Setting the Standard for Automation™

ISA São Paulo Section
Palestra Técnica

Protegendo minha rede industrial – Best practices e equipamentos

Palestrante: Newton de Carvalho Fernandez

30 de agosto de 2017

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

O que é TI?

Tecnologia da Informação, tradicionalmente...

- Consiste na aplicação de computadores e outros hardwares e softwares para produzir, transmitir e armazenar dados, tipicamente num ambiente de "carpete" ou enterprise.

- Está associado com funções como faturamento, gerenciamento de ativos, informação de clientes, marketing, etc.

* Prioridade - Confidencialidade

O que é TO?

Tecnologia das Operações/Automação

Rede e Computação “Industrial”

- Consiste de sistemas de hardware e software que monitoram e controlam equipamentos e processos nas mais diversas indústrias (....).

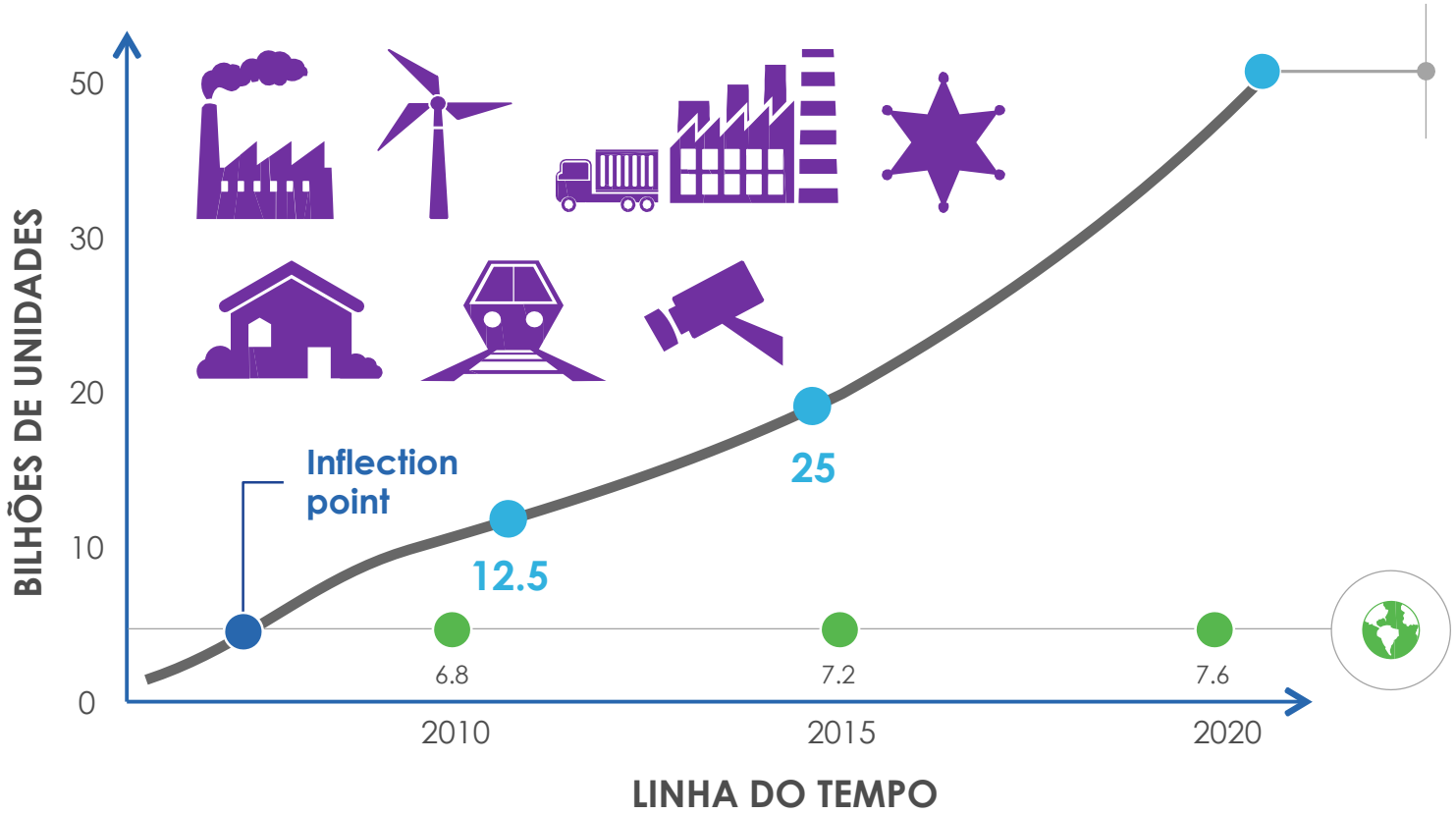
- Esta tecnologia utiliza muitos termos próprios (PLC, RTU, IED, SCADA) e é familiar a operadores e engenheiros nesses setores.

- Os sistemas de controle aqui envolvidos, muitas vezes são proprietários.

- Ambiente agressivo, requer equipamentos mais robustos.

* Prioridade - Disponibilidade

IoT é agora – e crescendo!!



50 Bilhões de Objetos Inteligentes

5X mais rápido que o que aconteceu com a eletricidade e com a telefonia

População Mundial

IoT é uma rede de equipamentos e objetos físicos que contém uma tecnologia embarcada para comunicar e sentir ou interagir com um ambiente externo!

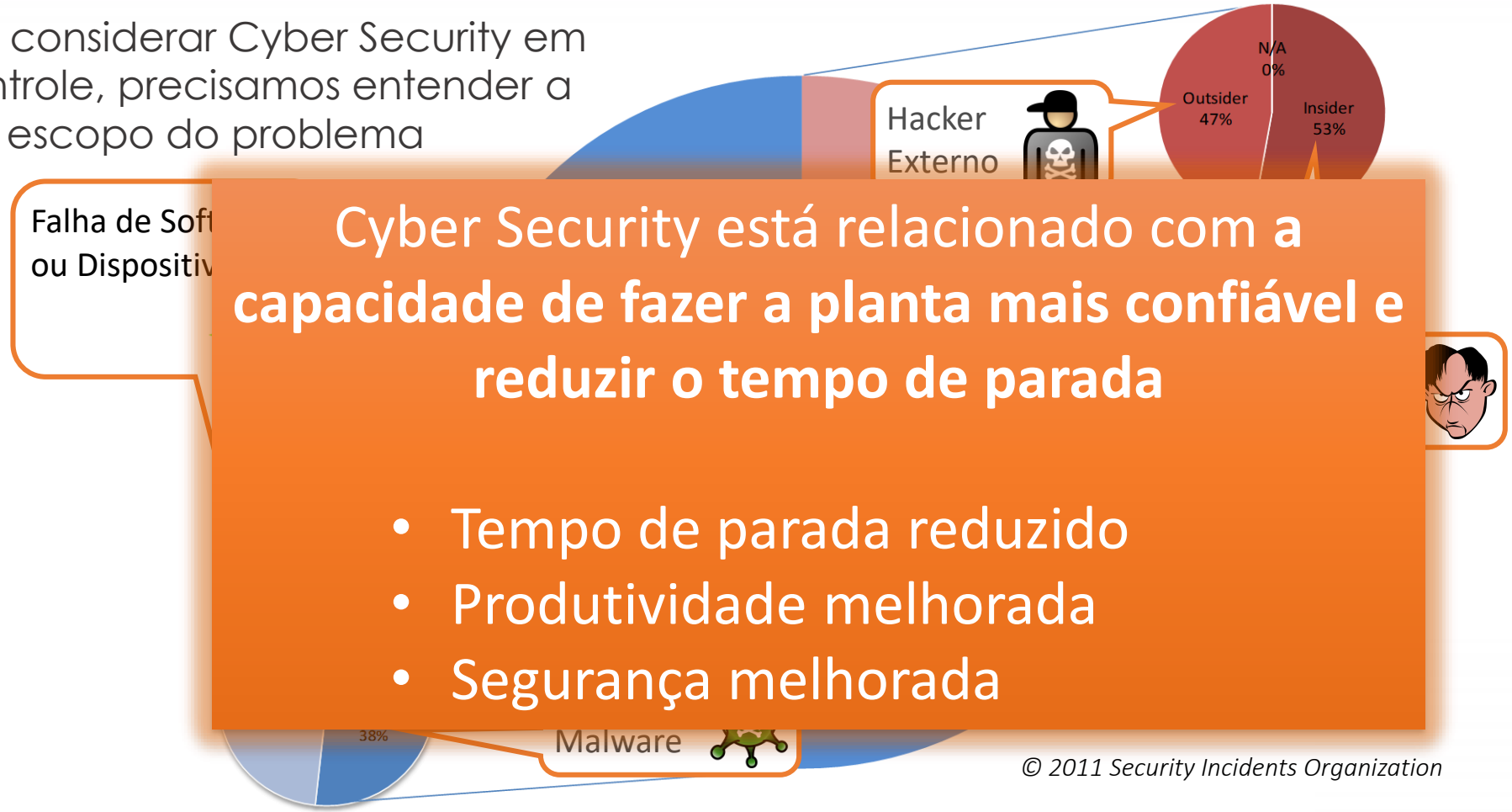
Informação sobre Segurança

Definição de Segurança
“ **Uma coleção** de meios adotados para previnir uso não autorizado, malicioso, negação de serviço ou modificação da informação, fatos, dados ou recursos…preocupação com a integridade, confidencialidade e disponibilidade do dado.”

E qual a diferença entre Segurança da informação, Segurança Cibernética e Segurança de Rede?

Segurança de Rede - Tipos de Incidentes

Se quisermos considerar Cyber Security em redes de controle, precisamos entender a natureza e o escopo do problema



Cyber Security está relacionado com **a capacidade de fazer a planta mais confiável e reduzir o tempo de parada**

- Tempo de parada reduzido
- Produtividade melhorada
- Segurança melhorada

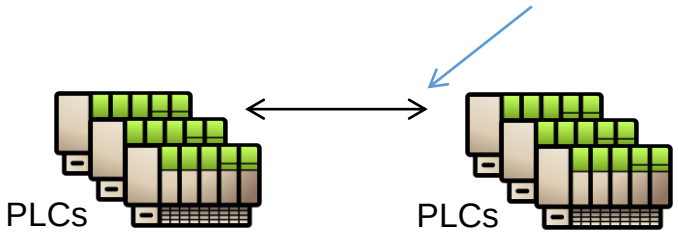
As ameaças

- Os componentes numa planta estão sendo cada vez mais conectados
- Os ambientes de uma planta estão ampliando sua abertura para influências externas
- Os ataques são simples de serem criados usando ferramentas padronizadas que são atualizadas com frequencia
- Protocolos (TCP/IP) e redes (Ethernet) são vulneraveis (*)
- Ataques são difíceis de se rastrear
- Os ataques possuem diferentes propósitos

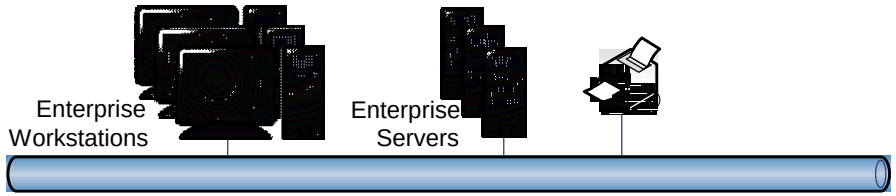
Como chegamos aqui?

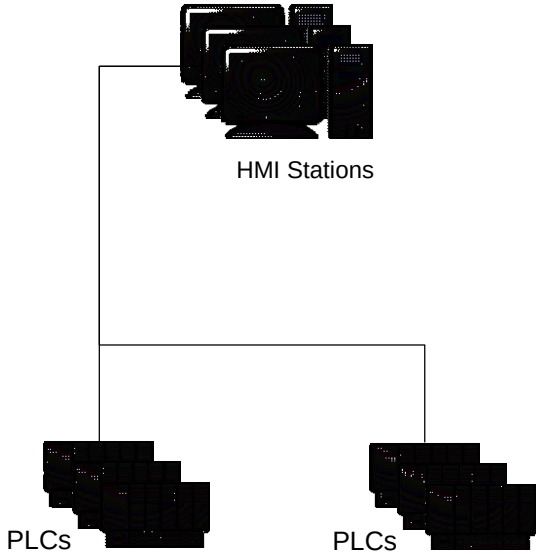
Automação nos anos 1980 – "ilhas" isoladas

Link de Comunicação Serial ou Proprietário



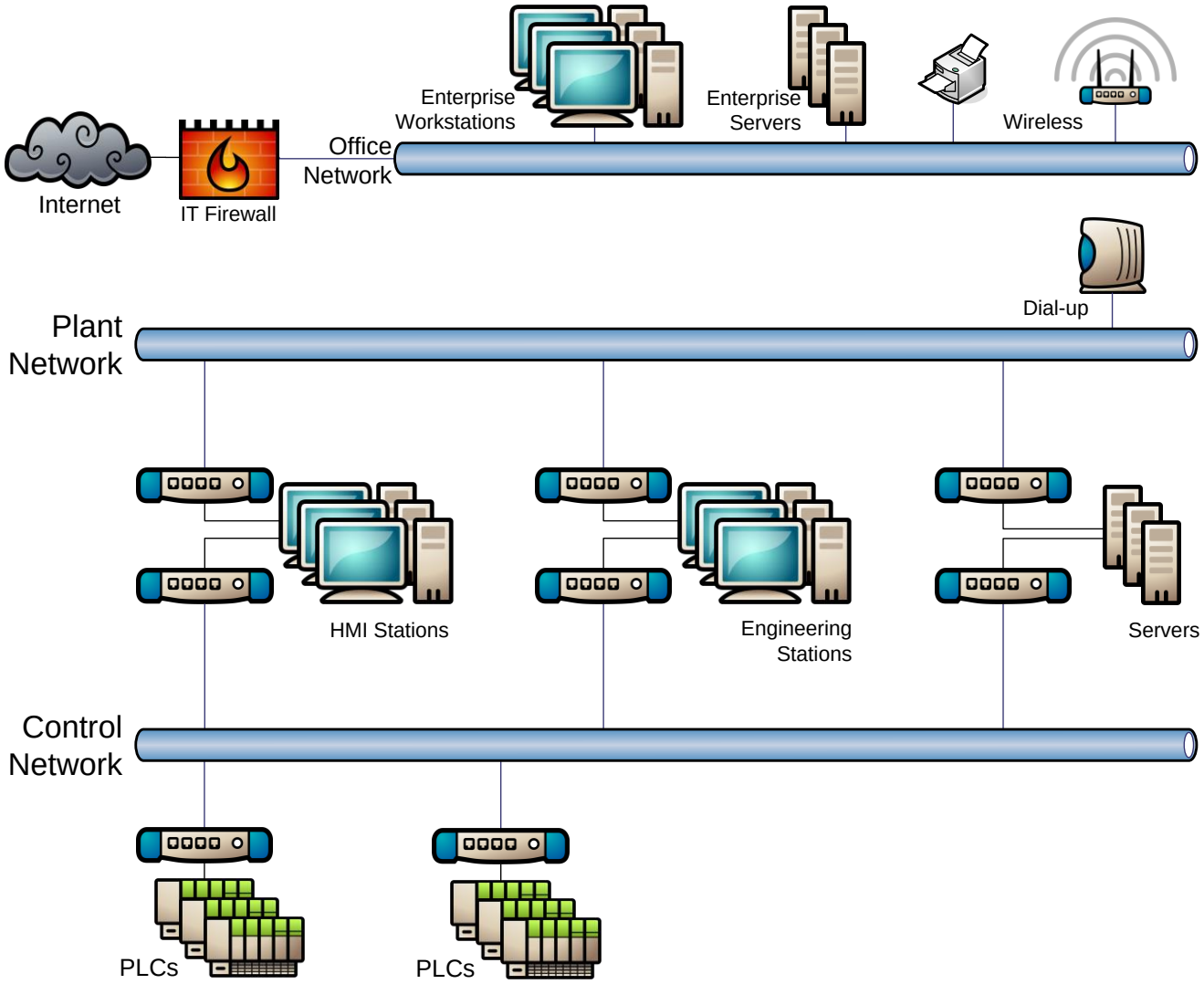
Início dos anos de 1990 – Influxo do Windows PC





A disponibilidade dos poderosos e "baratos" PCs geraram uma revolução nas redes de controle..
Isso continua até hoje..

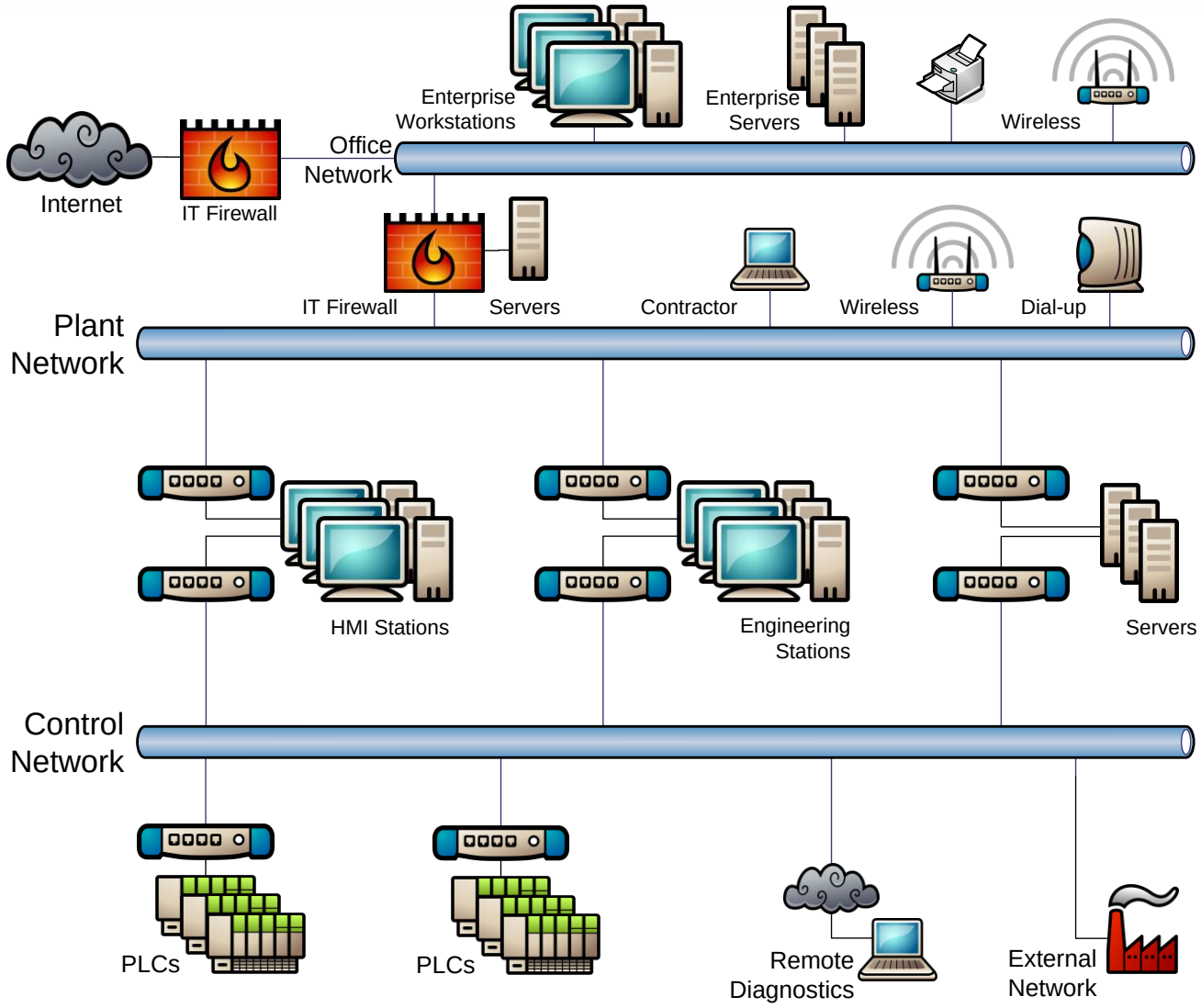
Final dos anos de 1990 – Ethernet Industrial



Introdução da Ethernet Industrial e das redes TCP/IP – as redes do chão de fábrica poderiam crescer rapidamente em tamanho e complexidade

Ainda separadas da rede de Enterprise

Anos 2000 – Interconexão com sistemas Enterprises



- Os sistemas ICS se tornaram interconectados com as outras áreas
- Essa mudança produziu uma imensa melhoria na produtividade mas sujeitavam as redes de controle a estresse e situações que não estavam preparadas para gerenciar.
- Não foram tomadas as medidas de segurança nessas redes

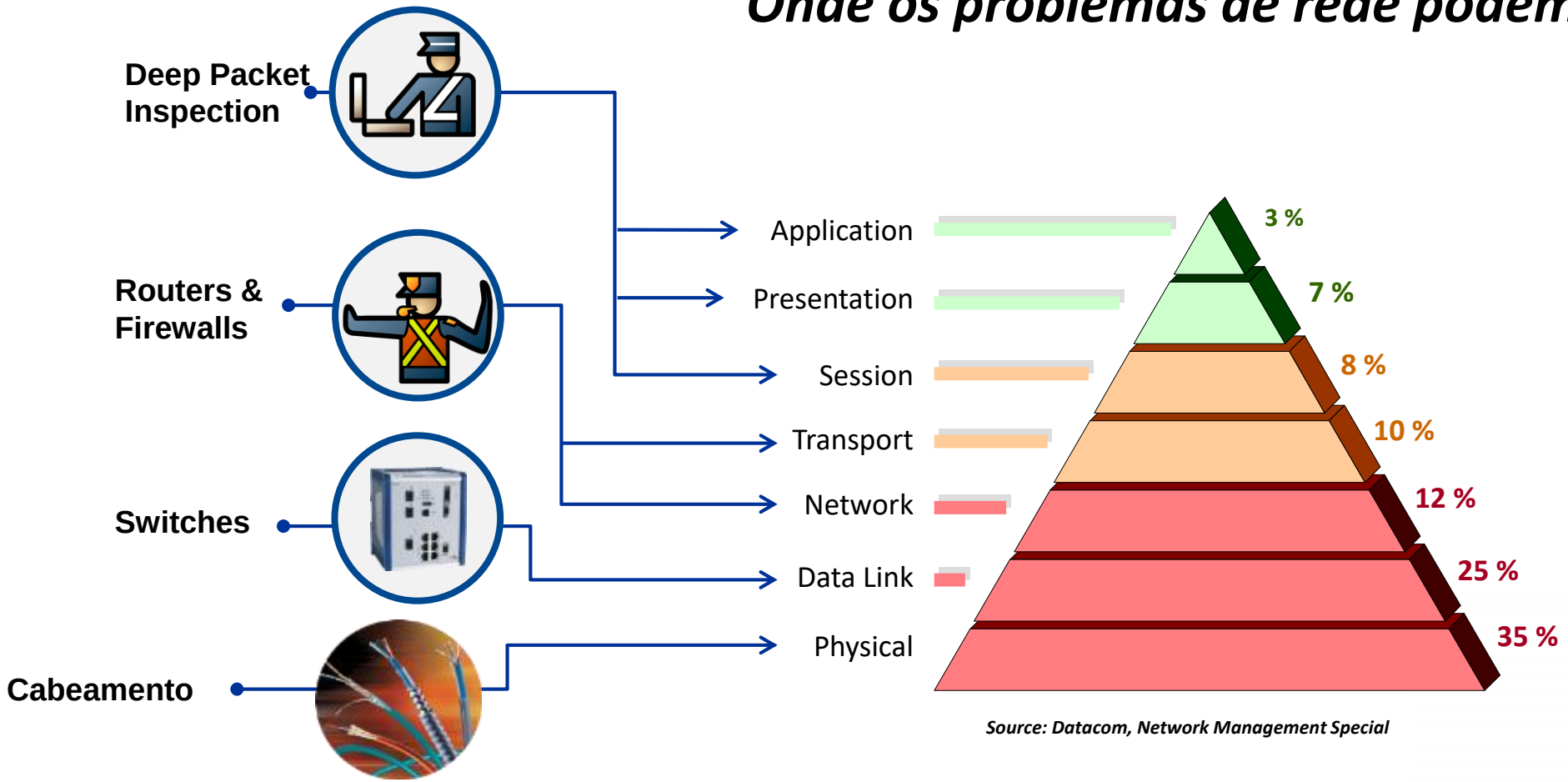
Questões de Segurança em Redes de Controle

Podemos perceber que a maioria das questões de Segurança cabem em 3 categorias principais:

- “Alvos fáceis”
  - PCs funcionam 24x7 sem atualização de segurança ou mesmo antivirus
  - Controladores são otimizados para I/O real-time, e não para conexões robustas de rede
- Múltiplos pontos de entrada na rede
  - A maioria dos incidentes de cyber security se origina de um segundo ponto de entrada da rede
  - USB, conexões de manutenção, laptops, etc.
- Frágil segmentação de rede
  - Muitas redes de controle são “abertas” sem isolação entre diferentes subsistemas
  - Como resultado, os problemas são espalhados rapidamente por toda a rede

Confiabilidade de rede no Modelo OSI

Onde os problemas de rede podem ocorrer...

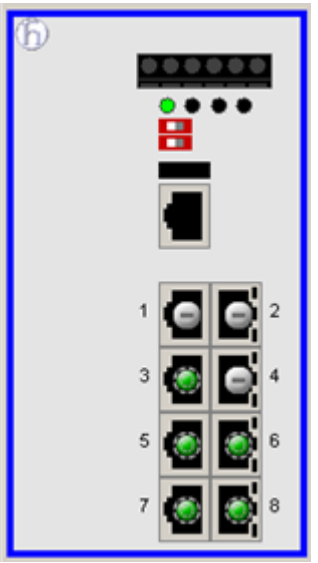


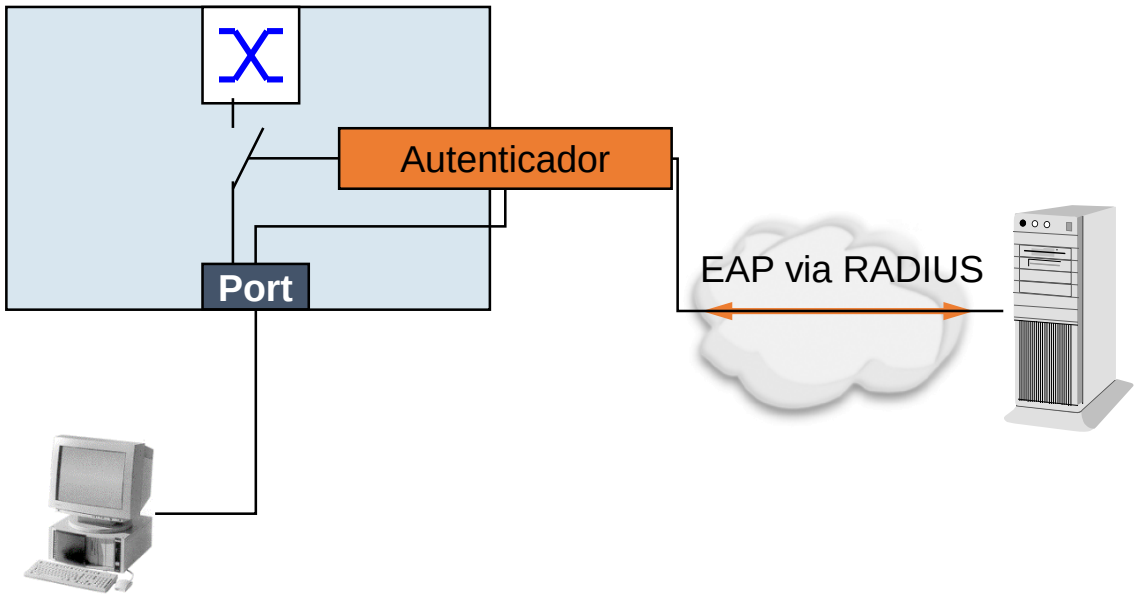
Source: Datacom, Network Management Special

Como nos proteger? – Dificultando o acesso fisico

Como nos proteger? – Segurança por Switch ou Roteador

- Portas não usadas podem ser desabilitadas – sem acesso à rede
- Segurança lógica de porta – o acesso à rede pode ser limitado a determinados dispositivos (por IP ou MAC Address).
- Autenticação IEEE 802.1X - RADIUS

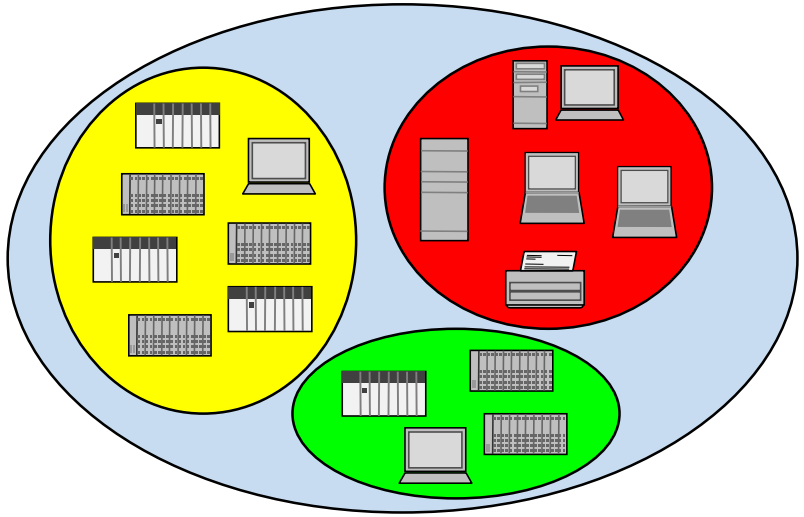


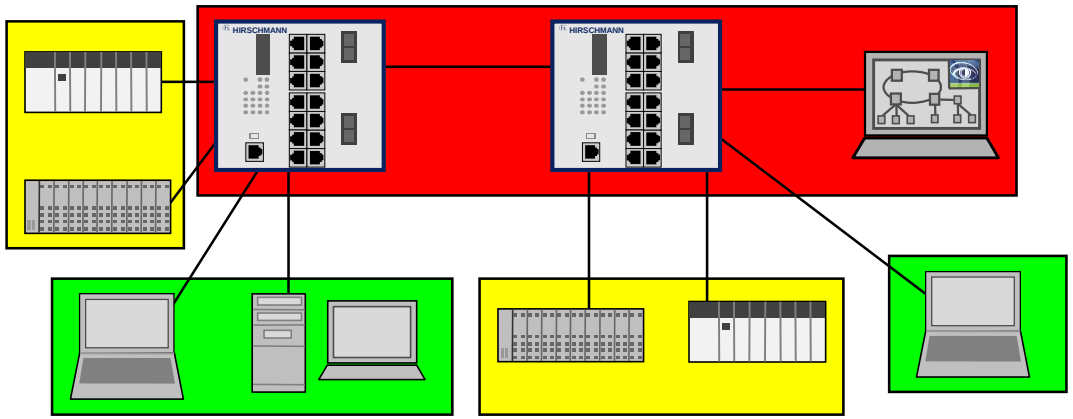


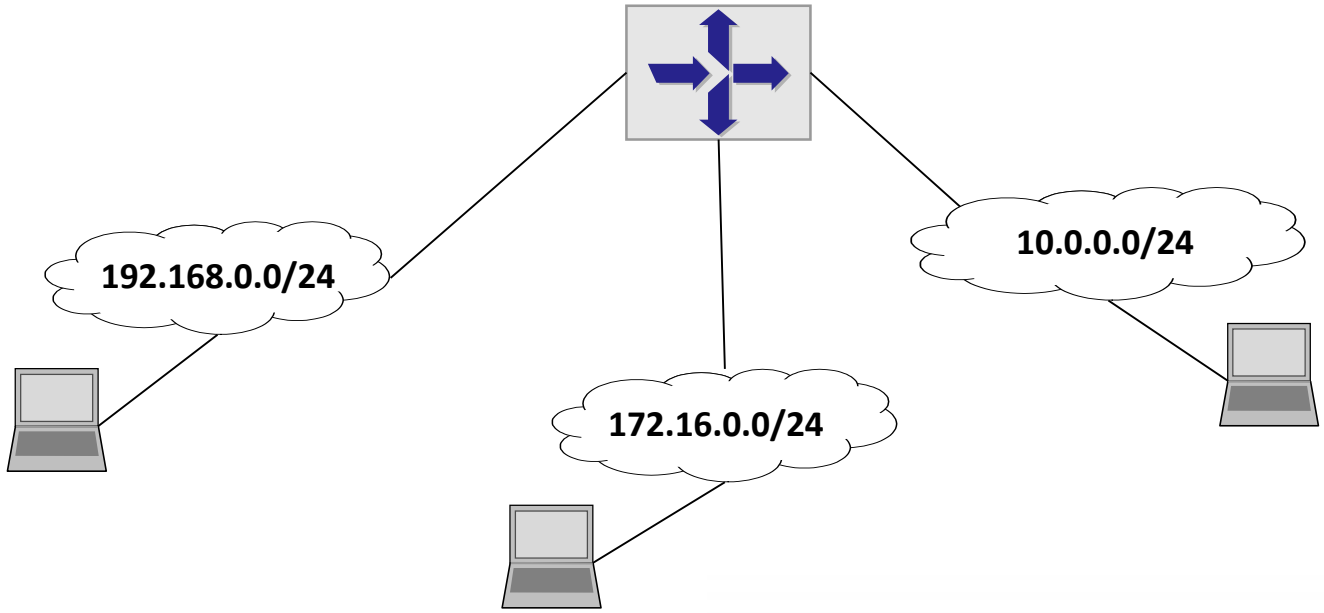
Module	Port	Port Status	Allowed MAC Address	Current MAC Address	Allowed IP address	Action
1	1	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	2	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	3	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	4	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	5	enabled	00:00:00:00:00:00	08:00:20:0A:34:7E	0.0.0.0	none
1	6	enabled	00:00:00:00:00:00	00:80:63:39:F8:85	0.0.0.0	none
1	7	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	8	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none

Como nos proteger? – Segurança por Switch ou Roteador

- Separação entre redes (física ou virtualmente)



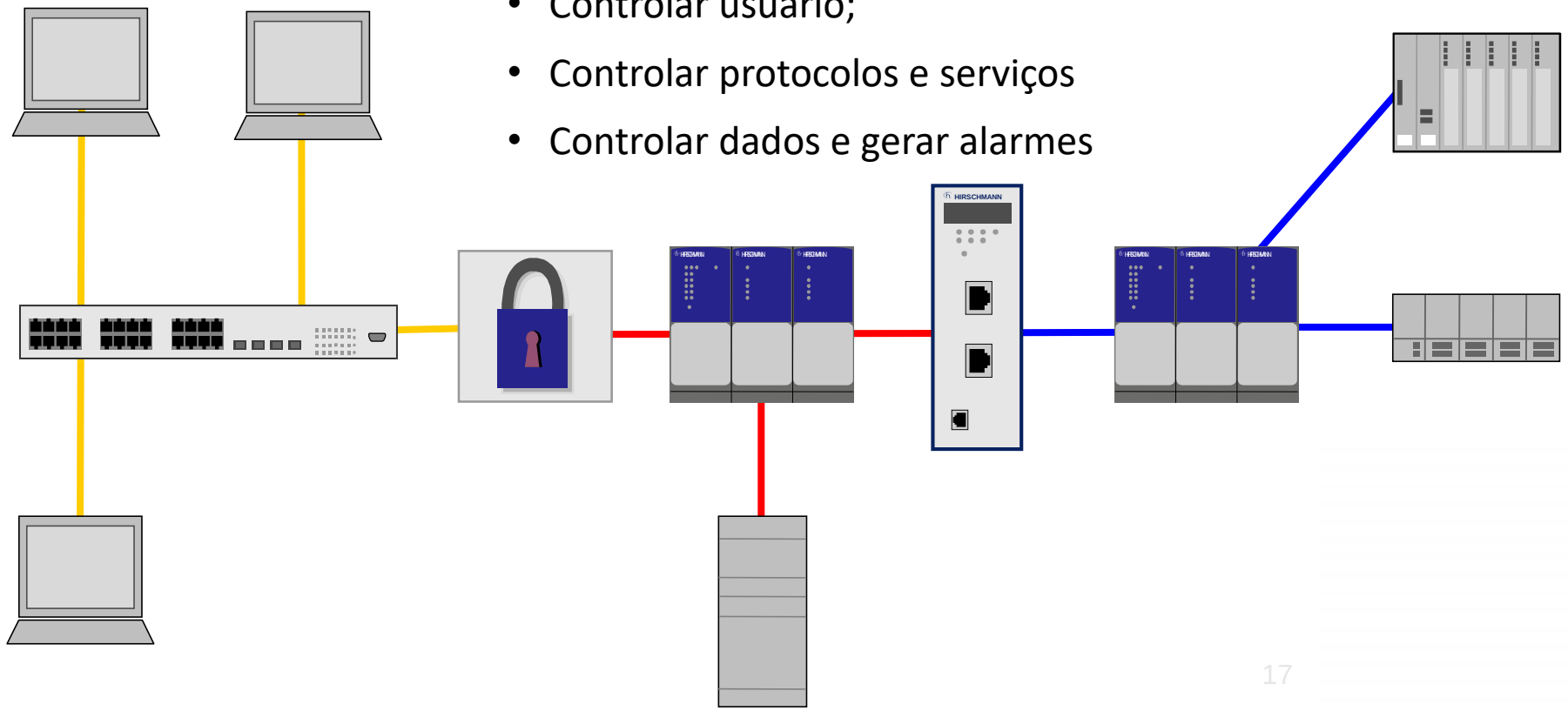




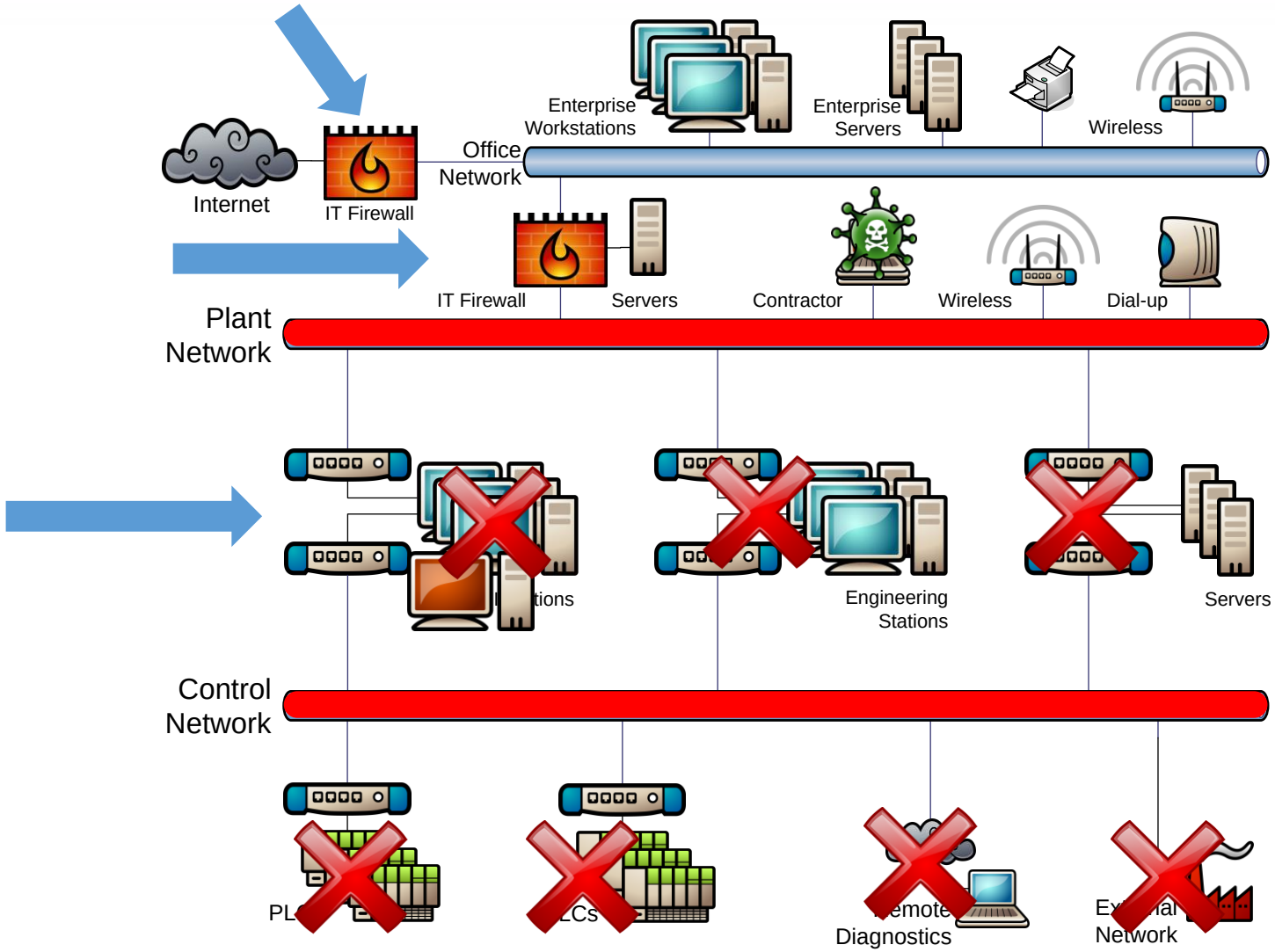
Como nos proteger?

- O que é um firewall?

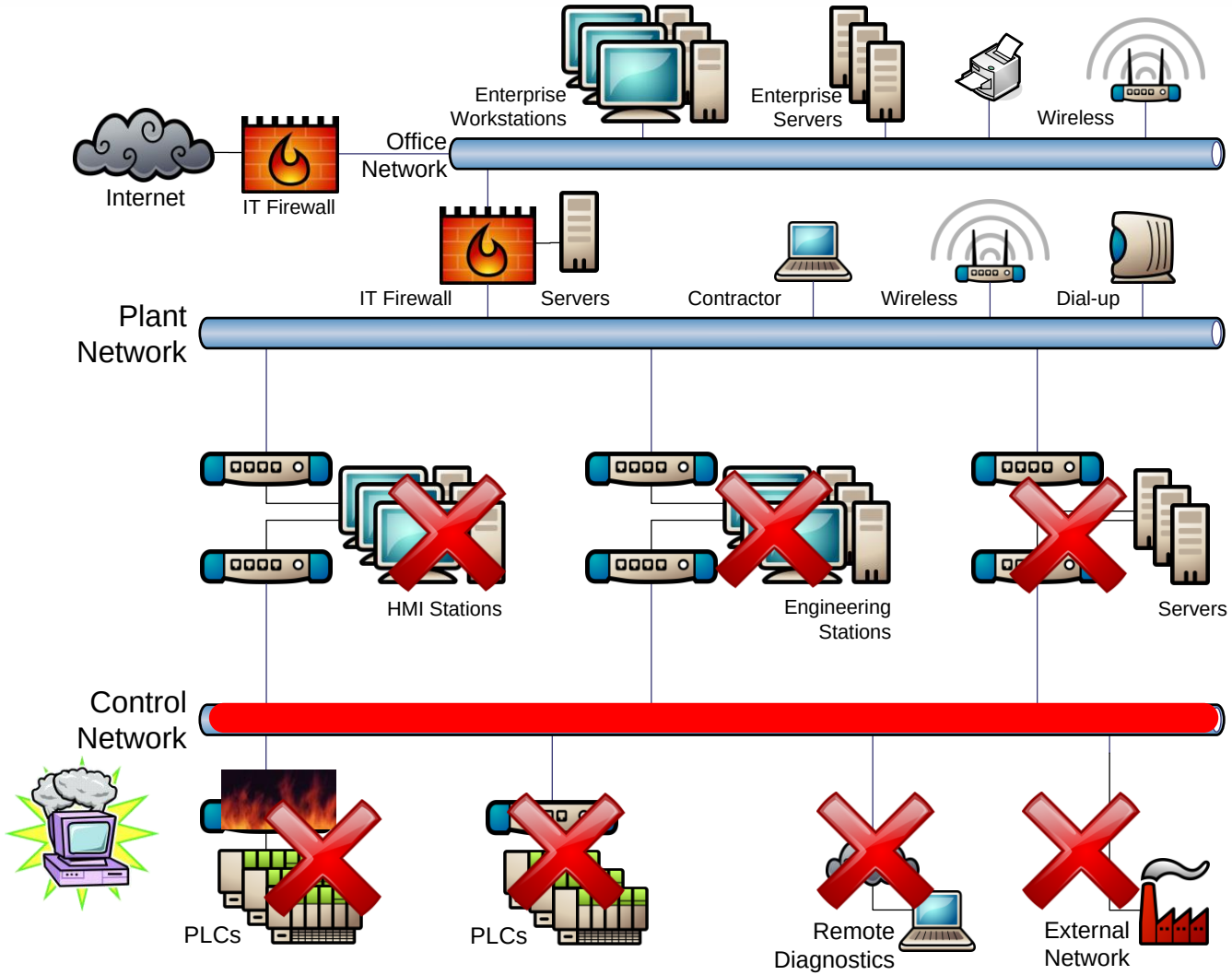
- Proteger contra ataques de redes inseguras;
- Esconder a infraestrutura da rede;
- Controlar acesso;
- Controlar usuário;
- Controlar protocolos e serviços
- Controlar dados e gerar alarmes



Proteção por Firewall - Temos um firewall. Não estamos seguros?



Temos um firewall. Não estamos seguros?



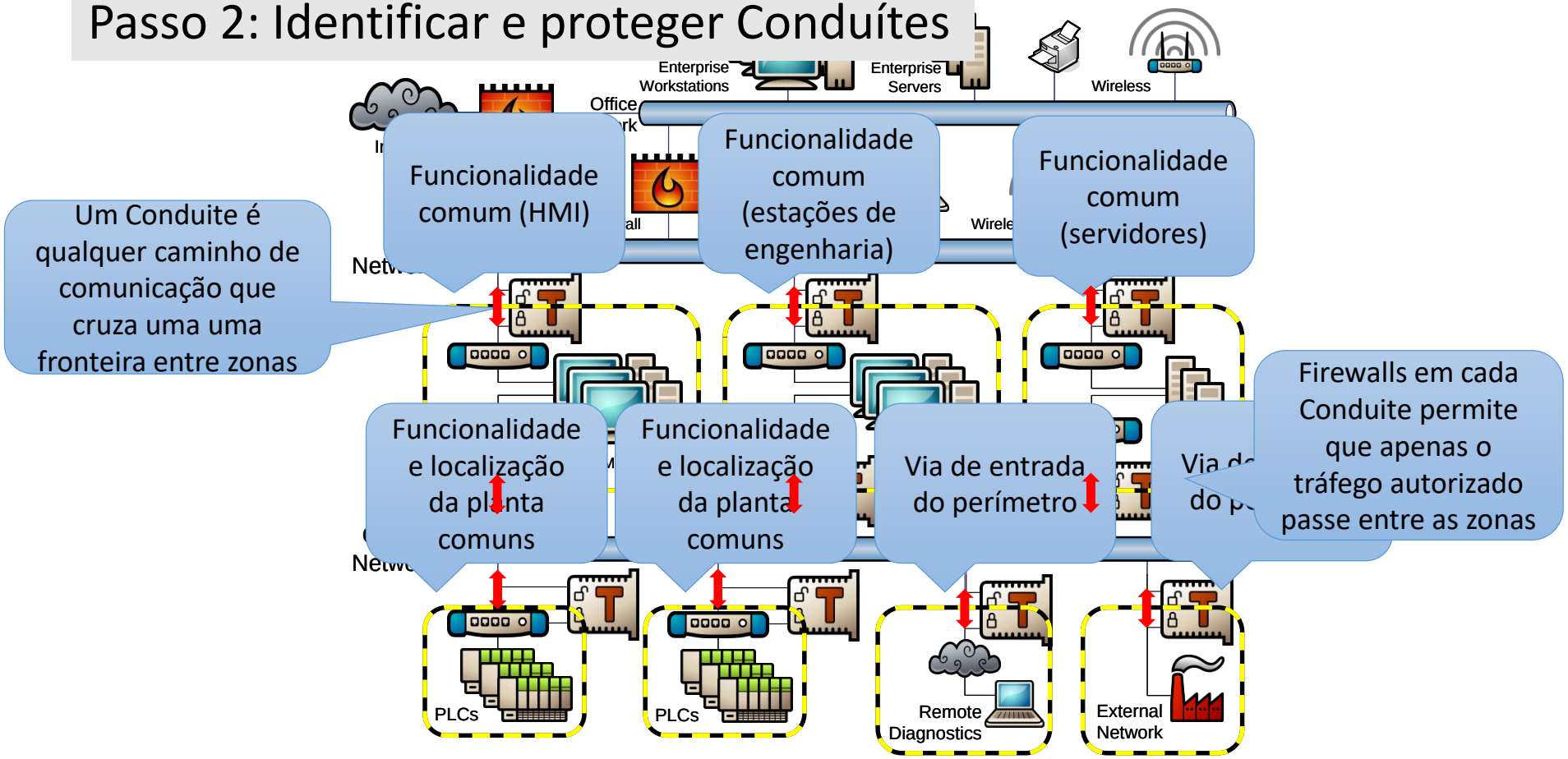
Defesa Periférica não é suficiente

- Não se pode “apenas” instalar um firewall na borda da rede e achar que tudo está seguro.
  - Os “bad guys” irão eventualmente entrar
  - Muitos problemas se originam de dentro da rede de planta
- É preciso “endurecer” o chão de fábrica.
- Precisamos de Defesa em profundidade.
  - Identificar as ‘Zonas’ e ‘Conduites’ ISA99 na rede
  - Permitir apenas que o mínimo tráfego requerido pela rede passe entre as zonas
  - Gerar alarmes quando o tráfego for bloqueado

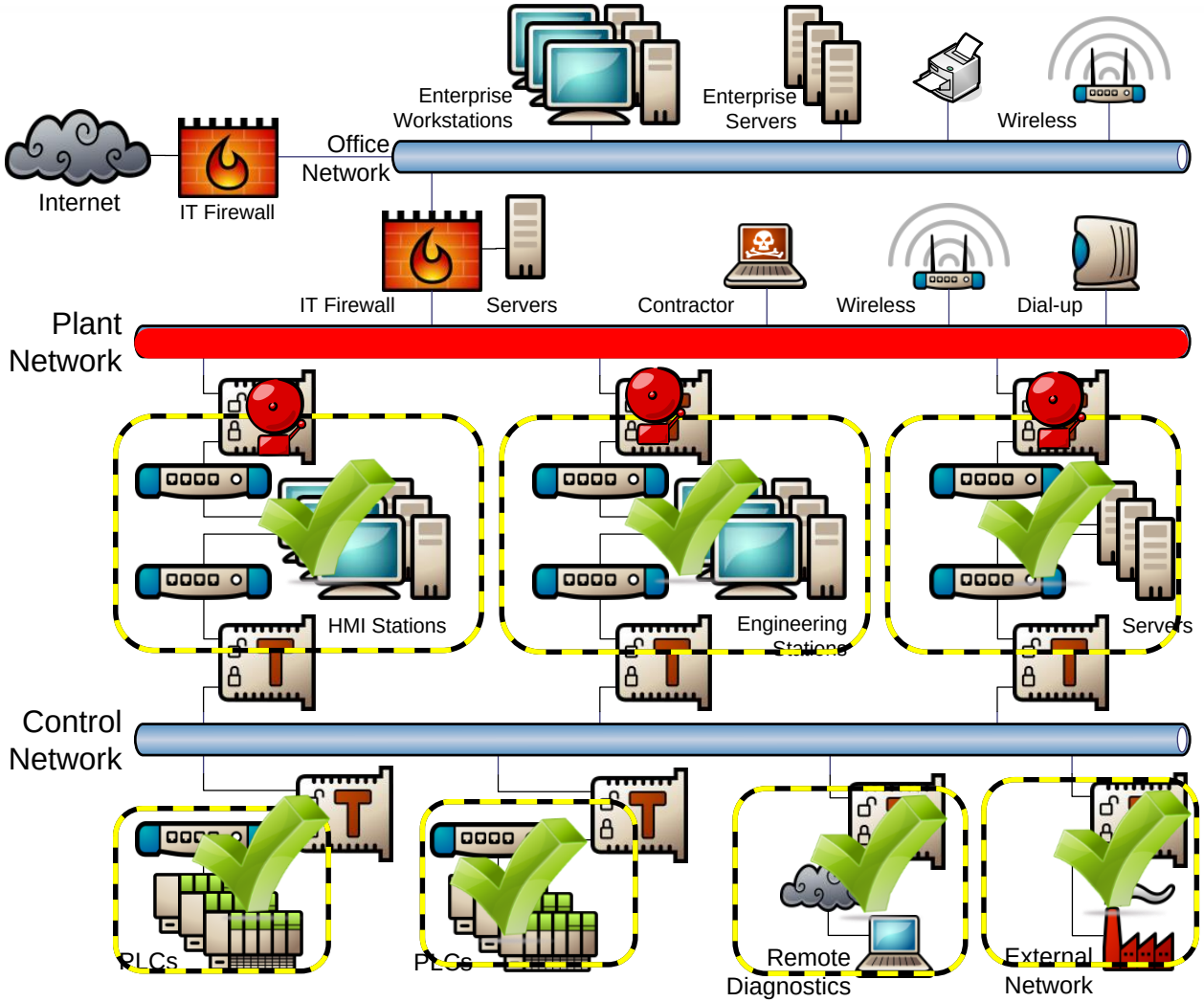
Zonas e Conduites fornecem Defesa em Profundidade

Passo 1: Identificar Zonas de Segurança baseadas em funcionalidades

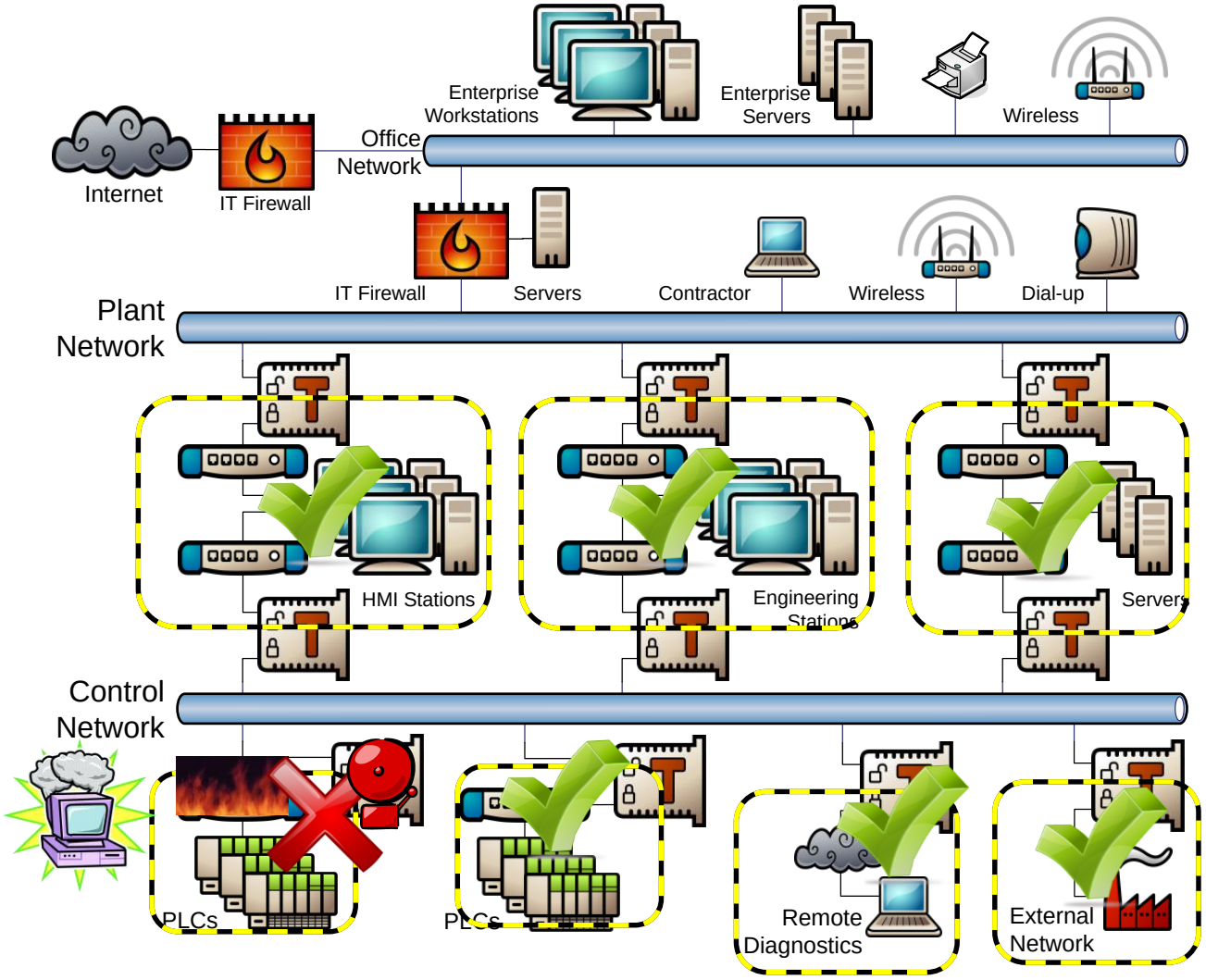
Passo 2: Identificar e proteger Conduítes



Defesa em profundidade no chão de fábrica



Defesa em profundidade no chão de fábrica



Diferenças nas Prioridades TI/TO

Políticas de Segurança	IT Network	OT Network
Foco	Proteger propriedade intelectual e ativos da empresa	Operações 24/7, Segurança, e facilidade de uso
Prioridades	1. Confidencialidade 2. Integridade 3. Disponibilidade	1. Disponibilidade 2. Integridade 3. Confidencialidade
Tipos dos dados de tráfego	Rede Convergente de Dados, Voz e Vídeo (Hierárquica)	Rede convergente de dados, Protocolos de controle, Informação, Segurança e Motion (P2P, Hierárquico)
Controle de Acesso	Estritamente Aute Políticas de Acess	
Implicações de uma falha no dispositivo	Continua a operar	causar danos físicos
Proteção contra ameaças	Shut Down do acesso para detectar e remediar a ameaça	Continuação da operação com detecção da ameaça
Upgrades e gerenc. de patch	ASAP durante Uptime	Agendado durante Downtime

As necessidades mais comumente escutadas são: disponibilidade, segurança e facilidade de uso

Firewall Industrial – principais características

Highlights do firewall para TO

Facilidade de uso

Gerenciamento On-box
Gerenciamento por software proprietário

Confiabilidade e Continuidade de operação

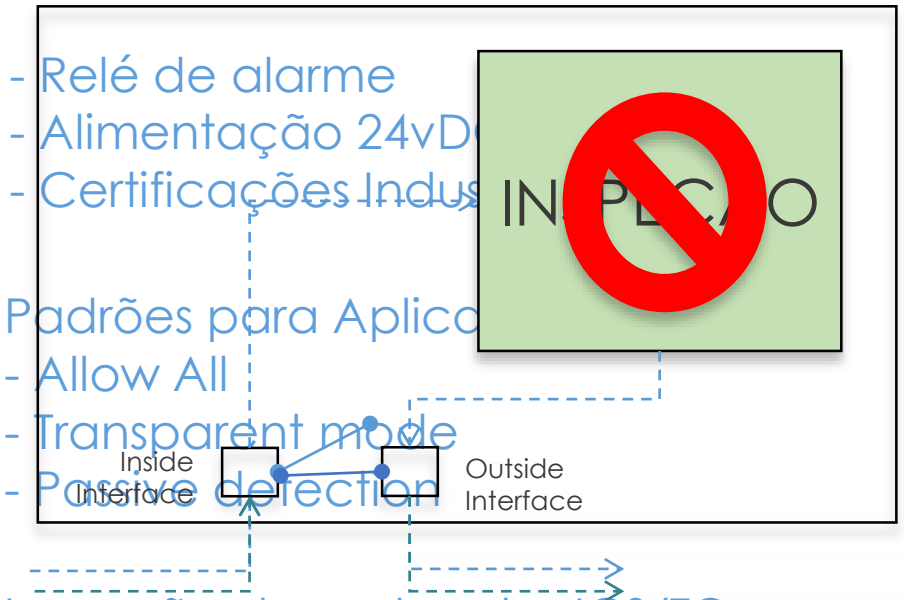
- Dual-power inputs
- Hardware Bypass

Integração de Infraestrutura TO

- Relé de alarme
- Alimentação 24vD
- Certificações Indus

Simples aplicação

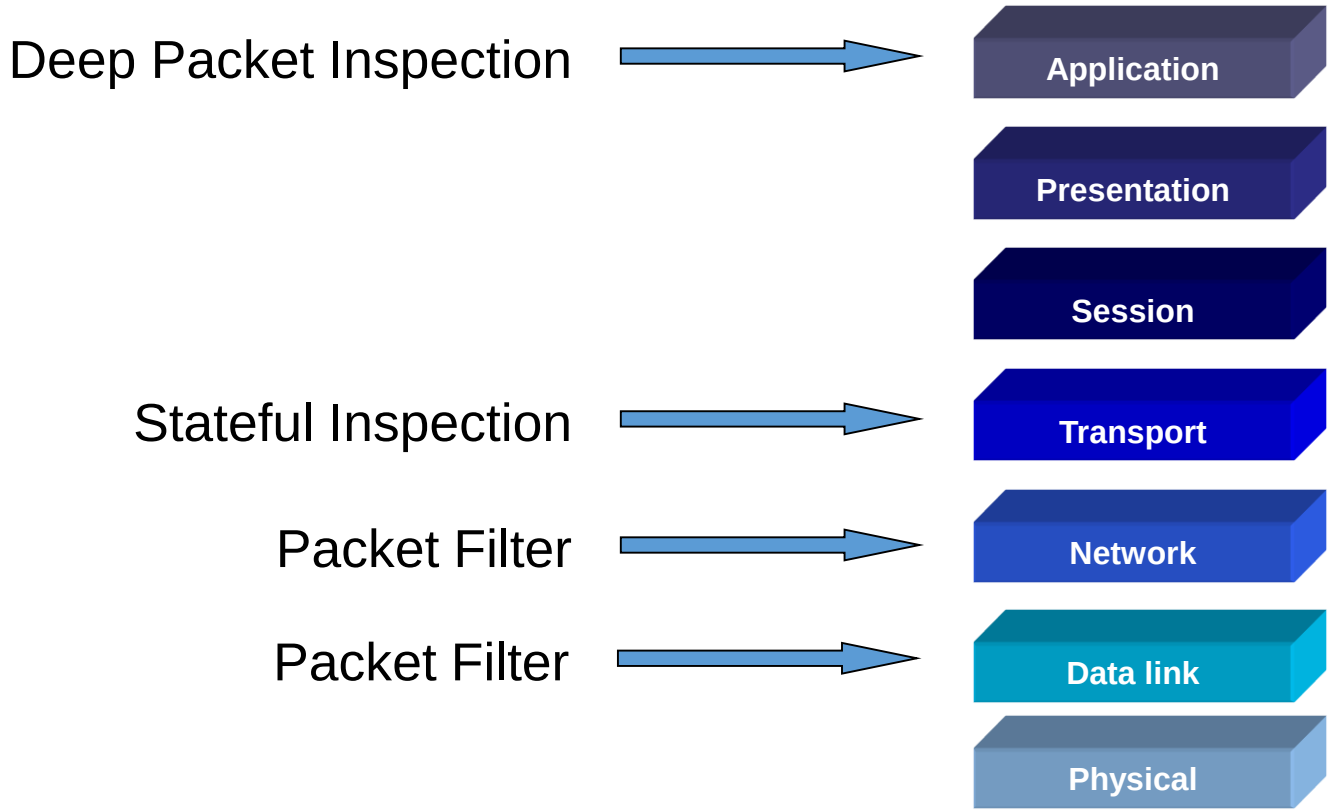
Padrões para Aplica
- Allow All
- Transparent mode
- Passive detection



Extensões específicas de TO

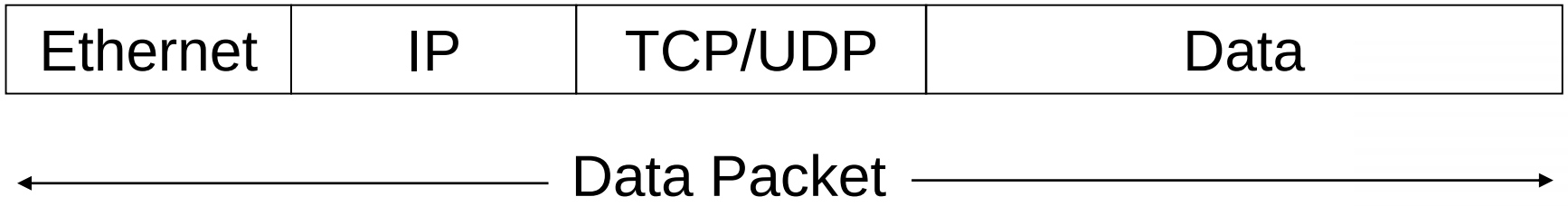
Inspeção de protocolos ICS/TO
- Aplicações
- Comando
- Ameaças

Firewall e o modelo OSI



Deep Packet Inspection

- Examina os dados dentro do pacote
- Aceita ou nega pacotes baseados nos valores dos dados
- Atende a um determinado protocolo



Deep Inspection

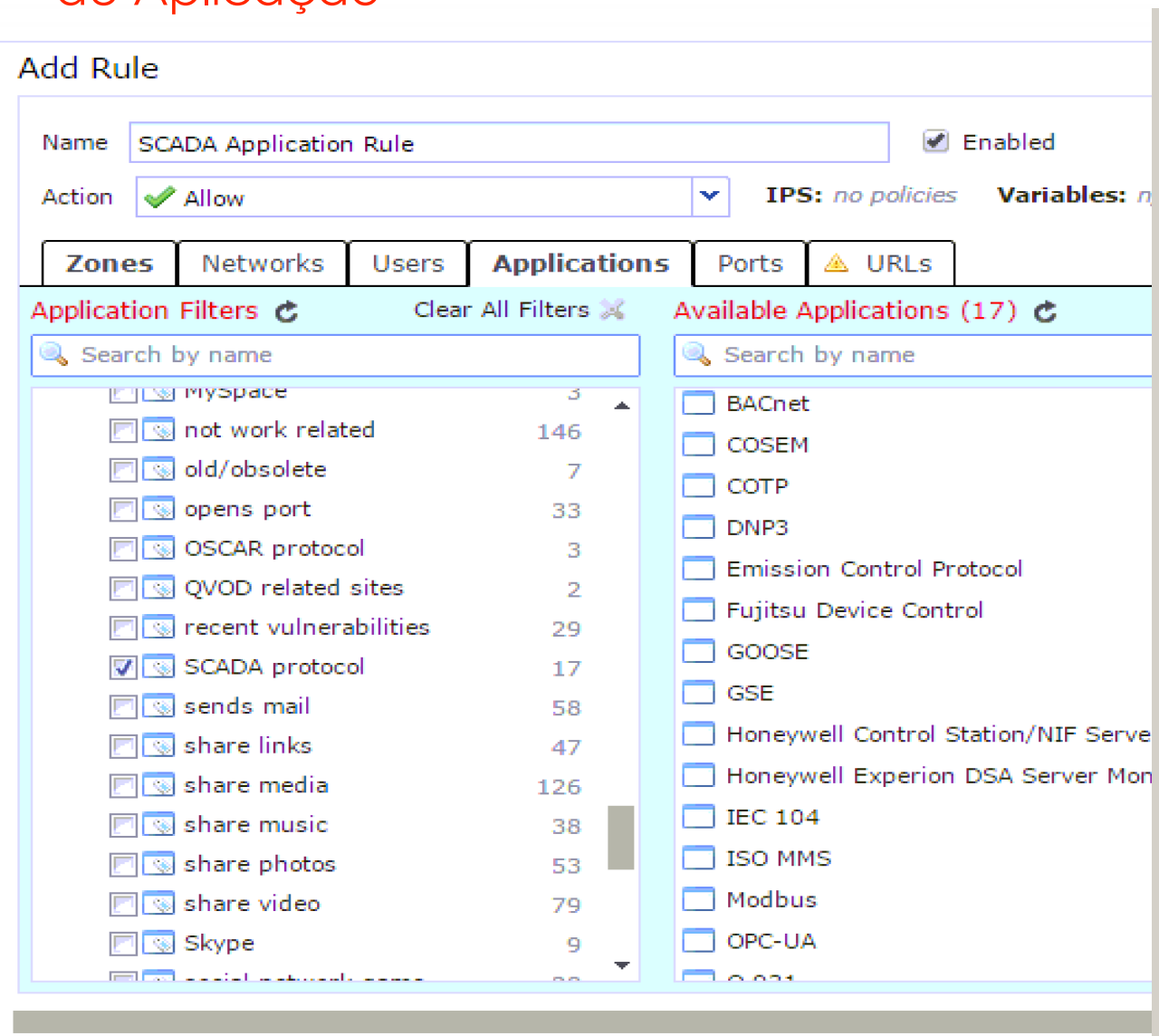
- **Firewall industrial** com **Deep Packet Inspection (DPI):** fácil configuração e desenvolvido para segurança de redes industriais:
  - Focado nos protocolos e dispositivos industriais
  - Desenhado para não interromper a operação
  - Fácil configuração pelos profissionais de Automação

– Um firewall te permite controlar quais dispositivos são permitidos que falem entre si (endereço IP) e quais serviços eles podem acessar (número da porta, Modbus é 502)

– DPI permite controlar oque eles podem dizer um ao outro – exemplo, que comando Modbus pode ser executado

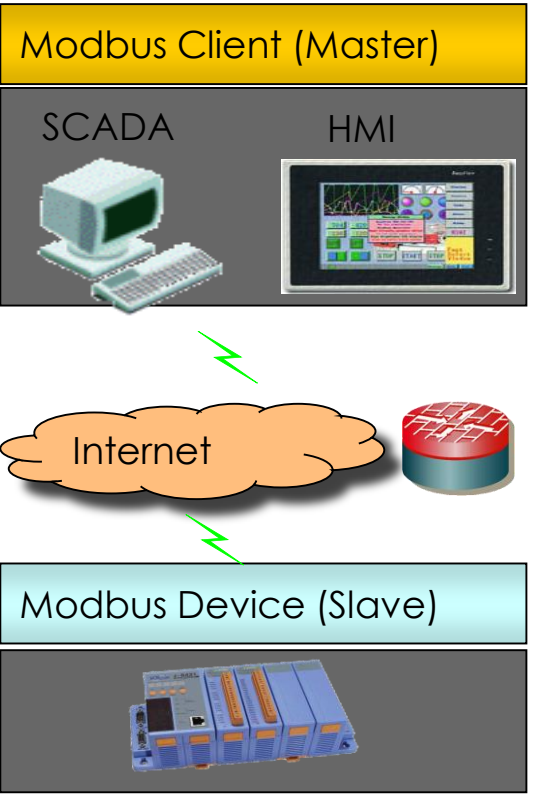
- Permitir que o comando de escrita Modbus para a bobina 56 do terminal de manutenção
- Permitir apenas que o supervisor dispare um comando para o PLC.

Reconhecimento de aplicação TO - Controle e Visibilidade de Aplicação



Caso para aplicação + Comando + Inspeção de Protocolo

Típica Comunicação Modbus: sem Autenticação e Criptografia



Modbus function code (0x2B, 43) - Read Device Identification

A Resposta é –

- VendorName
- ProductName
- ModelName
- ProductCode
- MajorMinRevision

Modbus não é o único – outros protocolos possuem similaridades

- **DNP3**
- **IEC 60870**
- **IEC 61850**
- **Ethernet/IP**

etc

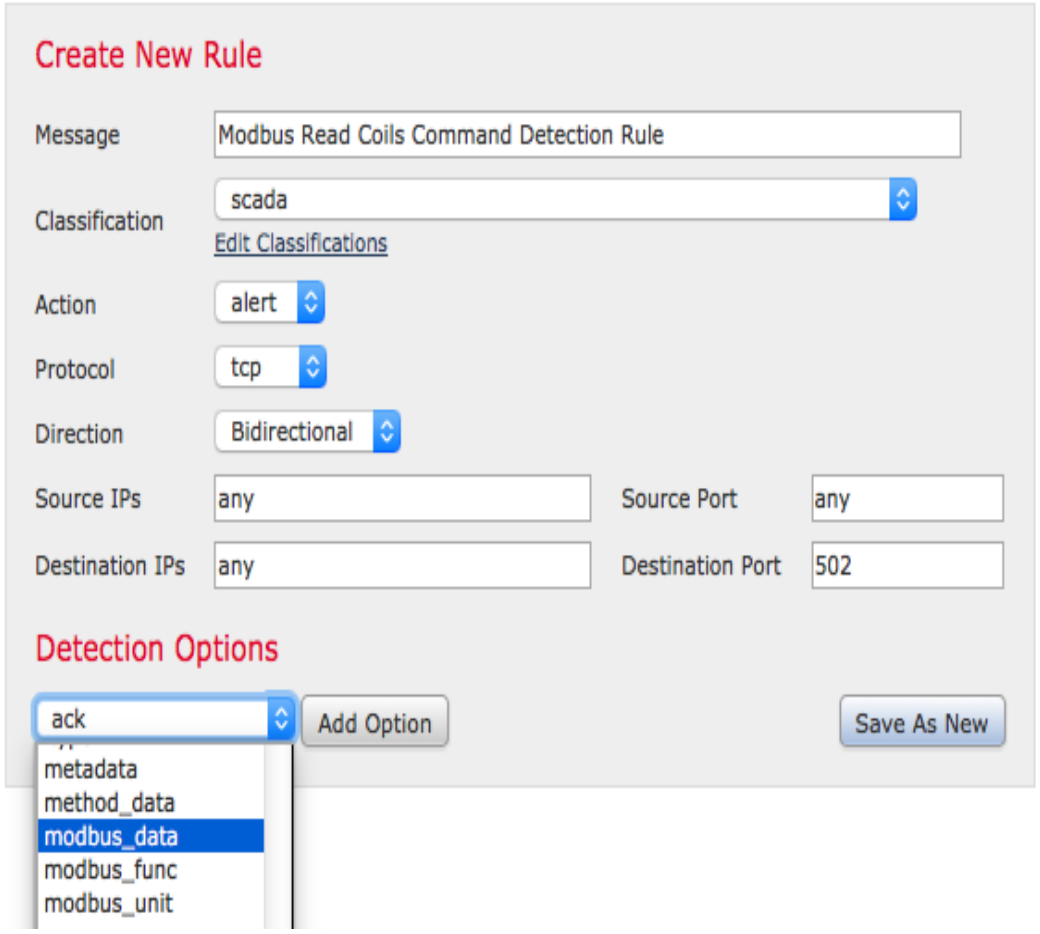
Pacote Modbus – *Sem escopo para Autenticação da origem, precisa de algo (firewall industrial) no meio*

MBAP Header	Function Code	Data

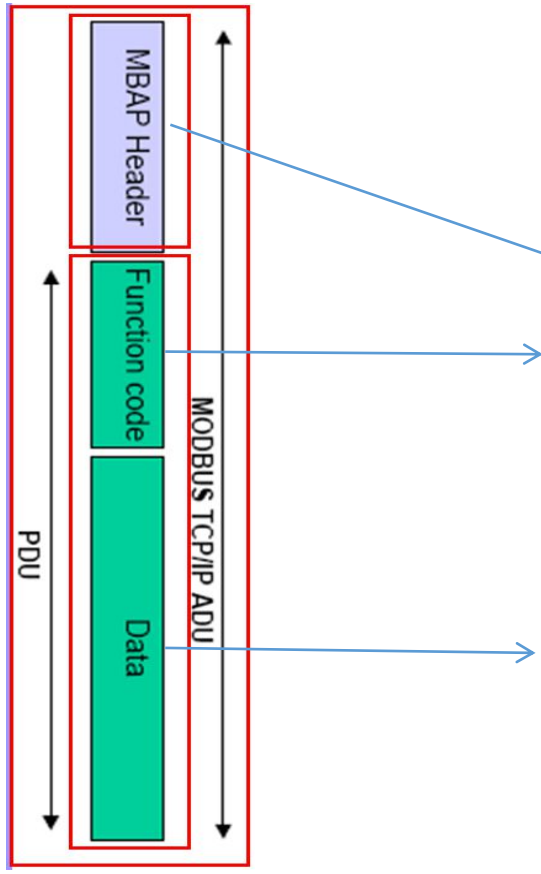
Precisa de alguma coisa entre o Mestre e o Escravo para proteger a comunicação

Pré processador TO – inspeção de comando Modbus

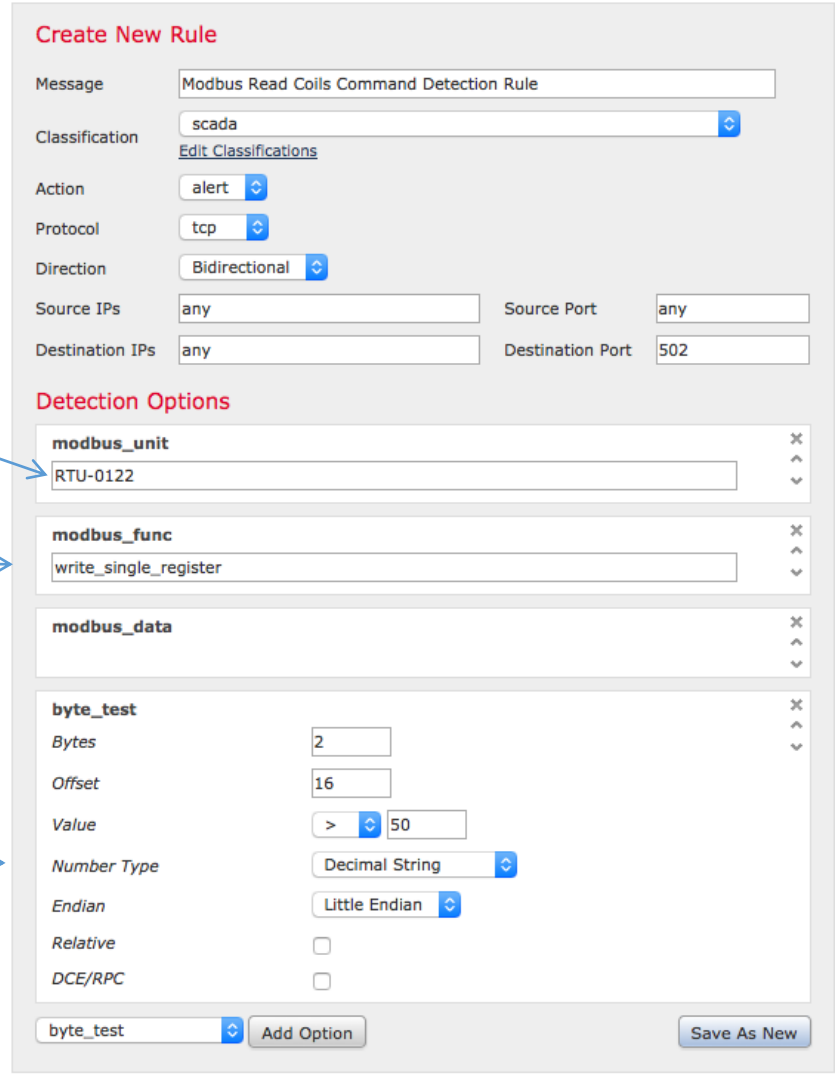
As opções de regras IPS para o Modbus cobre o pacote Modbus inteiro



Modbus packet



Uma regra Modbus para previnir o aumento do limite > 50 em RTU-0122




Lembre-se:
Nunca se contente com uma rede INSEGURA!!!
© EPA

Obrigado!

newton.fernandez@baumier.com.br
11 4332-3280
www.baumier.com.br