

Redes Industriais e Sistemas Supervisórios

Prof^o José W. R. Pereira
jose.pereira@ifsp.edu.br
josewrpereira.github.io/docs

SLTRISS



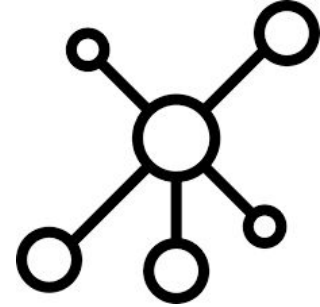
Índice

Fundamentos de Redes

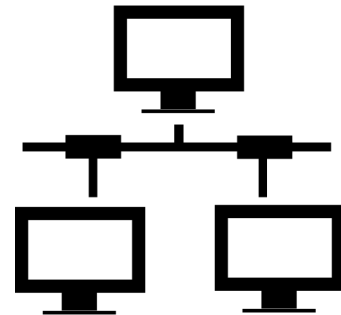
- **1. Redes**
- **2. Redes de Computadores vs. Redes Industriais**
 - **2.1. Diferenças Essenciais**
- **3. O Modelo ISO/OSI na Indústria**
- **4. Aspectos Físicos e Lógicos da Rede Industrial**
 - **4.1. Meios Físicos e Interfaceamento**
 - **4.2. Topologias e Protocolos (Lógica)**
- **5. Do Campo à Gestão (Integração TA + TI)**
 - **5.1. Instrumentação de Campo e CLP**
 - **5.2. Fluxo de Dados e Camada de Gestão (IIoT)**
- **6. Segurança Cibernética no Ambiente Industrial**
- **Referências**

1. Redes

Uma **rede** é um sistema estruturado para a troca de informações e compartilhamento de recursos entre entidades autônomas.



Rede de computadores: é definida como um conjunto de computadores autônomos interconectados por uma única tecnologia, permitindo que troquem dados através de diversos meios, como fios de cobre, fibras ópticas ou micro-ondas.



1. Redes

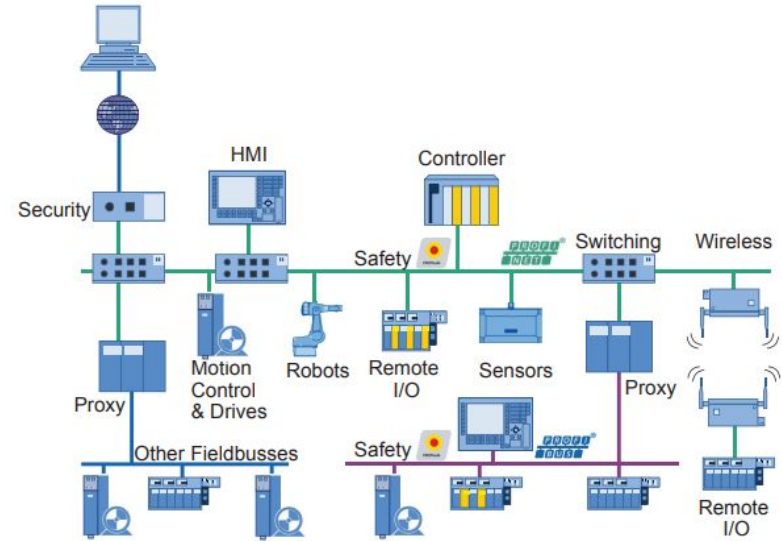
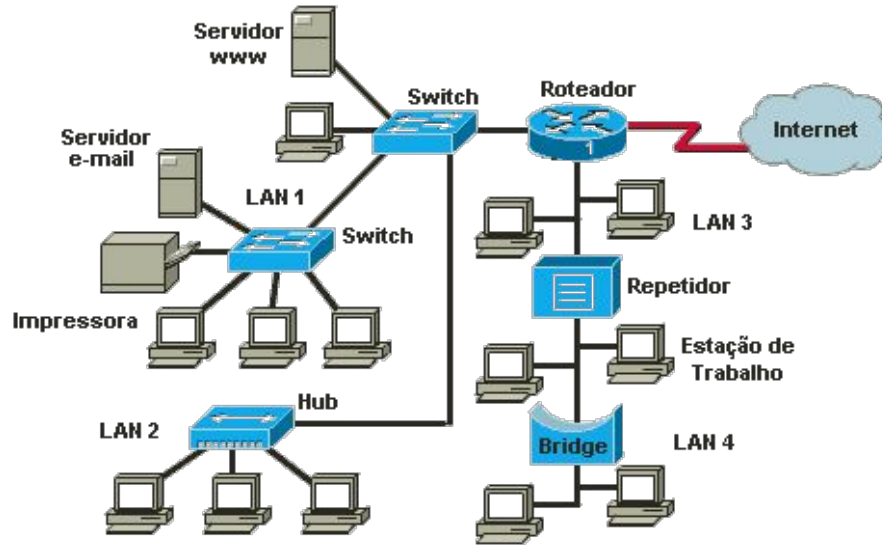
As redes de computadores são classificadas pela sua **escala de abrangência**:



- **PAN (Personal Area Network):** Redes de curtíssimo alcance, destinadas a uma única pessoa.
- **LAN (Local Area Network):** Abrangem prédios ou campi.
- **MAN (Metropolitan Area Network):** Cobrem cidades inteiras.
- **WAN (Wide Area Network):** Estendem-se por países ou continentes.
- **Internet:** O exemplo máximo de uma "rede de redes", interconectando sub-redes globalmente.



2. Redes de Computadores vs. Redes Industriais

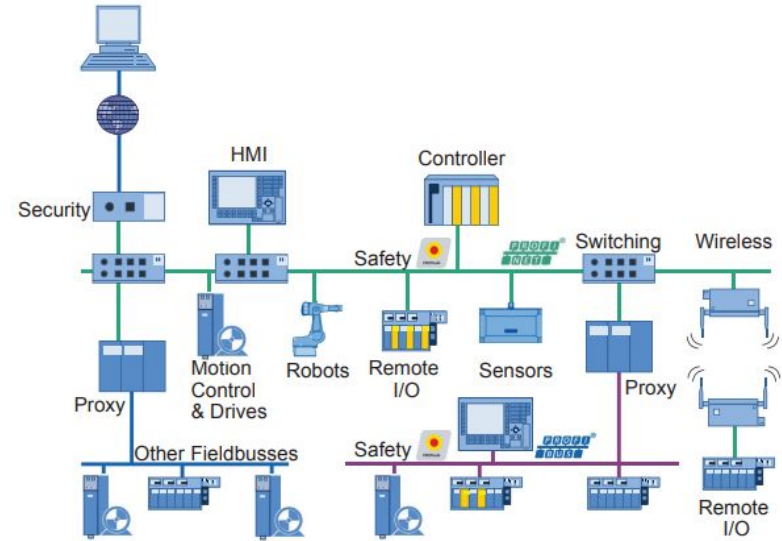
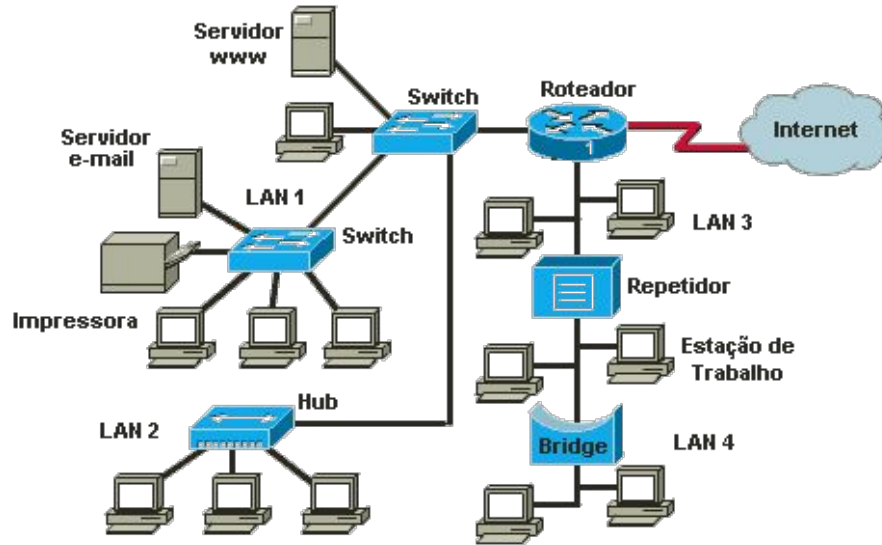


Compartilhem **princípios fundamentais** porém **diferem** drasticamente nos **requisitos operacionais**

Volume de dados e Flexibilidade << Prioridade >> **Determinismo temporal e Robustez**

- **Criticidade:** Uma falha na rede:
 - de escritório pode causar atrasos administrativos;
 - no chão de fábrica pode paralisar uma linha de montagem em segundos ou causar acidentes.

2. Redes de Computadores vs. Redes Industriais



Compartilhem **princípios fundamentais** porém **diferem** drasticamente nos **requisitos operacionais**

Volume de dados e Flexibilidade << **Prioridade** >> **Determinismo temporal e Robustez**

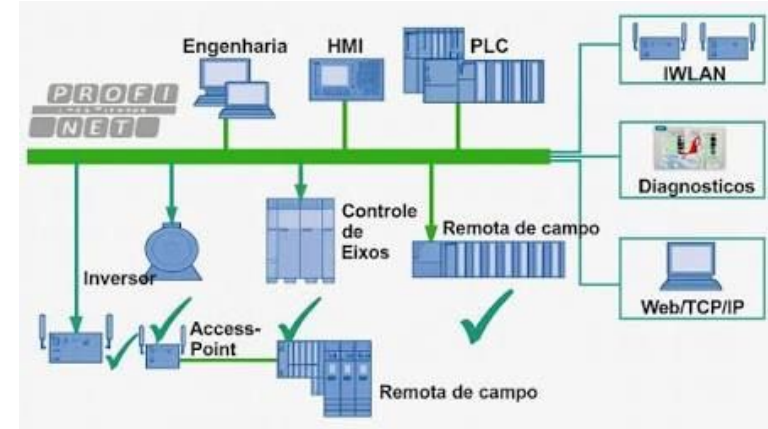
- Ambiente:**

- As redes industriais operam em condições severas de ruído eletromagnético, vibração e temperaturas extremas.

2.1 Redes Industriais - Tipos

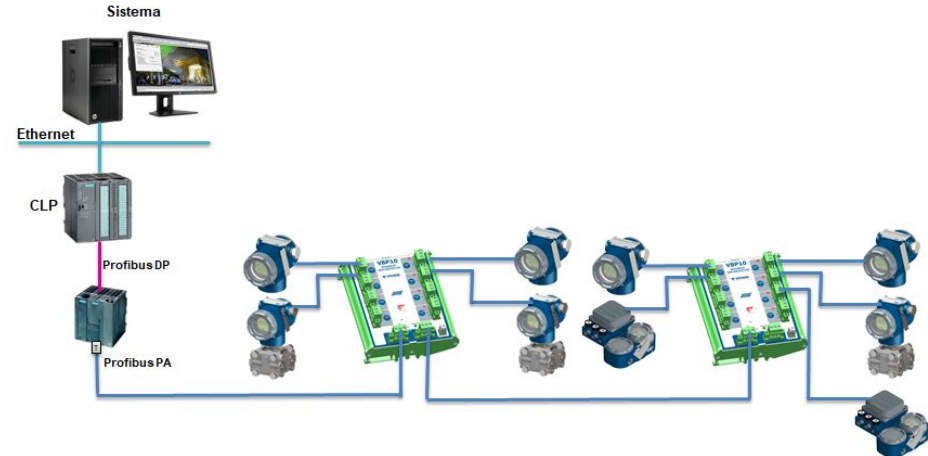
Redes de Manufatura

- Focadas em alta velocidade e pacotes pequenos para automação discreta.
- Ex: Profinet, Ethernet/IP.



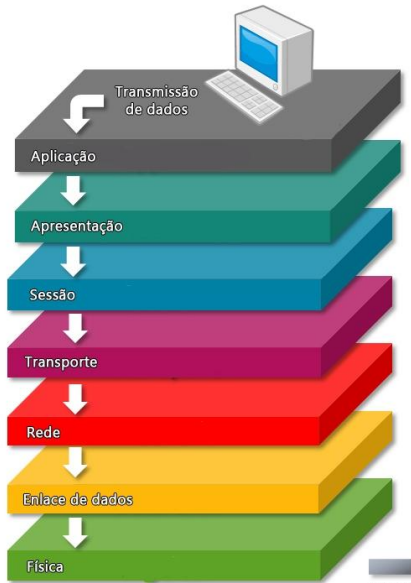
Redes de Processo:

- Priorizam a continuidade e segurança intrínseca em ambientes quimicamente agressivos.
- Ex: Profibus PA, Foundation Fieldbus.



3. O Modelo ISO/OSI

- **Interconexão de sistemas abertos**
 - *Open System Interconnection - OSI*
- É um **modelo conceitual** criado pela Organização Internacional de Normalização
 - *International Organization for Standardization - ISO*
- Permite que diversos sistemas de comunicação se comuniquem usando protocolos padronizados.



3. O Modelo ISO/OSI

CAMADA

7

APLICAÇÃO

- É a interface entre o usuário e os aplicativos que utilizam a rede.
- Define os serviços e comandos específicos de cada aplicação.

Exemplos: HTTP, SMTP, Modbus



APLICAÇÕES

- Ler temperatura
- Enviar e-mail
- Acessar sistema SCADA
- Comandar um motor

CAMADA

6

APRESENTAÇÃO

- Formata, converte e codifica os dados para que possam ser entendidos.
- Compacta dados e aplica criptografia quando necessário.
- Garante que o formato seja compatível entre sistemas.



SSL/TLS



CAMADA

5

SESSÃO

- Estabelece, mantém e encerra a comunicação entre dois dispositivos.
- Sincroniza a troca de dados e controla pontos de verificação (checkpoints).



✓ Iniciar

SESSÃO



✓ Sincronizar



✓ Encerrar

3. O Modelo ISO/OSI

CAMADA

4

TRANSPORTE

- Garante a entrega de ponta a ponta confiável.
- Divide os dados em segmentos e faz controle de fluxo e de erros.
- Assegura que os dados cheguem completos e na ordem correta.

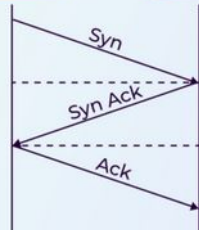


TCP

SENDER



RECEIVER

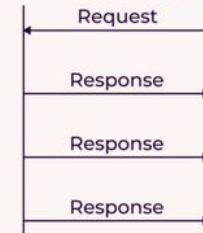


UDP

SENDER



RECEIVER



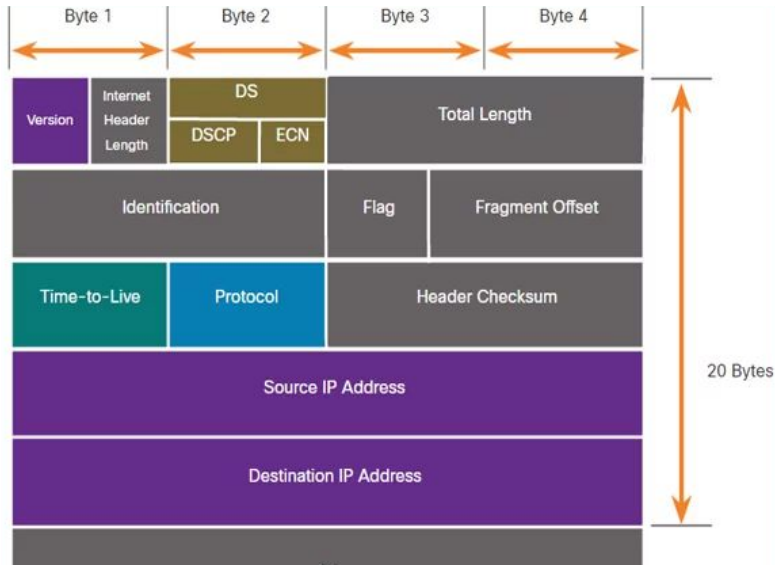
3. O Modelo ISO/OSI

CAMADA

3

REDE

- Roteia os dados entre redes diferentes até o destino.
- Seleciona o melhor caminho para os dados.
- Divide os dados em pacotes e adiciona endereços lógicos (IP).



IP (Internet Protocol) é o protocolo responsável por **identificar dispositivos e encaminhar pacotes de dados entre diferentes redes**, permitindo que a informação encontre o caminho correto até seu destino.



IP: 192.168.1.50
Mask: 255.255.255.0



IP: 192.168.1.60
Mask: 255.255.255.0

3. O Modelo ISO/OSI

CAMADA

3

REDE

- Roteia os dados entre redes diferentes até o destino.
- Seleciona o melhor caminho para os dados.
- Divide os dados em pacotes e adiciona endereços lógicos (IP).



1.0.0.0~126.255.255.255

Classe A **0** Rede (7bit) Host (24bit)

128.0.0.0~191.255.255.255

Classe B **1 0** Rede (14bit) Host (16bit)

192.0.0.0~223.255.255.255

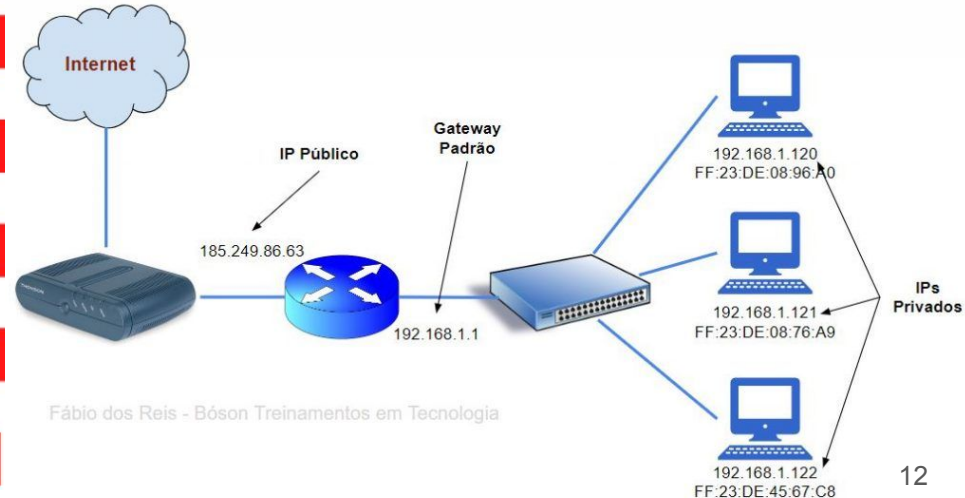
Classe C **1 1 0** Rede (21bit) Host (8bit)

224.0.0.0~239.255.255.255

Classe D **1 1 1 0** Multicast Address

240.0.0.0~255.255.255.255

Classe E **1 1 1 1 0** Reserved



Fábio dos Reis - Bóson Treinamentos em Tecnologia

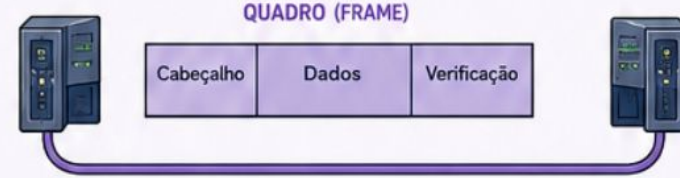
3. O Modelo ISO/OSI

CAMADA

2

ENLACE

- Organiza os dados em quadros (frames).
- Controla o acesso ao meio físico para evitar conflitos.
- Detecta erros e garante a entrega entre dispositivos no mesmo enlace.



CAMADA

1

FÍSICA

- Define os meios físicos de transmissão.
- Especifica cabos, conectores, sinais elétricos e características físicas.
- Transmite bits brutos (0 e 1) pelo meio físico.



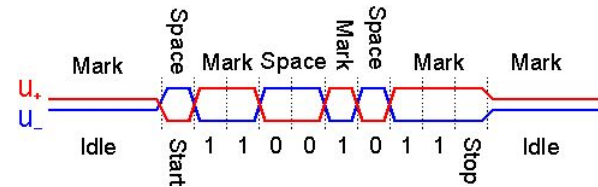
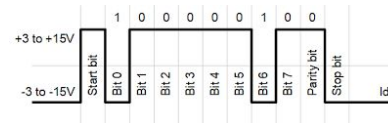
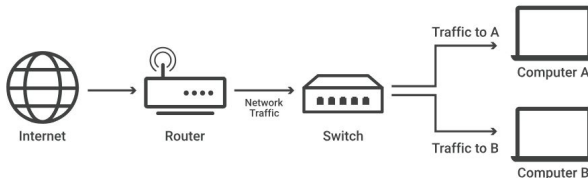
PAR TRANÇADO



SINAL ELÉTRICO



CONECTOR



3. O Modelo ISO/OSI na Indústria

7

CAMADA 7 – APLICAÇÃO

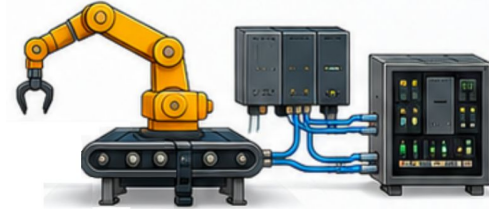
Define os comandos industriais específicos e a troca de dados entre sistemas e dispositivos.

- Ler temperatura
- Acionar motor
- Enviar setpoint
- Ler status



TEMPO REAL

Comunicação rápida e determinística, essencial para controle industrial.



2

CAMADA 2 – ENLACE

Organiza os dados em quadros (pacotes) e controla o acesso físico ao meio (cabo). Garante detecção de erros e entrega confiável.



10	10011	10
----	-------	----

Quadro



CONFIABILIDADE

Menos camadas e foco na transmissão garantem entrega de dados segura.



MAIS DISPONIBILIDADE

Menos pontos de falha e melhor desempenho em ambientes críticos.

1

CAMADA 1 – FÍSICA

Define os meios físicos de transmissão: cabos, conectores e sinais elétricos (brutos). Responsável pela transmissão de bits.



24 V  ++



SIMPLICIDADE

Arquitetura reduzida facilita configuração e manutenção.

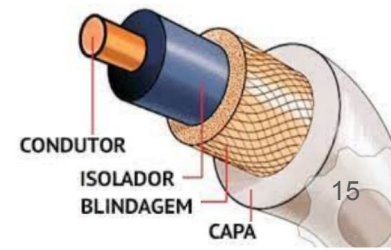


INTEGRAÇÃO

Facilita a integração entre dispositivos de campo e sistemas superiores (OT + TI).

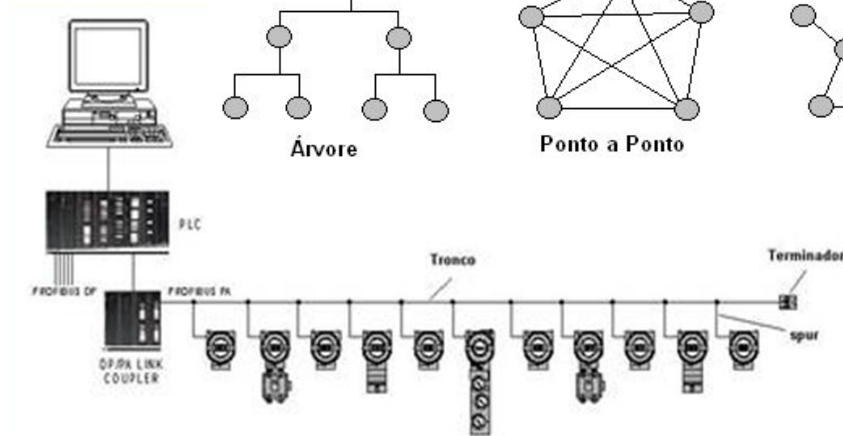
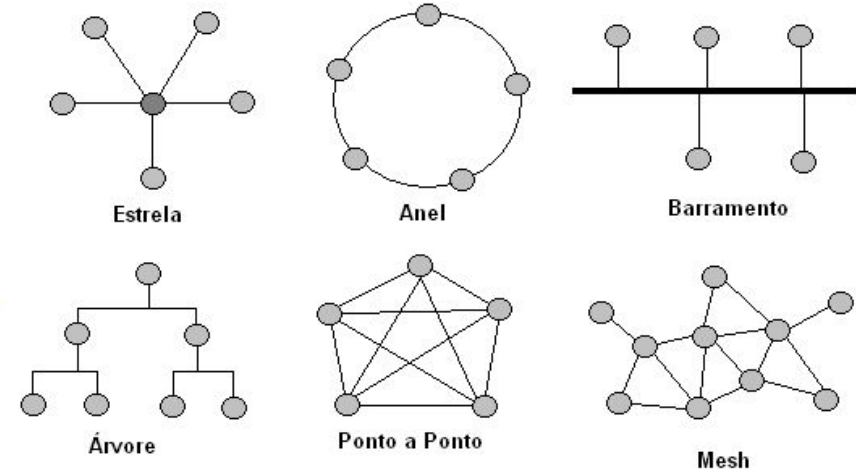
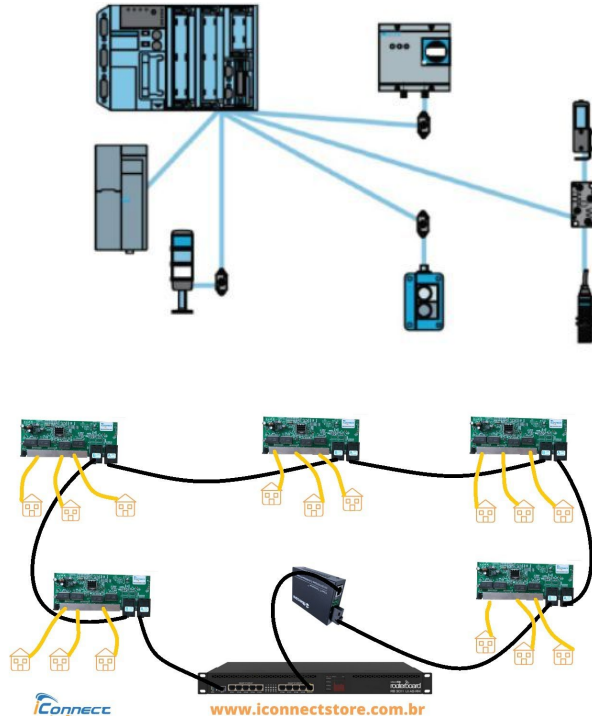
4. Aspectos Físicos e Interfaceamento

- **Cabo de Par Trançado (RS-485):** Utiliza sinalização diferencial para cancelar interferências, permitindo distâncias de até 1.200 metros.
- **Fibra Ótica:** Essencial em ambientes com altíssima interferência eletromagnética ou para longas distâncias.
- **Conectores Robustos:** Uso de padrões como o **M12** em vez do RJ-45 convencional para suportar vibrações e umidade.



4.1 Topologias e Protocolos (Lógicos)

As redes podem ser organizadas em **Estrela** (nó central), **Barramento** (linear), **Anel** (redundância) ou **Árvore**.



4.1 Topologias e Protocolos (Lógicos)

No nível lógico, os protocolos definem as regras de conversação:

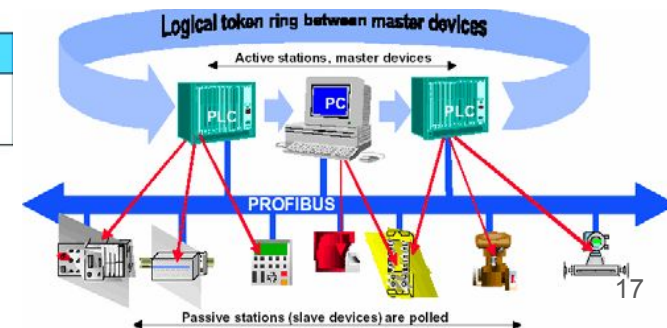
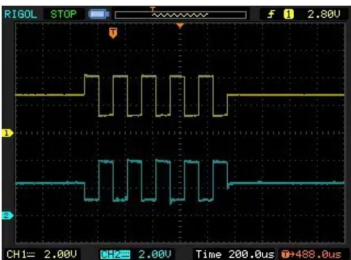
- **Modbus RTU:** Baseado em mestre-escravo, onde um mestre inicia transações lendo ou escrevendo em registros de escravos.
- **Profibus:** Utiliza passagem de bastão (*Token Pass*) entre mestres para evitar colisões e mestre-escravo para dispositivos de campo.
- **Foundation Fieldbus:** Distribui o controle através de blocos funcionais diretamente nos instrumentos de campo.

Modbus RTU Frame Format

Start	Address	Function	Data	CRC	End
≥3.5 char	8 bit	8 bit	N * 8 bit	16 bits	≥3.5 char

Modbus ASCII Frame Format

Start	Address	Function	Data	LRC	End
;	2chars	2chars	N * 1 chars	2chars	CR, LF



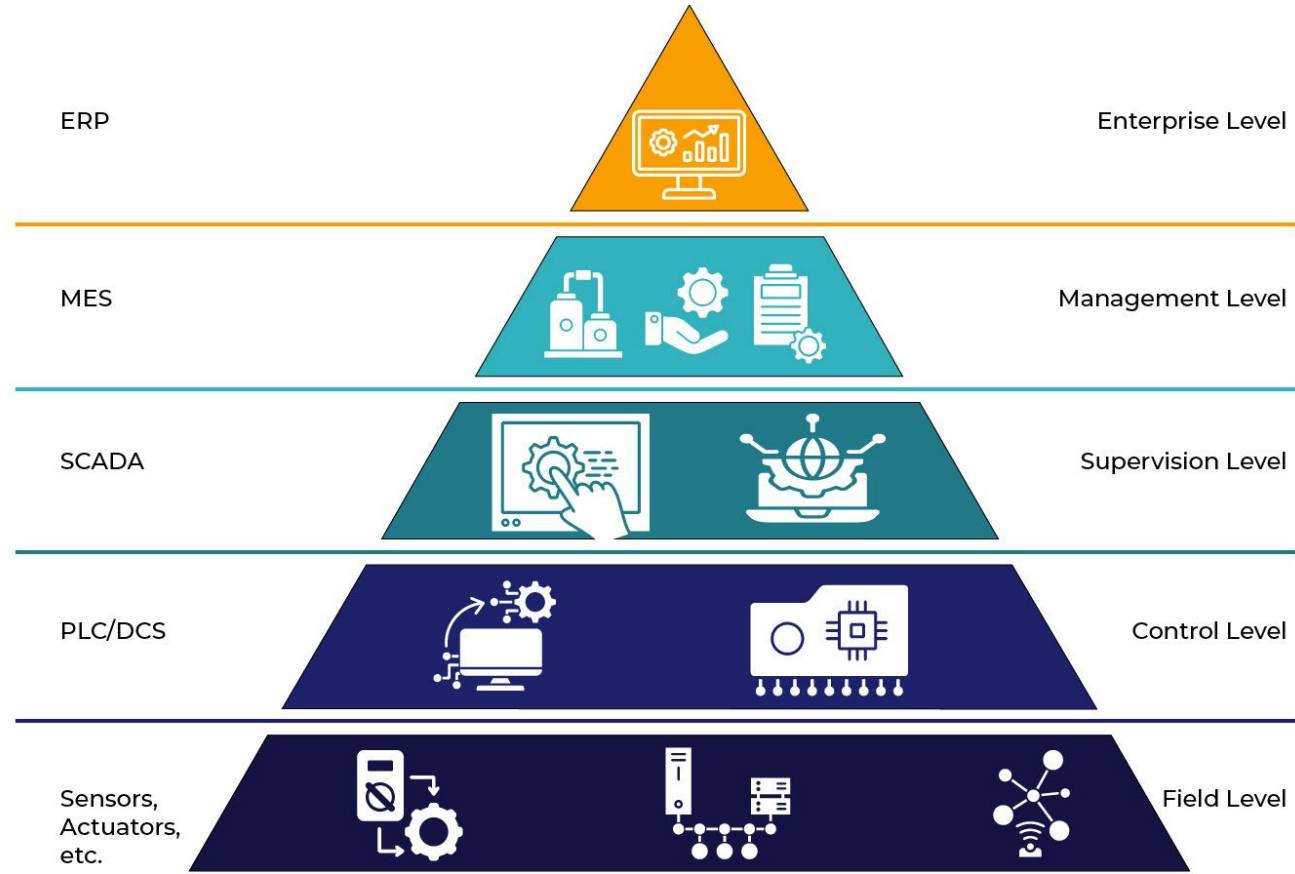
5. Do Campo à Gestão (Integração TA + TI)

Ethernet, TCP/IP,
OCP, DDE, DCOM

Ethernet, TCP/IP,
OCP, DDE, DCOM

ControlNet, EthernetDP,
OCP, **ModBus**, ProfibusFMS,
DP, Profinet

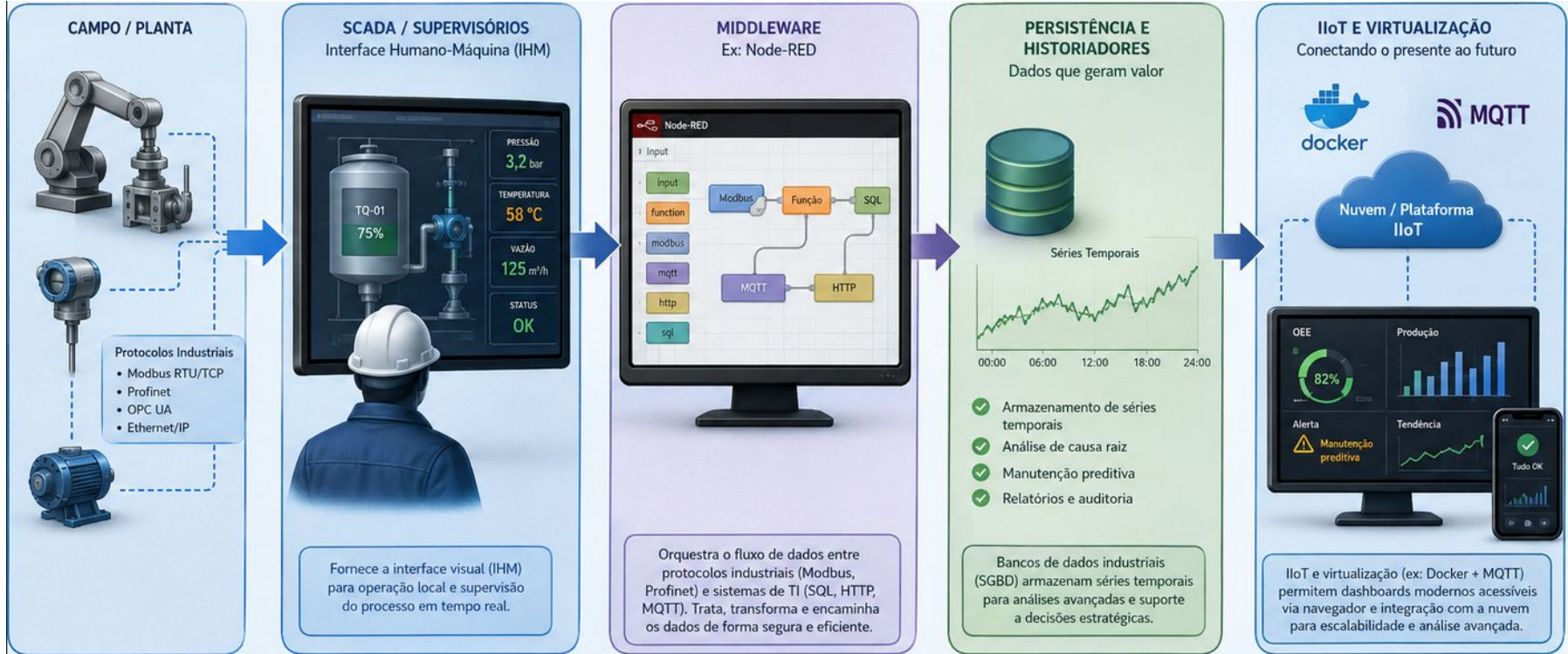
Fieldbus H1, CAN,
Profibus DP, HART, ASi



5. Do Campo à Gestão (Integração TA + TI)



5. Fluxo de Dados e Camada de Gestão (IIoT)



BENEFÍCIOS



Visibilidade em tempo real



Decisões mais rápidas



Manutenção preditiva



Redução de custos



Eficiência e sustentabilidade

6. Segurança Cibernética no Ambiente Industrial

1. ISOLAMENTO (VLANS INDUSTRIAIS)

Separação do tráfego crítico do administrativo

VLAN 10 REDE INDUSTRIAL (Crítico - OT)

- CLPs
- SCADA
- IHM
- Dispositivos de campo

VLAN 20 REDE ADMINISTRATIVA (TI)

- Workstations
- Servidores
- Internet
- E-mail, etc.



Tráfego isolado, riscos reduzidos.

2. CRIPTOGRAFIA (WPA3)

Proteção avançada para redes sem fio industriais



Criptografia
mais forte



Proteção contra
ataques offline



Ambientes
industriais seguros

3. CONTROLE DE ACESSO

Proteção de portas, containers e interfaces



Acesso físico controlado
Portas e containers protegidos



Autenticação e autorização
Acessos apenas para usuários autorizados



Monitoramento e auditoria
Registros e alertas em tempo real

AMBIENTE PROTEGIDO, OPERAÇÃO CONFIÁVEL



DISPOSITIVOS
INDUSTRIAIS



SEGREGAÇÃO
VLAN



CRIPTOGRAFIA
WPA3



CONTROLE DE
ACESSO



DADOS SEGUROS
E CONFIÁVEIS

BENEFÍCIOS



Proteção da operação
e da planta



Redução de riscos
e vulnerabilidades



Conformidade com
normas e boas práticas



Menor impacto
financeiro em incidentes



Continuidade operacional
e segurança de dados

Referências

ALBUQUERQUE, Pedro Urbano Braga de; ALEXANDRIA, Alzuir Ripardo de. **Redes industriais**: aplicações em sistemas digitais de controle distribuído. 2. ed. São Paulo: Ensino Profissional, 2009.

ALTUS. **Protocolos de comunicação**: o que são e quais os principais padrões utilizados na indústria. [S. l.]: Altus. E-book.

COELHO, Marcelo Saraiva. **Redes de comunicação industrial**: padrões industriais. [S. l.: s. n.], 2009. Apostila.

LAGES, Walter Fetter; PEREIRA, Carlos Eduardo. **Redes industriais**. Porto Alegre: UFRGS, 2004. Apresentação em slides.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

Este material foi produzido com auxílio de
ferramentas de Inteligência Artificial:



Redes Industriais e Sistemas Supervisórios - RISS

Profº José W. R. Pereira

jose.pereira@ifsp.edu.br

josewrpereira.github.io/docs



Pós-Ref 0 - Estudo de caso

A INVESTIGAÇÃO CONTINUA.

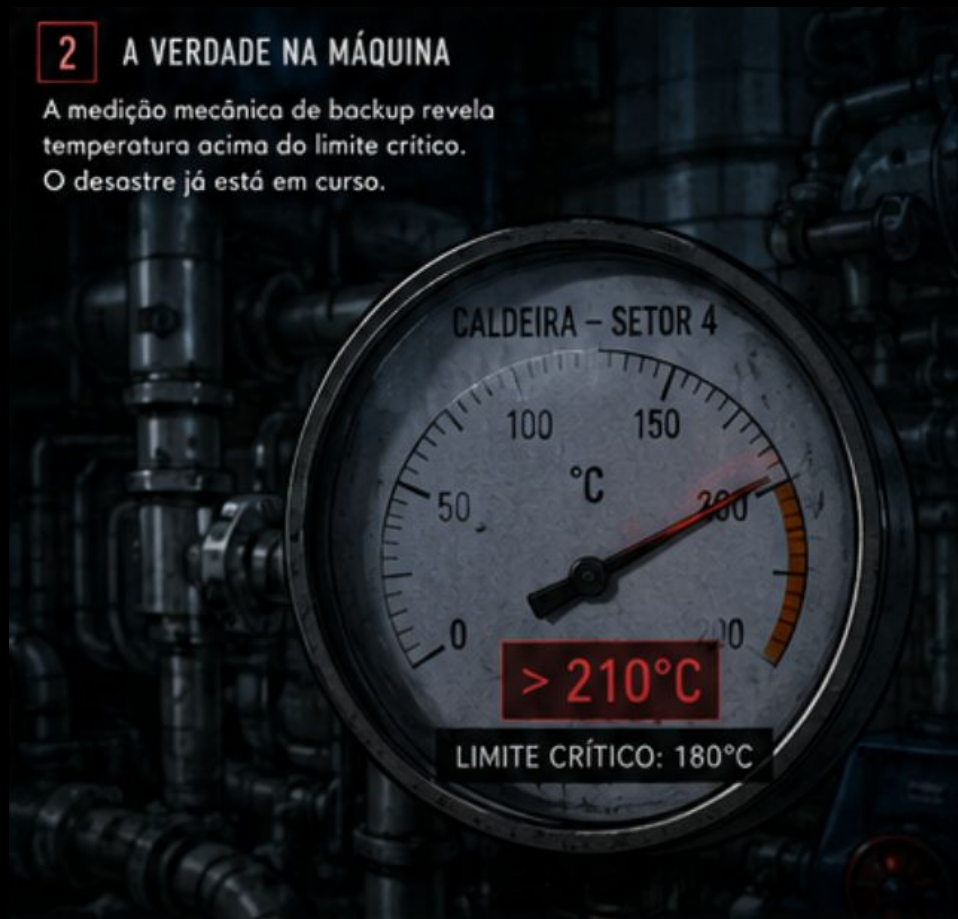
A segurança da planta depende
de enxergar o invisível.





2 A VERDADE NA MÁQUINA

A medição mecânica de backup revela
temperatura acima do limite crítico.
O desastre já está em curso.



3 A INVESTIGAÇÃO – BUSCA POR FALHAS

Peritos analisam o software
e o sistema supervisório.
A aplicação está intacta.
A tela apenas parou de atualizar.

A leitura ficou congelada
no último valor válido,
enquanto a realidade
era catastrófica.

SUPERVISÓRIO – SETOR 4

TEMP. REATOR	65 °C
PRESSÃO	3,2 bar
VAZÃO	120 t/h
STATUS	NORMAL

CONGELADO



TEMPERATURA DO REATOR (°C)



4 A PISTA NOS DADOS – CAMADA DE ENLACE

Análise dos registros de tráfego revela centenas de quadros rejeitados por erros de paridade e CRC exatamente quando os motores foram acionados.

HORA	ORIGEM	DESTINO	FRAME	ERROS
03:13:58	SETOR 4	SUPERVISÓRIO	0xA7F3	PARIDADE
03:13:59	SETOR 4	SUPERVISÓRIO	0xA7F4	CRC
03:14:00	SETOR 4	SUPERVISÓRIO	0xA7F5	CRC
03:14:00	SETOR 4	SUPERVISÓRIO	0xA7F6	PARIDADE
03:14:01	SETOR 4	SUPERVISÓRIO	0xA7F7	CRC
...				

03:13:58
INÍCIO DOS ERROS

03:14:00
ACIONAMENTO DOS
MOTORES DO COMPRESSOR

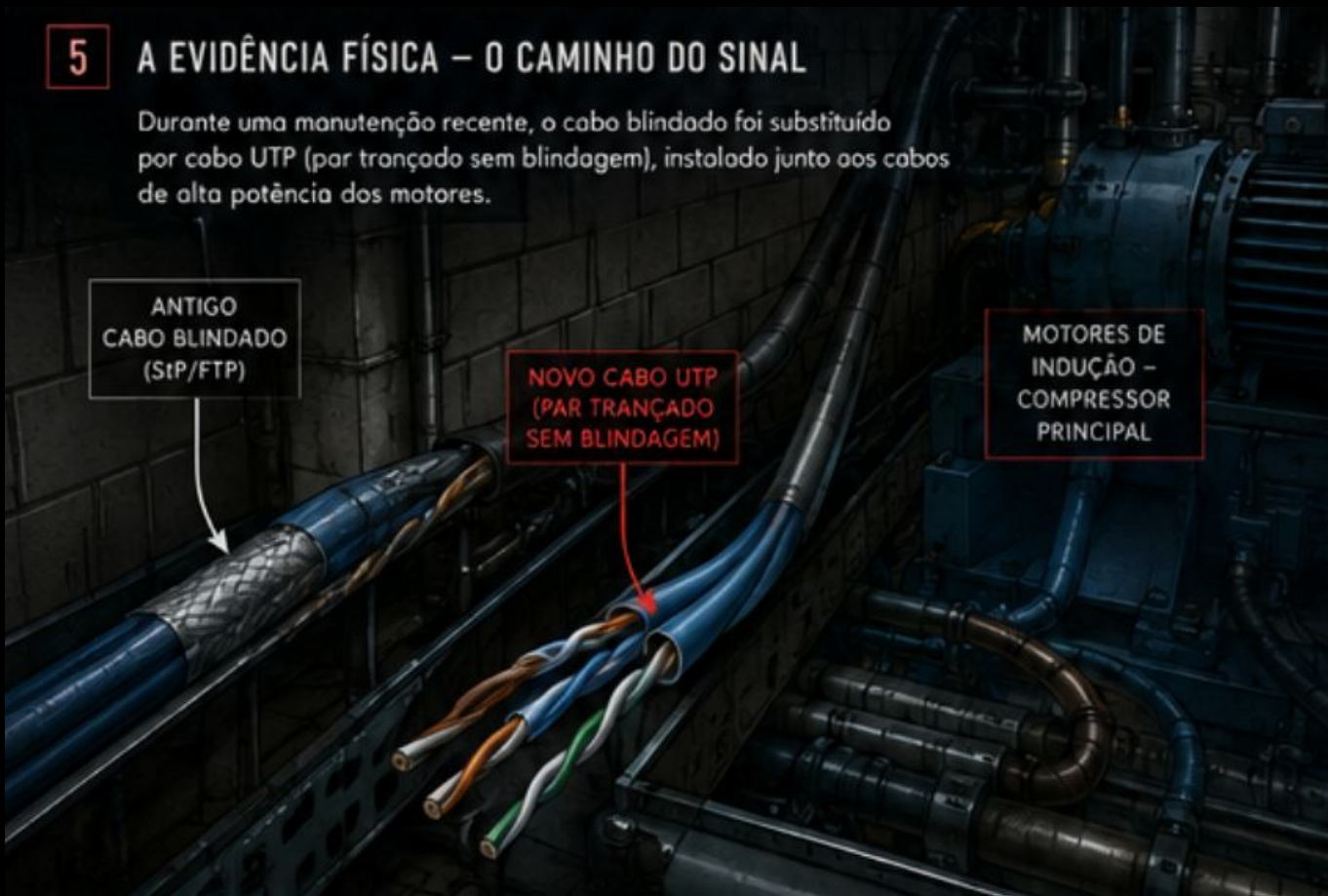
5 A EVIDÊNCIA FÍSICA – O CAMINHO DO SINAL

Durante uma manutenção recente, o cabo blindado foi substituído por cabo UTP (par trançado sem blindagem), instalado junto aos cabos de alta potência dos motores de alta potência dos motores.

ANTIGO
CABO BLINDADO
(StP/FTP)

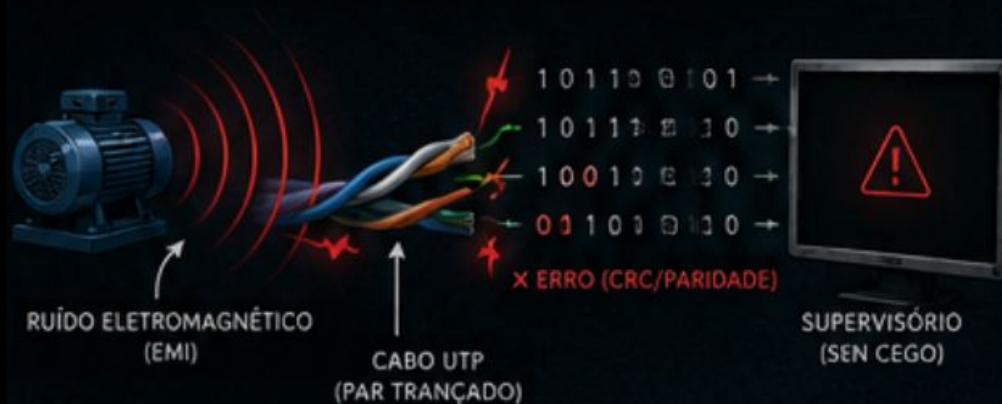
NOVO CABO UTP
(PAR TRANÇADO
SEM BLINDAGEM)

MOTORES DE
INDUÇÃO –
COMPRESSOR
PRINCIPAL



6 A HIPÓTESE

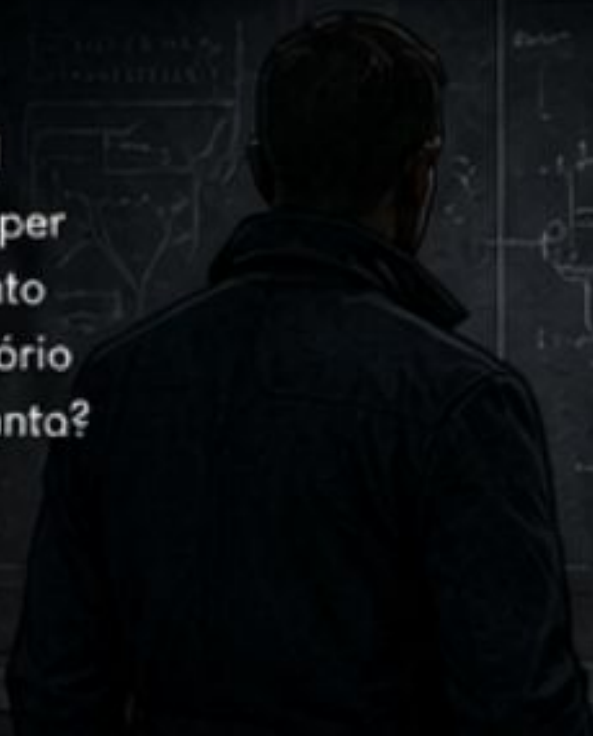
Interferência eletromagnética gerada pelos motores de alta potência induz ruído nos cabos UTP, corrompendo os bits durante a transmissão. Os frames chegam com erros, são descartados e o supervisor fica "cego".



**RESULTADO: DADOS PERDIDOS. SISTEMA CEGO.
PLANTA DESLIGADA. RISCO REAL.**

A QUESTÃO QUE RESTA

Como um evento elétrico invisível
no meio físico foi capaz de corromper
os bits do quadro de dados a ponto
de cegar a aplicação do supervisor
e provocar o desligamento da planta?



A INVESTIGAÇÃO CONTINUA.

A segurança da planta depende
de enxergar o invisível.

