JOANA MARIA RIQUELME AGAPITO DE PAULA

Estudo Preliminar de vulnerabilidades e interferências de uma rede em um ambiente metroferroviário

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para Conclusão do Curso de Especialização em Tecnologia Metro-Ferroviária.

São Paulo
2016

JOANA MARIA RIQUELME AGAPITO DE PAULA

Estudo Preliminar de vulnerabilidades e interferências de uma rede em um ambiente metroferroviário

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para Conclusão do Curso de Especialização em Tecnologia Metro-Ferroviária.

Área de Concentração: Tecnologia Metro-Ferroviária

Orientador: Prof. Dr. João Batista Camargo Junior
Co-orientador: Prof. Dr. Rodrigo Filev Maia

São Paulo
2016

Dedico este trabalho a todos os profissionais que me inspiraram direta ou indiretamente. À minha mãe, que mesmo longe me dá força. Ao meu pai, meu irmão e à Wilma pelo exemplo de vida, simplicidade e persistência. Aos meus amigos, marido e filho por terem sido pacientes nas ocasiões em que não pude estar presente.

AGRADECIMENTOS

Aos professores Dr. João Batista Camargo Junior e Dr. Rodrigo Filev Maia, pela orientação, paciência, suporte, correções e pelo constante estímulo transmitido durante todo o trabalho.

Aos demais professores, amigos e todos que colaboraram direta ou indiretamente, na execução deste trabalho.

RESUMO

O ambiente metroferroviário é composto de diversos sistemas e equipamentos interligados através de redes sem fio e cabeadas. Estas redes visam a garantia da operação do sistema de forma segura, com alto desempenho e ainda possibilitar o controle e monitoração dos equipamentos através de sistemas supervisórios baseados em arquitetura SCADA. Devido a esta característica de integração, algumas falhas podem se propagar de um sistema ou equipamento e afetar os critérios de segurança (*security* e safety), confiabilidade e desempenho de outros sistemas. Em geral esses critérios de segurança são analisados de forma individualizada para cada conjunto de sistemas. Este trabalho apresenta uma proposta de metodologia de análise de risco combinada para *safety* e *security* aplicada para os sistemas supervisórios baseados em SCADA propondo a análise conjunta dos requisitos de segurança (*safety* e *security)* com o intuito de identificar potenciais riscos e respectiva criticidade, tendo como foco a rede cabeada, rede sem fio e os sistemas supervisórios baseados em SCADA.

Palavras-chave: Segurança. Rede. SCADA. Análise de Risco.

ABSTRACT

The subway-railroad structure comprises several systems and equipment connected via wireless networks and wired. These networks ensure the secure system operation with high performance and also enable the control and monitoring of equipment through supervisory systems based on SCADA architecture. Due this need of integration, some failures could propagate from a system or equipment and affect criteria of safety or security, reliability and performance of others systems. In general the criteria of safety and security are analyzed individually for each group of system and equipment, This work presents a combined risk analysis of the safety and security requirements for the systems based on SCADA architecture, proposing the joint analysis of safety and security requirements in order to identify potential risks and their critically, focused on the wired and wireless network and SCADA based supervisory systems.

Keyword: Safety, Security, Network, SCADA, Risk Analysis.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AMV	Aparelho de Mudança de Via
CCO	Centro de Controle Operacional
PSD	*Platform Screen Doors* ou Sistema de Portas de Plataforma
RTD	Rede de Transmissão de Dados
SCADA	*Supervisory Control and Data Acquisition* ou Sistema de Supervisão e Aquisição de Dados
SCC	Sistema de Controle Centralizado
SCL	Sistema de Controle Local
SCT	Sistema de Controle de Tráfego
SCMVD	Sistema de Comunicações Móveis de Voz e de Dados
TPD	Terminal Portátil de Dados
UTO	*Unattended Train Operation* ou Operação do Trem Não-assistida
VLAN	*Virtual Local Area Network* ou Rede Local Virtual

SUMARIO

1. INTRODUÇAO

1.1. MOTIVAÇÃO

Para atender a operação do sistema de forma segura e com alto desempenho, os sistemas e equipamentos que compõem o ambiente metroferroviário estão cada vez mais integrados.

Os sistemas e equipamentos mencionados visam aumentar os níveis de segurança, agilizar o atendimento em situações de emergência, otimizar o desempenho operacional e estruturar os meios de comunicação para permitir uma interação dinâmica entre os diversos sistemas que são implantados no Centro de Controle Operacional (CCO), pátios, subestações, estações, vias e trens.

A peça chave desta integração é a rede de comunicações (tanto cabeada como sem fio).

1.2. OBJETIVO

Este trabalho visa a abordagem das redes do ambiente metroferroviário, considerando vulnerabilidades, riscos e interferências que podem ocasionar falhas de segurança em todo o ambiente considerado. Este trabalho visa apresentar uma metodologia para análise conjunta dos requisitos de segurança (*safety* e *security)* com o intuito de identificar potenciais riscos e respectiva criticidade, tendo como foco a rede de transmissão de dados, rede sem fio e os sistemas supervisórios (SCC e SCL).

Como a tradução dos termos em inglês "*safety*" e "*security*" não possui diferença na língua portuguesa, foram adotados os termos em inglês neste trabalho, abordando:

- *Safety*: Conforme o dicionário Cambridge[1], *safety* representa o estado de ser salvo de dano ou perigo, em tradução literal.

  Este trabalho considera como *safety*, a garantia da integridade física do usuário ou profissional.
- *Security*: Também conforme o dicionário Cambridge[1], *security* é o que pode ser feito para manter alguém ou alguma coisa seguro ou ainda a proteção contra falha ou perda de alguma coisa, em tradução literal.

  Este trabalho considera como *security*, a proteção dos dados e informações dos sistemas e equipamentos.

[1] CAMBRIDGE UNIVERSITY PRESS 2015

Esta metodologia tem como objetivo a análise conjunta dos requisitos de *safety* e *security para determinados sistemas,* permitindo a identificação de potenciais riscos e sua criticidade aos demais sistemas inter-relacionados.

1.3. JUSTIFICATIVA

Este trabalho apresenta as interfaces dos sistemas existentes no ambiente metroferroviário, tendo como foco a rede (cabeada e sem fio) que permite a interconexão destes sistemas, bem como as interfaces entre esta rede e outros equipamentos e sistemas conectados com redes distintas (incluindo as interfaces com os sistemas supervisórios e os respectivos equipamentos controlados e monitorados).

Estas interfaces e interconexões podem afetar requisitos de segurança (*safety* e *security*), confiabilidade e desempenho nos sistemas deste ambiente metroferroviário. Tendo isso em vista, este trabalho aborda um estudo de caso aplicando uma metodologia de análise conjunta dos requisitos de segurança.

No ambiente metroferroviário, os sistemas costumam ser especificados e licitados de forma isolada (na maior parte das vezes fornecido em contratos com prazos de execução e fornecedores distintos), dificultando a análise conjunta dos requisitos de *safety* e *security* entre estes sistemas.

2. LEVANTAMENTO DAS REFERÊNCIAS BIBLIOGRÁFICAS

Na elaboração deste trabalho foram considerados artigos abordando a análise de riscos envolvendo segurança em ambientes críticos. Esta análise embasou a metodologia abordada no Capítulo 3 e aplicada no estudo de caso do Capítulo 4.

O ponto comum dos artigos analisados envolvendo *safety* e *security* é a integração entre os sistemas bem como a análise conjunta de vulnerabilidades e falhas em tecnologias e ambientes críticos.

Eames e Moffett (1999) abordam a integração de requisitos de *safety* e *security* em sistemas computacionais. Este artigo cita alguns processos de análise de riscos para *safety* e *security*, em que é possível notar algumas lacunas entre estes dois processos visto que cada um aborda requisitos específicos tanto para *safety* como para *security* e não com uma visão integrada.

Este artigo também aborda técnicas visando esta integração, de forma a combiná-las seja em uma abordagem de unificação, seja de harmonização.

Ao verificar os processos de análise de risco de *safety* e de *security*, pode-se notar similaridades entre os processos, sendo possível a simplificação, torando a análise unificada e mais completa.

A análise de risco de *safety* e *security* podem resultar em restrições que podem conflitar com requisitos funcionais ou de performance. O processo de resolução de conflitos é útil pois possibilita uma melhor compreensão do sistema e seu domínio.

Como as técnicas em cada domínio evoluíram, visando produzir uma análise mais profunda e completa, tentar unificar estas duas técnicas pode levar a uma análise incompleta. Um perigo adicional é que uma abordagem unificada pode realmente esconder os requisitos conflitantes que visa resolver.

Eames e Moffett (1999) também mencionam que é possível identificar algumas áreas que podem dificultar a tentativa de harmonizar as técnicas de requisitos *de safety e security,* tais como: Diferentes modelos desenvolvidos para *safety* e *security;* estruturas de documentação diferentes para análise e bem como os resultados; interação dos requisitos de *safety* e *security* e isolação dos processos dos requisitos de *safety* e *security.*

Este artigo é abordado com mais detalhes no Capítulo 3, onde destaca a importância desta integração na elaboração da metodologia de análise.

Novak e Gerstinger (2010) tratam da interação entre os sistemas de campo de forma que seja possível o comando e monitoração destes a partir de sistemas

supervisórios. Esse artigo ressalta uma característica comum com o ambiente metroferroviário que é a ausência de integração nos critérios de *safety* e *security* nos sistemas e equipamentos de campo. Estes sistemas e equipamentos são interligados com os sistemas supervisórios através de uma rede, porém não é possível garantir a manutenção da integridade dos seus requisitos de segurança visto que os critérios não são compartilhados. Este artigo também propõe uma abordagem conjunta dos requisitos de *safety* e *security* podendo, inclusive, ser adotados alguns processos citados por Eames e Moffett (1999). Esta abordagem também é destacada no Capítulo 3 e no Capítulo 4.

Lautieri; Cooper e Jackson (2005) mencionam a certificação de sistemas baseado em requisitos de *safety* e *security* que ainda ocorrem de forma isolada. O artigo cita os benefícios de uma abordagem conjunta, agrupando as similaridades de *safety* e *security*, na certificação de um sistema. Este projeto, denominado SafSec, foi patrocinado pela agência de defesa britânica visando a verificação de sistemas computacionais complexos, particularmente aqueles desenvolvidos para a IMA (*Integrated Modular Avionics*).

Esse artigo aborda os benefícios em se realizar uma análise combinada tanto para *safety* como *security*, podendo realizar um paralelo com o ambiente metroferroviário pois é um ambiente similar ao ambiente militar, com intolerância a falhas na maior parte dos sistemas de campo. Esta análise combinada também é considerada na metodologia proposta no Capítulo 3 e no estudo de caso do Capítulo 4.

Smith; Russel e Looi (2003) apresentam *security* como uma questão de *safety* em comunicações ferroviárias, mencionando inclusive que os sistemas que possam causar danos a outros sistemas ou pessoas não podem mais ser construídos baseando o controle de erros e falhas individualmente, também considerando a segurança das informações utilizadas na operação. Esse artigo aborda os conceitos de dependabilidade e segurança, bem como a abordagem de *safety* no ambiente ferroviário, principalmente no que diz respeito ao sistema de sinalização e suas interfaces. Os conceitos abordados por este artigo são considerados no estudo de caso apresentado no Capítulo 4.

Amey e Hilton (2001) identificam as propriedades de sistemas utilizados em domínios confiáveis e os métodos de desenvolvimento necessários para alcançar estas propriedades.

Como grande parte dos sistemas é baseada em software, este artigo menciona que a característica de um sistema de alta integridade é a capacidade de demonstrar, antes de qualquer utilização, que o software atende aos requisitos, comprovando através de métodos e técnicas de verificação.

Este artigo reforça a importância do uso correto de técnicas e métodos para garantir a confiabilidade do sistema, que são abordadas no estudo de caso apresentado no Capítulo 4.

Brostoff e Sasse (2001) descrevem que a elaboração de aplicações de segurança deve considerar mais do que elementos técnicos, visto que praticamente todos os sistemas de segurança também possuem usuários, que por sua vez podem comprometer a segurança.

Para tal, o artigo menciona a adoção de um novo modelo visto que os atuais não consideram que a segurança é um sistema técnico-social e que todas as partes do sistema devem interagir de forma a atingir a segurança esperada.

Com base no exposto, este trabalho explora a falta de integração dos requisitos de *safety* e *security* nos equipamentos em campo, bem como as possíveis consequências para o ambiente metroferroviário. Tendo isso em vista, também aborda uma proposta de integração dos requisitos de *safety* e *security* minimizando as consequências abordadas. Esta integração é abordada na metodologia exposta no Capítulo 3 e no estudo de caso do Capítulo 4.

Os artigos citados a seguir não relacionam *safety* como uma questão de *security,* porém apresentam vulnerabilidades que costumam afetar redes e sistemas similares aos implantados no ambiente metroferroviário e no estudo de caso deste trabalho. Também foram considerados artigos a respeito da arquitetura, características, vulnerabilidades e segurança para sistemas SCADA. As informações contidas nestes artigos foram utilizadas na análise de risco de *security* para o estudo de caso, apresentada no Capítulo 4.

Estes artigos apresentam informações envolvendo critérios de segurança e vulnerabilidades de sistemas SCADA implantados em ambientes críticos, tendo foco principal falhas envolvendo *security.*

Ten; Liu e Manimaran (2008) apresentam uma avaliação de vulnerabilidades que podem afetar sistemas SCADA.

Também mencionam a rede do SCADA com os equipamentos de campo, a qual costumava ficar segregada das demais redes existentes, está cada vez mais

integrada com as redes e com a Internet. Esta integração tem trazido diversas vulnerabilidades para o sistema que podem afetar os requisitos de segurança (*security*).

Algumas destas vulnerabilidades são apresentadas na análise de risco de *security* para o estudo de caso do Capítulo 4.

Zhu; Joseph e Sastry (2011) abordam a criticidade de um ataque aos sistemas SCADA uma vez que estes estão cada vez mais padronizados (através de protocolos de comunicação pré-estabelecidos), facilitando possíveis ataques.

Como o uso de sistemas SCADA é aplicado em infraestrutura crítica envolvendo energia, telecomunicações, água, transporte, dentre outros, qualquer ameaça à segurança (*security*) pode afetar operações, perda econômica, contaminar o meio-ambiente e ainda mais grave, causar mortes.

Algumas formas de ataque, vulnerabilidades exploradas e respectivos riscos, são apresentados na análise de risco de *security* para o estudo de caso do Capítulo 4.

3. METODOLOGIA

Conforme observado nos artigos citados no levantamento das referências bibliográficas, a importância dos requisitos de *safety* e *security* é um tema recorrente e de suma importância no ambiente metroferroviário.

Este assunto tem fundamental importância visto que as especificações dos sistemas são escritas por equipes distintas e muitas vezes são publicadas em editais em diferentes momentos.

Tendo isto em vista, neste capítulo será detalhada a metodologia que será aplicada no estudo de caso abordado no capítulo 4.

Para a análise dos riscos de *safety* e *security*, foram adotadas as técnicas citadas por Eames e Moffett (1999).

3.1. PROCESSO DE ANÁLISE DE RISCO DE SAFETY

Este processo combina a análise qualitativa e quantitativa para identificar os componentes críticos, funcionalidades e interfaces. Esta análise considera as falhas ao qual os sistemas analisados podem ser expostos e qual o perigo resultante.

Esta análise visa auxiliar na identificação de medidas e requisitos que o sistema necessita para ser aceito.

3.1.1. ANÁLISE FUNCIONAL E TÉCNICA

Esta análise reúne os dados sobre os sistemas, utilizando-se a documentação técnica, visando a obtenção das informações e requisitos dos sistemas a serem analisados.

Esta análise compreende a identificação das funcionalidades e interfaces necessárias entre os sistemas.

3.1.2. ANÁLISE QUALITATIVA

Com base nas informações colhidas na análise funcional e técnica, são investigadas as causas das falhas e perigos que podem afetar o *safety* do sistema. O objetivo desta análise é a identificação da combinação de falhas que podem levar a situações perigosas que podem ou não ser aceitas.

3.1.3. ANÁLISE QUANTITATIVA

Esta análise consiste em enumerar o resultado da análise qualitativa, com base em probabilidade para a obtenção de ameaça relativa dos perigos.

Como esta análise possui um certo grau de incerteza, deve ser elaborado um modelo probabilístico tendo como fonte resultados de testes, registros operacionais e de falhas. Este modelo deve considerar a probabilidade, a criticidade e a quantidade de ocorrências de cada um dos perigos relacionados.

A análise quantitativa fornece uma medida da ameaça relativa dos perigos, permitindo focar a atenção nas áreas críticas.

3.1.4. CONCLUSÃO

Com base nos resultados das etapas anteriores, pode-se elaborar as medidas e requisitos que devem ser seguidos ou corrigidos para que o sistema seja classificado como seguro (*safe*).

3.2. PROCESSO DE ANÁLISE DE RISCO DE SECURITY

Este processo compreende os estágios descritos a seguir:

3.2.1. IDENTIFICAÇÃO DE ATIVOS

Serão identificados os recursos que necessitam de proteção (*security*), incluindo hardware, software, dados, documentação e serviços e processos computacionais, utilizando como base a documentação técnica dos sistemas envolvidos.

3.2.2. ANÁLISE DE VULNERABILIDADE

Serão determinadas as vulnerabilidades em função das informações obtidas no passo anterior.

Também deve ser considerado o nível de dano que cada ativo pode gerar, observando a garantia de integridade, sigilo e disponibilidade dos dados.

3.2.2.1. RISCOS POTENCIAIS

Serão listados os riscos potenciais para a rede e/ou para os sistemas interconectados, considerando a exploração da vulnerabilidade em questão.

3.2.3. ANÁLISE DE PROBABILIDADE

O objetivo desta análise é verificar quantas vezes o sistema pode ser exposto a cada uma das vulnerabilidades identificadas. Esta análise deve considerar as vulnerabilidades, medidas de proteção e o ambiente nas quais são aplicadas. Assim como a análise quantitativa citada no item 3.1.2, esta análise de probabilidade também deve considerar a elaboração de um modelo probabilístico tendo como fone resultados de testes, registros operacionais e de falhas.

3.2.4. AVALIAÇÃO DE CONTRAMEDIDAS

Com base nas informações obtidas nas etapas anteriores, será verificado se o resultado determinou que o dano gerado seja inaceitável, apresentando contramedidas visando a proteção do ativo.

3.3. METODOLOGIA UNIFICADA

Ao verificar os processos de análise de risco de *safety* e de *security* expostos anteriormente, podemos notar similaridades entre eles.

Neste trabalho não abordaremos a análise quantitativa devido à carência de informações de falhas no ambiente avaliado.

Neste trabalho iremos adotar a metodologia descrita a seguir:

3.3.1. DEFINIÇÃO DOS LIMITES DO SISTEMA, FUNCIONALIDADES E INTERFACES

Nos dois processos de análise de risco, esta definição é o primeiro estágio. Esta análise compreende a análise funcional e técnica na análise de riscos de *safety* (item 3.1.1) e a identificação de ativos na análise de riscos de *security* (item 3.2.1).

A partir das funcionalidades identificadas, é possível descrever as interfaces necessárias entre os sistemas para garantia de atendimento a estas funcionalidades.

Nesta etapa é necessário identificar e descrever as informações sobre os sistemas a serem analisados (incluindo hardware, software, dados e funcionalidades), utilizando a documentação técnica dos sistemas envolvidos e os artigos consultados, conforme as referências bibliográficas.

3.3.2. IDENTIFICAÇÃO PRELIMINAR DE PERIGO E ANÁLISE PRELIMINAR DE RISCOS E VULNERABILIDADES

Uma vez identificados os limites, funcionalidades e interfaces dos sistemas, a identificação preliminar de perigo é realizada para identificar os perigos que podem acometer os sistemas analisados.

Após a identificação preliminar do perigo, é feita uma análise preliminar dos riscos e vulnerabilidades para cada um dos perigos identificados.

Nos dois processos de análise de risco, a identificação preliminar de perigo e a análise preliminar de riscos e vulnerabilidades compreende a análise qualitativa na análise de riscos de *safety* (item 3.1.2) e a análise de vulnerabilidade (item 3.2.2) e os riscos potenciais (item 3.2.2.1) na análise de riscos de *security*.

Esta etapa visa a investigação das causas das falhas, perigos, vulnerabilidades e riscos potenciais que podem afetar o sistema. Também são consideradas a combinação de falhas que podem levar a situações perigosas, bem como o nível de dano que estas podem gerar no sistema.

Essa análise deve utilizar como base a documentação técnica dos sistemas envolvidos bem como os perigos conhecidos de sistemas semelhantes.

3.3.3. CONCLUSÃO

Tendo como base o resultado das etapas anteriores, deve ser possível a identificação de medidas e requisitos que devem ser seguidos, corrigidos ou monitorados.

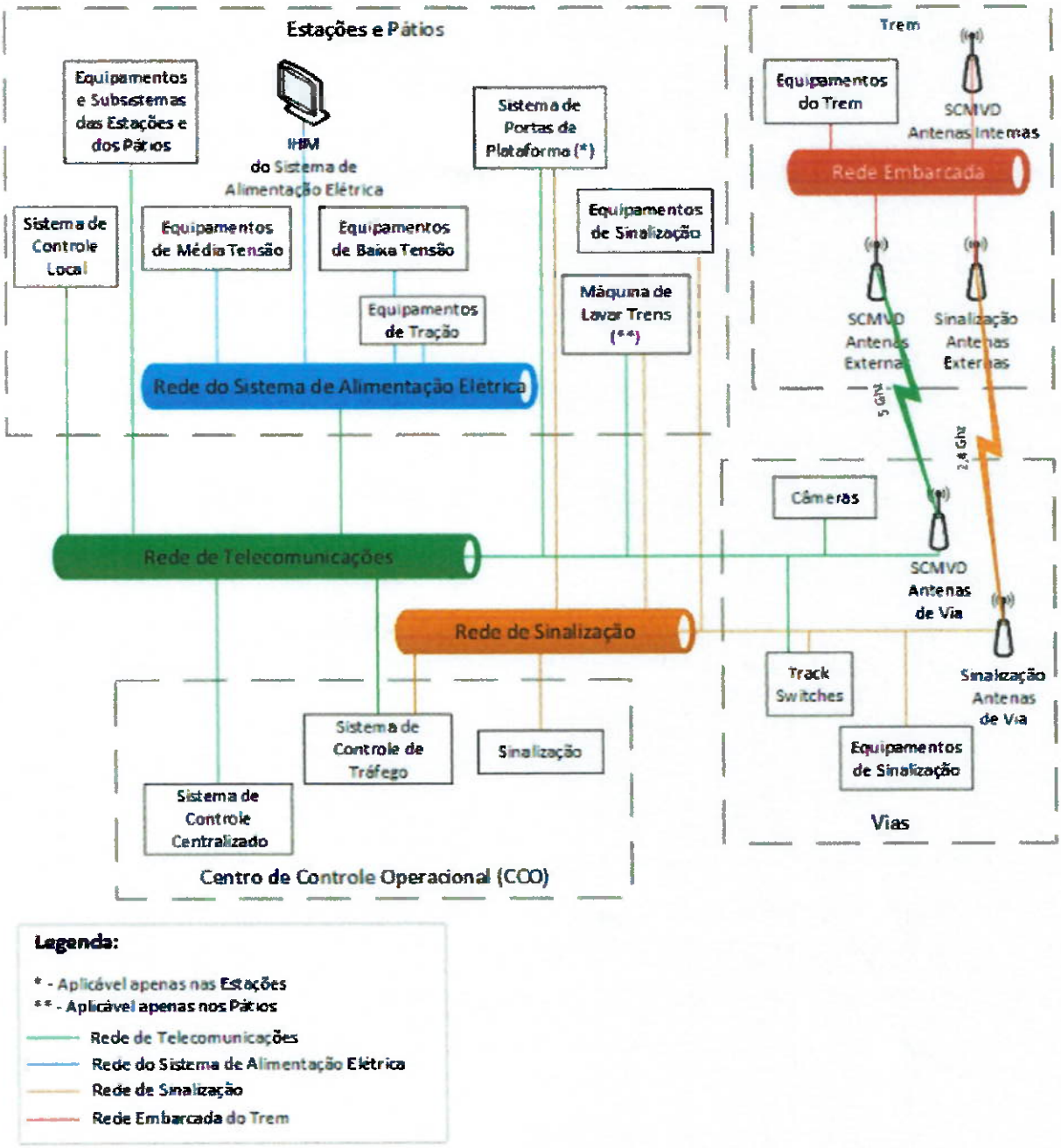
3.3.4. CONSIDERAÇÕES A RESPEITO DA METODOLOGIA

Tendo em vista a ausência de registros com informações de falhas do ambiente estudado, não foi possível a elaboração de um modelo probabilístico, possibilitando a análise quantitativa e de probabilidade de safety e de security. O estudo de caso abordado a seguir está concentrado na análise qualitativa tanto para *safety* como para *security*.

4. ESTUDO DE CASO

Conforme já mencionado, o ambiente metroferroviário é composto de diversos subsistemas interligados. A Figura 1 apresenta alguns destes subsistemas bem como as estruturas utilizadas para a interconexão destes de forma a garantir sua operação de forma segura e nos parâmetros de desempenho esperados.

Figura 1 – Arquitetura das Redes do Ambiente Metroferroviário



Fonte: Elaborada pela autora

Conforme pode-se observar na Figura 1, existem 4 estruturas principais de comunicação:

- Rede de Telecomunicações (em verde);
- Rede do Sistema de Alimentação Elétrica (em azul);
- Rede de Sinalização (em laranja);
- Rede Embarcada do Trem (em vermelho).

Estas redes garantem a interconexão de todos os sistemas e equipamentos existentes nas estações, vias e nos pátios.

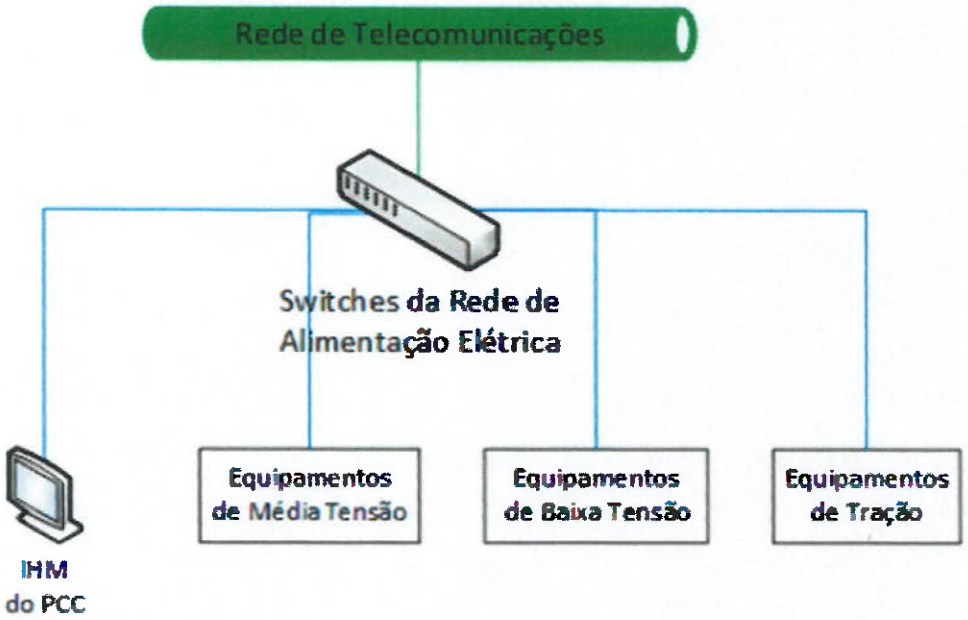
A seguir, estas estruturas são apresentadas com maiores detalhes.

4.1. ESTRUTURAS DE COMUNICAÇÃO

4.1.1. REDE DO SISTEMA DE ALIMENTAÇÃO ELÉTRICA

A Figura 2 apresenta a rede do Sistema de Alimentação Elétrica.

Figura 2 – Rede do Sistema de Alimentação Elétrica



Fonte: Elaborada pela autora

Esta rede interconecta todos os equipamentos do sistema de alimentação elétrica garantindo o nível de proteção adequado de forma a garantir a segurança (safety) dos intertravamentos existentes entre os equipamentos.

A comunicação com a rede de telecomunicações é feita a partir de switches redundantes e as informações dos equipamentos são lidas em um servidor próprio pelos sistemas supervisórios (SCL – Sistema de Controle Local e SCC – Sistema de Controle Centralizado), desta forma, os sistemas supervisórios acessam apenas o Painel de Comando e Controle (PCC), não possuindo acesso direto à rede de alimentação elétrica.

4.1.2. REDE DE TELECOMUNICAÇÕES

A Rede de Telecomunicações é composta por duas redes: Rede de Transmissão de Dados (RTD) que é uma rede cabeada e uma rede sem fio do Sistema de Comunicações Móveis de Voz e de Dados (SCMVD).

4.1.2.1. RTD

A RTD é uma rede de missão crítica, responsável por interconectar todos os subsistemas das estações com as estações adjacentes, equipamentos das vias, pátios e o Centro de Controle Operacional.

A RTD provê suporte às comunicações de voz, dados e imagens permitindo a operação, manutenção e administração do sistema metroferroviário.

Esta rede é implantada de forma que todas as redes, sub-redes, subsistemas e equipamentos pertencentes à infraestrutura de comunicação da RTD podem ser acessados por outros subsistemas pertencentes a outras infraestruturas de comunicação.

A infraestrutura da RTD provê recursos para que cada serviço trabalhe em suas condições especificadas de forma independente, sem sofrer interferências dos demais serviços e sistemas usuários, permitindo a utilização de tecnologia de circuitos virtuais, oferecendo reserva de recursos e mecanismos de gerenciamento de tráfego.

A RTD possui, dentre outros, os seguintes mecanismos de segurança da informação:

- Bloqueio de tráfegos não autorizados e que não pertencem aos subsistemas designados;
- Garantia de autenticidade dos subsistemas e de seus usuários e a confidencialidade dos fluxos de dados classificados como sensíveis.

Não está prevista a interconexão da RTD com a Rede de Sinalização nem com a Rede de Informática Administrativa. Porém alguns subsistemas necessitam da interface tanto com a rede de telecomunicações como com a rede de Sinalização, como por exemplo:

- Sistema de Portas de Plataforma;
- Máquina de Lavar Trens;
- Track Switches;
- Sistema de Controle de Tráfego;
- Rede embarcada do Trem.

4.1.2.2. SCMVD

O SCMVD fornece os serviços de comunicações móveis de voz e de dados aos empregados a serviço nas dependências do ambiente metroferroviário e os serviços de comunicações terra-trem de voz e dados aos equipamentos embarcados nos trens.

Este sistema opera com rede sem fio nas vias, estações e pátio utilizando rede sem fio de comunicação padrão IEEE 802.11n e operando na faixa de 5 GHz ou de 2,4GHz (frequências livres de licenças de operação).

As comunicações entre as estações rádio base, pontos de acesso e demais componentes do SCMVD, bem como as comunicações destes equipamentos e dispositivos com os demais sistemas são realizadas através da RTD.

O SCMVD contempla o uso de smartphones denominados Terminais Portáteis de Dados (TPDs) para os funcionários do quadro operativo e de manutenção, de forma que seja possível o estabelecimento de comunicação entre grupos específicos, bem como o uso de aplicativos instalados neste dispositivo de forma a operar alguns sistemas e funcionalidades a partir deste dispositivo.

O SCMVD provê cobertura para os TPDs nas áreas internas das estações, vias, trens (mesmo em movimento), áreas internas e externas do pátio, áreas das bases de manutenção, áreas das subestações e áreas internas do CCO.

4.1.3. REDE DE SINALIZAÇÃO

É uma rede que possui trechos cabeados e trechos sem fio utilizando a tecnologia Wi-Fi na frequência de 2.4 GHz.

Esta rede interconecta elementos vitais para a condução automática dos trens de forma segura visto que a condução destes é sem operador (UTO).

4.1.4. REDE EMBARCADA DO TREM

A rede embarcada do trem interconecta os equipamentos embarcados nos trens com as antenas do SCMVD e da Sinalização, que são responsáveis pelo envio e recebimento das informações destes equipamentos com os demais sistemas nas estações e no pátio.

Dentro dos trens o SCMVD possui Access Points de forma a oferecer cobertura aos TPDs.

Estes equipamentos são interconectados à rede embarcada utilizando uma VLAN específica de forma a segregar o tráfego de informações destes equipamentos com os demais tráfegos do trem.

4.2. EQUIPAMENTOS E SISTEMAS INTERCONECTADOS

Além das estruturas de comunicação abordadas anteriormente, a Figura 1 também apresenta os equipamentos e sistemas interconectados a estas estruturas.

Estes equipamentos e sistemas são compostos por:

- Equipamentos Auxiliares e Sistemas de Telecomunicações;
- Câmeras nas Vias;
- Sistema de Alimentação Elétrica;
- Sistema de Portas de Plataforma (PSD)
- Máquina de Lavar Trens (MLT)
- Track Switches
- Sistema de Controle Local (SCL)
- Sistema de Controle Centralizado (SCC)
- Sistema de Controle de Tráfego (SCT)

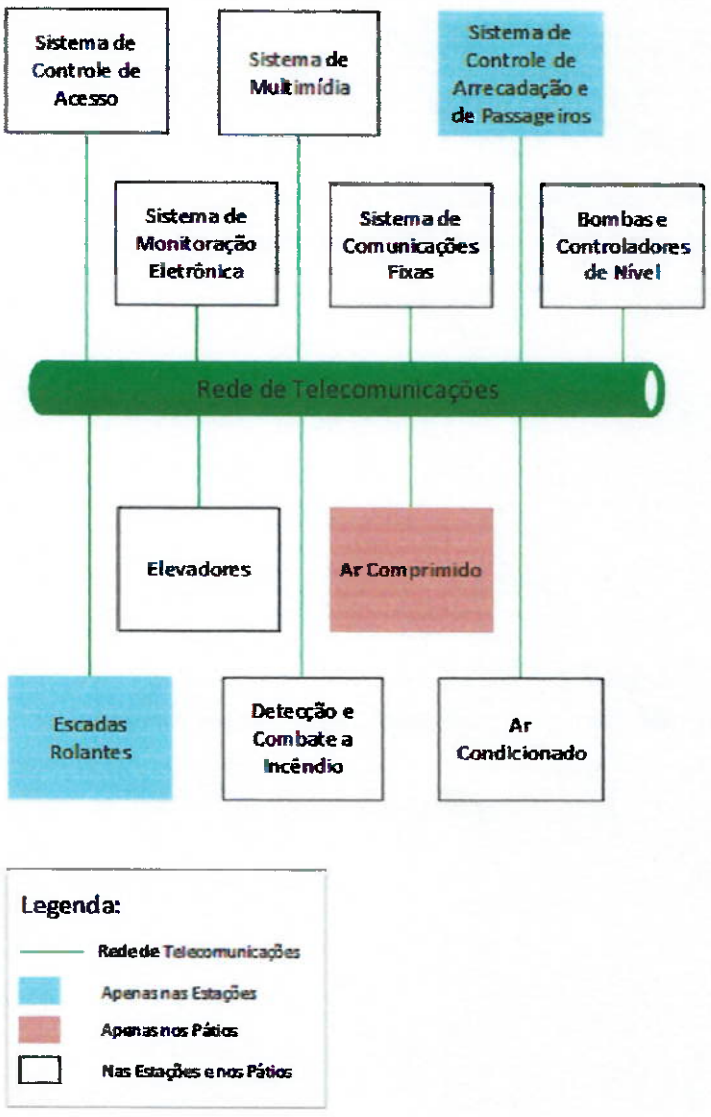
A seguir, estes equipamentos e sistemas são apresentados com maiores detalhes.

4.2.1. EQUIPAMENTOS AUXILIARES E SISTEMAS DE TELECOMUNICAÇÕES

Conforme pode-se observar na Figura 1, as estações e pátios possuem diversos equipamentos e subsistemas que necessitam de conexão à rede para envio e recebimento de informações de forma a garantir o funcionamento integrado de todo o ambiente metroferroviário.

Os equipamentos e subsistemas descritos a seguir estão representados na Figura 1 no quadro "Equipamentos e Subsistemas das Estações e dos Pátios", e detalhados na Figura 3.

Figura 3 – Equipamentos e Subsistemas das Estações e dos Pátios



Fonte: Elaborada pela autora

4.2.2. CÂMERAS NAS VIAS

É composto por câmeras móveis instaladas em postes localizados na via e interconectadas à Rede de Telecomunicações (RTD) da estação mais próxima através de fibra óptica.

4.2.3. SISTEMA DE ALIMENTAÇÃO ELÉTRICA

É o sistema que provê alimentação elétrica a todos os demais sistemas e equipamentos existentes nas estações, pátios e trechos de via.

É composto por:

- Média Tensão (22 kV)
- Sistema 125 Vcc
- Sistema de Baixa Tensão
- Sistema de Tração
- Grupo Gerador Diesel

Todo o Sistema de Alimentação Elétrica é supervisionado e controlado pelo SCL e SCC. Estas informações trafegam através da rede de telecomunicações (RTD).

4.2.4. SISTEMA DE PORTAS DE PLATAFORMA (PSD)

É o sistema responsável por propiciar uma barreira envidraçada entre cada plataforma e as vias de forma a impedir que pessoas ou objetos venham a cair nestas vias.

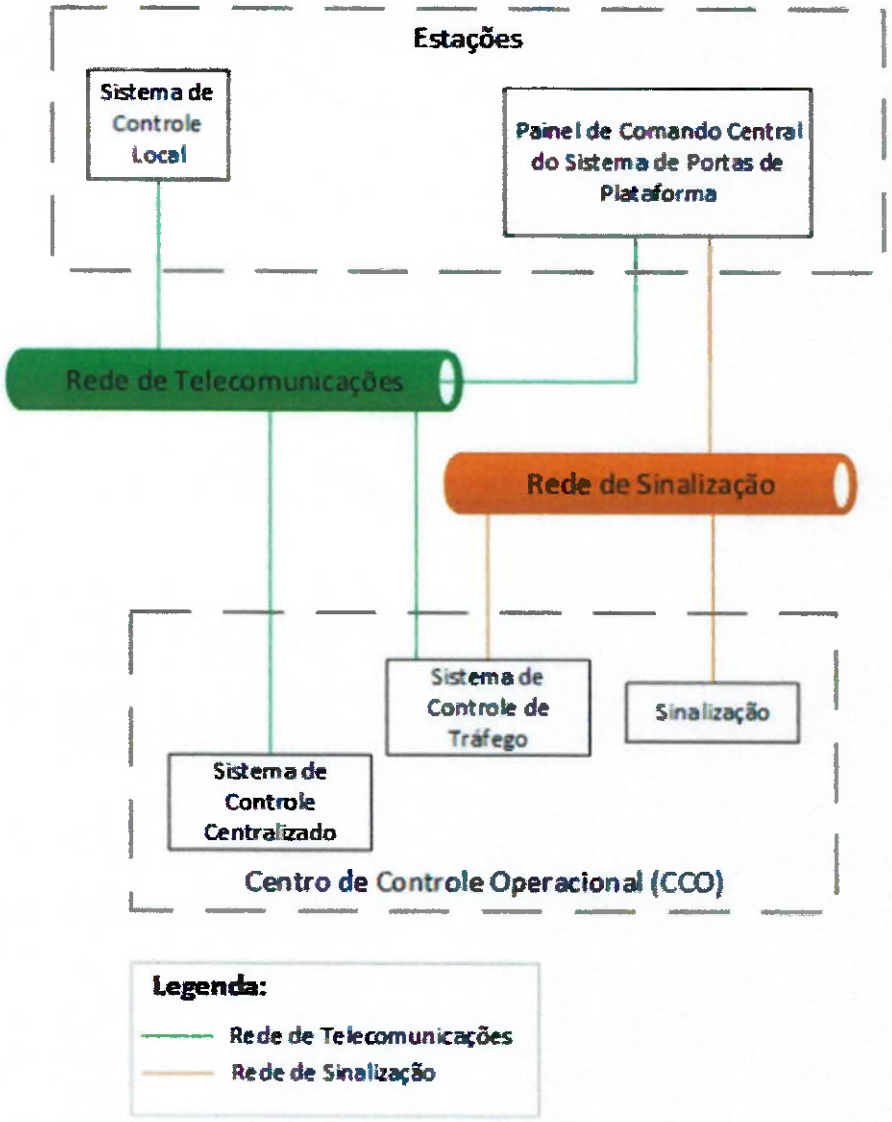
Este sistema opera em conjunto com o sistema de sinalização e sistema de controle de tráfego para que as portas de plataforma se abram de forma coordenada com as portas do trem.

Estas portas possuem abertura automática desde que recebam a informação de habilitação para abertura pelo sistema de sinalização.

Este sistema está interconectado ás redes de Telecomunicações e à rede de sinalização através de duas placas de rede do Painel de Comando Central do PSD.

Esta solução está sendo revista pelos fornecedores devido á insegurança que esta configuração gera em toda a estrutura de comunicação. Esta interconexão é apresentada na Figura 4.

Figura 4 – Conexão do PSD às redes de telecomunicações e de sinalização



Fonte: Elaborada pela autora

O Sistema de Portas de Plataforma também envia informações de status aos sistemas supervisórios (Sistema de Controle Local – SCL e Sistema de Controle Centralizado – SCC) através da rede de telecomunicações (RTD).

Este sistema também está interconectado à rede de Sinalização para comunicação de sinais não-vitais, tais como intertravamentos de portas.

Os sinais vitais trocados entre o PSD e a rede de sinalização são transmitidos por cabo dedicado.

4.2.5. MÁQUINA DE LAVAR TRENS

É uma máquina para lavagem externa dos trens, incluindo a limpeza da frente, traseira, laterais e teto do trem.

Para esta limpeza, a máquina é automática e movimenta o trem em uma velocidade constante.

Esta máquina possui interface com o sistema de sinalização para controle e movimentação do trem, porém também envia informações de status e diagnósticos ao sistema supervisório SCC através da rede de telecomunicações (RTD).

4.2.6. TRACK SWITCHES

O Aparelho de Mudança de Via (AMV) compreende o Track Switch e os Dispositivos de Transmissão de Dados entre o Trem e a via, além de sinaleiros e sensores.

O Track Switch permite a movimentação de um trecho da viga de forma a possibilitar que o trem alterne entre as duas vigas, visando o atendimento às necessidades operacionais.

Estes aparelhos possuem comando e controle individualizados, sendo monitorados pelo Centro de Controle Operacional (CCO) através do Sistema de Controle de Tráfego com o objetivo de alinhamento de rotas, manutenção preditiva e tomada de decisões em casos de falhas. A comunicação com o Centro de Controle Operacional ocorre através da rede de sinalização.

Caso algum Track Switch não esteja corretamente posicionado e travado, o Sistema de Sinalização impede o movimento de trens e veículos de manutenção nesta região.

O Sistema de Sinalização também impede que o Track Switch se movimente sob um trem ou veículo de manutenção ou quando estes estiverem em uma região de aproximação.

As indicações de posicionamento e recebimento de comandos do SCT são transmitidas através de uma rede de fibras ópticas dedicadas.

As indicações de status e informações para monitoração são encaminhadas ao SCC e ao SCL através da rede de telecomunicações (RTD).

4.2.7. SISTEMA DE CONTROLE LOCAL

É um sistema supervisório baseado em arquitetura SCADA (*Supervisory Control and Data Acquisition*), responsável pela supervisão e controle de todos os equipamentos instalados nas estações e trecho de via sob seu domínio. A comunicação com os equipamentos de campo é realizada através da rede de telecomunicações (RTD).

Para evitar que o SCL e o SCC comandem o mesmo equipamento, é implementada uma máquina de estados que estabelece a prioridade de comandos entre subsistemas entre estes dois sistemas supervisórios.

Esta máquina de estados garante que para determinado subsistema, apenas um dos sistemas supervisórios pode enviar comandos. Esta permissão pode ser cedida ao outro sistema supervisório, porém o que cedeu também perde o direito de comandar até que receba de volta esta permissão.

4.2.8. SISTEMA DE CONTROLE CENTRALIZADO

Assim como o Sistema de Controle Local (SCL), é um sistema supervisório baseado em arquitetura SCADA e também é responsável pela supervisão e controle de todos os equipamentos instalados nas estações e trechos de via.

Diferentemente do SCL, o SCC possui a óptica de gerenciamento de uma linha e não apenas de uma estação isoladamente.

Um de seus subsistemas é o Sistema de Controle de Tráfego que possui interface tanto com a rede de telecomunicações como a rede de sinalização.

A comunicação com os equipamentos de campo é realizada através da RTD. Conforme descrito para o SCL, existe um mecanismo que impede que tanto o SCC como o SCL comandem o mesmo grupo de equipamentos.

4.2.9. SISTEMA DE CONTROLE DE TRÁFEGO

Este sistema permite a supervisão e controle do processo de movimentação dos trens, utilizando as funcionalidades de ATP (*Automatic Train Protection*), ATO (*Automatic Train Operation*) e ATS (*Automatic Train Supervision*).

Possui interface com outros sistemas de forma a receber informações para a tomada de decisão, dentre elas: a informação do estado da alimentação elétrica dos trilhos (3º e 4º trilho), demanda de passageiros nas estações, dentre outros.

Este sistema se comunica com os trens e as vias utilizando a rede de sinalização tanto cabeada como wireless (comunicação com o trem).

4.3. ANÁLISE DE RISCO

A análise deste trabalho considera os equipamentos e sistemas que podem propagar falhas de *security* a outros sistemas e equipamentos interconectados, podendo afetar inclusive o *safety* destes sistemas e equipamentos.

Devido à carência de informações de falhas no ambiente avaliado, o estudo apresentado não aborda a análise quantitativa, focando na análise qualitativa tanto para *safety* como para *security*.

Desta forma, serão considerados os seguintes sistemas nesta análise:

- Sistema de Controle Local (SCL)
- Sistema de Controle Centralizado (SCC)

Esta análise de risco considera os sistemas supervisórios baseados em SCADA em virtude da alta complexidade, integração e possibilidade de propagação de erros através da interconexão destes sistemas com os demais equipamentos de campo através da rede cabeada e sem fio. Também serão consideradas as vulnerabilidades destes sistemas que podem ser exploradas para que o sistema modifique seu comportamento previsto, podendo gerar condições inseguras tanto para *safety* como para *security*.

Os demais equipamentos e sistemas citados anteriormente não serão considerados neste estudo, porém, como poderá ser observado no decorrer desta análise, podem ter seu comportamento ou segurança (*safety* e/ou *security*) afetados por uma falha de *security* na rede.

A seguir, segue a análise realizada tendo como base a metodologia descrita no item 3.

4.3.1. DEFINIÇÃO DOS LIMITES DO SISTEMA, FUNCIONALIDADES E INTERFACES

Na Tabela 1 são apresentados os sistemas, funcionalidades e respectivas interfaces, tendo como base a documentação técnica dos sistemas.

Tabela 1 – Definição dos limites do sistema, funcionalidades e interfaces

Sistema	Interface	Descrição
SCL e SCC	Modo de Controle	Máquina de estados compartilhada entre os dois supervisórios, que garante que apenas um dos sistemas supervisórios pode controlar um grupo de sistemas.
SCL e SCC	Equipamentos e Sistemas das Estações, Pátios e Vias	Permite o monitoramento e controle (mediante obediência ao modo de controle) dos equipamentos localizados nas estações e nos pátios.

Fonte: Elaborada pela autora

4.3.2. IDENTIFICAÇÃO PRELIMINAR DE PERIGO E ANÁLISE PRELIMINAR DE RISCOS E VULNERABILIDADES

Com base nas informações identificadas no passo anterior e exibidas na Tabela 1, foi realizada a identificação preliminar de perigo para estes itens, que está descrita na Tabela 2.

Tabela 2 – Identificação preliminar de perigo

Sistema	Interface	Falha	Perigo
SCL e SCC	Modo de Controle	Informações incorretas no modo de controle, permitindo o envio de um comando para um sistema que deveria apenas estar monitorando	Tomada de decisão incorreta, podendo danificar equipamentos ou ferir pessoas.
SCL e SCC	Equipamentos e Sistemas das Estações, Pátios e Vias	Recebimento de estado diferente do estado real do equipamento em campo.	Tomada de decisão incorreta, podendo danificar equipamentos ou ferir pessoas.
SCL e SCC	Equipamentos e Sistemas das Estações, Pátios e Vias	Envio de comando inválido ou não esperado para um subsistema ou equipamento.	Possibilidade de danificar equipamentos ou ferir pessoas.

Fonte: Elaborada pela autora

Após a identificação preliminar do perigo, foi realizada a análise preliminar dos riscos para cada um dos perigos identificados, com base na documentação técnica dos sistemas e dos artigos de Amey e Hilton (2001), Ten; Liu e Manimaran (2008) e Zhu; Joseph e Sastry (2001).

Como os sistemas supervisórios são baseados em protocolos de mercado para troca de informações com os equipamentos de campo e também das informações pertinentes ao modo de controle, a Tabela 3 apresenta as vulnerabilidades e riscos potenciais para os protocolos utilizados em sistemas supervisórios.

Esta análise foi realizada para cada um dos perigos descritos na Tabela 2.

Tabela 3 – Análise Preliminar de Riscos e Vulnerabilidades - Protocolos

Vulnerabilidade	Riscos Potenciais
Protocolos sem controle de segurança efetivo (o acesso de leitura e funções de diagnóstico destes protocolos são particularmente vulneráveis a ataques virtuais e físicos).	Como praticamente não existe autenticação na origem e os dados ficam disponíveis na rede, é possível ler e escrever informações e assim, modificar as informações transmitidas entre os equipamentos de campo e o sistema supervisório. Essa mudança nas informações pode levar à tomada de decisão incorreta, podendo danificar equipamentos ou ferir pessoas.
Uso de um programa para quebra de senha de acesso ao software supervisório	Permite acesso não autorizado, porém com todas as credenciais para realizar comandos e monitorar os estados dos equipamentos controlados. Esse tipo de acesso pode permitir o comando de qualquer equipamento ao qual o sistema supervisório tenha permissão. Essa ação pode danificar equipamentos ou ferir pessoas.

Fonte: Ten; Liu e Manimaran (2008)

Além dos riscos e vulnerabilidades dos protocolos, os sistemas supervisórios também estão expostos aos riscos e vulnerabilidades das redes cabeadas e sem fio que se interconectam no ambiente metroferroviário, conforme exposto na Figura 1. A Tabela 4 apresenta os riscos e vulnerabilidades das redes cabeadas e a Tabela 5, das redes sem fio.

Tabela 4 – Análise Preliminar de Riscos e Vulnerabilidades – Rede

Vulnerabilidade	Riscos Potenciais
Varredura e analisador de rede (*sniffer)*: Varre endereços IP para determinar as portas de serviço na máquina que, ou estão em execução ou em estado de escuta para conexão com potenciais pontos de acesso. O analisador de rede é usado para capturar os pacotes transmitidos nas redes.	Descobrir os protocolos / pacotes e endereçamento IP permite simular sinais entre equipamentos e sistemas supervisórios, podendo gerar divergências entre o sinal real do equipamento e o sinal apresentado no supervisório. Essa mudança nas informações pode levar à tomada de decisão incorreta, podendo danificar equipamentos ou ferir pessoas.
Vulnerabilidades nos protocolos comuns	Dados falsos de entrada e saída no controlador obtidos através de sensores comprometidos e/ ou do comprometimento da rede entre o equipamento e o controlador. Essa mudança nas informações pode levar à tomada de decisão incorreta, podendo danificar equipamentos ou ferir pessoas.
Backdoors na rede Cavalos de Tróia Vírus	É possível que contenham programas e códigos maliciosos para permitir um ataque de indisponibilidade de serviço (*Denial of Service*). Esse ataque pode impedir o acesso a rede ou aos sistemas interconectados. Essa ação pode danificar equipamentos ou ferir pessoas.

Fontes: Ten; Liu e Manimaran (2008); Zhu; Joseph e Sastry (2001)

Tabela 5 – Análise Preliminar de Riscos e Vulnerabilidades - Rede sem fio

Vulnerabilidade	Riscos Potenciais
Os sinais das antenas wireless podem se propagar além do espaço físico do ambiente metroferroviário.	Tentativa de ataque fora do ambiente metroferroviário. Todas os riscos e vulnerabilidades da rede cabeada também se aplicam.
Conexão de um ponto de acesso na rede existente (mesmo SSID - *Service Set IDentifier*) com nível de frequência superior ao ponto de acesso da rede ou desativação do ponto de acesso existente.	Permite a interconexão da rede existente com qualquer outro computador que este ponto de acesso também possuir acesso. Todas os riscos e vulnerabilidades da rede cabeada também se aplicam.

Fonte: Elaborada pela autora

4.3.3. CONCLUSÃO DA ANÁLISE DE RISCO

Com base no exposto, os riscos identificados podem afetar o *safety* dos sistemas interconectados visto que, dependendo do ataque que o sistema ou a rede sofrer, as informações trocadas entre os sistemas supervisórios e os equipamentos controlados podem não ser confiáveis, tornando todo o sistema suscetível a falhas.

Conforme apresentado, devido às vulnerabilidades na rede e nos protocolos, é possível modificar as informações transmitidas entre os equipamentos de campo e o sistema supervisório.

Essa situação pode gerar falhas nos sistemas interconectados, podendo inclusive afetar os requisitos de *safety* destes sistemas.

Além desta situação, também pode ocorrer a mudança de comportamento direto no equipamento de campo, sem passar pelo sistema supervisório (SCC ou SCL) e sem validação do comando, podendo resultar numa operação indevida ou ainda em algum acidente.

É importante ressaltar os riscos de *security* abordados para as redes (em especial a sem fio), pois muitas vezes a rede SCADA é considerada uma rede isolada da rede corporativa e sem acesso externo. Infelizmente esta não é mais uma realidade no ambiente metroferroviário onde cada vez mais as redes necessitam de integração.

5. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Conforme exposto na análise de risco apresentada anteriormente, pode-se notar que os requisitos de segurança de um sistema, quer seja baseado em *safety*, que seja baseado em *security*, não podem ser elaborados e analisados de forma isolada.

Como apresentado, existem falhas de *security* que afetam o *safety* de outros sistemas. De acordo com Smith; Russel e Looi (2003), os sistemas que podem causar danos a outros sistemas ou pessoas não podem mais serem construídos baseando o controle de erros e falhas de forma individual.

Tendo isso em vista, necessitamos garantir que a solução atenda aos requisitos de segurança (*safety* e *security*) e de confiabilidade, comprovando através de métodos e técnicas de verificação, conforme Amey e Hilton (2001).

Também devem ser considerados os riscos que a integração das redes traz ao sistema como um todo. Estes riscos também devem ser levados em conta na análise, bem como as vulnerabilidades conhecidas para todos os componentes do sistema, incluindo equipamentos, sistemas operacionais e softwares.

Este estudo pode prosseguir, quantificando a análise dos riscos de *safety* e de *security* para o ambiente metroferroviário. É necessário criar um modelo probabilístico demonstrando as condições que foram identificadas.

É possível contribuir com este modelo probabilístico através dos dados operacionais das falhas de *safety* e de *security* para determinada linha ou modal de forma a confirmar ou refutar os valores calculados.

Como trabalho futuro, é possível realizar a análise de risco para *safety* e *security* de todos os sistemas apresentados na Figura. Esta análise serviria como base para a elaboração em conjunto das especificações destes sistemas, criando uma matriz de interfaces e de requisitos de *safety* e *security* que deve ser referenciada em todas especificações e obedecida por todo o fornecimento.

6. REFERÊNCIAS

AMEY, P.; HILTON, A. Practical Experiences of Safety- and Security- Critical Technologies. **Ada User Journal**, [S.l.], v. 22, n. 1, p. 1-8. 2001.

BROSTOFF, S.; SASSE, M. Safe and Sound: A Safety-Critical Approach to Security. In: New Security Paradigms Workshop 2001, Cloudcroft. **Proceedings of the New Security Paradigms Workshop 2001.** [S.l.]: ACM Press, 2001. p.41-50.

CAMBRIDGE UNIVERSITY PRESS 2015. Cambridge. Cambridge Dictionaries Online. Disponível em: <http://dictionary.cambridge.org/dictionary/british/>. Acesso em: 14 mar. 2015.

EAMES, David Peter; MOFFETT, Jonathan. The Integration of Safety and Security Requirements. In: 18TH INTERNATIONAL CONFERENCE SAFECOMP'99, 18. 1999 Toulouse. **Computer Safety, Reliability and Security.** [S.l.]: Springer-Verlag Berlin Heidelberg, 1999. p. 468-480.

NOVAK, Thomas; GERSTINGER, Andreas. Safety- and Security-Critical Services. In: Building Automation and Control Systems. **IEEE Transactions on Industrial Electronics,** [S.l.], v. 57, n. 11, p. 3614-3621, 2010.

LAUTIERI, Samantha; COOPER, David; JACKSON, David. SafSec: Commonalities Between Safety and Security Assurance. In: SAFETY CRITICAL SYSTEMS SYMPOSIUM, 13, 2005 Southampton. **Constituents of Modern System-safety Thinking.** London: Springer-Verlag London Ltd, 2005. p. 65-75.

SMITH, J.; RUSSEL, S.; LOOI, M. Security as a Safety Issue in Rail Communications. In: 8TH AUSTRALIAN WORKSHOP ON SAFETY CRITICAL SYSTEMS AND SOFTWARE (SCS'03), 8, 2003 Canberra. **Safety Critical Systems and Software 2003.** [S.l.]: [s.n.], 2004. p. 79-88.

TEN, Chee-Wooi; LIU, Chen-Ching; MANIMARAN, Govindarasu. Vulnerability Assessment of Cybersecurity for SCADA Systems. **IEEE Transactions on Power Systems**, [S.l.], v. 23, n. 4, p. 1836-1846. 2008

ZHU, B.; JOSEPH, A.; SASTRY, S. A Taxonomy of Cyber Attacks on SCADA Systems. In: 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011 Dalian. **iThings/CPSCom 2011.** [S.l.]: CPS Conference Publishing Services, 2011. p. 380-388.