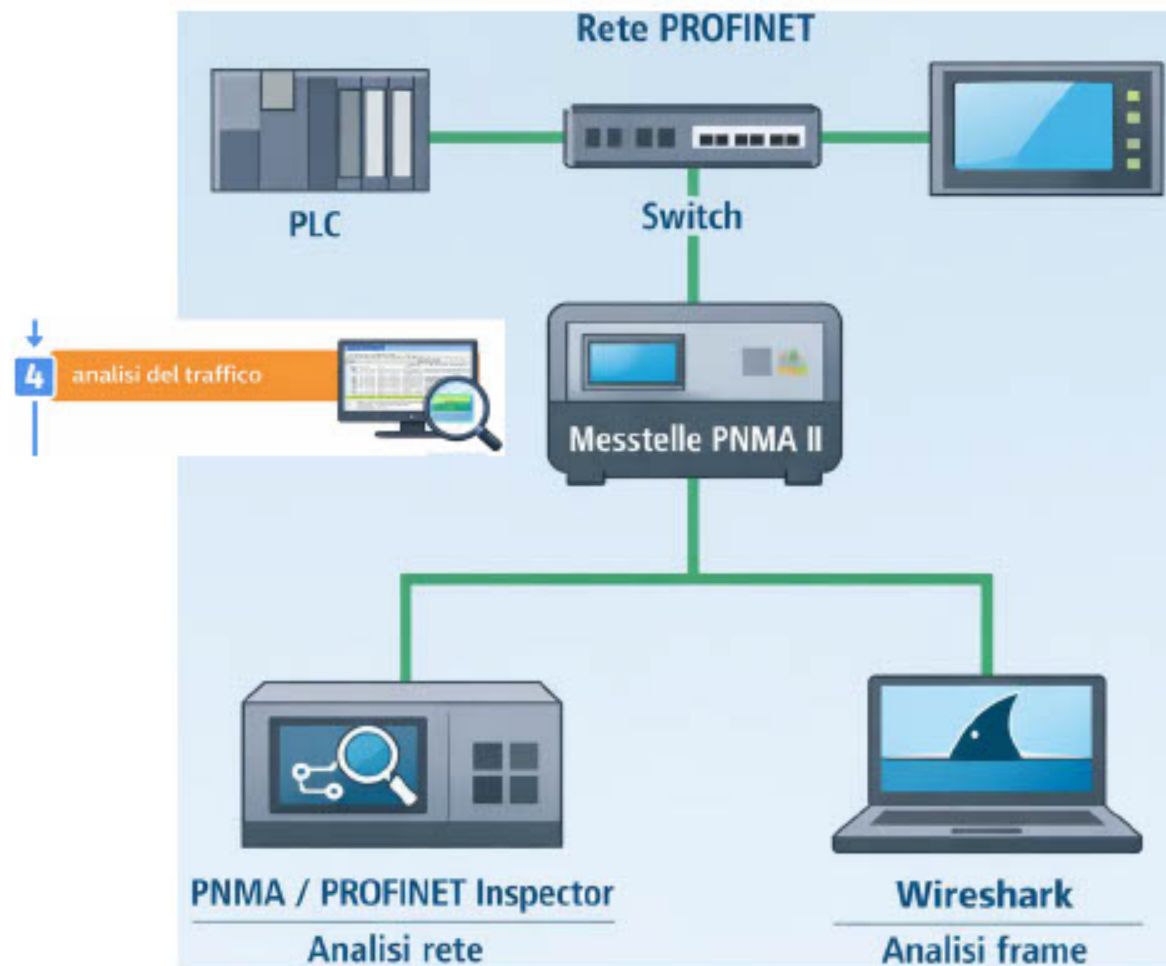
- In alto nella figura c'è la rete reale ad esempio:
  - ✓ **Controller (PLC)**
  - ✓ **Switch**
  - ✓ **Dispositivi di campo**
- Il traffico PROFINET scorre normalmente tra questi dispositivi.

PLC — Switch — Device

- ✓ Qui **non viene modificato nulla** della rete.

## 2. Livello 2 — Messstelle PNMA II (stazione di misura)

- La **Messstelle PNMA II** è il dispositivo verticale inserito nella rete. “Messstelle” in tedesco significa **stazione di misura**.
- Funzioni principali:
  - ✓ si collega alla rete PROFINET
  - ✓ intercetta il traffico
  - ✓ lo duplica
  - ✓ invia la copia verso gli strumenti di analisi
- È quindi il punto di acquisizione dei dati.

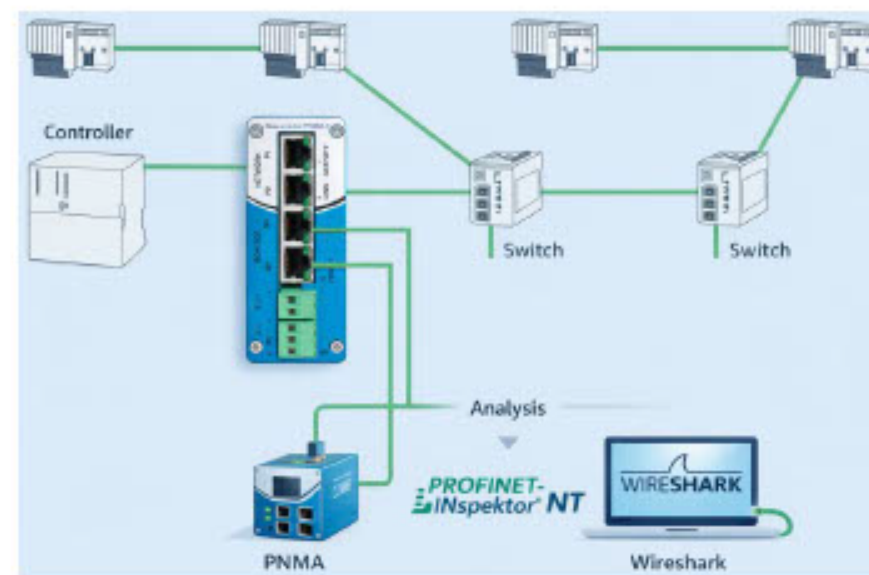


# Architettura PNMA II in reti PROFINET



## 3. Livello 3 — Analisi (PNMA / Software / Wireshark)

- Il traffico duplicato viene inviato agli strumenti di analisi.
- Possono essere:
  - **PNMA / PROFINET-Inspector** analisi delle **prestazioni della rete** che calcola:
    - ✓ jitter
    - ✓ telegram gaps
    - ✓ carico della rete
    - ✓ qualità della comunicazione
    - ✓ stabilità del ciclo PROFINET
  - Wireshark che fa l'analisi del **contenuto dei pacchetti** ad esempio:
    - ✓ DCP
    - ✓ LLDP
    - ✓ RPC
    - ✓ configurazione IP
    - ✓ handshake PROFINET



# Architettura PNMA II in reti PROFINET



Wireshark serve **perché fa un tipo di analisi completamente diverso rispetto a PNMA II / PROFINET-Inspector**. Sono **complementari**, non alternativi. La differenza fondamentale è questa:

Strumento	Tipo di analisi
PNMA II / PROFINET-Inspector	analisi delle prestazioni della rete
Wireshark	analisi del contenuto dei telegrammi

Il **Messstelle PNMA II** quindi svolge la funzione di:

- TAP attivo / network tap
- stazione di misura

**PNMA / PROFINET Inspector** è lo **strumento di analisi** che riceve il traffico duplicato e calcola:

- jitter
- telegram gaps
- carico di rete
- qualità della comunicazione
- stabilità dei cicli PROFINET



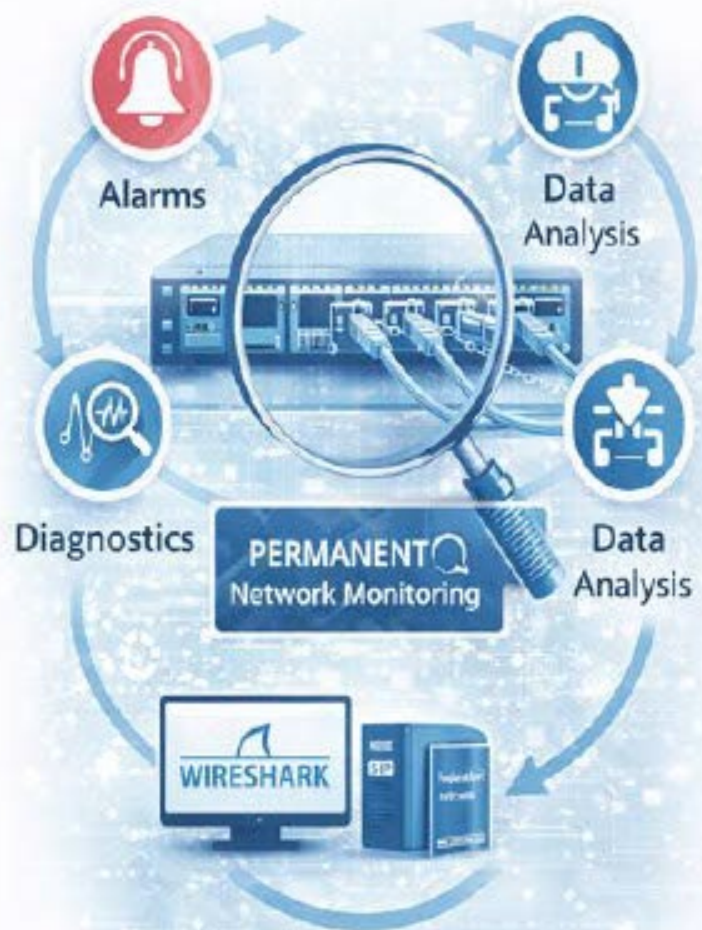
# PNMA / PROFINET Inspector - WIRESHARK



Funzione	Wireshark	PNMA / PROFINET-Inspector
Jitter	⚠ Non diretto – bisogna esportare i timestamp e calcolarlo	✓ Calcolato automaticamente
Telegram gaps	⚠ Analisi manuale dei tempi tra i frame	✓ Rilevati automaticamente
Load di rete	✓ Sì (statistiche traffico / throughput)	✓ Sì
Errori di comunicazione	⚠ Visibili nei frame ma non classificati automaticamente	✓ Identificati e classificati
Problemi di timing	⚠ Possibile solo con analisi manuale	✓ Evidenziati automaticamente
Topologia di rete automatica	✗ No	✓ Sì
Diagnostica dei dispositivi	⚠ Parziale (leggendo pacchetti DCP / LLDP)	✓ Sì
Analisi dei cicli real-time	⚠ Possibile ma manuale	✓ Sì
Qualità del bus / qualità rete	✗ No	✓ Sì
Jitter deterministico	✗ No	✓ Sì



## PERMANENT NETWORK MONITORING



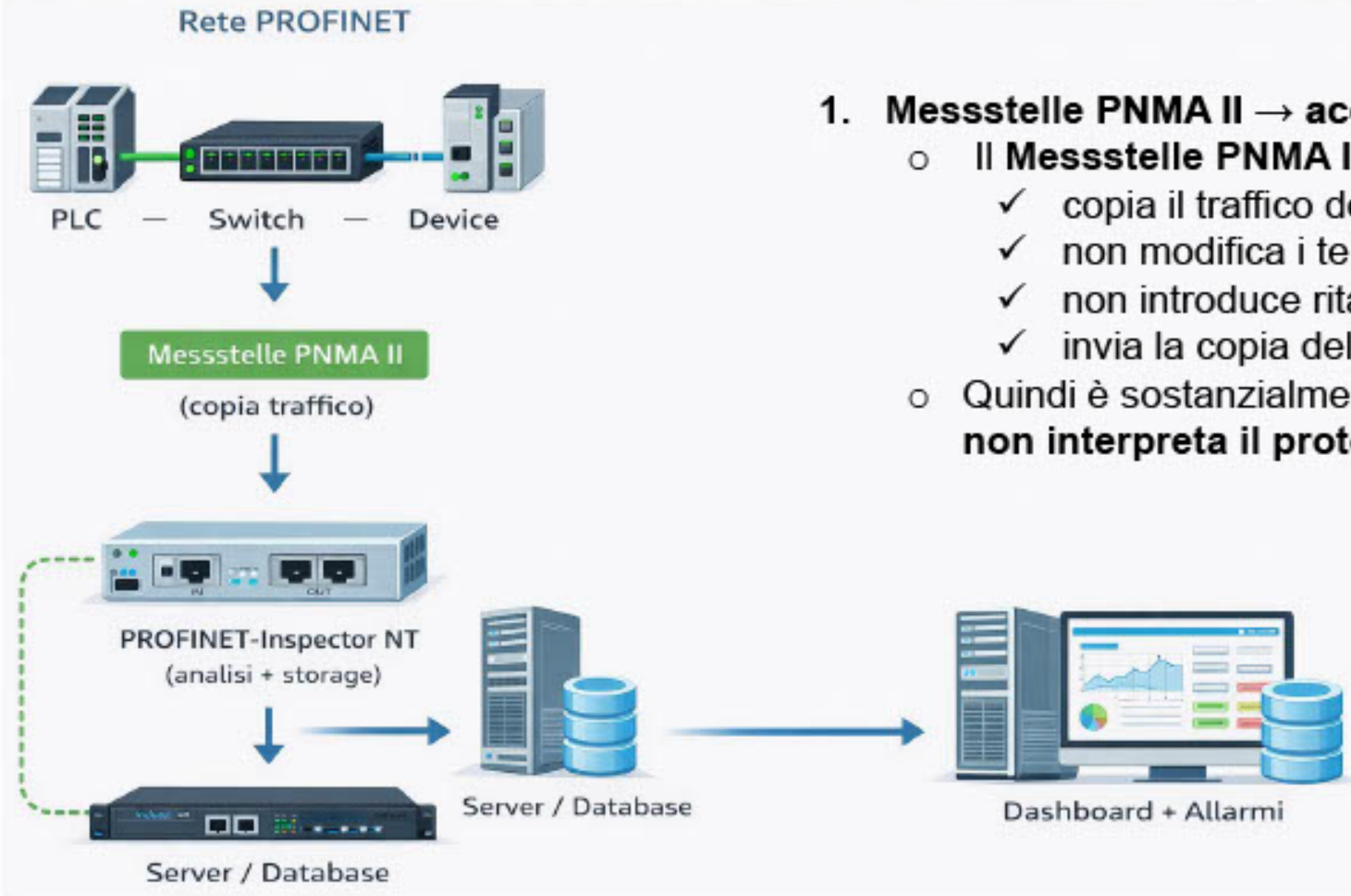
## Permanent Network Monitoring



5 Network troubleshooting

6 Permanent Network Monitoring

# Architettura Permanent Network Monitoring



## 1. Messstelle PNMA II → acquisizione traffico

- Il **Messstelle PNMA II** è installato nella rete PROFINET e:
  - ✓ copia il traffico della rete
  - ✓ non modifica i telegrammi
  - ✓ non introduce ritardi
  - ✓ invia la copia del traffico alla porta di analisi
- Quindi è sostanzialmente: **un TAP di rete industriale permanente che non interpreta il protocollo.**

# Architettura Permanent Network Monitoring



## 2. PROFINET-Inspector NT → analisi del traffico

- Il **PROFINET-Inspector NT** è il software di analisi che gira su:
  - ✓ PC industriale
  - ✓ server
  - ✓ appliance dedicata
- Questo software:
  - ✓ riceve il traffico dal PNMA II
  - ✓ decodifica il protocollo PROFINET
  - ✓ calcola parametri di qualità della rete
  - ✓ Ad esempio analizza:
    - cycle time
    - jitter
    - ritardi telegrammi
    - perdita telegrammi
    - carico di rete
    - errori PROFINET
    - cambiamenti di topologia

# Architettura Permanent Network Monitoring



## 3. Il server di monitoraggio

- Quando il sistema è configurato per **Permanent Network Monitoring**, il **PROFINET-Inspector NT** diventa il **nodo centrale**. È lui che:
  - i. riceve i dati dal **Messstelle PNMA II**
  - ii. li **analizza in tempo reale**
  - iii. li **memorizza nel database storico**
  - iv. li **visualizza nella dashboard**
  - v. genera **allarmi**

## 4. Che dati manda il PROFINET-Inspector NT al server

- Non manda i telegrammi raw (come Wireshark), ma **metriche di qualità della rete**.
- Tipicamente:
  - ✓ stato della comunicazione
  - ✓ jitter per device
  - ✓ cycle time
  - ✓ load di rete
  - ✓ errori telegrammi
  - ✓ eventi di diagnostica
- Questi dati vengono:
  - ✓ salvati nel database
  - ✓ visualizzati nel web interface
  - ✓ usati per generare allarmi

# PNM – Permanent Network Monitoring



# PNM – Permanent Network Monitoring

