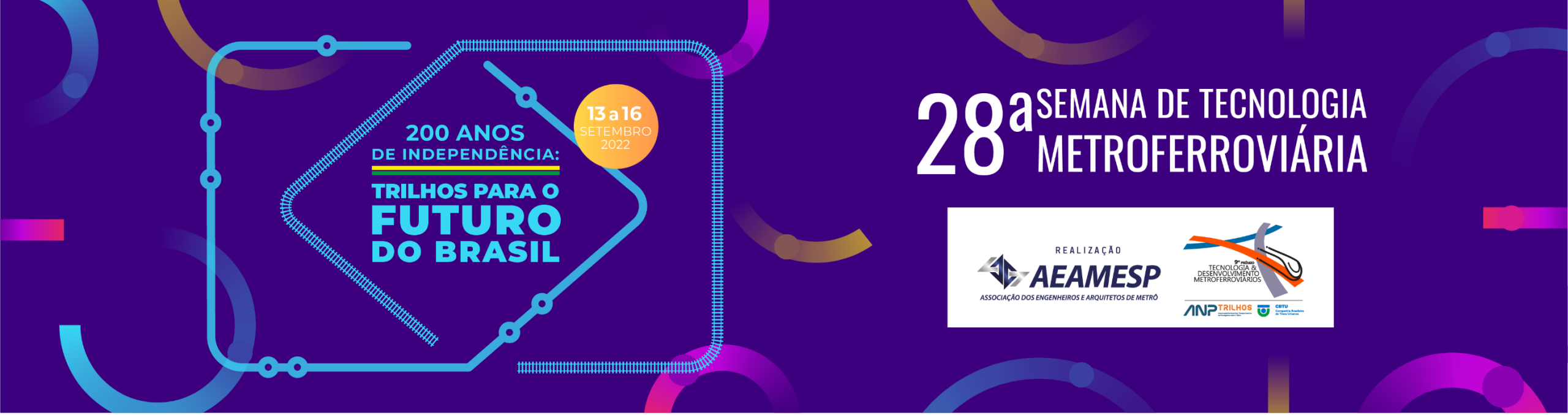


SEGURANÇA CIBERNÉTICA NOS TRILHOS
APLICAÇÃO PRÁTICA EM PROJETOS DE SISTEMAS

Ricardo Frade Mouriño

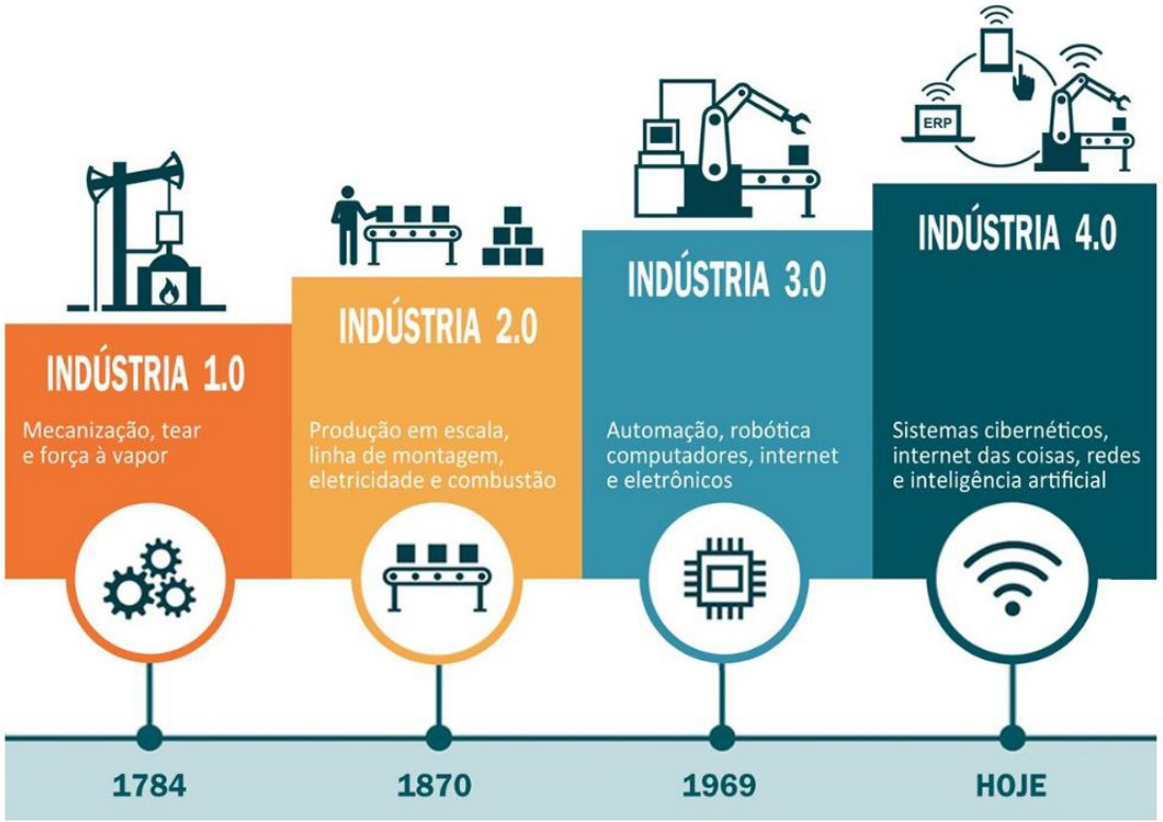
Currículo

- Engenheiro Eletrônico: FEI São Bernardo do Campo
- Especialista em Tecnologia Metroferroviária: Escola Politécnica da USP
- Especialista em Gestão e Tecnologias de Segurança da Informação: FEI São Paulo

- No Metrô de São Paulo:

  ✓Engenheiro de Projetos de Sistemas de Telecomunicações.
  ✓Membro do Comitê Permanente de Avaliação de Riscos Cibernéticos.

Evolução Tecnológica



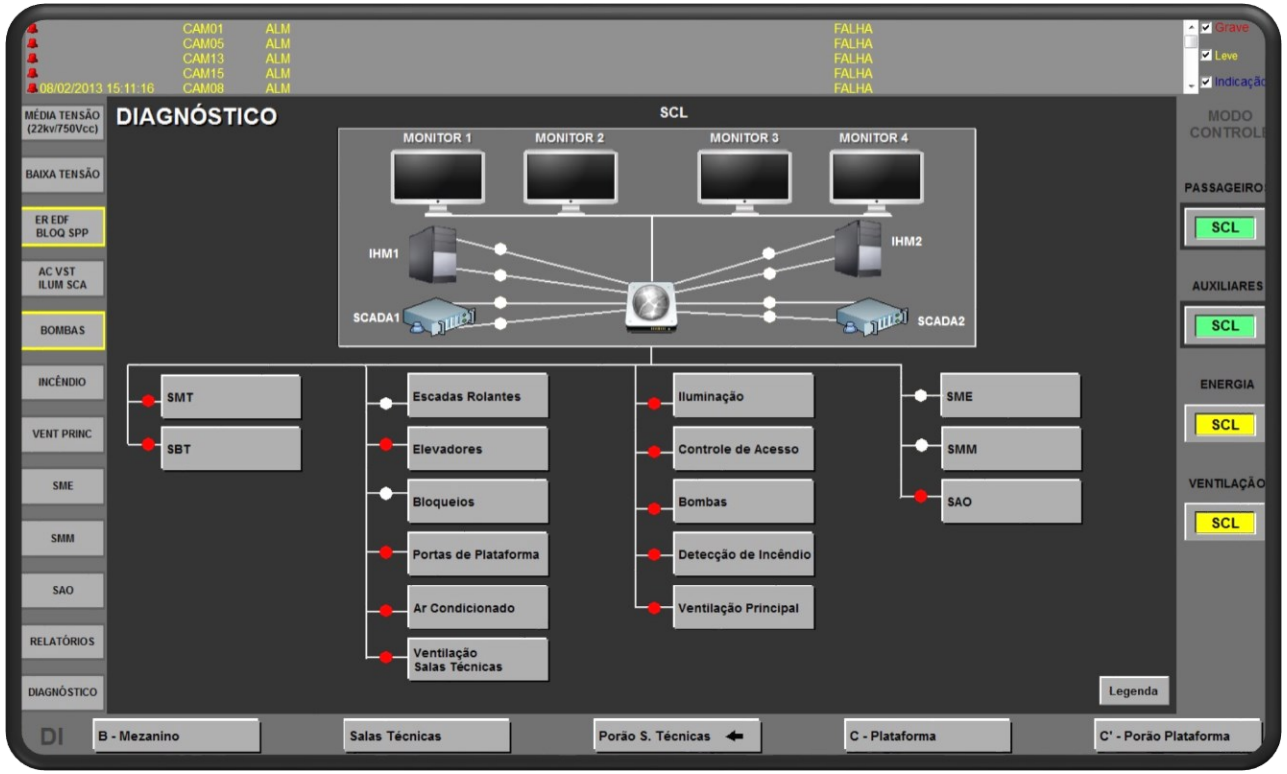
Necessidade de interoperação entre T.I. e T.O.

- Volume de dados
- informações de campo
- Gestão
- ERPs (SAP, etc)
- Atualização de Paths
- Atualização Antivírus
- Informações em nuvem (BigData)
- IA para administração, manutenção e segurança

Serviços de natureza não operacional. Administrativos, gestão e apoio

Evolução tecnológica no setor metroferroviario

Console de Controle Local



SCL – Sistema de Controle Local (SCADA)

Crimes Cibernéticos

Segundo a consultoria alemã Roland Berger, o Brasil foi o 5º país que mais sofreu crimes cibernéticos em 2021

Logo no início do ano tivemos um vazamento que expôs os dados de 223 milhões de brasileiros.

CPF, RG, nome, data de nascimento, veículos, CNPJs, endereços, fotos, escolaridade e renda.

Alguns casos divulgados em 2021/2022

- Facebook
- JBS
- Renner
- CVC
- Atento
- Ifood
- Grupo Fleury
- Americanas
- Sites do Governo

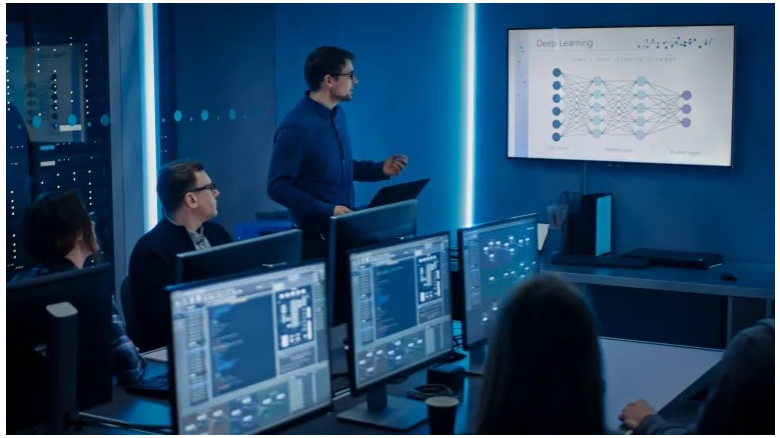
Investimentos em Cibersegurança

Gastos com cibersegurança chegarão a mais de R$980bilhões até 2025.

Fonte: https://seginfo.com.br/

O mercado de segurança de tecnologia operacional (OT) deve crescer de um valor estimado de US$ 15,5 bilhões em 2022 para US$ 32,4 bilhões até 2027

Fonte: https://seginfo.com.br/



Impactos de Crimes Cibernéticos em infraestruturas críticas

O Gartner adverte que,em 2025, 30% das organizações de infraestrutura crítica enfrentarão uma violação de segurança que resultará na interrupção de um sistema ciberfísico de missão crítica ou operacional.

A segurança da infraestrutura crítica tornou-se uma preocupação principal para governos em todo o mundo, com os EUA, Reino Unido, UE, Canadá e Austrália, cada um identificando setores considerados "infraestrutura crítica", por exemplo, comunicações, transporte, energia, água, saúde e instalações públicas.

https://www.convergenciadigital.com.br/

Impactos de Crimes Cibernéticos no setor Metroferroviário

Em 2018 Metrô da Dinamarca para de rodar ao sofrer ataque hacker massivo

https://www.tecmundo.com.br/

Totens são hackeados para exibir pornografia em aeroporto do Rio de Janeiro

05/2022 https://tecnoblog.net/

Em 2016 Ataque de ransomware no metrô de São Francisco faz com que passageiros andem de graça

https://www.perallis.com/

Irã sofre novo ataque cibernético que interrompeu trens e sistemas de transporte causando um “caos sem precedentes” em estações em toda a nação.

07/2021 https://gizmodo.uol.com.br/

Após ataque hacker, Rumo interrompe parte da operação de ferrovias

Os sistemas operacionais estão sendo religados progressivamente

2020 https://epocanegocios.globo.com/

Normas e recomendações sobre segurança cibernética

- NBR/ISO/IEC 27001

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos

- ISA 99 / ISA IEC 62443

Industrial communication networks - Network and system security

(Redes de comunicação industrial - Segurança de redes e sistemas)

- NIST SP 800-82-r2

Guide to Industrial Control Systems (ICS) Security

(Guia de Segurança de Sistemas de Controle Industrial – ICS)

Segurança Cibernética no setor Metroferroviário

- Preocupação Europeia

Com o objetivo de apresentar requisitos e recomendações de cibersegurança no setor ferroviário, o Reino Unido, por meio do Committee GEL/9 - Railway Electrotechnical Applications, desenvolveu uma publicação chamada CLC/TS 50701:2021, baseada na ISA/IEC 62443.

- Dificuldades no Brasil

  - Pouco material traduzido
  - Poucos cursos e certificações especializados
  - Consequentemente: falta de mão de obra especializada

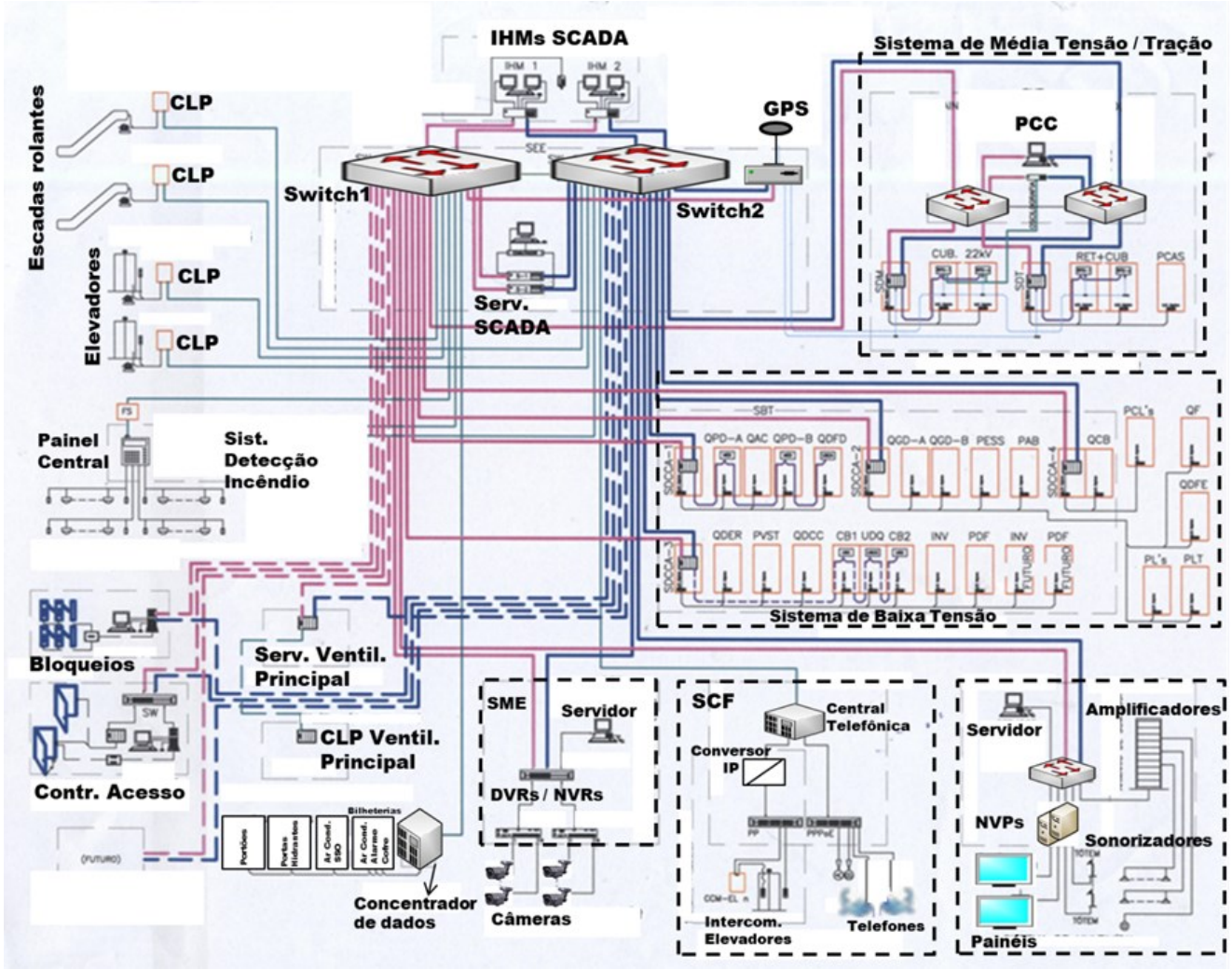
ESCOPO DO TRABALHO

Aplicação da ISA/IEC 62443, apresentando modelos de arquiteturas e requisitos de segurança cibernética aplicados a sistemas metroferroviários brasileiros.

Diagnósticos

Projetos com baixa maturidade em segurança cibernética

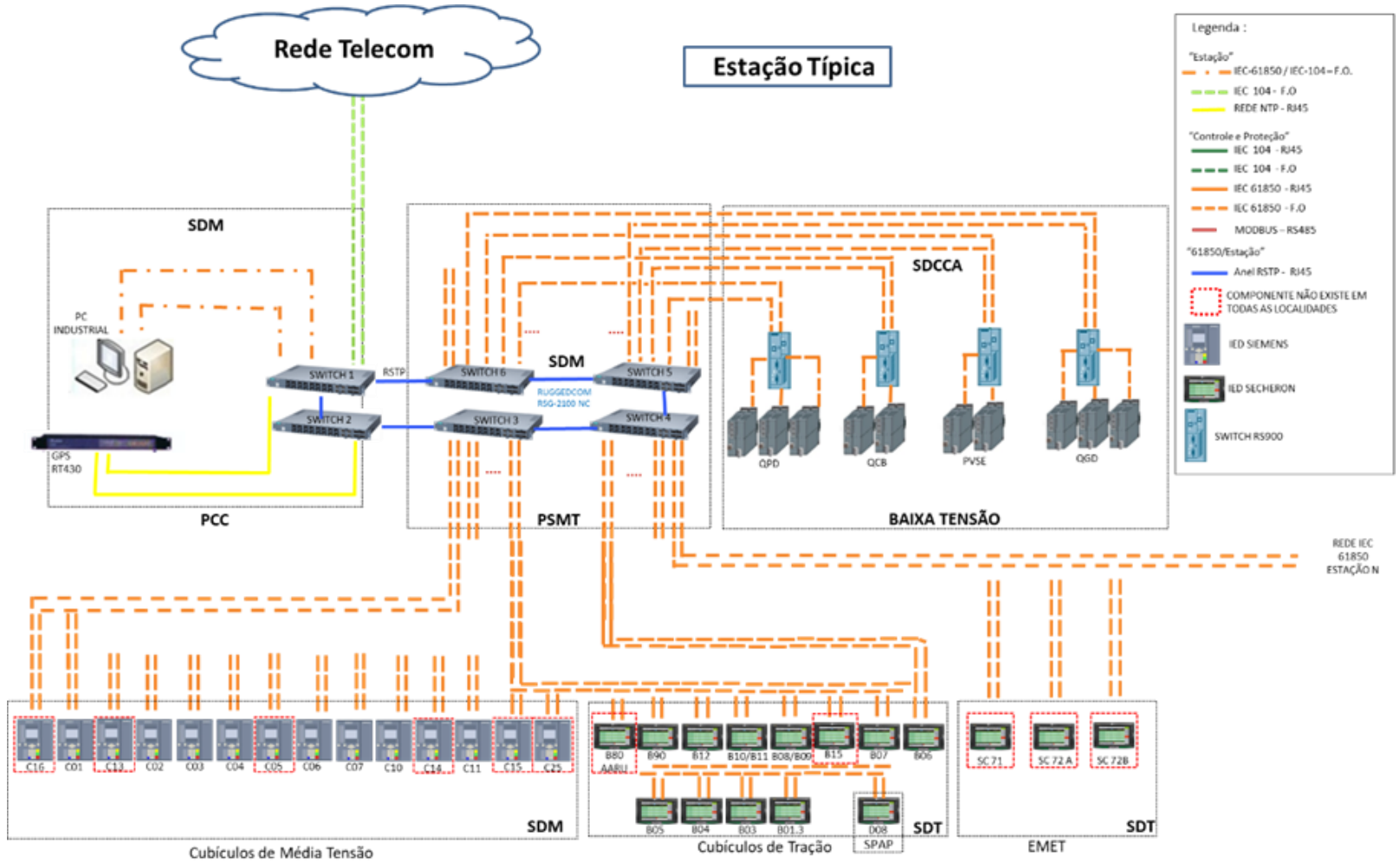
Exemplo: Arquitetura de Sistema de Estação



Diagnósticos

Projetos com baixa maturidade em segurança cibernética

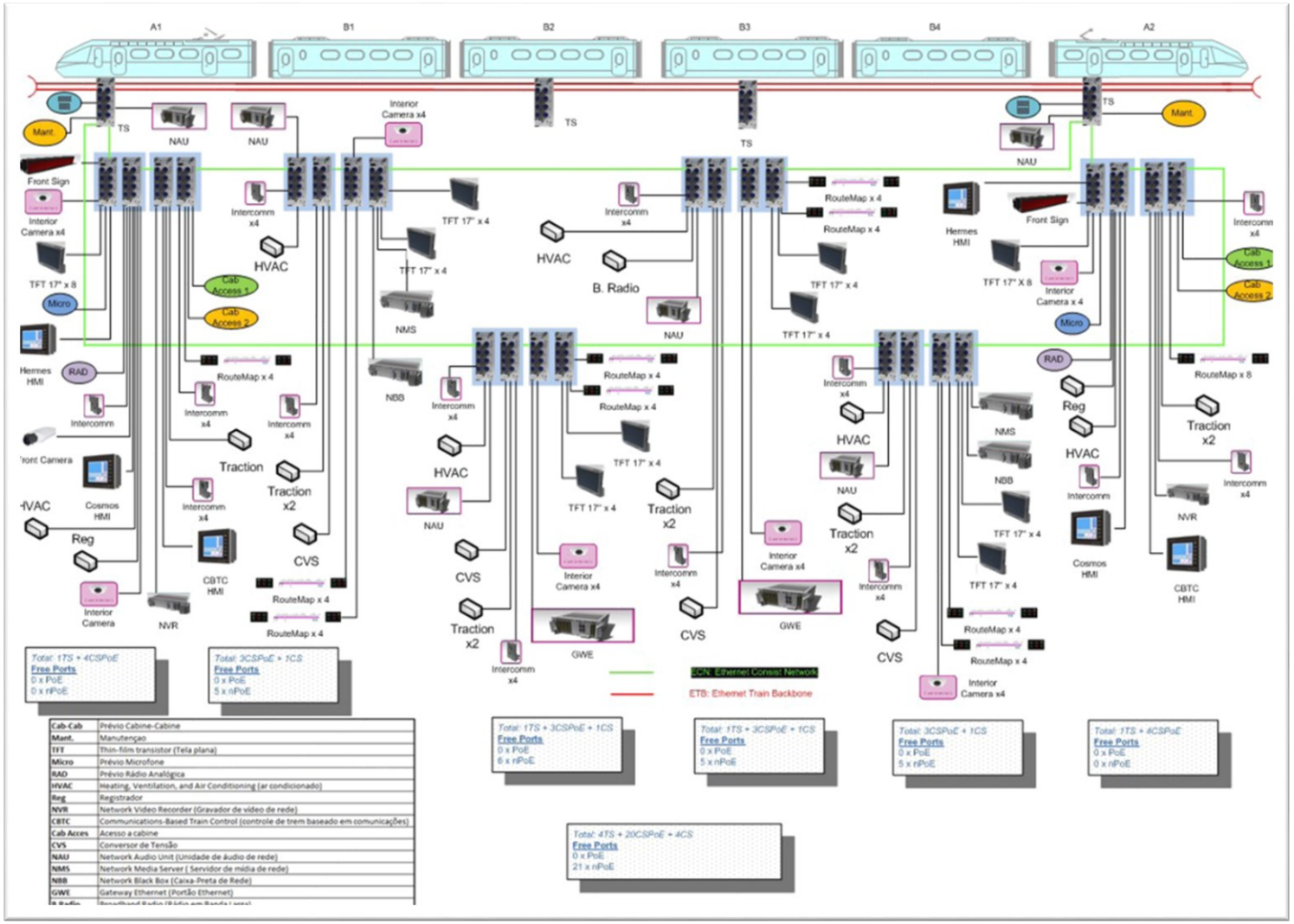
Exemplo: Arquitetura de Sistema de energia elétrica



Diagnósticos

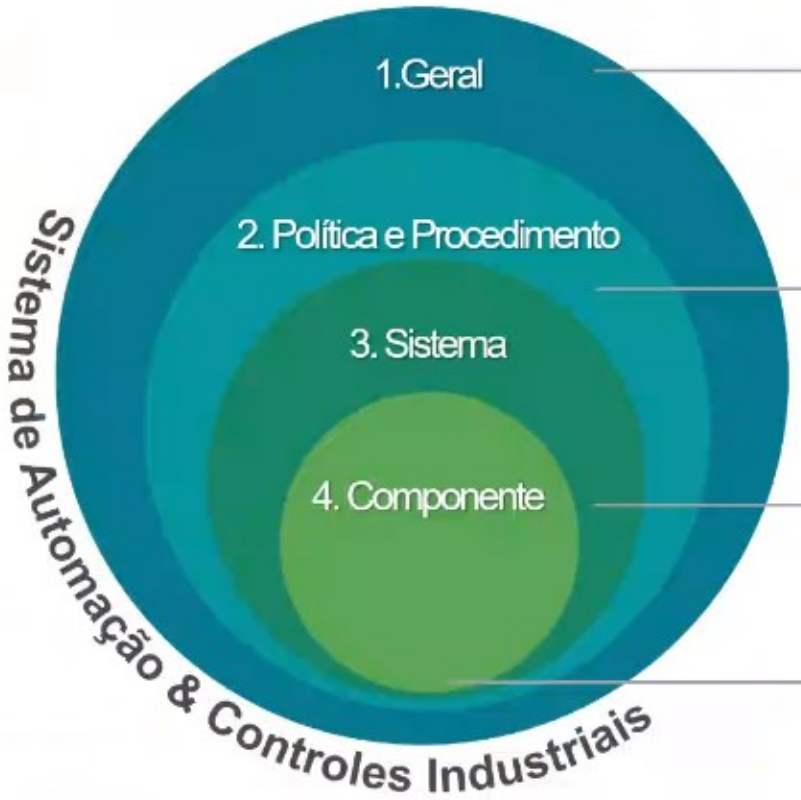
Projetos com baixa maturidade em segurança cibernética

Exemplo: Arquitetura de Sistemas de um trem



Família Normativa ISA/IEC 62443

Norma ISA99/IEC62443



Escopo da Norma ISA99/IEC62443

1-1: Terminologia e Conceitos
1-2: Glossário Principal
1-3: Métricas de conformidade de segurança do sistema
1-4: Ciclo de vida e casos de uso de segurança do IACS

2-1: Requisitos para um sistema de gerenciamento de segurança IACS
2-2: Guia de implementação
2-3 Gerenciamento de Patchs
2-4 Instalação e Manutenção
Aplicação ao responsável pelo ativo

3-1: Tecnologias de Segurança para IACS
3-2: Níveis de segurança e zonas e conduítes
3-3: Requerimentos e níveis de segurança para sistemas
Aplicação ao responsável pelo Integrador de sistema

4-1: Requerimentos para desenvolvimento de produtos
4-2: Requerimentos técnicos para componentes para IACS
Aplicação ao responsável pelo fornecedor do componente

Aplicação prática de segurança cibernética em projetos de sistemas metroferroviários

Para que os projetos de sistemas elaborados com atendimento às normas ISA/IEC 62443, ISO27001 e Guia NIST SP 800-82, sejam efetivamente implantados, operados, administrados e mantidos, existem uma série de processos a serem organizados pela empresa operadora.

Esses processos devem seguir, principalmente, a ISA/IEC 62443 nas partes

1 – Geral

2 – Política e procedimento

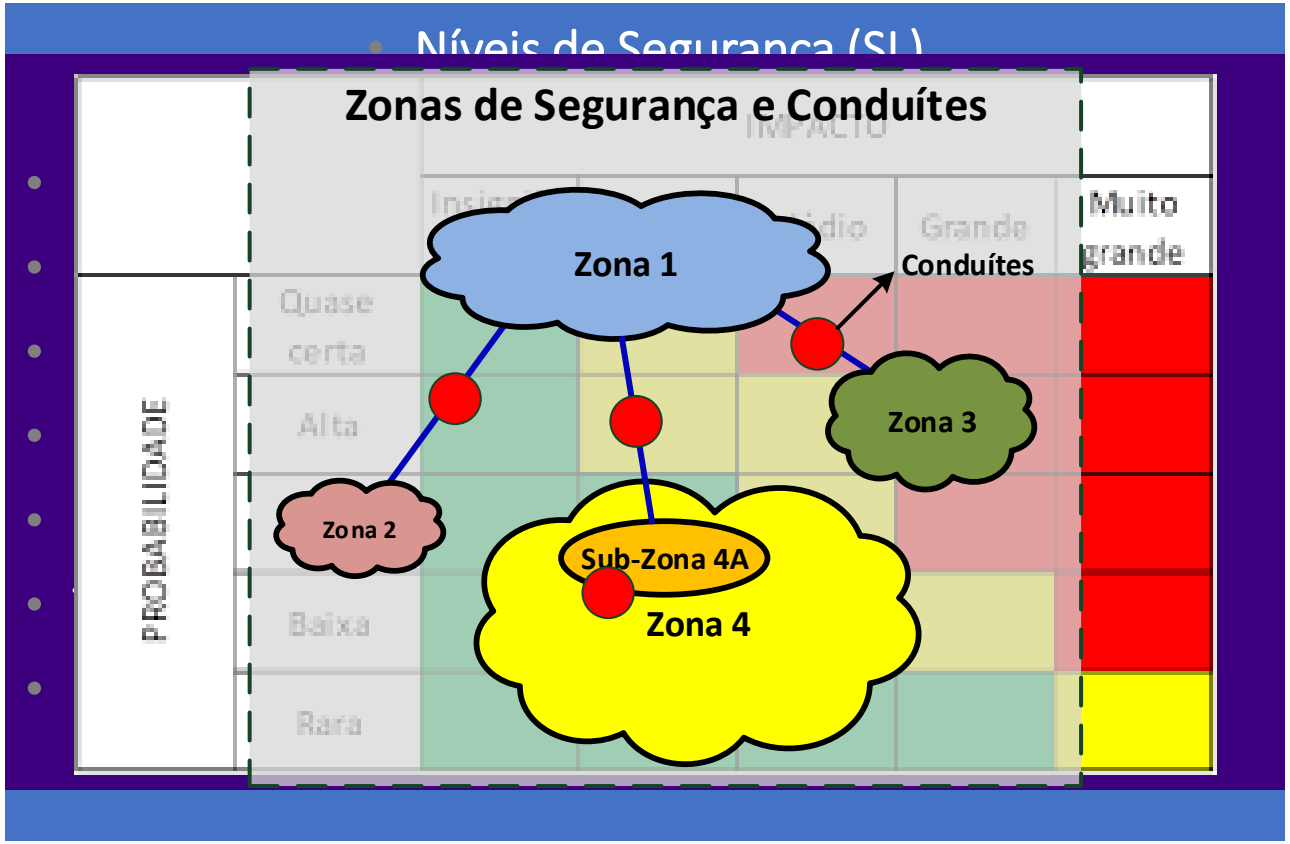
O foco deste trabalho é na etapa de projeto de sistemas de T.O. – Partes:

3 – Sistema

4 – Componente

Conceitos da ISA/IEC 62443 aplicados no trabalho

- Niveis de Segurança (SL).
- Requisitos Fundamentais (RF).
- Defesa em Profundidade.
- Análise de Riscos
  - ➢Avaliação preliminar de riscos
- Zonas e Conduítes.



Recomendações

- Operação, administração e monitoramento

  É muito importante que a empresa operadora se estruture para ter áreas que executem as seguintes funções:

  1. Centro de Operações de Redes (NOC – Network Operation Center).
  2. Centro de Operações de Segurança (SOC – Security Operation Center).
  3. Monitoramento de ativos.

- Domínio de rede operacional
- Plano de Endereçamento IP

Separação dos sistemas em zonas de segurança

Sistemas de T.O. - dispositivos não servidores ou centralizadores (Hosts)

SISTEMA	ÁREA	VLAN/S.R.	ZONA SEG.	NÍVEL SEG.
Monitoração Eletrônica	Telecom	SME	Z-Geral-1	SL-3
Telefonia	Telecom	SCF	Z-Geral-1	SL-3
Multimídia (Monitores)	Telecom	SMM	Z-Geral-1	SL-3
Áudio (P.A.)	Telecom	SMM	Z-Geral-1	SL-3
Controle de Acesso	Telecom	SCA	Z-Geral-1	SL-3
Arrecadação	Telecom	Arrec	Z-Geral-1	SL-3
Bloqueios	Telecom	SCAP	Z-Geral-1	SL-3
Rádio	Telecom	SCM	Z-SCM-1	SL-3
Rede de Transmissão de Dados	Telecom	RTD	Z-Geral-1	SL-3
Rede sem fio	Telecom	RSF	Z-RSF-1	SL-3

Nível de Segurança - SL 3

Proteção contra violação intencional usando meios sofisticados com recursos moderados, habilidades específicas em T.O. e motivação moderada.

Controle Centralizado	CCO	Controle	Z-CTRL-1	SL-3
Controle de Energia	CCO	Controle	Z-CTRL-1	SL-3
Controle de Eq. Aux.	CCO	Controle	Z-CTRL-1	SL-3
Contr. de Fluxo de Passag.	CCO	Controle	Z-CTRL-1	SL-3
Controle do Pátio	CCO	Controle	Z-CTRL-1	SL-3
Controle Local (estações e subest.)	CCO	Controle	Z-Geral-1	SL-3
Simul. de Tráfego de Trens	CCO	Simulador	Z-CTRL-0	SL-3
Simul. Energia, Aux. Fluxo Passag.	CCO	Simulador	Z-CTRL-0	SL-3

Separação dos sistemas em zonas de segurança

Sistemas de T.O. - dispositivos não servidores ou centralizadores (Hosts)

Sist Dig. da Primária	SAL	SAL	Z-SAL-2	SL-3
Sist Dig. de Tração	SAL	SAL	Z-SAL-2	SL-3
Seccion. e contat. de vias	SAL	SAL	Z-SAL-2	SL-3
SPAP / Desern. Catenária	SAL	SAL	Z-SAL-2	SL-3
Sist Dig. de Média Tensão	SAL	SAL	Z-SAL-2	SL-3
Sist. Dig. de Com. Ctrl e Aq. dados	SAL	SAL	Z-SAL-2	SL-3
Sistema de Baixa Tensão	SAL	SAL	Z-SAL-1	SL-3
Grupo Gerador Diesel	SAL	SAL	Z-SAL-1	SL-3
Carreg. Baterias-Inversor-Chv Estát.	SAL	SAL	Z-SAL-2	SL-3
PLs - Iluminação	SAL	SAL	Z-SAL-1	SL-3

Elevador	Auxiliares	Controle	Z-Geral-1	SL-3
Escada Rolante	Auxiliares	Controle	Z-Geral-1	SL-3
Ventilação Principal	Auxiliares	Controle	Z-Geral-1	SL-3
Ar-condicionado	Auxiliares	Controle	Z-Geral-1	SL-3
Bombas	Auxiliares	Controle	Z-Geral-1	SL-3
Vent. Salas téc. e oper.	Auxiliares	Controle	Z-Geral-1	SL-3
Portas de plataforma	Auxiliares	PSD	Z-PSD-1	SL-3
Trat. de Efluentes	Auxiliares	Controle	Z-Geral-1	SL-3
Aquecedores Solares	Auxiliares	Controle	Z-Geral-1	SL-3
Esteiras Rolantes	Auxiliares	Controle	Z-Geral-1	SL-3
Iluminação e Tomadas	Auxiliares	Controle	Z-Geral-1	SL-3

Sinalização e Ctrl (rádios CBTC)	Sinalização	SSC	Z-SSC-3	SL-3
Sinalização e Controle (Outros)	Sinalização	SSC	Z-SSC-2	SL-3
Manut. da Sinalização	Sinalização	SSC	Z-SSC-1	SL-3
Ctrl de Tráfego e Reg. de Trens	Sinalização	SSC	Z-SSC-1	SL-3
Monitoramento de Ativos	Manutenção	SMA	Z-Geral-1	SL-3
Sistemas Externos	Sis-Externos	Não Apl.	Z-SisExt-1	SL-3

Separação dos sistemas em zonas de segurança

Sistemas de T.O. servidores ou centralizadores

SISTEMA	ÁREA	VLAN/S.R.	ZONA SEG.	NÍVEL SEG.
Sincronismo	Telecom	Sinc	Z-Geral-2	SL-3
Detecção de incêndio	Auxiliares	DI	Z-DI-1	SL-3
Servidores / centraliz.	Geral	Serv-Ger	Z-Geral-2	SL-3
Servidores / centraliz.	SCM	Serv-SCM	Z-SCM-2	SL-3
Servidores / centraliz.	RSF	Serv-RSF	Z-RSF-2	SL-3
Servidores / centraliz.	PSD	Serv-PSD	Z-PSD-2	SL-3
Servidores / centraliz.	SAL	Serv-SAL	Z-SAL-3	SL-3
Servidores / centraliz.	CCO	Serv-CCO	Z-CTRL-2	SL-3
Servidores / centraliz.	Simuladores	Serv-Simul	Z-CTRL-0	SL-3
Servidores / centraliz.	SSC	Serv-SSC	Z-SSC-4	SL-3
Servidores / centraliz.	Sis-Externos	Serv-SisExt	Z-SisExt-2	SL-3
Servidores / centraliz.	DMZ	DMZ	DMZ	SL-3

Separação dos sistemas em zonas de segurança

Sistemas de T.O. embarcados

SISTEMA	ÁREA	VLAN/S.R.	ZONA SEG.	NÍVEL SEG.
TCMS	MR-Controle	MR-Ctrl	Z-MR-Ctrl-3	SL-3
PA PIS	MR-Telecom	MR-Tel.	Z-MR-Tel-2	SL-3
Comunic. Trem/terra (exceto CBTC)	MR-Telecom	MR-Tel.	Z-MR-Tel-1	SL-3
Regist. de Eventos Op.	MR-Controle	MR-Ctrl	Z-MR-Ctrl-1	SL-3
Sistema de Climatização	MR-Controle	MR-Ctrl	Z-MR-Ctrl-1	SL-3
Tração e Frenagem Elét.	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Freio de Atrito e Antidesliz	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Sistema de Portas	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Suprim. de Ar Comprim.	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Suprim. Elétrico Auxiliar	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Lubrificador de Friso de Rodas	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Detecção e Combate a Incêndio	MR-DCI	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Engate e Acoplamento	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Detector de Descarrilhamento	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Iluminação interna trem	MR-Controle	MR-Ctrl	Z-MR-Ctrl-1	SL-3
Console de Operação	MR-Controle	MR-Ctrl	Z-MR-Ctrl-1	SL-3
Monitoração de Via	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Sistema Pantógrafo	MR-Controle	MR-Ctrl	Z-MR-Ctrl-2	SL-3
Coleta e Armazenamento de Dados	MR-Controle	MR-Ctrl	Z-MR-Ctrl-1	SL-3
Sistema CBTC	MR-Sinaliz.	MR-SSC	Z-MR-SSC-1	SL-3
Sistemas Externos em Trens	MR-Sis-Ext	MR-Sis-Ext	Z-MR-SE-1	SL-3

Diagrama Geral de Zonas de Segurança e Conduítes

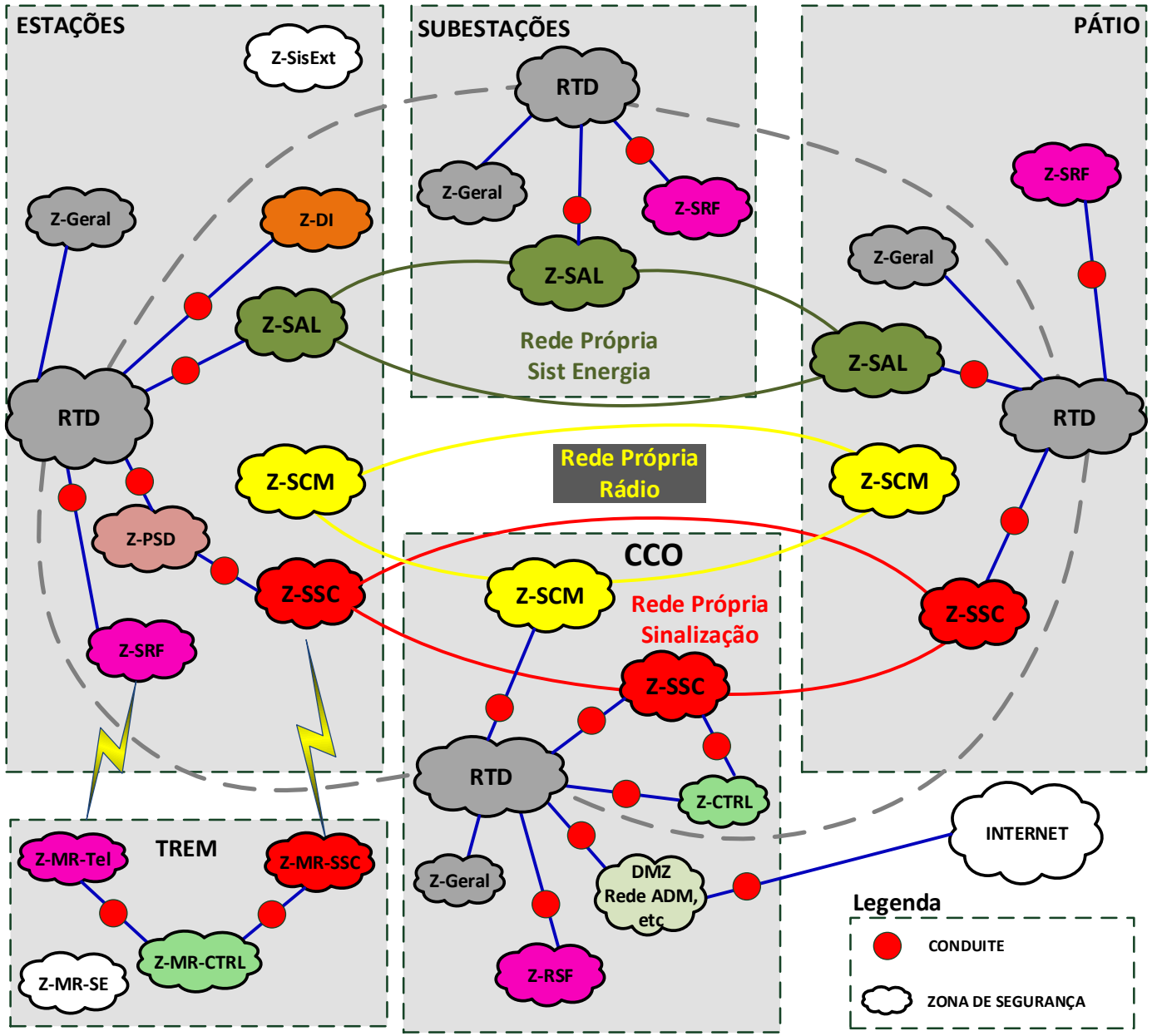


Diagrama de Zonas, Subzonas de Segurança e Conduítes em uma Estação

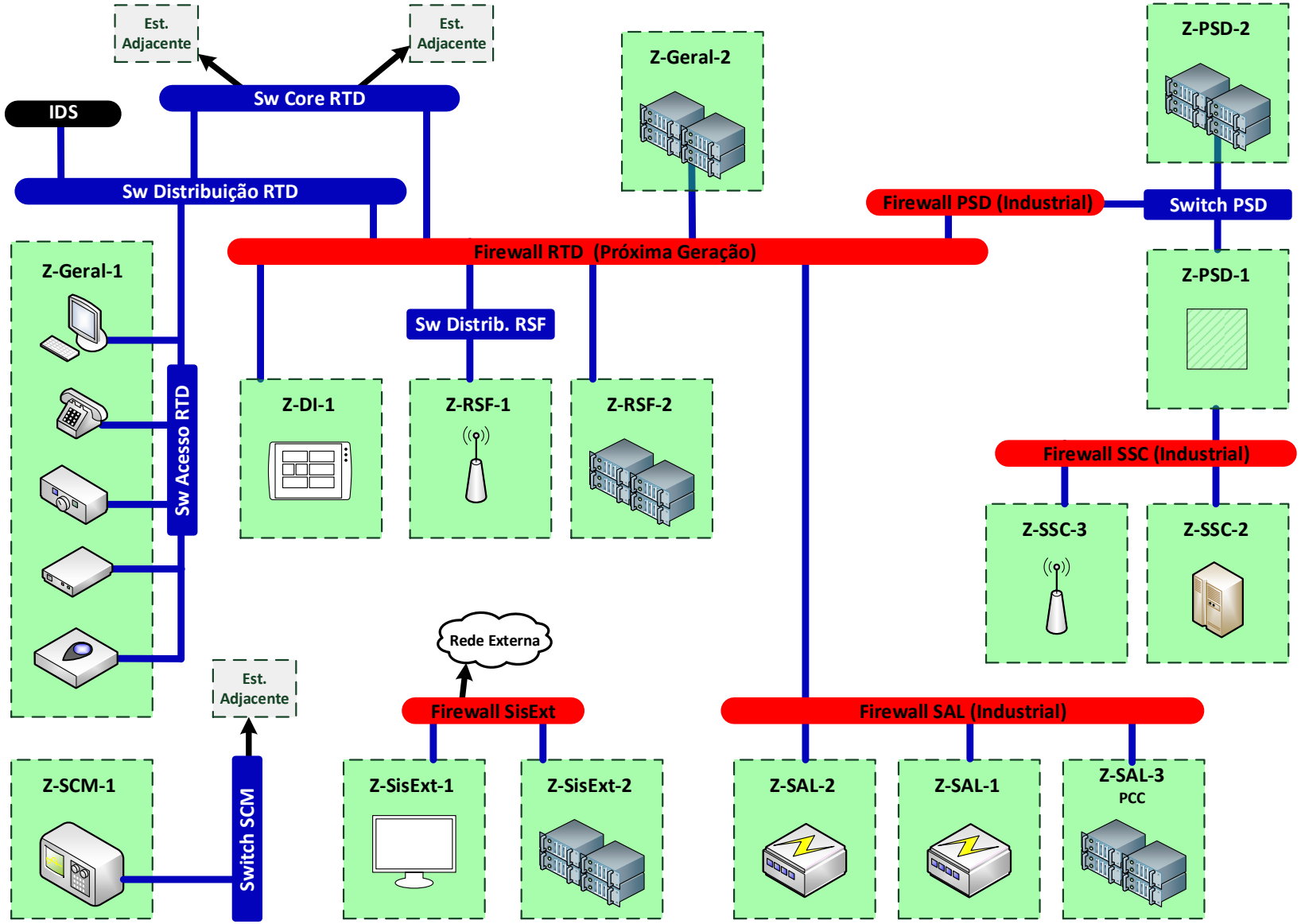


Diagrama de Zonas, Subzonas de Segurança e Conduítes no CCO

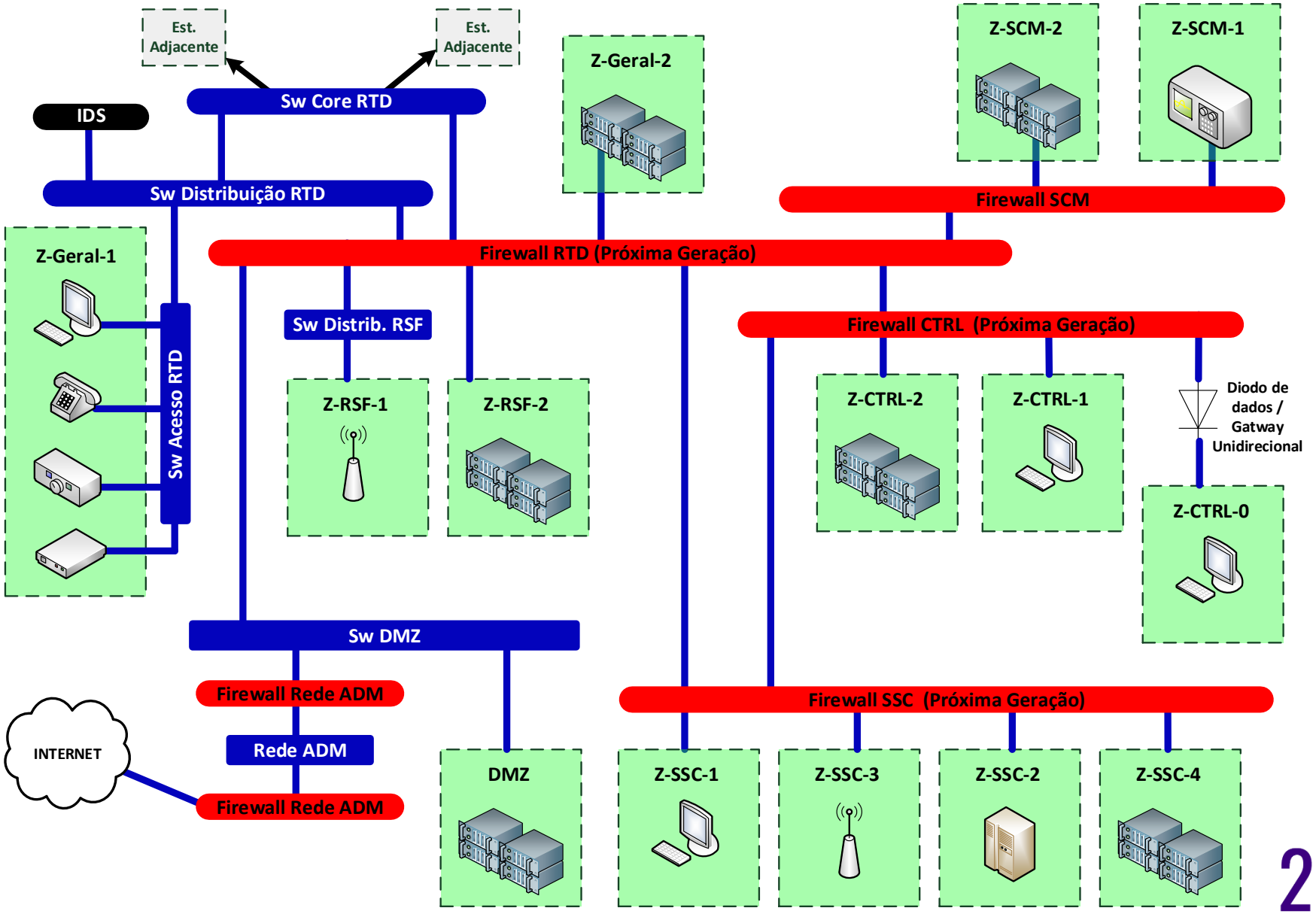


Diagrama de Zonas, Subzonas de Segurança e Conduítes em um Trem

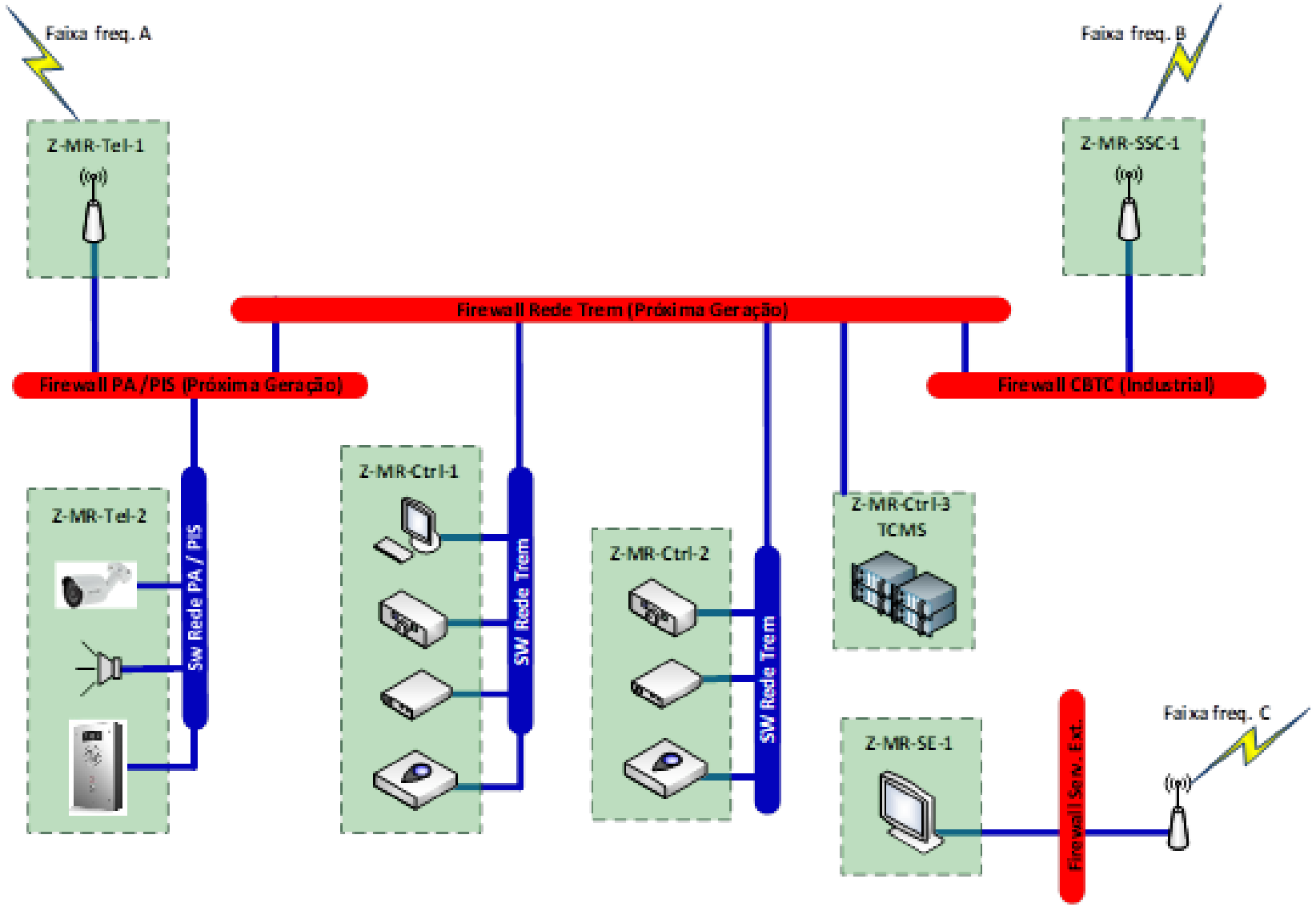
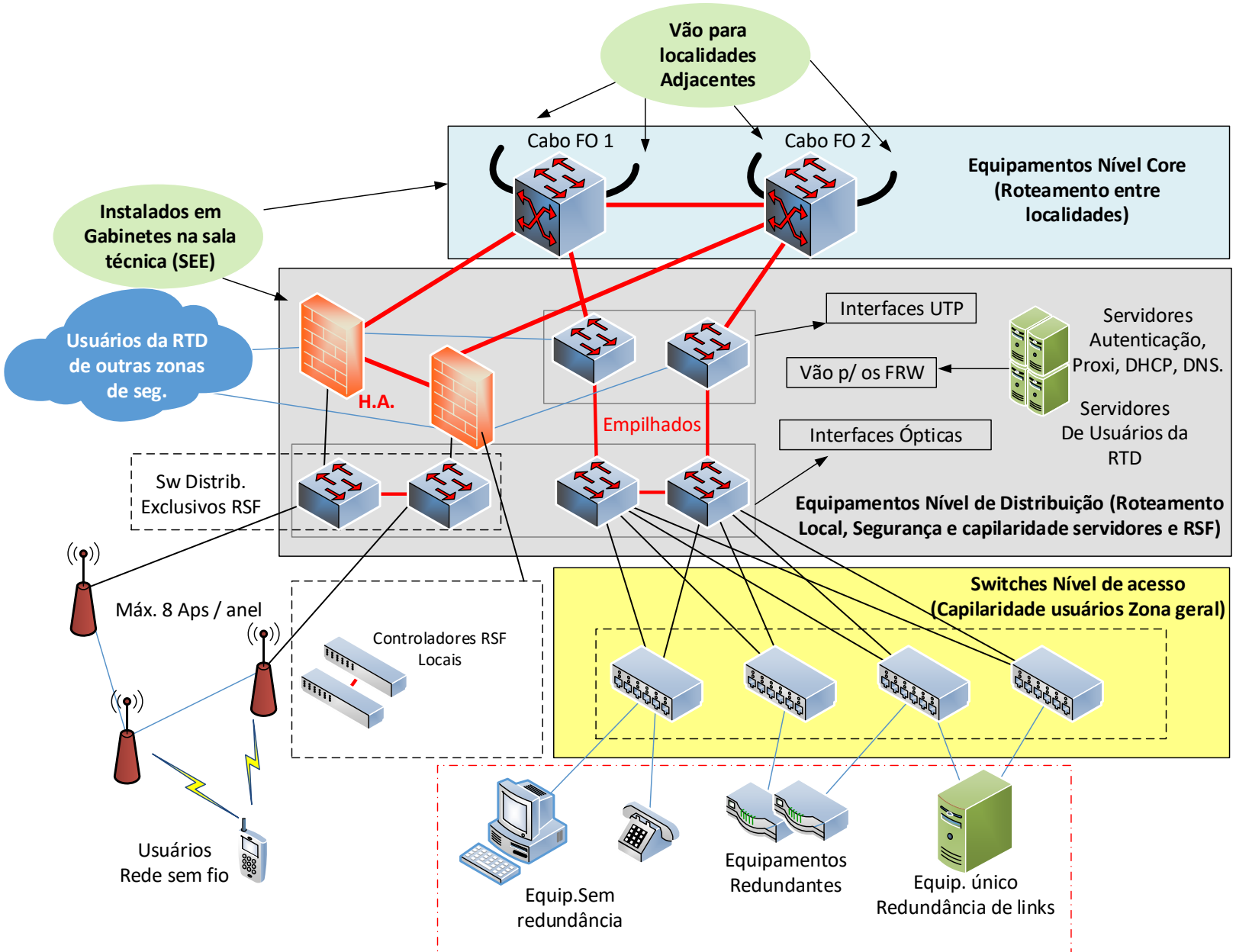


Diagrama da Rede de Transmissão de Dados de uma Localidade Tipo



Requisitos para especificações de cada sistema de T.O.

- Gerais, ex:
  - Todo o sistema deve estar de acordo e atendendo as normas ISO 27001 e ISA/IEC62443 na versão mais atual ou normas que venham a substituí-las.
  - Todos os dispositivos ou equipamento que necessitar de endereços IP devem seguir o plano de endereçamento IP da Contratante.
  - Todos os equipamentos computacionais devem utilizar o conceito de Hardening, permitindo apenas as funções necessárias para o funcionamento correto do sistema.
- Requisitos de AAA – Autenticação, Autorização e Auditorias, ex:
  - Devem existir sistemas de autenticação nas redes de T.O. de forma que todos os humanos, processos de software e dispositivos que acessarem a rede sejam autenticados. Devendo permanecer, sempre, o conceito de menor privilégio.
  - Autenticações remotas devem utilizar critérios de autenticação multifatoriais.
- Requisitos de Redes de Comunicação, ex:
  - A rede do sistema em consideração deve negar o tráfego de rede por padrão e permitir o tráfego de rede por exceção.
  - Os mecanismos de segurança devem, entre outros que garantam o atendimento aos requisitos desta especificação, incluir, segregação por VLANs, criptografia, autenticação entre nós para formação de redes IPSec, Port security, ACLs, controle de mensagens, portas e protocolos.
  - Todas as portas ou interfaces de comunicação em equipamentos de comunicação que não estiverem em uso devem permanecer desabilitadas (em shutdown).

Resultados

O assunto cibersegurança vem sendo muito discutido nos últimos anos no Metrô de São Paulo.

Existe uma preocupação crescente em aumentar a maturidade em segurança da informação na Cia.

Foram criados alguns grupos e comitês multidisciplinares para a discussão do assunto e implantação das melhores práticas em todo o ciclo de vida dos sistemas de T.I. e de T.O.

Na área de projetos de sistemas estamos aplicando os conceitos apresentados neste trabalho e, apesar de ainda serem projetos recentes, alguns já foram implantados e estão em plena operação.

Estamos verificando tanto na teoria, debatida nos grupos de discussão, quanto na prática que os resultados são muito positivos, pois, temos tido sucesso na defesa dos nossos sistemas de T.O., conseguindo inibir alguns incidentes e evitar problemas de segurança cibernética.

Conclusão

- Apresentados modelos de arquitetura, recomendações e requisitos de sistemas totalmente aplicados ao setor metroferroviário.
- Enquadramos os sistemas metroferroviários nos conceitos da norma ISA/IEC 62443, facilitando a sua aplicação no setor, de tal forma que os projetistas metroferroviários tenham condições de aplicá-los nas especificações técnicas dos projetos de sistemas.
- Os modelos, recomendações e requisitos apresentados neste trabalho servem como base e podem ser utilizados para o desenvolvimento de quaisquer projetos de sistemas metroferroviários, bastando adequar e fazer ajustes em possíveis diferenças observadas.
- IMPORTANTE:

Considerar no escopo dos projetos todos os equipamentos de rede, de segurança e do sistema em consideração, possíveis de serem previstos e quantificados.

Referências Bibliográficas

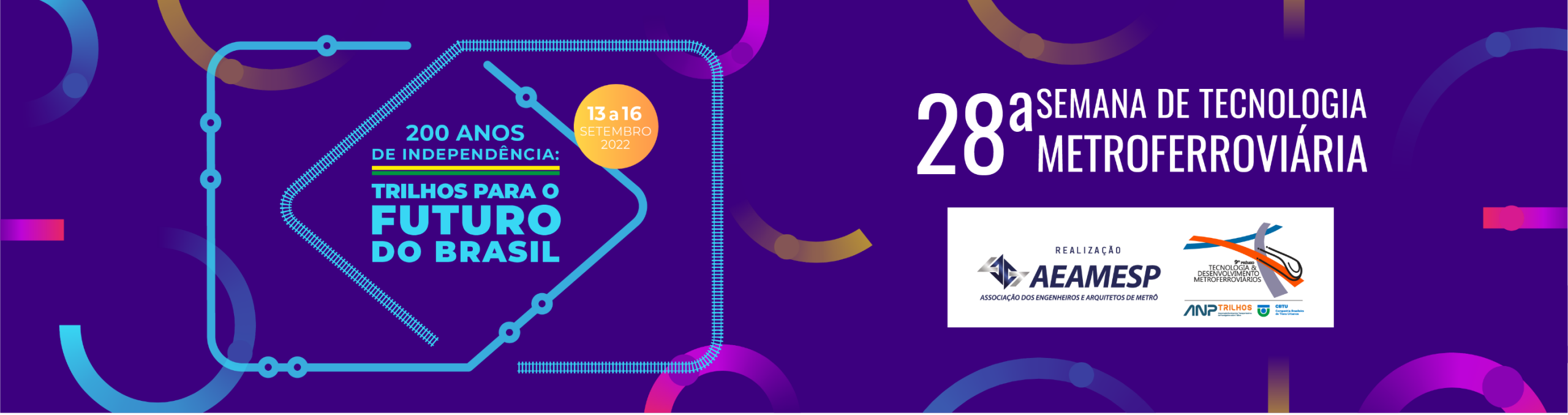
- Normas: Família NBR/ISSO/IEC 27000, ISA/IEC 62443, Guia NIST SP 800-82.
- Especificação Técnica: CLC-TS_50701.
- Livro: Segurança Cibernética Industrial – Autores: Tiago Branquinho e Marcelo Branquinho, Editora Alta Books.
- Monografia de graduação: INDÚSTRIA 4.0 - OS DESAFIOS E OPORTUNIDADES NO BRASIL EM MEIO À PANDEMIA DE COVID-19. Autor: VALDEMAR DE OLIVEIRA PORTO NETO – Ouro Preto, 2021

Sites: Acesso em 21/07/2022 as 21h22:

- https://www.cisoadvisor.com.br/gasto-global-com-seguranca-deve-superar-us-150-bi-neste-ano/
- https://seginfo.com.br/2022/05/19/gastos-com-ciberseguranca-chegarao-a-mais-de-980-bilhoes/

Acesso em 22/07/2022 as 18h15:

- https://stringfixer.com/pt/IEC_62443
- https://senhasegura.com/pt-br/avaliacao-de-riscos-de-seguranca-cibernetica-de-acordo-com-a-isa-iec-62443-3-2/
- https://ldra.com/iec-62443/



SEGURANÇA CIBERNÉTICA NOS TRILHOS
APLICAÇÃO PRÁTICA EM PROJETOS DE SISTEMAS

Ricardo Frade Mouriño

Obrigado!