UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE INFORMÁTICA
CURSO DE ENGENHARIA DE COMPUTAÇÃO

VINÍCIUS LINDORFER BOHRZ

Estudo de caso de Normas de Segurança em um Sistema Movimentador Automático de Pessoas

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Computação

Orientadora: Prof. Dr. Taisy Silva Weber
Co-orientador: Prof. Dr. Sérgio Luis Cechin

Porto Alegre
2017

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Reitor: Prof. Rui Vicente Oppermann
Vice-Reitor: Prof.ª Jane Fraga Tutikian
Pró-Reitor de Graduação: Prof. Vladimir Pinheiro do Nascimento
Diretor do Instituto de Informática Prof.ª Carla Maria Dal Sasso Freitas
Coordenador do Curso de Engenharia de Computação: Prof. Renato Ventura Henriques
Bibliotecária-Chefe do Instituto de Informática: Beatriz Regina Bastos Haro

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a Deus por esse feito que Ele me ajudou a construir ao longo dos anos, também agradeço aos meus pais, Sergio e Mara, pelo apoio incondicional, apesar da distância que nos separou nos anos de graduação, mas que sempre esteve presente. Dedico esse feito a vocês, meus pais, que sempre me incentivaram aos estudos, me apoiaram e deram força para que tudo isso fosse possível. Ainda no âmbito familiar, agradeço do fundo do meu coração aos meus avós maternos, Inês e Oldemar, e paternos, Victória e Hugo, pelo apoio e orações ao longo desses anos de faculdade, por serem sempre um porto seguro e pela dedicação que sempre demonstraram a mim.

Aos meus amigos e colegas de faculdade, agradeço por sempre me acompanharem e me apoiarem durante a minha trajetória. Aos amigos de infância e colégio, só resto dizer que vocês foram de fundamental importância para minha formação, tanto na formação do meu caráter quanto profissionalmente. Gostaria de citar cada um de vocês aqui, mas creio que faltaria linhas para isso. Mas vocês sabem que estou falando de cada um de vocês e sabem quão importantes são para mim.

Além de amigos e família, tenho meus mais sinceros agradecimentos a minha professora orientadora, Prof.ª. Dr. Taisy Silva Weber, aos seus ensinamentos, dedicação e trabalho exemplar no âmbito acadêmico. Agradeço por ter me aceito como seu aluno, por me orientar nesse trabalho de conclusão de curso e pela grande pessoa que você é.

RESUMO

O estudo de caso de normas de segurança (safety) em sistemas de transporte de pessoas com controle e supervisão distribuídos é cada vez mais importante à medida que esses sistemas crescem e se tornam cada vez mais presentes no nosso dia-a-dia. Para o caso de um sistema movimentador automático de pessoas (em inglês, Automated People Mover), a segurança é um assunto crítico, uma vez que os frequentadores desse sistema são seres humanos e qualquer falha pode acarretar danos irreparáveis. Tendo isso em mente, o objetivo desse estudo é analisar as normas de segurança (safety) aplicáveis a esse tipo de sistema de movimentação de pessoas automático, assim como as funções de segurança que as normas e padrões internacionais recomendam para prover a segurança dos passageiros e das instalações que fazem parte do Automated People Mover (APM). Entre as diversas medidas de segurança sugeridas pelas normas, a análise desse trabalho restringe-se ao impacto causado nos níveis de segurança do sistema APM, ao utilizarmos protocolos de comunicação seguros. Além disso, são escolhidas algumas situações onde ocorram falhas de comunicação no sistema e assim, avaliar como o sistema reage às falhas e que procedimentos e/ou estados o sistema assume.

Palavras-Chave: Normas. Segurança. Movimentador Automatizado de Pessoas. Falhas. Comunicação.

SAFETY STANDARDS APPLIED IN AN AUTOMATED PEOPLE MOVER ENVIRONMENT

ABSTRACT

The case study of safety standards in passenger's transport systems with distributed control and supervision is increasingly important as these systems grow and become more present in our lives. In the case of an Automated People Mover type system, the security issue is a critical issue since the patrons of the system are human beings and any failure can cause unimaginable damages. With this in mind, the aim of this study is to analyze the safety standards applicable to this type of people drive system, as well as the security features that international norms and standards recommend to provide passenger safety as well as the facilities that are part of the Automated People Mover system. Among the several security measures suggested by the standards, we will restrict our analysis on this paper to the impact on the APM system security levels, when we use safe communication protocols. Beyond that, were chosen some situations where communication failures can happen and evaluate how the system reacts to failures and what procedures and / or states it assumes.

Keywords: Standards. Safety. Automated People Mover. Failures. Communication.

LISTA DE FIGURAS

Figura 2.1 - Aeromóvel de Porto Alegre – RS 15

Figura 3.1 - Visão 3D da topologia com trilho retilíneo 34

Figura 3.2 - Visão Aérea da topologia com trilho retilíneo 35

Figura 3.3 - Visão 3D da topologia com trilhos circulares com duas estações e um veículo 35

Figura 3.4 - Visão Aérea da topologia com trilhos circulares com duas estações e um veículo 36

Figura 3.5 - Visão 3D da topologia com trilhos circulares, com duas estações e dois veículos 37

Figura 3.6 - Visão Aérea da topologia com trilhos circulares, com duas estações e dois veículos 37

Figura 3.7 - Visão 3D da topologia circular com duas estações e intersecções de trilhos 39

Figura 3.8 - Visão Aérea da topologia circular com duas estações e intersecções de trilhos 39

Figura 3.9 - Visão 3D da topologia circular com duas estações, com intersecção de trilhos e dois veículos 40

Figura 3.10 - Visão Aérea da topologia circular com duas estações, com intersecção de trilhos e dois veículos 40

Figura 4.1 - Plano de Eixos 47

Figura 4.2 - Topologia Retilínea 48

Figura 4.3 - Gráfico de Posição/Velocidade vs Tempo em uma frenagem normal. 50

Figura 4.4 - Gráfico de Posição/Velocidade vs Tempo em uma frenagem de emergência 51

Figura 4.5 - Gráfico de Posição/Velocidade vs Tempo caso de uma falha de comunicação 53

Figura 4.6 - Topologia Circular 54

Figura 4.7 - Topologia Circular com Intersecções 60

Figura 4.8 - Trechos enumerados da Topologia com Intersecções 62

Figura 4.9 - Presença de falha na topologia circular com intersecções 64

Figura 4.10 - Gráfico de Frenagem de Operação 71

Figura 4.11 - Gráfico de Frenagem de Emergência.....73

LISTA DE TABELAS

Tabela 4.1 - Valores de aceleração/desaceleração 47

Tabela 4.2 - Dados referentes a topologia retilínea em caso normal de operação 50

Tabela 4.3 - Dados referentes a topologia retilínea utilizando frenagem de emergência 51

Tabela 4.4 - Dados referentes a topologia retilínea em caso de falha na comunicação 52

Tabela 4.3.1 – Grandezas Físicas dos Veículos APM 69

Tabela 4.3.2 – Valores referentes a Frenagem de Operação 70

Tabela 4.3.3 – Valores referentes a Frenagem de Emergência 72

LISTA DE ABREVIATURAS E SIGLAS

APM	Automated People Mover
ASCE	American Society of Civil Engineers
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
CBTC	Communication-Based Train Control
IEC	International Electrotechnical Commission
NBR	Norma Brasileira
SIL	Safety Integrity Level

SUMÁRIO

1 INTRODUÇÃO.....12
2 CONCEITOS REFERENTES AO ESTUDO DE CASO.....14
2.1 Sistemas Movimentadores Automáticos de Pessoas.....14
2.1.1 Communication-Based Train Control (CBTC).....16
2.1.2 Subsistemas presentes em um APM.....16
2.1.3 ATC Fail-safe.....17
2.2 Conceitos Relacionados a Níveis de Integridade de Segurança.....19
2.2.1 Funções de Segurança.....20
2.2.2 Normas de Segurança.....21
2.2.3 Níveis de Integridade de Segurança (SIL).....21
2.3 Normas de Segurança Aplicáveis a APMs.....22
2.3.1 IEC 61508.....22
2.3.2 IEC 61784-3.....23
2.3.3 Protocolos de Comunicação Seguros.....24
2.3.4 Norma ASCE Automated People Mover Standards.....26
2.4 Normas e Certificação no Brasil.....29
3 TOPOLOGIAS DE VIAS SOBRE TRILHOS.....32
3.1 Topologias de Vias de um APM.....33
3.2 Análise de Falhas em um APM.....40
3.3 Falhas Comunicação em um APM.....42
3.3.1 Modelo de um Sistema de Controle.....42
3.4 Análise de Falhas de Comunicação em um APM.....43
4 DADOS ANALÍTICOS DE UM APM.....45
4.1 Estudo de caso em uma Topologia Retilínea.....47
4.2 Estudo de caso para uma Topologia Circular com dois ou mais veículos.....53
4.2.1 Premissas Relativas ao Sistema.....55
4.2.2 Independência de Fatores.....56
4.2.3 Falhas Múltiplas.....57
4.3 Estudo de caso para uma Topologia Circular com Intersecções.....59
4.3.1 Operação em Condições Normais.....61

4.3.2 Operação na Presença de Falhas 63
4.3.3 Análise de Falhas 67
5 CONCLUSÕES 74
REFERÊNCIAS 76

1 INTRODUÇÃO

Como se sabe, transporte de pessoas de maneira eficiente, rápida e de baixo custo está se tornando uma necessidade cada vez maior em ambientes onde o fluxo de pessoas é consideravelmente alto. Uma solução que se mostrou eficaz ao longo dos anos são sistemas movimentadores automáticos de pessoas, ou do inglês, APMs (Automated People Mover). Os APMs possuem um custo de implementação relativamente baixo (basicamente estrutural), um custo de operação pequeno e uma eficiência no transporte muito elevada. Informações favoráveis como estas sugerem o uso em larga escala desses tipos de transporte, porém o motivo para isso não acontecer passa desapercebido na maioria das vezes por se tratar de requisitos técnicos que o sistema impõe.

Um sistema do tipo APM, como o Aeromóvel situado na cidade de Porto Alegre, tem como característica principal sua automatização frente aos demais transportes urbanos. Para essa automatização ser possível, precisamos de um sistema de controle bem planejado, robusto e que tenha níveis de segurança adequados para que tal operação automatizada possa ser realizada com sucesso, agregando assim, um nível de confiabilidade adequado e que permita minimizar riscos de falhas no sistema. Dessa forma, o ponto crucial em um sistema de controle em tempo real para movimentadores automatizados de pessoas é a comunicação entre os diversos membros desse sistema, sejam eles um sistema tipo mestre-escravo, clusters ou, no caso do APM, um controlador central (centro de controle) e diversos atuadores (os veículos).

Quando falamos a respeito da dificuldade de estabelecer uma comunicação segura e eficiente para sistemas distribuídos, estamos nos referindo a um número considerável de falhas de comunicação que podem acontecer durante uma transmissão de dados, sejam essas falhas de mascaramento de mensagens, duplicação ou perda de pacotes. E no caso de um sistema que transporta pessoas onde o controle do mesmo é feito por troca de mensagens (comunicação entre a central e o veículo), uma falha na comunicação não tratada ou despercebida pode ser decisiva para que ocorra acidentes (ZHIVICH; CUNNINGHAM, 2009).

Com o objetivo de realizar uma comunicação segura, nos deparamos com a necessidade, e o fator que motivou esse trabalho, de realizar um estudo das normas de segurança aplicáveis à comunicação entre dispositivos de controle e possíveis soluções para introduzir um certo nível de segurança ao sistema. Assim, com o estudo de normas de segurança, como por exemplo a IEC 61508 e a norma ASCE, será feita uma análise

sobre as boas práticas de projeto e métodos aplicáveis a esse tipo de sistema de transporte, APMs, para fins de obter robustez e minimizar a probabilidade de falhas no sistema.

Relativo aos objetivos previamente citados, será analisado como se comporta um sistema movimentador automatizado de pessoas idealizado na presença de falhas. Como em um sistema complexo como o de um APM, onde falhas de diferentes naturezas podem acontecer, como falhas estruturais, falhas elétricas ou mecânicas, o escopo de análise deste trabalho será restrito a somente falhas de comunicação. Ainda, vale ressaltar que o objetivo do trabalho não é elaborar um sistema APM ou servir como base para a criação de um, e sim em realizar uma análise de riscos do sistema proposto/modelado em situações específicas.

Esse documento está organizado da seguinte forma: Capítulo 2 apresenta uma visão geral do sistema Aeromóvel, de funções de segurança, normas relacionadas e conceitos relativos a área de segurança, sobre os quais a análise é baseada. O capítulo 3 trata de uma análise sobre topologias de vias utilizadas na análise posterior, junto com uma análise de falhas sobre sistemas APMs. Já no capítulo 4, é feito a análise de dados referentes ao modelo proposto e o fechamento da análise teórica iniciada anteriormente e por último, no capítulo 5 são apresentadas as conclusões relativas ao trabalho.

2 CONCEITOS REFERENTES AO ESTUDO DE CASO

Como o objetivo desse trabalho é um estudo sobre normas de segurança, topologias de um movimentador automatizado de pessoas (APMs), conceitos relativos à níveis de integridade e protocolos de comunicação, é apresentado a seguir um conjunto de definições relativas a cada um desses itens. A importância de definir esses conceitos se dá, principalmente, pelo fato de palavras sinônimas no linguajar coloquial possuírem sentidos variados em uma análise de tolerância a falhas, evitando interpretação dúbia de alguns termos. Além de dar o embasamento necessário para análise nos capítulos que se seguem.

2.1 Sistemas Movimentadores Automáticos de Pessoas

Sistemas movimentadores automáticos de pessoas (APMs) são sistemas de transporte de passageiros com operação completamente automatizada, trafegando em vias exclusivas (somente um carro/vagão por sentido) e possuem uma alta taxa de serviço. Normalmente são sistemas de transporte de pequeno porte, com carros/vagões de capacidade inferior a trens de passageiros e têm por característica trafegarem em vias elevadas ao chão, evitando assim a presença de obstáculos na via (KUNZ, G.; PERONDI; MACHADO, 2011).

Esses APMs se diferenciam do sistema ferroviário tradicional uma vez que são completamente automatizados, ou seja, não há ninguém operando o sistema (maquinista, por exemplo). O controle dos APM é feito via comunicação de dados com uma central em terra, de onde é possível desempenhar todas as funções necessárias para o funcionamento do sistema sem precisar da presença humana.

Aplicações típicas desse sistema de transporte são encontradas em terminais aeroportuários, comunicação entre centros comerciais e/ou universitários e parques temáticos. Como por exemplo, em Porto Alegre - RS, existe um sistema APM denominado Aeromóvel, visto na figura 2.1, que atua no transporte de passageiros entre o Aeroporto Internacional Salgado Filho e o terminal de trens interurbanos da cidade (Trensurb). Assim, esse sistema é adequado a qualquer local que haja a necessidade de transportar um número relativamente alto de pessoas em curtas distâncias (VUCHIC, 2002).

Ou ainda, para casos onde não haja alternativas físicas para expansão dos meios de transporte, como regiões cuja densidade de pessoas é grande e não há como aumentar o número ou vazão das vias terrestres ou pouco orçamento para construção de metrôs (SCHERER; WICHSER; VENCKAUSKAITE, 2009).

Figura 2.1 - Aeromóvel de Porto Alegre –RS

Fonte: "Conexão Metrô-Aeroporto - Trensurb - Empresa de Trens Urbanos de Porto Alegre S.A."

Como em qualquer outro sistema de transporte de pessoas, o *Automated People Mover* (APM) requer um nível altíssimo de segurança em todos os seus aspectos funcionais para que se possa garantir um bom funcionamento e uma baixíssima taxa de falhas no sistema. Para que isso seja possível, é necessário seguir as normas de segurança e práticas de projeto que ao longo do tempo foram desenvolvidas e testadas, como por exemplo, normas ASCE relacionadas ao sistema APM e padrões como o IEC 61508.

Lembrando que normas de projeto e padrões trazem um nível de segurança considerável a certas camadas do sistema, mas uma ressalva é necessária uma vez que os mesmos não garantem que o sistema implementado seja imune a falhas ou defeitos. Tais padrões servem mais como diretrizes de como se executar um projeto robusto e confiável, porém são essenciais para projetos que almejam a certificação por entidades certificadoras internacionais. Porém, nem sempre se deseja ou mesmo é requerido que o produto seja realmente certificado e aprovado por tais entidades, como no caso brasileiro

de normas de segurança (norma NBR16074-1) para o setor de movimentadores automatizados de pessoas.

Tendo conhecimento disso, esse projeto tem como objetivo principal analisar como um sistema automatizado de transporte de pessoas, nesse caso, um Automated People Mover, se comporta na presença de falhas na comunicação entre o APM e sua central de controle em terra. Através de uma análise do modelo de falhas dos protocolos de segurança que são aconselháveis a implementação nesse tipo de sistema, com o auxílio de modelagem e simulações, escolheremos algumas falhas comuns de comunicação e observaremos como algumas funções de segurança do APM reagem às falhas, analisando assim quais estados o sistema assume para garantir sua integridade e também a segurança dos seus passageiros.

2.1.1 Communication-Based Train Control (CBTC)

Sistemas de movimentadores automatizados de pessoas fazem parte de um grupo de sistemas que possuem seu controle de movimento feito à distância, diferentemente de sistemas ferroviários. Por exemplo, os APMs fazem parte de um grupo especial, chamado CBTC, ou sistemas de controle baseados em comunicação (MORAR, 2010).

Esse sistema faz uso de técnicas mais apuradas para se obter melhores resultados e até benefícios em certas situações, como o uso de sistemas de altíssima precisão para localização dos trens/veículos (não há necessidade de sensores nos trilhos), uma comunicação contínua e de alta capacidade com o exterior (central de comando) e hardware dentro do próprio veículo para suporte ao sistema de controle automático do veículo e subsistemas do mesmo (VEHICULAR TECHNOLOGY SOCIETY *et al.*, 1999).

2.1.2 Subsistemas presentes em um APM

Para o correto funcionamento do sistema movimentador automatizado de pessoas, alguns subsistemas são projetados para garantir que as mais diversas funções presentes em um APM, como movimentação do veículo, controle de portas e sistemas de segurança possam executar de acordo com a norma americana relativa a movimentadores

automatizados de pessoas, denominada ASCE. Entre os subsistemas temos o ATC, que é o sistema principal presente em um APM, e outros três subsistemas (ATO, ATP e ATS) que fazem parte do sistema ATC e são responsáveis pelo funcionamento básico do veículo como serão descritos a seguir(VEHICULAR TECHNOLOGY SOCIETY *et al.*, 1999).

- Controle Automático de Trens (ATC)

  O sistema para controle automático do movimento dos trens, segurança e direção de operações dos mesmos. ATC é composto de três outros subsistemas para garantir o correto funcionamento de cada parte do sistema. São eles, o subsistema para operação de trem automático (ATO), o subsistema de proteção automática de trem (ATP) e o de supervisão automática de trens (ATS).

- Operação automática do Trens (ATO)

  O subsistema dentro do sistema de controle automático (ATC) executa qualquer uma ou todas as funções de regulação de velocidade, parada programada, tempo de porta e tempo de permanência na estação e outras funções atribuídas de outra forma a um maquinista humano.

- Proteção Automática de Trens (ATP)

  O subsistema dentro do sistema de controle automático (ATC) fornece a proteção primária para os passageiros e equipamentos contra perigos de uma operação baseada em controle automático do veículo.

- Supervisão Automática de Trens (ATS)

  O subsistema dentro do sistema de controle automático (ATC) que monitora e gerencia o funcionamento geral do sistema APM e fornece a interface entre o sistema e o operador (localizado na central de operação).

2.1.3 ATC Fail-safe

Ao considerar o mundo real, as vezes é difícil perceber que falhas e erros acontecem diariamente em dispositivos que utilizamos, seja nos smartphones, nos veículos ou computadores pessoais. Apesar dessas falhas acontecerem, elas não atrapalham o uso de nenhum desses dispositivos uma vez que o projeto dos mesmos

consegue mascarar a maioria das falhas ocorridas. E ainda no caso em que a falha perdure, o projeto do sistema faz com que o dispositivo não cause danos a si próprio ou ao seu usuário.

Essa característica é a marca de um sistema/dispositivo *fail-safe*, onde o sistema ao não conseguir tratar uma falha, consegue atingir um estado estável e seguro, de modo a preservar a integridade do sistema e dos seus usuários. Para a aplicação APM, onde todo o controle é automatizado, a necessidade de um sistema *fail-safe* é considerável pois o próprio sistema é o responsável pela integridade tanto dos passageiros quanto do sistema em si.

Em relação ao sistema APM, o aspecto *fail-safe* começa pelo sistema de controle automático de trens (ATC), onde cada parte do sistema que é considerada crítica, no aspecto de segurança, deve ser desenvolvida de acordo com os princípios *fail-safe*. Tais princípios podem serem vistos como diretrizes de projeto, no sentido de desenvolver o sistema com características intrínsecas de segurança ou com métodos confiáveis capazes de realizarem uma checagem no sistema em busca de possíveis estados que levem o sistema a falhas e impedir que o sistema atinja esses estados (AMERICAN SOCIETY OF CIVIL ENGINEERS, 2006a).

Assim, uma maneira de se projetar um sistema *fail-safe* é usando componentes, sejam eles elétricos, mecânicos ou de outra natureza, com características capazes de serem verificadas. Ou seja, cada componente usado deve ser passível de testes e o conjunto dessas verificações serem processadas para análise da probabilidade de falha no sistema.

Uma outra maneira e, normalmente mais empregada, é o uso de componentes que não sejam verificáveis, como software ou circuitos integrados para desenvolver o sistema. Nesse caso, técnicas de redundância são normalmente aplicadas e posteriormente ainda o sistema é submetido a testes de verificação e validação, para de fato comprovar a efetividade da técnica aplicada.

Entre as técnicas passíveis de serem aplicadas temos a duplicação e comparação (do inglês, *checked-redundancy*) onde dois sistemas paralelos realizam a mesma tarefa de maneira idêntica e suas saídas são comparadas, a programação em N-versões (do inglês, *N-version programming*) onde programas são escritos de formas diferentes, mas realizando a mesma função, evitando assim bugs de programação. E ainda existe o método de diversidade e auto checagem, que trata de se aplicar hardware e software

diferentes para a mesma operação crítica e verificar se os resultados são idênticos além de realizar rotinas de auto verificação em seus próprios hardwares afim de verificar a inexistência de falhas.

2.2 Conceitos Relacionados a Níveis de Integridade de Segurança

Nesse trabalho, será discutido sobre a necessidade e importância da padronização dos níveis de SIL para a indústria, uma vez que a falta da uniformidade traz prejuízos tanto econômicos quanto temporais, na questão de maior investimento para se adequar o projeto a um certo SIL desejado. Entre os diversos conceitos relativos a níveis de integridade, segue uma lista das principais abstrações relativas ao SIL (JOANNOU; WASSYNG, 2014).

- Consequências Adversas

Consequências resultantes em um certo nível de perda. Normalmente resultante de uma combinação entre o sistema estar em uma condição de perigo e o ambiente apresentar o pior caso possível.

- Condição de Perigo

Definido como um estado do sistema que, se combinado com uma condição adversa do ambiente, pode levar o sistema inteiro a um estado de consequência adversa.

- Nível de Integridade

Normalmente definido como o grau de confiança que o sistema alcança quando esse segue as reinvindicações de integridade propostas.

- Reinvindicação de Nível de Integridade

Definido como um conjunto de requerimentos para redução de risco. Corriqueiramente, essa reinvindicação é definida em termos dos requisitos para evitar, controlar ou mitigar as consequências adversas, provendo uma certa tolerância de risco.

- Requisitos de Nível de Integridade

Esse conjunto de requisitos, quanto atingido, provê um nível de confiança ao sistema.

- Critério de Risco

Funciona como um termo de referência pelo qual se avalia a significância do risco, como por exemplo, critério de risco relativo a segurança, financeiro ou ambiental.

- Medidas para Redução de Risco

Contramedidas que são inseridas no sistema para que, caso se atinja uma situação de risco real, essas medidas possam mitigar o real efeito desse risco. Como por exemplo, o sistema de *airbag* de um carro "alivia" os efeitos da colisão, mas não evita o risco de ocorrer a colisão, ou o sistema de freios redundantes de um trem, que caso os principais falhem, os auxiliares são usados para diminuir ao máximo a violência do impacto.

2.2.1 Funções de Segurança

O termo "funções de segurança", do inglês "*Functional Safety*", precisa ser bem definido para evitar más interpretações. Separando o termo em dois, temos que segurança é definida como "ser livre" de riscos inaceitáveis que atentem contra a integridade das pessoas envolvidas, a estrutura de um sistema ou meio ambiente. Ou ainda, pode ser definido, dentro do escopo de segurança funcional, como uma função a ser implementada por um sistema de segurança ou outra medida de redução de risco, que se destina a alcançar ou manter, em um estado seguro, o equipamento sob um evento perigoso específico (DALE; ANDERSON, 2011, cap. Introduction and Revision of IEC 61508).

Já funções de segurança são relativas a uma parte do sistema que provê a segurança ao todo. Ou seja, é um equipamento ou um subsistema que tem como objetivo atuar corretamente independentemente de suas entradas (IEC 61508). Um exemplo de uma função de segurança é o controle das válvulas de pressão de tanques de lastro em navios.

Os tanques de lastro em embarcações têm como objetivo manter o peso e a estabilidade em navios que estejam vazios, ou a medida que a quantidade de combustível vai baixando ou ainda com alguma ruptura de casco. Esses tanques possuem válvulas de pressão que movimentam a água tanto do exterior para o interior do navio e vice-versa, quanto de um tanque para o próximo, de modo que se mantenha o equilíbrio na embarcação. Nesse caso, essas válvulas de pressão atuam como uma função de segurança de embarcações, as quais precisam ser abertas rapidamente (em um curto espaço de tempo) quando houver uma pressão barométrica superior a "X" em um dos lados da

válvula, por exemplo, para que a água flua para o tanque vizinho e evite que o navio acabe adernando para algum lado e, consequentemente, entre em um estado de perigo.

Ainda referente a funções de segurança, temos que lembrar que elas são, normalmente, executadas por algum subsistema/equipamento do sistema principal. Mas, há casos em que o sistema que realiza a função de segurança é o próprio sistema da aplicação, ou seja, um mesmo equipamento é responsável tanto por operar o sistema quanto operar as funções de segurança. Em casos como esse, a estabilidade do sistema deve ser relativamente alta, uma vez que se o sistema principal parar de responder por uma falha, a própria função de segurança, que deveria atuar a fim de restabelecer a correta operação do sistema, também não será executada devido à falha no sistema principal.

2.2.2 Normas de Segurança

As normas de segurança funcional têm, em comum, a obrigatoriedade do emprego de técnicas de prevenção e de tolerância a falhas para a redução de risco, além do projeto criterioso e documentado, desde as primeiras fases do ciclo de desenvolvimento do sistema. Essas normas permitem certificação de sistemas construídos segundo suas recomendações, que tenham sido devidamente verificados e validados e são conceitos presentes tanto da parte do hardware como do software (Brown, 2000).

Visando garantir os níveis de integridade de segurança adequados para a correta troca de informações entre os dispositivos de controle e instrumentação em sistemas caracterizados como críticos, por exemplo, um sistema de transporte automatizado, são aplicadas as normas IEC 61508, IEC 61784-3 (comunicação segura) e ASCE (Automated People Mover Standard).

2.2.3 Níveis de Integridade de Segurança (SIL)

Níveis de integridade de segurança, conhecidos também por níveis de SIL (do inglês, Safety Integrity Level), são responsáveis por estabelecerem um certo grau de confiança a um determinado sistema dado que esse sistema satisfaça propriedades críticas relativas à segurança do sistema quanto a critérios de riscos pré-estabelecidos. Esses níveis são, comumente, atribuídos a um sistema por agências certificadoras ou entidades

governamentais que estabelecem os níveis de integridade baseados no julgamento das pessoas/sociedade referentes ao risco presente para certo domínio.

Dependendo da norma aplicável, junto com os níveis de integridade, temos um conjunto de regras/práticas que quando seguidos trazem consigo essa confiança do sistema, por exemplo, em validações de sistemas, quanto maior o nível do SIL requerido, mais rigorosas e exaustivas tendem a ser essas validações. A determinação de um certo nível de SIL traz consigo uma margem de redução da probabilidade de ocorrência de um sinistro, que por si auxilia quais práticas de projeto devem ser utilizadas no sistema pelos desenvolvedores do mesmo (JOANNOU; WASSYNG, 2014).

Para um projeto ser realizado, há duas maneiras de prosseguir com os níveis de integridade que ele seguirá, ou via análise de riscos feito por engenheiros contratados ou com base nas normas previamente especificadas para o domínio em questão. Por exemplo, uma vez estabelecidos os níveis de integridade para certo domínio, seja via análise ou normas, os projetistas de um APM, podem adequar os níveis de integridade desse sistema APM para estar em conformidade com os riscos toleráveis para o domínio em questão.

2.3 Normas de Segurança Aplicáveis a APMs

Com a finalidade de entender melhor as normas e o que cada uma delas exige em termos de segurança, segue uma descrição das normas citadas e a importância delas para um projeto do tipo *Automated People Mover*. Fazendo um adendo ao que foi dito, as normas presentes a seguir são muito mais complexas e extensas do que esse resumo aqui apresentado, além de abranger conceitos que não estão em estudo nesse trabalho.

2.3.1 IEC 61508

A IEC 61508 (IEC 1999) trata da segurança funcional de sistemas elétricos, eletrônicos e eletrônicos programáveis e serve como base para outras normas relacionadas com segurança (BELL, 2006).

O principal objetivo da norma é orientar o trabalho de equipes técnicas no desenvolvimento de equipamentos computacionais de segurança, visando alcançar níveis compatíveis com os exigidos por agências reguladoras em vários domínios de aplicação, incluindo os setores de óleo e gás, geração e distribuição de energia, máquinas e equipamentos, e transportes, entre outros (GALL, 2008).

Ainda relacionado a norma, a IEC 61508 visa fazer com que projetos desenvolvidos usando os padrões da norma e o desempenho desses mesmos sistemas possam alcançar metas toleráveis de risco, levando em conta tanto falha randômica de hardware como falhas sistêmicas, tanto em hardware quanto em software (Brown, 2000).

Para classificar os sistemas quanto às metas citadas anteriormente, a norma especifica quatro níveis de desempenho para uma função de segurança, chamados de níveis de integridade de segurança, SIL (*Safety Integrity Level*). O nível mais baixo corresponde a SIL 1, enquanto o mais alto corresponde ao SIL 4. Os requisitos para um determinado SIL são mais rigorosos a medida em que se aumenta o nível desse SIL.

No nível de comunicação de dados, a norma restringe a forma com que a comunicação é feita. O uso de qualquer aplicação que faça uso de comunicação de dados em sistemas seguros requer também que essa comunicação possua uma taxa de falhas que seja de acordo com os padrões estabelecidos.

Um aspecto importante relativo a IEC 61508 diz respeito ao fato de que, dado um sistema projetado em conformidade com a norma, qualquer subparte desse sistema também deve obedecer às diretrizes da norma. Ou seja, cada subsistema legado ao principal também deve estar em conformidade com a norma para que o sistema principal possa ser considerado de acordo com a IEC 61508. Então, para implementar uma comunicação segura em um APM, não bastaria somente ter um protocolo seguro, e sim toda a camada inferior de comunicação à do protocolo também necessitaria ser segura, fato que resultaria em um alto custo de implementação (GAJ; JASPERNEITE; FELSER, 2013).

Porém, há uma alternativa que está sendo utilizada que é a aplicação de um novo conceito, apresentado na norma IEC 61784-3, chamado de canal escuro (do inglês, *black channel*),o qual é necessário apenas que a camada inferior de comunicação não ultrapasse um certo limiar de falhas (KUNZ, G. De O., 2012).

2.3.2 IEC 61784-3

De modo a evitar certificar o canal no qual se transporta os dados de um protocolo seguro de comunicação, pode-se utilizar a abordagem do canal escuro de comunicação (*Black Channel*). Este canal implementa um protocolo de comunicação de mais baixo nível, que não precisa seguir as recomendações da norma, e que suporta um protocolo de mais alto nível, este sim responsável pela segurança da comunicação. A principal

vantagem do uso do *Black Channel* é que partes do canal de comunicação não precisam ser projetadas e validadas de acordo com a IEC 61508.

O conceito é extremamente útil para o desenvolvedor de sistemas de segurança. É possível, desta forma, usar uma pilha convencional de protocolos de comunicação e se concentrar apenas na codificação do topo da pilha. Protocolos de comunicação seguros como EtherCAT, PROFIsafe, INTERBUS, openSAFETY e FOUNDATION Fieldbus se apoiam no conceito de Black Channel (NEUMANN, 2007).

2.3.3 Protocolos de Comunicação Seguros

Protocolos de comunicação seguros são usados para transmitir informações de alta prioridade e na maioria das vezes cruciais para o funcionamento seguro de máquinas em uma linha de produção, plantas de processo, ou ambientes industriais semelhantes. Esse tipo de informação pode ser, no caso do Automated People Mover em questão, o não recebimento de um sinal pelo veículo, vindo da central em terra, para iniciar a frenagem ao se aproximar da estação, fazendo com que o veículo entre na estação com uma velocidade superior à permitida, podendo causar descarrilamento ou até mesmo uma colisão com outro veículo lá parado.

Enquanto as soluções de segurança tradicionais dependem de linhas de comunicação dedicadas para os sistemas poderem se comunicar e enviar mensagens entre si, protocolos seguros não precisam de nenhum tipo de cabeamento especial para transmitir informações. Isso se deve ao fato dos protocolos serem capazes de interagir com conexões pré-existente de Ethernet entre os dispositivos de controle e atuadores, sendo capaz de inserir mensagens de controle e monitoramento nessa rede (“EPSG_WDP_304_V-1-4-0(MANUAL OPENSAFETY).pdf”, [s.d.]).

- **Modelo de Falhas**

Erros na comunicação são ocasionados por falhas de hardware, interferência eletromagnética e outros tipos de interferência ambiental. O modelo de falhas do protocolo abrange erros de transmissão, repetições, perda de mensagens, inserção, sequenciamento, corrupção, atraso e mascaramento de mensagens.

Erros de transmissão ocorrem quando causas externas ocasionam dados corrompidos, como interferência eletromagnética anormal. Corrupção é semelhante a

erros de transmissão, mas tem como causa elementos do próprio sistema. Repetição ocorre quando mensagens velhas são repetidas, como em casos de perda de um sinal de "acknowledge".

Atrasos geralmente ocorrem quando os enlaces de comunicação estão saturados e as mensagens gastam mais tempo para circular do que o previsto ou uma queda de um enlace inteiro, fazendo com que a mensagem tenha que ser transmitida por um caminho mais longo. E por fim, o mascaramento mistura mensagens relevantes e sem relevância para a segurança.

- **Cobertura de Falhas**

Dentre os mais variados mecanismos aplicados para cobrir as falhas de comunicação mais comuns temos o 'timestamp'. Esse mecanismo nada mais é que a inserção de uma marcação de tempo na mensagem que apesar da simplicidade é extremamente eficaz. O uso do 'timestamp' previne a duplicação (ou dupla leitura), o embaralhamento da ordem das mensagens enviadas e até mesmo o atraso no recebimento de uma mensagem no receptor. Para que esse mecanismo funcione corretamente, o sistema depende de uma sincronia dos relógios entre o destino e o destinatário da mensagem, normalmente feito por relógios distribuídos. Normalmente, os protocolos seguros usam a técnica de 'watchdog timers' para monitorar os nodos em tempo real e garantir que os mesmos estão funcionando dentro da normalidade e também a sincronização de todos os sensores e/ou atuadores presentes no sistema.

Uma vez que se consegue garantir a ordem das mensagens, agora é necessário garantir que a mensagem original está inalterada, ou seja, que não houve corrupção de seus dados. Para isso a técnica mais confiável empregada é o CRC (cyclic redundancy check), onde uma chave é gerada em combinação com os dados no pacote e é anexada junto à mensagem. Assim, quem recebe a mensagem pode realizar a mesma operação sobre os dados e conferir com o resultado anexado pelo emissor da mensagem para garantir a integridade do pacote. Em caso de incoerência nos resultados, os dados são descartados.

2.3.4 Norma ASCE Automated People Mover Standards

Este padrão estabelece o conjunto mínimo de requisitos necessários para atingir um nível aceitável de segurança e desempenho de um sistema de APM. Como tal, pode ser utilizado no processo de certificação de segurança. O objetivo global desta norma é ajudar a indústria e o público através do estabelecimento de normas para os sistemas movimentadores automatizados de pessoas. Esta norma inclui requisitos mínimos para a concepção, construção, operação e manutenção de sistemas de APM (AMERICAN SOCIETY OF CIVIL ENGINEERS, 2006a). Dentre os diversos requisitos apresentados pela norma ASCE, apenas serão exibidos nesse trabalho os requisitos relativos a funções de segurança cuja implementação pode exigir protocolos seguros de comunicação para o controle dos APMs.

A. Detecção de Presença (*Presence Detection*)

Em um sistema automatizado, como o caso de um movimentador de pessoas, a detecção de todo e qualquer trem/veículo deve ser feita antes do sistema iniciar e ser contínua durante toda a operação desse sistema até o mesmo de ser desligado, garantindo assim o conhecimento da localização exata de todos os veículos independente da sua forma de operação (manual ou automatizada).

B. Garantia de Separação (*Separation Assurance*)

Em sistemas automatizados, é uma função básica e de mais alto grau de importância a garantia que veículos controlados por softwares mantenham uma distância mínima entre eles. Esse requisito evitará colisões frontais entre veículos trafegando em sentidos opostos na mesma via e traseiras entre veículos que seguem um mesmo sentido em determinado trilho. Essa garantia de separação é feita usando o pior caso imaginável no sistema, onde dado que um trem possa parar imediatamente, quão distante o trem que se aproxima do trem parado precisa estar para poder frear sem que haja colisão.

C. Detecção de Movimento não Intencional (*Unintentional Motion Detection*)

Esse requisito propõe que se um veículo realizar um deslocamento impróprio sobre a via, o mesmo deve ter seus freios de emergência acionados

imediatamente, seja esse movimento um deslize no sentido que está se movendo ou no sentido oposto ao sentido permitido.

D. Proteção contra Excesso de Velocidade (*Overspeed Protection*)

Requisito necessário para evitar acidentes com os veículos que estão em movimento nos trilhos, uma vez que regula a velocidade máxima permitida em qualquer trecho da via. O dispositivo de controle deve monitorar continuamente a velocidade do veículo e em casos de o mesmo ultrapassar a velocidade máxima da via, os freios de emergência devem ser acionados.

E. Proteção de Final de Via (*Overtravel Protection*)

Requisito imposto para sistemas APMs que permitam que os trens automatizados operem próximo a fins de linha. Esse requisito deve atuar conjuntamente com o requisito de garantia de separação e excesso de velocidade, para evitar colisões com os dispositivos de amortecimento localizados no final de linhas.

F. Proteção para Sistemas Parciais (*Parted Consist Protection*)

Esse requisito é aplicável a sistemas que permitam que dois ou mais veículos automatizados particionados possam se unir para compor um trem. Esse requisito deve atuar sobre veículos que possam eventualmente ou não se separar para compor diversos tamanhos de trem. Além disso, é responsável também por monitorar eventuais espaçamentos e/ou acoplamentos indesejado.

G. Proteção contra Perda de Sinal (*Lost Signal Protection*)

Listado como um dos mais importantes requisitos de um sistema APM, a proteção contra perdas de sinais de controle deve ser de suma importância para evitar acidentes. Independente das características de transmissão (periódicos ou contínuos), a ausência desse sinal deve resultar na frenagem de todos os veículos presentes no sistema.

H. Detecção de Ausência de Movimento (*Zero Speed Detection*)

Em sistemas APMs que paradas em estações são esperadas, a detecção que um veículo atingiu uma “velocidade zero” somente é registrada se sua velocidade é inferior a 0.3 m/s e o sinal de frenagem está ativo.

I. Abertura de Porta não Programada (*Unscheduled Door Opening Protection*)

Quando o veículo está em movimento e/ou fora da estação e o acionamento de abertura de portas ou portas de emergência é feito, o veículo deve realizar frenagem de emergência até uma parada total. Esse requisito é necessário para garantir a segurança dos passageiros do veículo.

J. Proteção de Travamento de Portas (*Door Control Protection Interlocks*)

Em um sistema APM, onde há embarque e desembarque em estações pré-definidas, esse requisito impõe algumas condições para ser atendido, como ausência de movimento detectada, alinhamento com a estação definida e propulsão suspensa.

K. Travamento de Portas para Partida (*Departure Interlocks*)

Esse requisito faz referência ao momento que antecede o início do movimento do veículo, uma vez que é necessário que todas as portas estejam fechadas e travadas para que o veículo possa começar a acelerar na via.

L. Travamento de Direção Reversa (*Direction Reversal Interlocks*)

O travamento de movimento na direção reversa deve ser garantido para sistemas automatizados que possibilitam que seus veículos trafeguem em ambos os sentidos da via, ou em casos de terminais de linha para manobras e/ou troca de sentido após acoplamento (em sistemas fechados).

M. Travamento de Propulsão e Frenagem (*Propulsion and Braking Interlocks*)

Esse requisito é necessário em qualquer sistema automatizado, onde dada uma falha ou condição que leve à uma falha os freios de emergência devem ser acionados e esse comando deve ser mantido até a frenagem total do veículo. Esse travamento faz menção ao comando de frenagem, que não pode ser sobreposto por nenhum outro comando até atingir a “velocidade zero”, dando uma prioridade superior ao comando frenagem sobre qualquer outro sinal recebido.

N. Travamento de Troca de Trilhos (Guideway Switch Interlocks)

Esse requisito é de suma importância para APMs que permitam que os veículos troquem de trilhos durante um percurso através de dispositivos instalados ao longo do percurso, como por exemplo, um trilho de desvio acionado pela passagem do veículo em certo ponto da via. Ele impõe que dado desvio só pode ser acionado antes de o veículo chegar nele ou somente após a travessia ter sido concluída, de modo a evitar o acionamento durante a transição desse veículo que acarretaria em um acidente, como por exemplo o descarrilamento dos trilhos.

2.4 Normas e Certificação no Brasil

Em linhas gerais, certificação de projeto, ou somente certificação, pode ser definido como o objetivo de verificar que um dado produto ou serviço que remeta segurança (por exemplo, setor de energia ou automação), fornecido por algum ator da indústria, de fato entrega os produtos ou serviços seguros. A certificação de projeto é dependente do domínio em que esse projeto se situa e com base na norma desse domínio é que o certificador analisará o projeto.

O ato de certificar um produto/serviço envolve normalmente um candidato (o produto ou serviço), um regulamento, uma autoridade certificadora (por exemplo, TÜV) e um organismo de avaliação (BAUFRETON *et al.*, 2010).

Na grande maioria das vezes, o regulamento é estabelecido por organizações internacionais que cooperam entre si para estabelecer padrões e regras (boas práticas) de projeto que ajudam a prevenir riscos. Como por exemplo, o sistema ferroviário europeu é composto por diversos países que, através de acordos, chegaram a um consenso sobre boas práticas e regras para a indústria ferroviária, facilitando assim a homogeneização do sistema, seja ele em trilhos iguais, sistema de placas e avisos e até mesmo supervisão dos trens.

Assim como existe a criação de padrões para o âmbito internacional e agências fiscalizadores e certificadoras, há também segmentos da indústria para os quais não existem agentes fiscalizadores e/ou certificadores para questões de segurança funcional, como é o caso da indústria automotiva e no caso brasileiro, os movimentadores automatizados de pessoas. Mas, apesar de não possuírem uma certificação funcional para o "todo", as partes que compõe tanto os veículos da indústria automotiva quanto os APMs

no Brasil precisam seguir as especificações técnicas de seu domínio, que é o caso por exemplo dos freios, aceleradores, amortecedores entre outros componentes presentes no veículo. As especificações técnicas precisam serem seguidas para o funcionamento adequado do mesmo e também para poderem serem comercializadas (só existe autorização de venda se há conformidade com as especificações de domínio) junto ao produto final, veículos automotivos ou APMs.

Vale salientar, que para todos os casos de certificação, caso ocorra um sinistro com o produto/serviço oferecido, a responsabilidade não recai sobre a entidade certificadora e sim sobre a entidade responsável por vender aquele produto (BAUFRETON *et al.*, 2010). Por exemplo, em caso de um acidente de veículos automotivos onde foi constatada falha em algum componente do mesmo, a única entidade passível de processo é a montadora do veículo, ou em casos mais particulares, a indústria responsável pela produção do componente, jamais a entidade que certificou o componente.

Diferentemente do cenário internacional, as normas utilizadas no Brasil e o caso de certificação de projetos sobre APMs sofrem algumas mudanças consideráveis quando comparadas com normas mais tradicionais, como a norma americana ASCE. Utilizando a norma ASCE como referência e comparando-a com a norma brasileira para movimentadores automatizados de pessoas, a norma NBR 16074, notamos uma simplificação da norma, não em termos de casos cobertos, mas no abreviamento desses casos.

Outro diferencial, e até mais curioso que o citado anteriormente, é o fato da norma brasileira NBR 16074 não mencionar em nenhum momento a necessidade de uma entidade certificadora ou mesmo uma certificação para o projeto de um movimentador automatizado de pessoas. Tal fato pode gerar até uma desconfiança quanto as garantias que o projeto deveria oferecer uma vez que não há qualquer agência certificadora para vistoriar se aquilo que foi proposto e aplicado está de fato em concordância com a norma utilizada como base para o projeto.

Para melhor ilustrar a problemática acima basta escolhermos outro meio de transporte similar ao APM, como um metrô ou trem de passageiros, onde as características são muito próximas, como o fato de transportarem pessoas, serem veículos que se movimentam sobre trilhos, possuem composições de vários tamanhos entre outras similaridades. Para um projeto de metrô ser aprovado, existe a necessidade de

certificações por entidades certificadoras externas ao projeto, assim como para trens de passageiros e outros meios de transporte para grandes quantidades de pessoas.

3 TOPOLOGIAS DE VIAS SOBRE TRILHOS

Vias de circulação de veículos sobre trilhos, como o caso de metrô, trens e APMs apresentam diferenças consideráveis entre si apesar de serem projetados para veículos que circulam sobre trilhos. Além das vias, esses sistemas são bastante diferentes entre si em relação da quantidade de usuários que frequentam cada sistema, das normas de segurança que cada sistema deve seguir e a rigidez dessas normas e das funções de segurança que devem estar presentes em cada domínio (metrô, trem ou APM).

Em relação às vias de circulação, as diferenças começam pelo modo como elas são construídas, por exemplo, o metrô apresenta vias subterrâneas e/ou a céu aberto além de possuir diversas intersecções de trilhos e cruzamentos de linhas, além disso pode haver ainda mais de um veículo circulando sobre o mesmo trilho e no mesmo sentido. No caso de trens de passageiros, esses possuem vias majoritariamente a céu aberto, possuem túneis e pontes em seus trajetos e também há uma grande quantidade de cruzamentos ao longo da sua extensão, também permitem mais de um trem trafegando no mesmo sentido pelo mesmo trilho e costumam percorrer distâncias maiores que metrôs. Por último, nos APMs, as vias são de caráter elevado ao solo, sem cruzamentos de trilhos e de distâncias curtas, não é permitido que mais de um veículo circule no mesmo trecho ao mesmo tempo, em outras palavras, exclusividade de via (WARREN, 2000).

Já a quantidade de usuários no sistema caracteriza a real diferença entre eles, pois é esse fator que faz com que as normas e, consequentemente, as funções de segurança presentes em cada sistema venham a ser mais rigorosas à medida que envolvem um maior número de pessoas. Tomando por exemplo o metrô de São Paulo –SP, a estação da Sé que possui as linhas mais movimentadas da cidade teve uma média de quinhentos mil usuários (entre embarque e desembarque) por dia no ano de 2016 ("Demanda | Portal da Transparência", [s.d.]).

Em relação a trens temos como exemplo a malha ferroviária francesa, em especial a estação Gare du Nord que no ano de 2013 alcançou um total de setecentos mil usuários (entre embarque e desembarque) por dia. E por fim, para o caso do APM citamos o movimentador automatizado de pessoas de Detroit, um dos mais movimentados do mundo que opera diariamente no transporte de seis mil pessoas entre suas treze estações (projetado para uma capacidade efetiva de até sessenta e sete mil pessoas por dia) ("About DPM | The People Mover.com").

Observando a diferença entre os sistemas, principalmente no quesito de usuários que frequentam esses sistemas, podemos imaginar que as normas de segurança, as funções de segurança e os níveis de SIL precisam ser diferentes para cada domínio. Supondo que ocorra uma falha no sistema de frenagem de um metrô, trem e em um APM, e essa falha origine um erro que por sua vez possa vir a transformar-se em um defeito e causar um acidente. A forma com que essa falha é tratada é um resultado da aplicação das funções de segurança implementadas em cada sistema, quão efetivas são essas funções de segurança (depende da norma do domínio) e quanto elas minimizam o risco dessa falha de fato vir a transformar-se em um erro.

Nesse cenário, a possibilidade de isso acontecer no sistema é particular de cada um e precisa haver um tratamento dessa falha ou uma contramedida (função de segurança) que seja relacionado ao SIL especificado ao domínio para evitar que ocorra um sinistro. Devido a essa diferença dos sistemas, as normas tendem a serem mais severas e o nível de SIL mais alto à medida que temos uma quantidade maior de usuários sendo transportados, pois quando relacionado com a quantidade de usuários presentes durante o sinistro, é expressiva a diferença de um domínio para o outro.

3.1 Topologias de Vias de um APM

Dentre as mais variadas topologias de vias possíveis e utilizáveis atualmente, a análise será restrita a vias básicas para demonstrar os requisitos exigidos pelas normas de segurança funcional e abstrair a complexidade da via em si. Assim, para cada topologia idealizada, será feito um estudo dos requisitos da norma para melhor entender as suas exigências no projeto de um APM.

A exigência de requisitos de segurança funcional aumenta à medida que os sistemas ficam maiores e demandam uma maior complexidade tanto do projeto quanto do funcionamento do sistema. Como exemplo disso, temos o caso da existência de mais de um veículo circulando ao mesmo tempo, de modo a atingir uma taxa de vazão no sistema aceitável, o sentido de circulação dos APMs em caso de algum desvio necessário, a existência ou não de intersecções no trajeto e se o sistema é escalável.

A escolha das topologias de vias aqui apresentadas se justifica por serem vias simples, que estão presentes em grande parte dos APMs funcionais da atualidade e são compostas basicamente por retas, curvas pouco acentuadas e desvios de trilho (vias secundárias ou de manutenção). Como exemplo de sistemas APMs podemos citar o

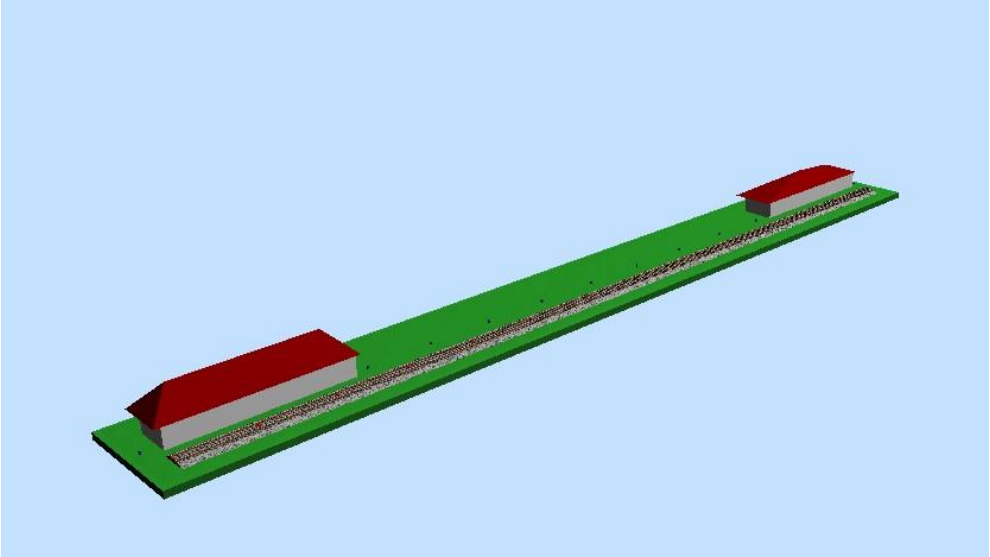
Aeromóvel de Porto Alegre – RS que é constituído por uma reta prolongada ligando duas estações e com poucas curvas em sua extensão ou o projeto do APM de Canoas – RS, que possui retas extensas, algumas curvas e troca de trilho entre estações. Ou ainda, sistemas presentes fora do Brasil, como o APM de Morgantown – EUA, cujo sistema mais complexo e com maiores opções de movimentação dos veículos é de interesse para o estudo a seguir (RANEY; YOUNG, 2000).

Logo a seguir estão listadas algumas topologias idealizadas para o estudo, onde cada uma delas apresenta requisitos de segurança diferentes e necessários para o funcionamento do movimentador automatizado de pessoas.

- Topologia com trilho retilíneo entre duas estações.

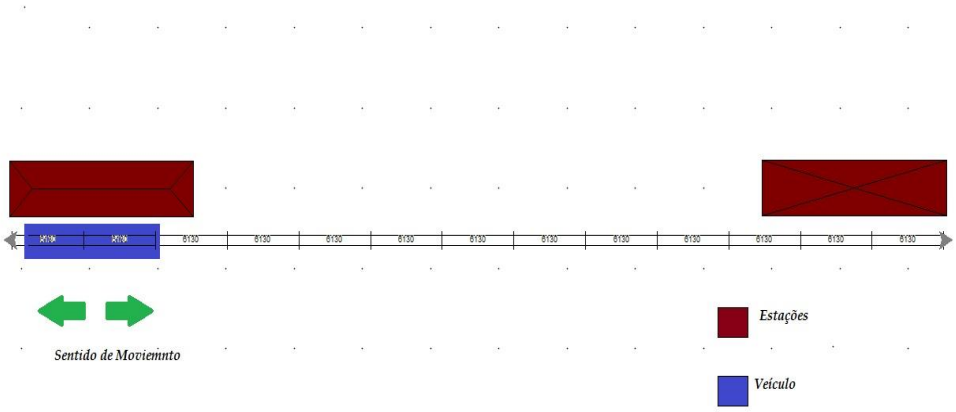
A topologia mostrada nas figuras 3.1 e 3.2 é uma via em linha reta, sem curvas, intersecções, obstáculos ou outros veículos que possam circular no mesmo trilho. Como se trata de um sistema fechado, sem trocas de trilhos e demais veículos, o fluxo de operação se dá exclusivamente pela partida do veículo de uma estação até a outra extremidade da linha, onde se situa a segunda estação. Ao chegar na estação, ocorre embarque/desembarque de passageiros, o sentido de movimento do veículo é alterado, de modo que o mesmo retorne à estação de origem pelo mesmo trilho, completando assim o percurso.

Figura 3.1 - Visão 3D da topologia com trilho retilíneo



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Figura 3.2 - Visão Aérea da topologia com trilho retilíneo

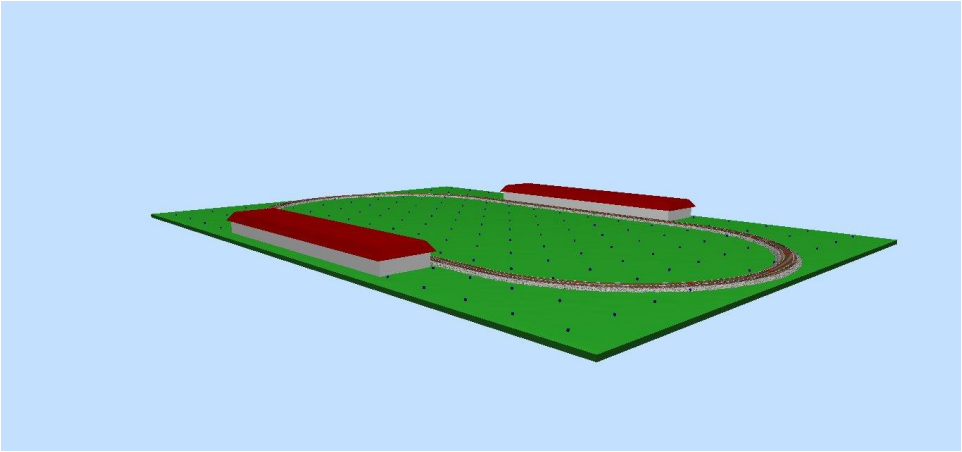


Fonte: SCARM – Simple Computer Aided Raillway Modeller

- Topologia com trilhos circulares com duas estações.

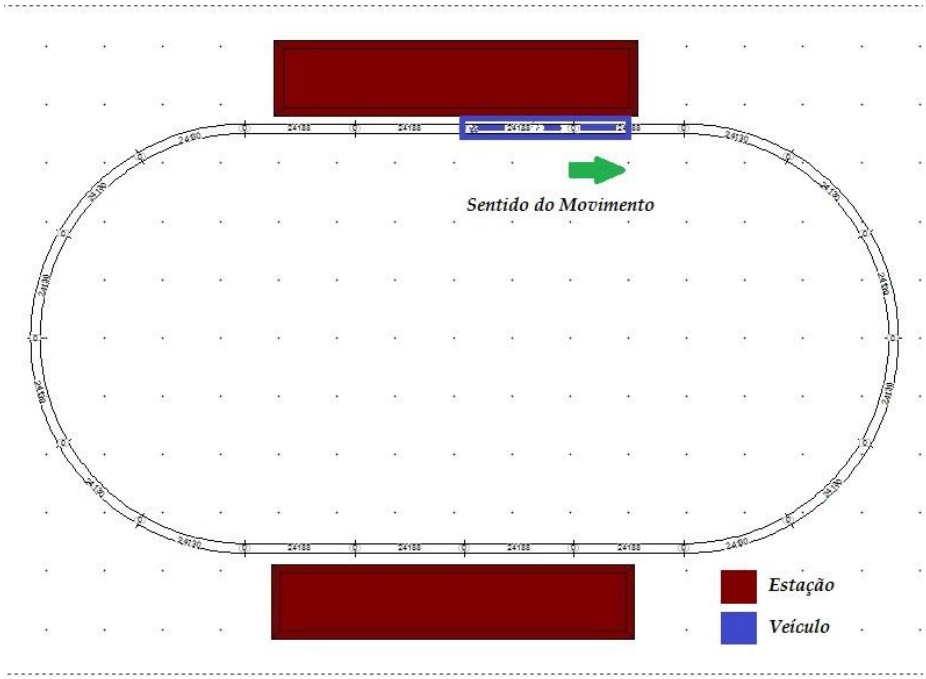
Em uma topologia de vias como essa descrita pelas figuras 3.3 e 3.4, nota-se que é uma via de caráter circular, com curvas leves e prolongadas, sem intersecções de trilhos ou cruzamentos e com somente um veículo trafegando na sua extensão. Tratando de um sistema fechado, onde não há entradas ou saídas de objetos do sistema, a operação do sistema inicia pela partida do veículo de uma estação. Ao chegar na curva pode haver uma desaceleração do mesmo para efetuar o movimento curvilíneo. Ao chegar na estação ocorre o embarque/desembarque de passageiros e o veículo segue, com o mesmo sentido de movimento para a estação de origem, completando assim o percurso.

Figura 3.3 - Visão 3D da topologia com trilhos circulares com duas estações e um veículo.



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Figura 3.4 - Visão Aérea da topologia com trilhos circulares com duas estações e um veículo.

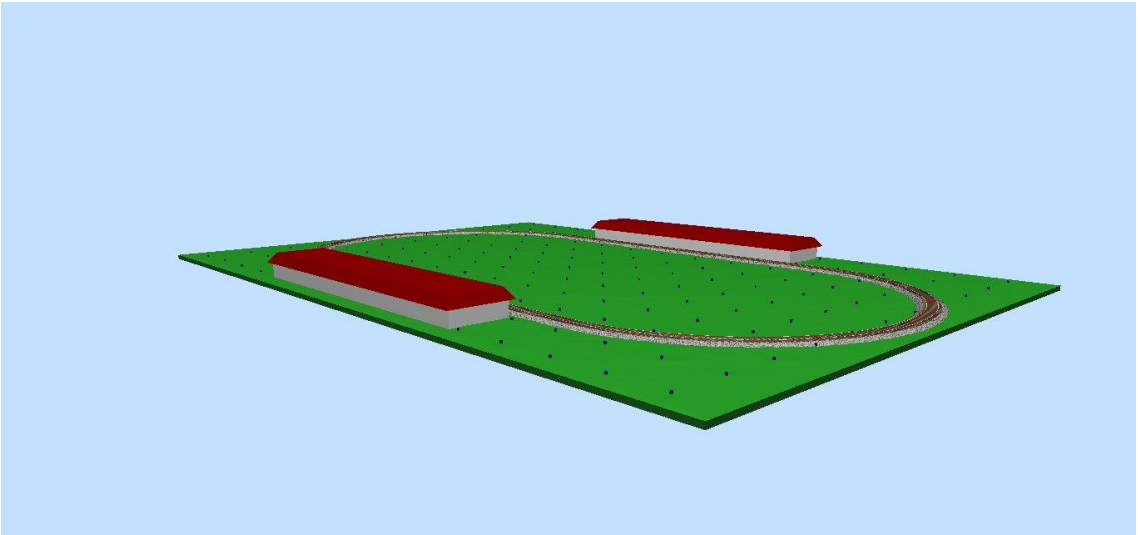


Fonte: SCARM – Simple Computer Aided Raillway Modeller

- Uma topologia circular, com duas estações e dois veículos.

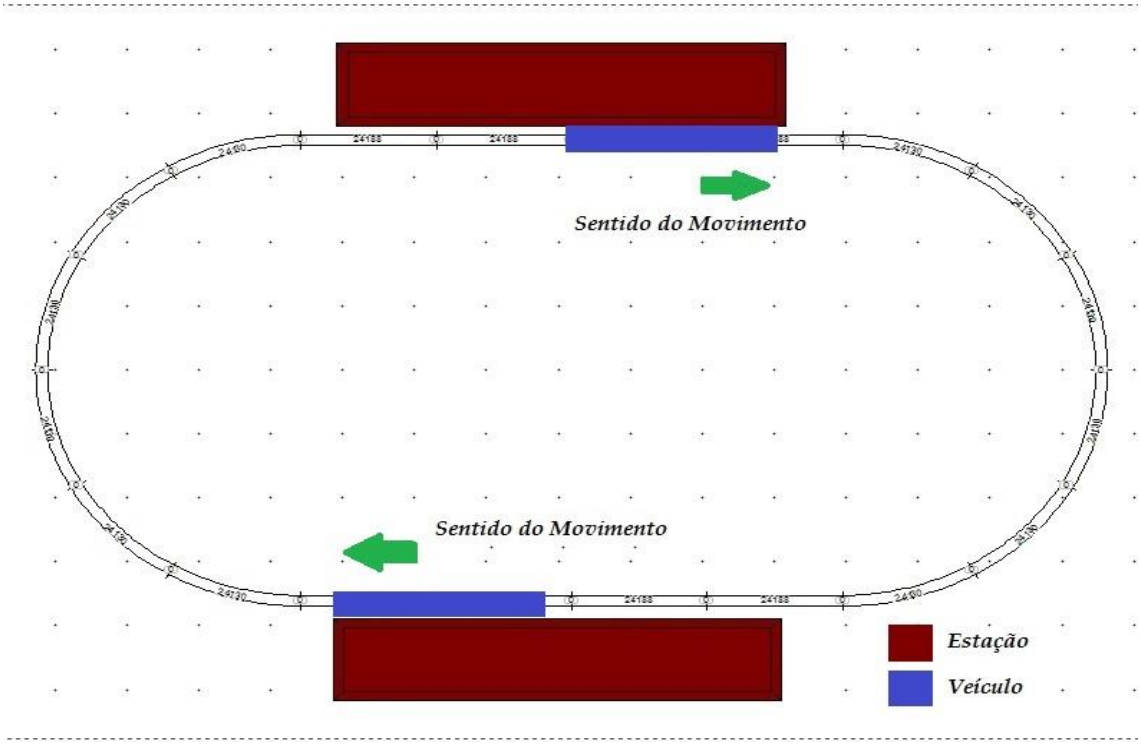
A topologia de vias como essa descrita pelas figuras 3.5 e 3.6, é uma via de caráter circular, similar a anterior, com curvas leves e prolongadas, sem intersecções de trilhos ou cruzamentos mas possui um segundo veículo operando no sistema. Tratando de um sistema fechado, onde não há entradas ou saídas de objetos do sistema, a operação do sistema se dá pela partida de um dos veículos de uma estação, não necessariamente ao mesmo tempo da partida do segundo veículo da outra estação e ambos circulam no mesmo sentido (sentido horário, por exemplo). Ao chegarem nas estações ocorre o embarque/desembarque de passageiros para os dois veículos. Após ambos terem completado essa etapa, os dois continuam o trajeto, com o mesmo sentido de movimento para as estações de origem que cada um partiu, completando assim o percurso.

Figura 3.5 - Visão 3D da topologia com trilhos circulares, com duas estações e dois veículos.



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Figura 3.6 – Visão Aérea da topologia com trilhos circulares, com duas estações e dois veículos.



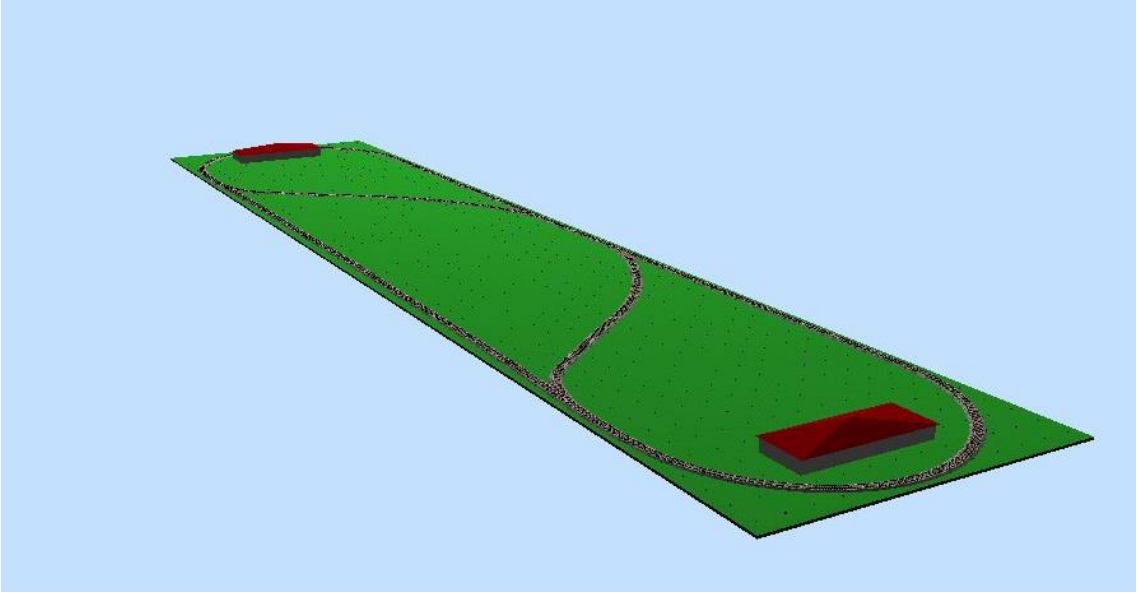
Fonte: SCARM – Simple Computer Aided Raillway Modeller

- Uma topologia circular com duas estações e intersecções de trilhos.

Esta topologia proposta acima é representada visualmente pelas figuras 3.7 e 3.8 e trata-se de uma via circular, com duas estações e um único veículo, mas diferente das demais por ser possível a troca de trilhos pelo veículo, utilizando vias auxiliares e mecanismos para o chaveamento de trilhos. Como as demais topologias, é um sistema fechado, sem a possibilidade de um veículo sair ou entrar na via, porém seu funcionamento é diferente.

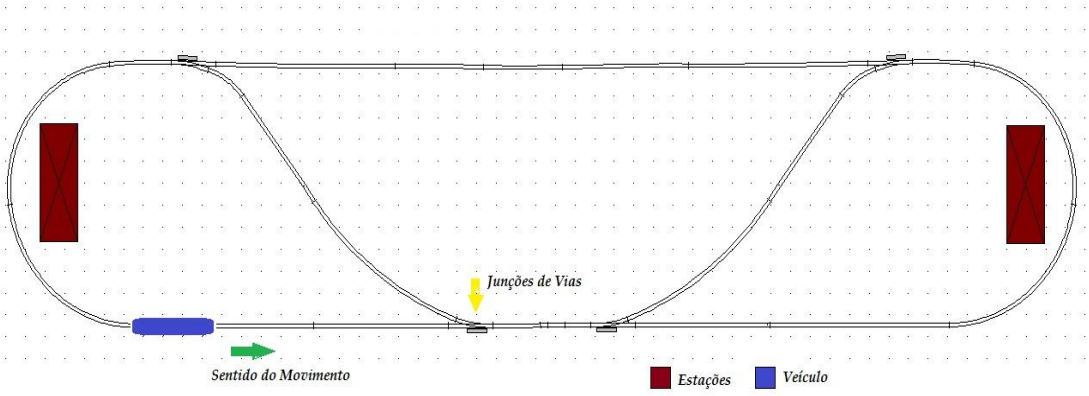
Nesse caso, o veículo parte da estação de origem e realiza o trajeto circular padrão pela via até chegar na outra estação para efetuar o embarque/desembarque de passageiros. Porém, essa topologia foi projetada com um nível de redundância na via, ou seja, caso trechos específicos do trajeto estejam com problemas, é possível manter a operação do sistema utilizando as vias secundárias através de junções de vias (vide figura 4.9). Assim, fazendo com que o veículo trafegue pela via auxiliar, entre na via padrão, mas pelo sentido oposto, trafegue até a próxima junção e retorne ao trajeto inicial utilizando a via auxiliar novamente, até concluir seu trajeto e chegar na estação de destino.

Figura 3.7 – Visão 3D da topologia circular com duas estações e intersecções de trilhos.



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Figura 3.8 – Visão Aérea da topologia circular com duas estações e intersecções de trilhos.



Fonte: SCARM – Simple Computer Aided Raillway Modeller

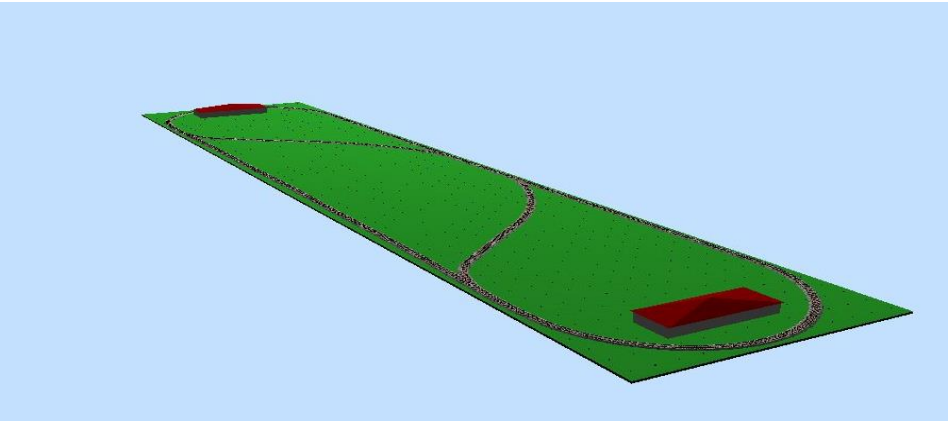
- Uma topologia circular com duas estações, com intersecção de trilhos e dois veículos

Esta topologia proposta acima é representada visualmente pelas figuras 3.9 e 3.10, percebe-se que se trata de uma via circular, com duas estações e dois veículos e é possível a troca de trilhos pelos veículos, utilizando vias auxiliares e mecanismos para o chaveamento de trilhos. Como as demais topologias, é um sistema fechado, sem a possibilidade de um veículo sair ou entrar na via, porém seu funcionamento com dois trens é um pouco mais complexo que a topologia anterior.

Nesse caso, os veículos partem das estações de origem e realizam o trajeto circular padrão pela via, ambos trafegando no mesmo sentido (sentido anti-horário, nesse caso) até chegarem na outra estação para efetuar o embarque/desembarque de passageiros. Novamente, essa topologia foi projetada com um nível de redundância na via, ou seja, caso trechos específicos do trajeto estejam com problemas, é possível manter a operação do sistema utilizando as vias secundárias através de junções de vias (vide figura 4.9).

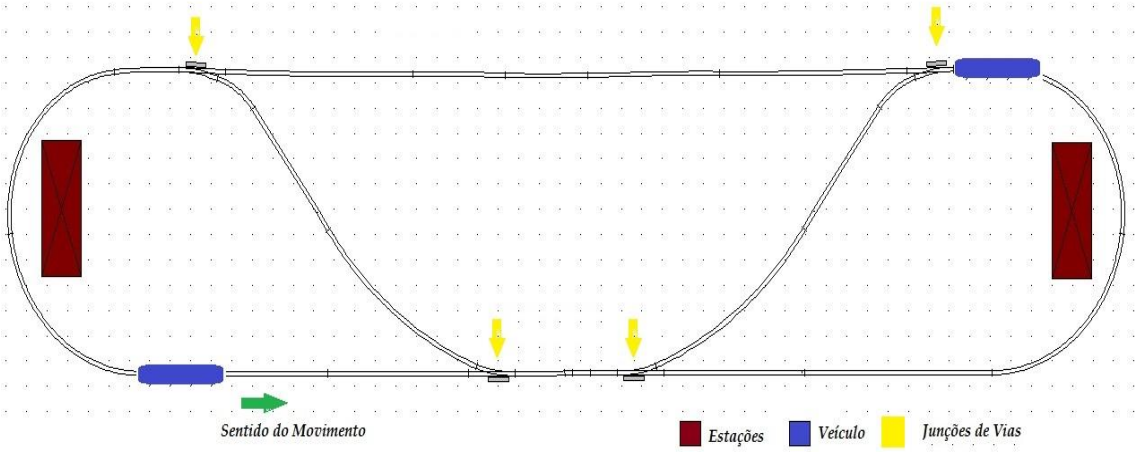
Assim, fazendo com que o veículo trafegue pela via auxiliar, entre na via padrão, mas pelo sentido oposto, trafegue até a próxima junção e retorne ao trajeto inicial utilizando a via auxiliar novamente, até concluir seu trajeto e chegar na estação de destino. Porém, nessa topologia, como há dois veículos circulando, o uso e a ativações de junções de vias deve ser projetado com cautela para evitar que veículos circulem em um mesmo trecho, mas em sentidos opostos.

Figura 3.9 – Visão 3D da topologia circular com duas estações, com intersecção de trilhos e dois veículos.



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Figura 3.10 – Visão Aérea da topologia circular com duas estações, com intersecção de trilhos e dois veículos.



Fonte: SCARM – Simple Computer Aided Raillway Modeller

3.2 Análise de Falhas em um APM

Em um sistema de vias elevadas e exclusivas, como o caso dos APMs, a presença de falhas dos mais variados gêneros pode ser possível. Como exemplo disso podem ser citadas falhas mecânicas nos sistemas de frenagem ou aceleração do veículo, seja por desgaste ou avaria em alguma peça ou algum sinistro mecânico ocorrido durante o trajeto (sistema de frenagem "emperrou" durante o acionamento).

Além de falhas mecânicas, há outras partes do sistema que podem ser passíveis de ocorrência de falhas, como a parte estrutural do sistema. Por exemplo, uma falha na construção das vigas de sustentação do trilho ou na própria estrutura do trilho devido ao uso de materiais de baixa qualidade ou impuros, que comprometeram a integridade da viga durante uma variação de pressão/temperatura na mesma.

Falhas elétricas dentro do veículo também são possíveis, como um curto circuito no sistema de abertura/fechamento de portas do veículo originado por uma falha no isolamento elétrico do veículo. E ainda é possível ter falhas no sistema de comunicação do APM, normalmente presentes no link de comunicação entre a estação de controle e o veículo, devido a mascaramento de mensagem, interferência eletromagnética ou atraso na propagação das mensagens devido à fragilidade do protocolo empregado na comunicação do sistema.

Levando em consideração as falhas previamente citadas e examinando as topologias idealizadas no item 3.1, nota-se que as falhas estruturais, elétricas, mecânicas e de comunicação trazem um risco considerável consigo, pois se não forem devidamente tratadas, podem colocar o sistema inteiro em risco. Caso uma falha estrutural ocorra, se não tratada pode haver um desmoronamento da estrutura da via, assim como uma falha mecânica não tratada pode levar o sistema a ser incapaz de realizar frenagem/propulsão.

E ainda, falhas elétricas sem contramedidas podem causar curto-circuito no sistema e prejudicar tanto os atuadores presentes no veículo, o próprio sistema de comunicação ou até mesmo eletrocutar um passageiro. E por fim, falhas no sistema de comunicação sem redundância ou em outra função de segurança podem ocasionar acionamentos indesejados de freios ou propulsores que podem levar o veículo a causar um acidente.

Como o escopo do trabalho é a análise das falhas de comunicação em relação as funções de segurança previstas pela norma, estas serão abordadas com mais detalhes no item 3.3 desse trabalho. Além disso, vale lembrar que para a maioria dos sistemas projetados, com foco em segurança, possuem um plano de segurança, onde é exigido que se faça uma análise teórica prévia das ameaças possíveis ao sistema e vulnerabilidades do mesmo. Esse plano, se bem executado, é uma forma de melhorar a prevenção de falhas no sistema assim como identificar pontos críticos e delicados do mesmo (AMERICAN SOCIETY OF CIVIL ENGINEERS, 2006b).

3.3 Falhas de Comunicação em um APM

Como as falhas de comunicação mais comuns de ocorrerem em uma transmissão de dados, cujo tratamento cabe ao protocolo seguro utilizado, foi assunto abordado na seção 2.3.3 desse trabalho, cabe aqui a análise das consequências dessas falhas quando não tratadas em um sistema APM. Para isso, antes de efetivamente começar a análise, precisamos idealizar o funcionamento do sistema de controle de um sistema movimentador de pessoas automatizado, a fim de fazer uso desse modelo para analisar como as falhas afetam o funcionamento do sistema e como esse reage na presença dessas falhas.

3.3.1 Modelo de um Sistema de Controle

Assim, abstraindo detalhes físicos do veículo como modo de propulsão (pneumática ou elétrica) ou número de portas, uma vez que não são detalhes de interesse no momento, começaremos pelo sistema de controle automatizado (ATC) do veículo. Ainda, como a norma ASCE não faz referência de como o sistema de controle, proteção, operação e supervisão (ATC, ATP, ATO e ATS respectivamente) de um APM deve ser implementado nem onde os mesmos devem ser situados, supomos, dessa forma, que o APM aqui modelado possui todo seu ATC centralizado na estação de comando do sistema, assim como os subsistemas ATO, ATP e ATS do mesmo.

Isso implica que todo o controle dos veículos (a operação, proteção e supervisão) se dá pela comunicação entre a central de controle e os veículos presentes no sistema. Uma vez tendo o controle centralizado, a central de controle é responsável pelo acionamento de propulsão/frenagem dos veículos, detecção de movimento não intencional, reconhecimento de final de trilhos, localização de cada veículo que compõe o sistema e acionamento de medidas de segurança (acionamento remoto quando for possível, caso contrário, contramedidas locais podem ser executadas) caso alguma função seja mal executada pelo veículo.

Como o veículo é comandado a distância, cada sinal de comando recebido pelo veículo é designado aos atuadores do mesmo, os quais são responsáveis por realizar as operações normais do sistema solicitadas pela central de comando ou funções de segurança que operam, em caso de falhas, sobre os atuadores. Assim, cabe ao veículo, no

momento de uma solicitação, acionar os mecanismos responsáveis para a correta execução dos comandos recebidos.

E, em caso de algum mecanismo falhar, o veículo deve ser capaz de enviar mensagem para a central para que essa solicite o acionamento das medidas de segurança aplicáveis. Vale ressaltar que em alguns casos, as funções de segurança do veículo podem ser acionadas diretamente por subsistemas dentro do veículo, para evitar casos onde o link de comunicação fique indisponível e o veículo fique sem controle algum.

Apesar do sistema de controle ser inteiramente externo ao veículo, algumas funções de segurança que a norma propõe são executadas sem necessidade de comunicação com a central em terra. Essas funções de segurança não necessitam de uma visão global do sistema (visão que a central de comando possui de toda a rede APM), mas apenas uma visão local, ou seja, a visão do próprio veículo em si. Como por exemplo dessas funções locais, o controle de excesso de velocidade pode ser controlado localmente com o uso de um acelerômetro no veículo ou o fechamento de portas em uma estação com o uso de um timer que se inicia no momento de abertura das portas do veículo.

3.4 Análise de Falhas de Comunicação em um APM

Como visto anteriormente na seção 2.3.3, entre as falhas de comunicação mais comuns que acontecem em uma transmissão de dados temos o atraso de envio de mensagens, mascaramento de mensagens e ainda pode ocorrer corrupção de dados por interferência. Esses tipos de falhas passíveis de acontecer, para um sistema automatizado orientado a comunicação, podem trazer um alto risco a integridade do sistema se não forem tratadas. Para melhor exemplificar, tomamos a topologia circular idealizada com somente um veículo transitando e o sistema de controle proposto anteriormente.

Nesse modelo de sistema APM, onde o veículo é equipado com atuadores e um sistema de comunicação para que o controle possa ser efetuado, qualquer problema na transmissão de uma mensagem entre a central e o veículo pode fazer com que o sistema entre em um estado de perigo. Supomos que uma mensagem seja enviada pelo ATO do sistema, contendo um comando para que o veículo comece o processo de frenagem por se aproximar de uma estação. Caso a mensagem sofra algum atraso no link ou perdida por uma interferência, na visão do veículo tudo está funcionando normalmente, pois ele não tem conhecimento que houve uma perda de mensagem.

Para a estação, o não recebimento de confirmação por parte do veículo (um sinal de "*acknowledge*") representa que houve uma falha na comunicação, porém não há como

saber se a falha ocorreu no envio da mensagem da estação para o veículo ou da resposta do veículo para a estação. Assim sendo, a estação pode tentar o reenvio da mensagem e receber um sinal de "*ack*" do veículo ou novamente pode haver silêncio no enlace (sem confirmação de recebimento por parte do veículo).

Caso não haja comunicação entre o veículo e a central, é necessário que haja mecanismos de redundância para supervisionar essa comunicação, seja um outro enlace de comunicação, o emprego de outro protocolo de comunicação ou a utilização de envio mensagens periódicas entre o veículo e a estação para garantir que a comunicação está sendo feita. Na maioria dos casos, o emprego de uma comunicação periódica é o modo mais usado e fácil de se detectar ausência de comunicação na rede, uma vez que um dos pares da comunicação cessar o envio de seus "*ticks*", o outro lado saberá que foi perdida a comunicação que havia entre eles.

Por exemplo, supondo que um veículo APM e sua central estão usando esse mecanismo para garantir que há comunicação entre eles e em determinado momento T o envio do sinal por um dos participantes da comunicação não é mais detectado, se no tempo $T+t$, sento 't' uma grandeza temporal, ainda não houve resposta mesmo com o reenvio do sinal, é tido que a comunicação foi perdida e houve uma falha de comunicação. Nesse momento é preciso que alguma função de segurança, responsável por "escutar" o link de comunicação, possa atuar sobre o sistema que está apresentado a falha de modo a levar o sistema a um estado seguro. No caso da norma ASCE, a orientação dada é que na detecção de ausência de sinal/comunicação, os freios de emergência devem ser acionados por todos os veículos presentes no sistema.

Para concluir essa questão sobre utilização ou não de protocolos seguros e outras contramedidas, vale a pena ressaltar que o emprego de protocolos seguros é um fator que contribui para redução de riscos e não a extinção deles. Ainda, caso não se use protocolos seguros, como alguns citados nesse trabalho, outros mecanismos precisam estar presentes nos sistemas para proporcionar uma maior segurança em casos de falha. Como exemplos desses mecanismos ou técnicas, temos o uso de redundância e mecanismos de detecção e correção de erros, que, se empregados, diminuem também o risco que as falhas proporcionam. Enfim, independentemente dos métodos usados, é de fundamental importância que exista medidas de correção no sistema para conter situações emergenciais.

4 DADOS ANALÍTICOS DE UM APM

Para a análise de caso no escopo deste trabalho, é usado um modelo onde as únicas grandezas de interesse são a velocidade máxima que o veículo atinge e a taxa de frenagem que ele pode exercer. Dados como distância de percurso, tempo de trajeto e peso do veículo, por exemplo, são grandezas dispensáveis para os cálculos uma vez que o cenário é um modelo proposto (distâncias e tempos não são, necessariamente, reais).

Além disso, como a norma fornece os valores máximos e mínimos de aceleração, conseguimos deduzir, com isso, os valores de interesse para o estudo de caso, como o tempo de frenagem necessário e distância mínima requerida para parar o veículo (dado uma velocidade de escolha). Esses valores de interesse, porém, podem sofrer variações significativas à medida que alguns fatores são acrescentados no modelo, como por exemplo, mais de um veículo no trilho e a presença de desvios de trilhos. Para esses fatores, trataremos os casos separadamente nas topologias apresentadas no item 3.1.

Para efetuar os cálculos necessários, segue abaixo algumas fórmulas e conceitos de mecânica e cinética, vide numeração do livro (HALLIDAY, RESNICK, WALKER; 2009, [s.d.]).

$$\Delta v = variação\ na\ velocidade\ = v1 - v0$$

$$t = tempo$$

$$\Delta t = variação\ temporal = t1 - t0$$

$$x = posição\ no\ espaço$$

$$\Delta x = deslocamento\ = x1 - x0$$

$$Smed\ = velocidade\ escalar\ média = \frac{\Delta x}{\Delta t}$$

$$Vmed\ = velocidade\ média = \frac{\Delta x}{\Delta t} = \frac{\mathrm{x1 - x0}}{\mathrm{t1 - t0}}$$

$$v = velocidade\ (instantânea) = \lim_{\Delta t \to 0} \frac{\Delta x}{\Delta t} = \frac{dx}{dt}$$

$$a = aceleração\ média = \frac{v - v0}{t1 - t0}\ = \frac{\Delta v}{\Delta t}$$

Caso de aceleração constante:

$$a = aceleração\ cte = \frac{\Delta v}{\Delta t} = \frac{v - v0}{t} \rightarrow$$

$$(\boldsymbol{Eq.2.11})\ v = v0 + at$$

Aplicando o mesmo conceito de aceleração constante na fórmula de velocidade média:

$$Vméd = \frac{x - x0}{t1 - 0} \rightarrow$$

$$(\boldsymbol{Eq.2.12})\ x = x0 + Vméd * t$$

Onde x0 é a posição em t=0 e Vméd é a velocidade média entre t=0 e t1 (arbitrário).

No caso de aceleração constante, a velocidade média, em função da Eq.2.11, pode ser reescrita como a média aritmética das velocidades iniciais e finais em um dado intervalo de tempo arbitrário, como por exemplo, entre 't0' e 't1'.

$$(\boldsymbol{Eq.2.13})\ Vméd = \frac{1}{2}(v0 + v) \rightarrow$$

E substituindo *v* pelo seu valor, dado pela Eq. 2.11, obtemos:

$$(\boldsymbol{Eq.2.14})\ Vméd = v0 + \frac{1}{2}at$$

Substituindo a Eq.2.14 na Eq.2.12 temos uma equação para a posição em um movimento acelerado.

$$(\boldsymbol{Eq.2.14}) \rightarrow (\boldsymbol{Eq.2.12})$$

$$(\boldsymbol{Eq.2.15})\ x - x0 = vot + \frac{1}{2}at^2$$

E por final, juntando as equações 2.11 e 2.15, obtemos a equação de Torricelli, útil quando o tempo não está envolvido no movimento.

$$(\boldsymbol{Eq.2.16})\ v^2 = v0^2 + 2a(x - x0)$$

Além das fórmulas apresentadas, será utilizada como base a tabela 4.1 abaixo, que consta os valores sugeridos pela norma ASCE para limites de aceleração e desaceleração em um APM. Tais valores fazem referência ao posicionamento dos passageiros no interior

de um veículo, sentados ou em pé, e estão relacionados com o conforto e bem-estar dos passageiros, de modo que a aceleração/desaceleração não traga desconforto aos ocupantes do veículo.

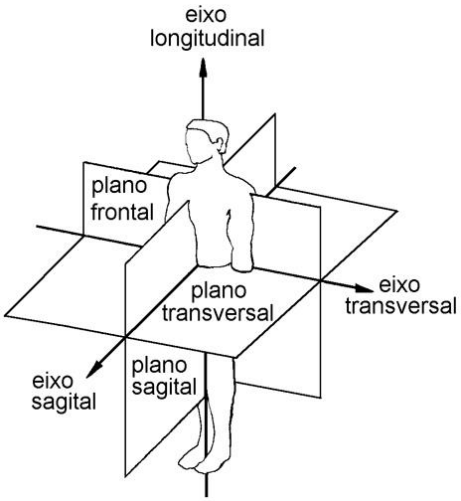
Tabela 4.1 – Valores de aceleração/desaceleração

Direção	Em pé	Sentado
Lateral	± 0.10g	± 0.25g
Vertical	± 0.05g	± 0.25g
Longitudinal	± 0.16g	± 0.35g
Longitudinal de Emergência	± 0.32g	± 0.60g

Fonte: (AMERICAN SOCIETY OF CIVIL ENGINEERS, 2006c)

Para esclarecer as direções das acelerações exibidas na tabela *4.1* referente a norma ASCE de 2006, segue a ilustração abaixo, figura 4.1, referente aos planos de eixos em um ser humano.

Figura 4.1 – Plano de Eixos



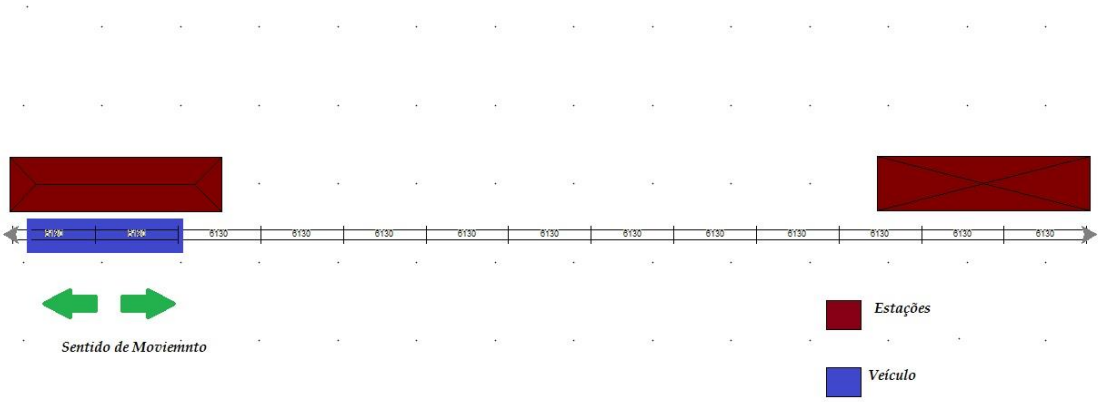
Fonte: (Ohara, T)

4.1 Estudo de caso em uma Topologia Retilínea

Considera-se uma topologia de trilhos em linha reta o Aeromóvel de Porto Alegre – RS, que é constituído por um trajeto (quase) linear entre suas duas estações, vide figura 4.2 a seguir, e um veículo APM em pleno funcionamento se deslocando para uma de suas

estações com passageiros acomodados tanto sentados quanto em pé. Em dado momento, um sinal de controle é perdido, vindo de sua central em terra, de início de frenagem por se aproximar da estação. Ao acionar os freios, sabe-se que o APM não pode infringir os requisitos de aceleração/desaceleração estabelecidos pela norma ASCE, ou seja, não pode haver uma aceleração ou desaceleração superior a um certo limiar de modo a manter o conforto e segurança dos passageiros no interior do veículo.

Figura 4.2 – Topologia Retilínea



Fonte: SCARM – *Simple Computer Aided Raillway Modeller*

Os limiares de desaceleração apresentados pela norma abrangem tanto ocupantes sentados quanto em pé no veículo. Uma vez que o APM suporta ambas as configurações de passageiros no seu interior, a análise precisa ser feita considerando o caso onde as acelerações e desacelerações suportáveis são menores. Assim, a análise será feita sobre os passageiros que estão em pé no interior do veículo por estarem mais suscetíveis aos efeitos de uma aceleração ou desaceleração brusca.

Para ocupantes em pé no APM, os valores apresentados pela norma ASCE são de +/- 0.16g (desaceleração longitudinal para ocupantes em pé) ou no caso de emergência +/- 0.32g (desaceleração emergencial longitudinal para ocupantes em pé). Sabendo os limites da norma para frenagem e que houve uma perda de sinal por parte do veículo, é necessário determinar quanto tempo o sistema ainda dispõe para parar na estação sem causar qualquer tipo de acidente.

Dada essa situação, sabe-se que a velocidade que o veículo trafegava no momento que perdeu o sinal era de $65km/h$, e que no máximo ele pode desacelerar (entende-se por aceleração negativa) a uma taxa de a = -1,569 m/s² (-0.16g) no caso normal de

frenagem ou uma taxa de a = -3,138 m/s² (-0.32g) em situação emergencial. Dado o valor da gravidade como g= 9,80665 m/s, temos:

$$V = 65\ {}^{km}/_{h} \approx 18{,}055\ m/s$$

Usando a equação 2.16, consegue-se determinar a distância mínima que o veículo precisa estar da estação para poder acionar os freios de operação ou emergenciais para parar o APM com sucesso.

$$(Eq.\ 2.16) \qquad v^2 = v0^2 + 2a(x - x0)$$

$$v^2 - v0^2 = 2a(x - x0)$$

$$v^2 - v0^2 = 2a\Delta x$$

$$\Delta x = \frac{v^2 - v0^2}{2\,|a|}$$

$$\Delta x = \frac{0 - 18{,}055^2}{2a}$$

Para o caso normal de frenagem, o valor da aceleração é $a = -1{,}569\ m/s^2$ e a distância mínima para acionamento dos freios é :

$$\Delta x = \frac{-326{,}003}{-3{,}138}$$

$$\Delta x = 103{,}88m$$

Para o caso de frenagem emergencial, o valor da aceleração é $a = -3{,}138\ m/s^2$ e a distância mínima para acionamento dos freios de emergência é :

$$\Delta x = \frac{-326{,}003}{-6{,}276}$$

$$\Delta x = 51{,}94m$$

Nesse cenário, pode-se notar que a perda de sinal de início de frenagem próximo do limite de distância necessário para frenagem normal, aproximadamente 104m de distância da estação, faz com que o sistema APM precise acionar os freios de emergência para parar o veículo a tempo. Para casos onde haja um atraso para acionar os freios de emergência e estes somente sejam acionados após a distância limite para frenagem emergencial, o veículo não conseguirá parar obedecendo as diretrizes da norma relativa ao conforto e/ou segurança de seus passageiros ao efetuar a frenagem.

A tabela 4.1.1 a seguir mostra o resultado em valores derivados do acionamento dos freios de operação, fazendo com que o sistema realize uma frenagem dentro dos

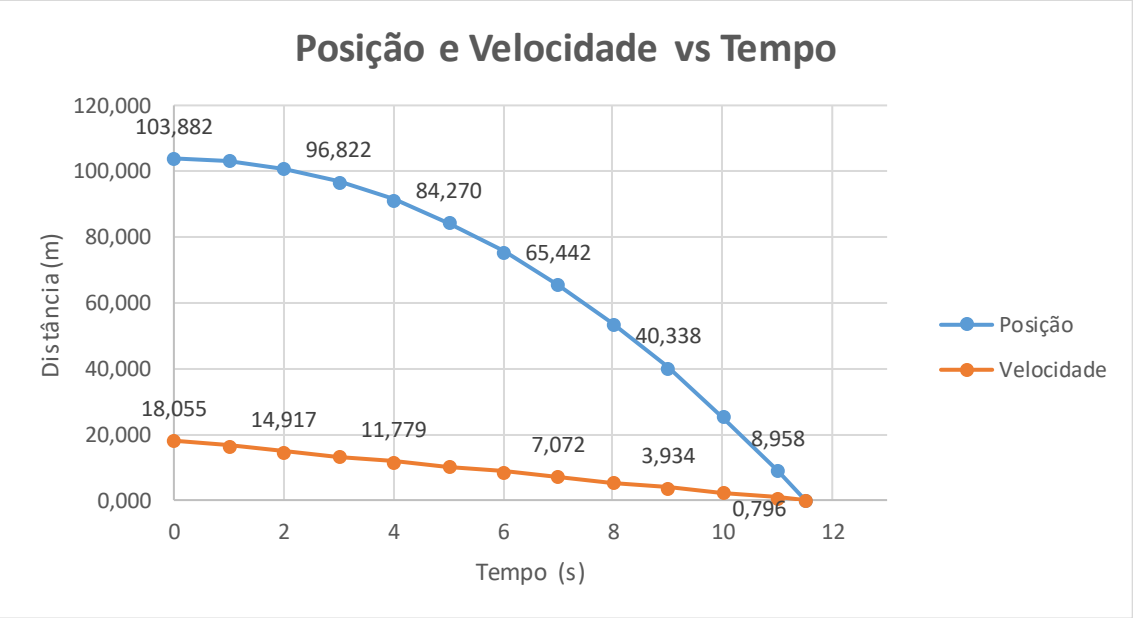
padrões da norma. Esses valores são uma relação entre velocidade e posição vs tempo do APM na configuração de frenagem normal.

Tabela 4.1.1 – Dados referentes a topologia retilínea em caso normal de operação.

Tempo (s)	**Posição (m)**	**Velocidade (m/s)**
0	103,882	18,055
2	100,744	14,917
4	91,330	11,779
6	75,640	8,641
8	53,674	5,503
11	8,958	0,796
11,50732951	0,000	0,000

Para uma melhor visualização, segue na figura *4.3* a comparação da relação velocidade e posição do veículo em função do tempo.

Figura 4.3 – Gráfico de Posição/Velocidade vs Tempo em uma frenagem normal.



Analisando a imagem *4.3*, nota-se que se o comando de início de frenagem for recebido pelo veículo e o mesmo iniciar a frenagem no instante *t=0*, ou seja, na distância mínima requerida pelo veículo para parar, é possível efetuar a frenagem obedecendo os requisitos da norma em termos de limites de aceleração/desaceleração. Assim, o veículo

é capaz de chegar na estação (posição zero), estar devidamente parado (velocidade zero), e em regime normal de operação.

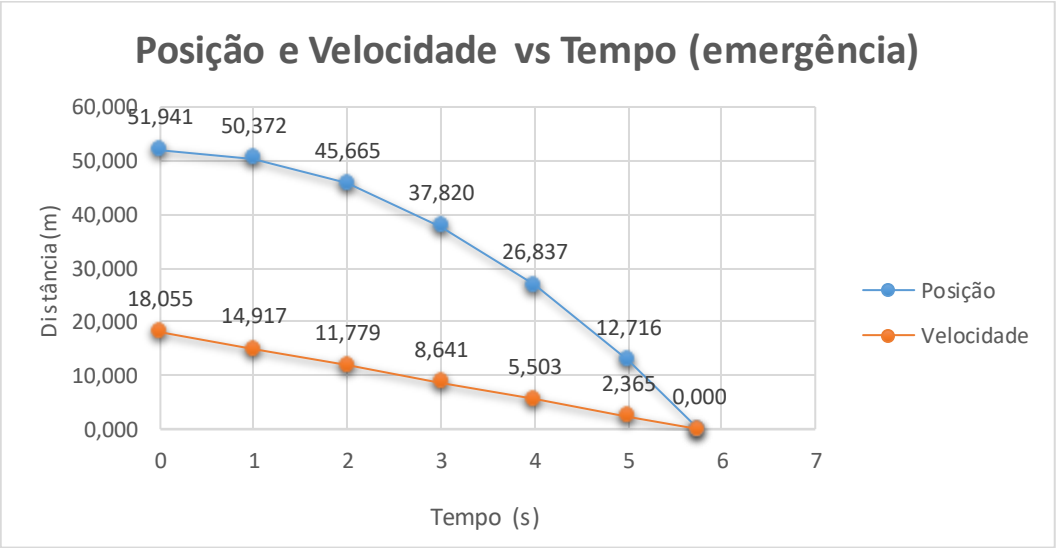
Por outro lado, em caso de falhas na comunicação com a central e o veículo perder a mensagem para acionamento dos freios, as funções de segurança precisam ser acionadas antes que o veículo atinja a distância mínima de 51,941m da estação. A tabela 4.1.2 apresenta com mais exatidão a relação entre tempo vs posição e velocidade do APM na configuração de falha.

Tabela 4.1.2 – Dados referentes a topologia retilínea utilizando frenagem de emergência.

Tempo (s)	**Posição (m)**	**Velocidade (m/s)**
0	51,941	18,055
2	45,665	11,779
4	26,837	5,503
5,753664755	0,000	0,000

Afim de comparar essas grandezas contidas na tabela segue o gráfico, figura *4.4*, que relaciona posição e velocidade do veículo em função do tempo em caso emergencial.

Figura 4.4 – Gráfico de Posição/Velocidade vs Tempo em uma frenagem de emergência.



Analisando o gráfico, nota-se que se o comando de início de frenagem for perdido pelo veículo em algum momento e o mesmo somente iniciar a frenagem no instante *t=0*,

ou seja, na distância mínima requerida pelo veículo para parar em caso de emergência, é possível efetuar a frenagem obedecendo os requisitos da norma em termos de limites de aceleração/desaceleração emergenciais. Assim, o veículo é capaz de chegar na estação (posição zero) e estar devidamente parado (velocidade zero), mas estando em uma situação de falha.

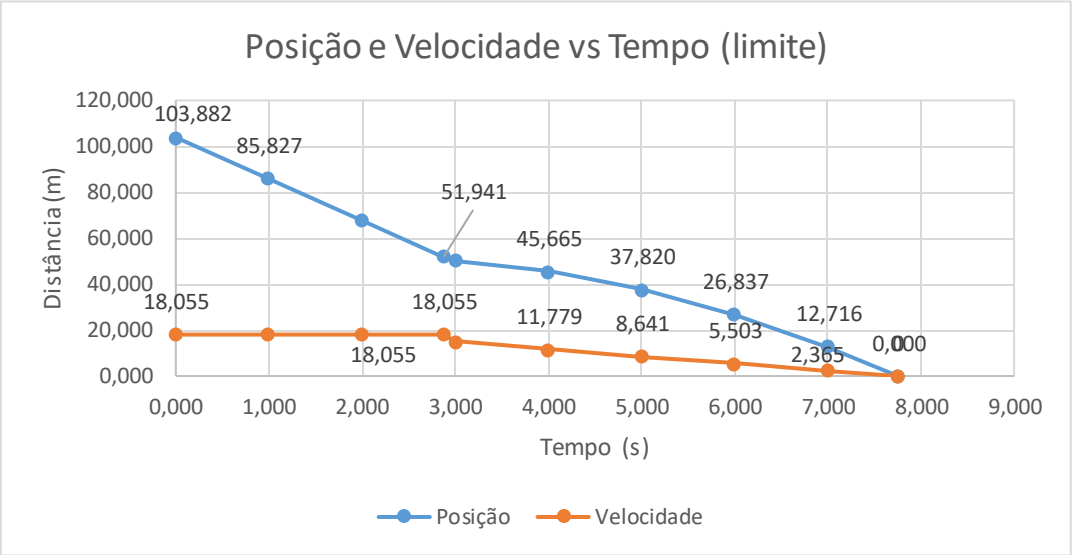
Efetuando uma breve análise dos instantes de tempo apresentados para a situação de uma topologia retilínea, pode-se concluir que o protocolo de comunicação e o enlace presentes na aplicação APM precisam ter um tempo mínimo de resposta para que caso se verifique a perda de mensagens, as funções de segurança possuam tempo para atuar. Ou seja, com a perda de uma mensagem o sistema possui uma janela de tempo pequena para que as funções de segurança assumam o controle e iniciem a frenagem de emergência.

Nesse exemplo, se o veículo perder a mensagem no limite de distância para efetuar a frenagem normal ($\Delta x = 103{,}88m$), o sistema precisa que em menos de três segundos (aproximadamente 2,83s) seja possível reconhecer a perda de sinal e acionar as funções de segurança para que elas assumam o controle do veículo e comecem a efetuar a frenagem emergencial. A tabela *4.1.3* e o gráfico, representado pela imagem *4.5* a seguir, demonstram essa situação.

Tabela 4.1.3 – Dados referentes a topologia retilínea em caso de falha na comunicação.

Tempo(s)	**Posição (m)**	**Velocidade (m/s)**
0,000	103,882	18,055
2,000	67,772	18,055
3,000	50,372	14,917
5,000	37,820	8,641
7,000	12,716	2,365

Figura 4.5 - Gráfico Posição de Velocidade vs Tempo caso de uma falha de comunicação.



Porém, caso a falha na comunicação custe um tempo $t \approx 3$ segundos para ser detectada ou as funções de segurança nesse intervalo não tenham ainda assumido controle do sistema, o acionamento dos freios de emergência não será suficiente para parar o veículo a tempo sem ultrapassar o limite imposto pela norma dos limites de desaceleração. Nesse caso, o acionamento dos freios emergenciais ou farão uma desaceleração muito forte para parar o veículo em tempo, possibilitando que haja o choque de passageiros com o interior do veículo ou, no pior caso, o veículo não irá parar a tempo, podendo vir a colidir com o final da linha, com outro veículo parado na estação ou simplesmente passar da estação.

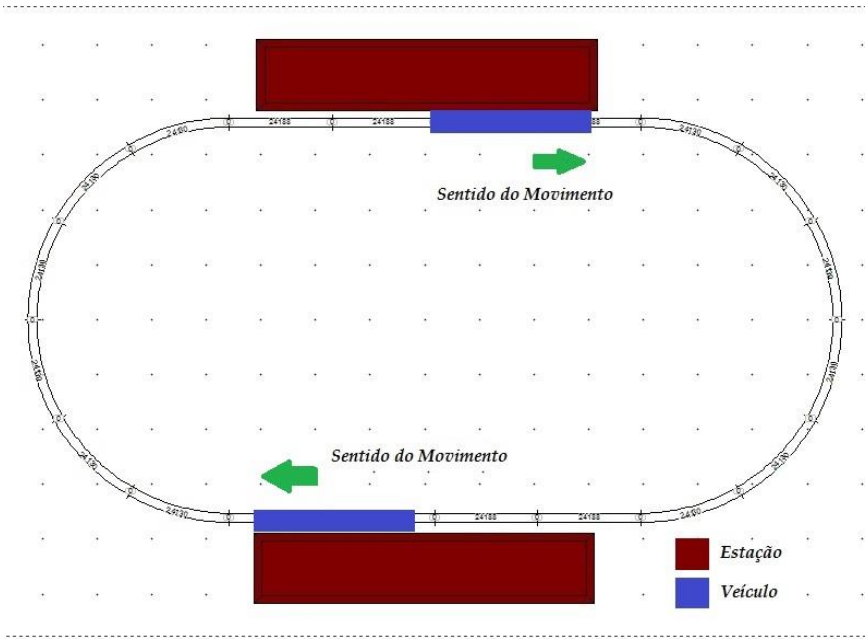
4.2 Estudo de caso para uma Topologia Circular com dois ou mais veículos

Diferente da topologia de trilhos linear, a topologia circular é um loop fechado, onde não há finais de via dispostos no percurso, mas como é um caso onde há dois veículos circulando na via com o mesmo sentido de movimento, situações específicas dessa topologia podem apresentar semelhanças físicas com a topologia retilínea com somente um veículo, como “finais de via lógicos”. Por exemplo, caso um dos veículos esteja parado em uma estação e o segundo se aproxime dessa mesma estação, a distância entre o veículo em movimento e o veículo parado é o total de trilho que o veículo em movimento possui para efetuar sua desaceleração, de modo a não colidir com o veículo

parado. Em outras palavras, o veículo parado pode ser considerado uma espécie de "final de via lógico" para o sistema de controle em termos do veículo que está em movimento. Não existindo fisicamente o término da via, mas havendo algo que, em determinado instante, seja interpretado como um. Assim, a análise de tempo em uma topologia circular com mais de um veículo, em situações como essa, é semelhante a análise de tempo de um veículo e um final de via, ou seja, a mesma análise feita no item anterior.

Além da possibilidade de termos um veículo em movimento e o outro parado na estação, temos ainda a opção onde os dois veículos estão parados, cuja análise é desnecessária devido ao caráter estático do sistema. E, por último, a opção onde os dois veículos estão circulando nos trilhos, no mesmo sentido de movimento (sentido horário, por exemplo). Ao dizer que o trajeto é circular, o mesmo admite *N* configurações de estações e curvaturas possíveis (diferentes graus de curvaturas e arcos de circunferência), números de estações e de veículos presentes no sistema. Para evitar uma abordagem muito ampla, será utilizada uma topologia de trilhos tal qual demonstrada a seguir, na figura 4.6.

Figura 4.6 – Topologia Circular



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Dessa forma, considera-se que a topologia não é um círculo perfeito, mas possui um caráter circular, com retas prolongadas e curvaturas em suas extremidades. As retas são longas o suficiente para que os veículos, após curvas ou paradas em estações, possam atingir a velocidade final, ou de cruzeiro, antes de precisarem iniciar os processos de frenagem novamente.

Além das retas longas, as curvaturas são suficientemente longas para que o efeito da aceleração lateral sofrida pelo veículo seja mínimo e também pela viabilidade da topologia. Afinal, topologias de trilhos circulares extremamente curtas perderiam o seu propósito, uma vez que a distância efetivamente percorrida por um veículo sobre trilhos seria muito maior que a distância que o indivíduo precisaria caminhar para chegar ao mesmo local da outra estação.

4.2.1 Premissas Relativas ao Sistema

Algumas premissas, relativas a topologia, precisam estar bem claras para podermos fazer uma análise concisa dos casos possíveis no sistema. A primeira premissa refere-se a norma ASCE e impõe direito exclusivo de via para o APM, ou seja, estabelece que só é possível a existência de um único veículo por trecho de trilho (entende-se trecho de trilho como a quantidade de trilho entre duas estações consecutivas). Assim, entre duas estações consecutivas somente pode haver um único veículo circulando naquele trecho específico. A segunda premissa se refere às estações, as quais são capazes de comportar a presença de dois veículos enfileirados, parados, ao mesmo tempo. Em outras palavras, a estação é longa o suficiente para que dois veículos possam estar estacionados um atrás do outro, como uma fila FIFO, onde o primeiro a chegar também é o primeiro a deixar a estação.

A terceira premissa, derivada da primeira, estabelece que a central de comando só pode autorizar a partida de um veículo da estação, no caso, a entrada do veículo em um outro trecho de trilho, uma vez que possua a confirmação de que o trecho de via está livre ou o veículo que ocupava aquele trecho já chegou a próxima estação. Caso se tenha confirmação que o veículo que ocupava o trilho chegou na sua estação, ainda é preciso confirmação que não há dois veículos parados na estação de destino, devido ao limite físico da estação de comportar, no máximo, dois veículos estacionados simultaneamente. Uma ressalva é importante fazer no sentido de que o sistema não requer sincronismo entre as partidas dos veículos, como por exemplo, os veículos partirem exatamente no mesmo momento de cada estação, somente necessita que seja obedecido o requisito de direito exclusivo de via.

As premissas apresentadas anteriormente para essa topologia são fortes o suficiente para garantir que, se obedecidas, o cenário de falhas e a análise temporal se restringem ao caso da topologia linear apresentada no item 4.1, independentemente das variações de tamanho, quantidade de estações e/ou veículos utilizados na topologia. A fim de comprovar tal fato, será demonstrado, através de uma idealização de um caso de falha de comunicação em um veículo APM na topologia circular que, se as premissas forem seguidas e o sistema operar em conformidade com as normas de segurança, a análise resultará na mesma feita no item 4.1.

4.2.2 Independência de Fatores

Assim, supondo que um veículo APM trafegue no trecho 'A' de uma topologia circular com 'N' estações e 'N' veículos, sendo $N \geq 2$ e , em dado momento, venha a perder o sinal de início de frenagem durante seu translado de uma estação para outra. Nesse caso, a central percebe a existência de um veículo com falha e emite um sinal para os demais veículos presentes no sistema para iniciarem a frenagem emergencial (imposição da norma ASCE por perda de sinal de controle). Levando os veículos em movimento em outros trechos a pararem por completo (velocidade zero), e os que estão parados nas estações a não iniciarem seu movimento até que a situação de falha possa ser corrigida. Nesse momento, a topologia circular com N veículos se reduz a um sistema com um único veículo operando na presença de uma falha, em um trilho exclusivo, e se movendo em direção a uma estação-destino (final de via), fazendo com que a análise de caso recaia na mesma feita sobre a topologia retilínea apresentada no item anterior.

Além disso, se ampliarmos o cenário desse sistema tendo agora dois veículos APM na presença de falhas de comunicação, como a perda do sinal de início de frenagem, a primeira premissa apresentada anteriormente é forte o suficiente para garantir que a falha de um dos veículos não afetará na resolução da falha do segundo e vice-versa, pois ambos estão em trechos diferentes e com exclusividade sobre o trecho em questão, recaindo novamente no caso apresentado no item 4.1 para cada um dos veículos com falha.

Com algumas considerações feitas em relação à topologia, pode-se notar que os casos que requerem atenção são casos de falhas múltiplas ou encadeadas no sistema de

modo a afetar um único veículo. Uma vez que casos de falhas isoladas, como a presença de uma única falha de comunicação por veículo, não introduzem um cenário diferente do estudado no item anterior.

4.2.3 Falhas Múltiplas

Dessa maneira, se considerarmos que um veículo APM, novamente, tenha uma falha de comunicação e perca um sinal de controle para início de frenagem ao se deslocar da estação de origem 'A' para a estação de destino 'B'. Porém, junto com essa falha acontece, simultaneamente, uma outra falha no sistema de controle do sistema que libera a saída de um segundo veículo da mesma estação 'A'. Essa segunda falha pode ter acontecido pelo fato da primeira falha desencadear uma cadeia de eventos que culmine em falhas diversas, por existência de erro de programação do sistema de controle ou por ser uma falha aleatória que aconteceu. Independente da origem, agora há duas falhas no sistema e ambos seus resultados afetarão o mesmo veículo, aquele que havia perdido o sinal de frenagem original.

Sobre essa situação, assumimos que o veículo APM que perdeu o sinal de frenagem, mesmo em estado de falha, conseguiu efetuar a frenagem através das funções de segurança do veículo sem que houvesse um sinistro. Agora, temos alguns fatores que podem variar a análise desse sistema, como por exemplo, quão longe o veículo que perdeu o sinal de frenagem está da estação de origem 'A' e do segundo veículo que foi liberado, ou no caso de um encadeamento de falhas pode ser que haja outras falhas em diferentes pontos do sistema (como o caso do link de comunicação estar indisponível) ou ainda, caso seja um erro de programação, pode ser que o sistema não reconheça a falha (tenha sido mascarada pelas outras falhas desencadeadas) e opere normalmente mesmo com dois veículos no mesmo trecho de trilho, sendo um deles em situação de falha.

Uma vez que se conhece os principais fatores que podem interferir na análise, cabe agora descobrir o quanto eles variam e se são possíveis de evitar. Assim, começando pelo caso onde o sistema não reconheça a existência da falha de comunicação com o primeiro veículo, o segundo veículo irá trafegar normalmente até o momento da ocorrência da colisão com o veículo que está parado na via, pois a inexistência de mecanismo de redundância de detecção de presença (além da comunicação, a existência de sensores na

via por exemplo) ou de redundância sobre o próprio sistema de controle (um sistema secundário que monitore o principal), a colisão é inevitável. Uma vez que o sistema de controle desconhece a presença de dois veículos no mesmo trecho e, sendo assim, não irá solicitar o acionamento dos freios por parte do veículo em movimento para evitar a colisão com o veículo parado.

Para o caso onde as falhas desencadeadas afetem uma região inteira do sistema (como o link de comunicação), é preciso que haja um subsistema local ao veículo para que o sinistro não ocorra. Pois se o veículo reconhecer a perda de mensagens com a central o mesmo irá, através das funções de segurança, ativar os freios de emergência e irá parar o APM logo após a detecção que a comunicação está indisponível, evitando, assim, a colisão com o veículo que está parado adiante na via. Nota-se aqui que o sinistro foi evitado por subsistemas locais aos veículos, pois a central de controle estava indisponível para atuar.

E por último, caso as falhas não comprometam nenhuma outra região do sistema e que o mesmo siga as premissas previamente estabelecidas, ao detectar que uma das suas premissas foi infringida, medidas de segurança serão tomadas para que o sistema alcance um estado seguro. Assim, ao liberar o segundo veículo em decorrência de uma falha, o sistema precisa parar esse veículo que foi liberado erroneamente antes que esse se choque com o primeiro veículo que parou devido a uma falha de comunicação. Para isso, duas coisas estão relacionadas e são de suma importância: a primeira é a distância que o veículo parado se encontra do veículo em movimento e, a segunda é o tempo que o sistema requer para detectar que há dois veículos no mesmo trecho da via.

Como o veículo que parou na via foi resultado de uma falha de início de frenagem, pressupõe-se que o mesmo estava prestes a chegar na estação de destino ‘B’, pois, em um trajeto circular é o único momento, em operação normal, que a central solicita frenagem para algum veículo. Dessa forma, conclui-se que o veículo está parado próximo do final do trecho em questão, dispondo assim ao segundo veículo distância suficiente para acionamento dos freios caso seja detectado, por parte de central, a presença dos dois veículos na via logo que o segundo veículo ingressa no trecho. Essa afirmação tem como base o fato de o trecho ser longo, como descrito anteriormente, e a aceleração, imposta pela norma, ser de baixa ordem quando comparada ao tamanho do trecho em si. Nesse caso, a análise temporal também irá recair sobre o item 4.1.

E, caso a verificação seja realizada de forma lenta ou esporádica a análise de caso recai sobre o item anterior também, pois teremos um veículo parado, sendo considerado um final de via lógico, e um veículo em movimento em direção a esse final de via. Nota-se ainda que, se a verificação da presença de mais de um veículo no trecho for extremamente lenta (na ordem de minutos, o que é improvável), é possível que o resultado da análise feita pelo item 4.1 anterior seja da impossibilidade de parar o veículo a tempo de evitar o sinistro.

É importante ressaltar que essa análise foi realizada para o caso descrito acima, de um veículo com uma falha de comunicação para início de frenagem por chegar próximo da estação destino e em um cenário de múltiplas falhas que ocasionaram a liberação de um segundo veículo da estação 'A'. Caso a falha em questão fosse de outra natureza ou as falhas encadeadas tivessem como resultado a liberação de um veículo da estação de destino 'B' em direção a estação de origem 'A', operando no sentindo oposto ao estabelecido pelo sistema, está análise não seria adequada. Casos onde há operações de veículos em sentidos opostos serão abordados no item 4.3 desse trabalho.

4.3 Estudo de caso para uma Topologia Circular com Intersecções

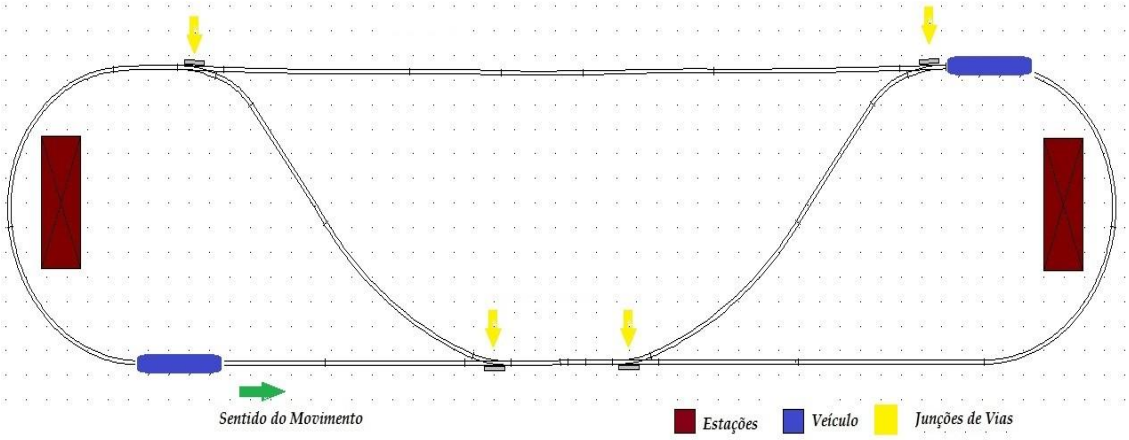
Diferentemente das topologias anteriores, a topologia circular quando permite intersecções de trilhos traz uma série de aspectos novos para a análise justamente por permitir a troca de via por parte do veículo, em decorrência de uma situação atípica de operação. Essa troca de trilhos pode ser resultado de algum defeito em um trecho específico do sistema, como uma falha estrutural da via ou mesmo um veículo parado por alguma falha. Ainda, em algumas topologias, a intersecção de trilhos pode trazer uma situação de troca de direção de movimento no sistema, onde um veículo pode ora trafegar no sentido horário quanto no sentido anti-horário em função da intersecção.

Essa troca de via de operação impacta diretamente na robustez do sistema de controle do APM, uma vez que o número de casos de falha e situações de perigo que podem acontecer é maior que os casos já estudados nesse trabalho. Além de surgirem novas situações de perigo passíveis de acontecer, há também a necessidade de rever as premissas elaboradas para o caso anterior uma vez que essas já não são suficientemente fortes e nem abrangem a totalidade de casos previsíveis para essa nova situação. Embora o caráter circular da topologia seja o mesmo, agora há a possibilidade de troca de trilho e

eventualmente direção de movimento sobre o mesmo trecho de trilho, fatos que justificam a revisão das premissas.

Em relação ao caráter físico da topologia, similarmente feito no item anterior, possui um caráter circular embora não seja um círculo propriamente dito, vide figura 4.7 abaixo. Possui retas longas o suficiente para que os veículos presentes possam desenvolver a velocidade de cruzeiro antes de realizarem uma nova frenagem. E as curvaturas da topologia são suaves e longas o suficiente para que a aceleração lateral não influencie na aceleração resultante sobre os passageiros do veículo.

Figura 4.7 –Topologia Circular com Intersecções



Como as demais considerações já foram feitas no item 4.2, cabe a descrição do diferencial da topologia, as conexões de trilhos e mecanismos para troca de trilho. Assim, nesse trabalho o caráter físico dos pontos de troca de trilho é tido como um desvio suave, com curvas bem amplas para que o veículo possa ingressar nesses trechos sem necessidade de frenagem prévia. Cabe ressaltar que a norma não traz descrições de como os desvios seriam implementados nem as características físicas dos mesmos, somente faz referência de como o sistema de proteção do sistema APM deve funcionar quando o veículo está operando sobre um desvio.

Dessa forma, como descrito pela norma ASCE na seção referente as funções de segurança providas pelo ATP de um sistema APM e resumidamente na seção 2.3 desse trabalho, o funcionamento do sistema de troca de trilhos segue uma série de diretivas para fornecer segurança ao veículo que está utilizando a via. Dentre as diretivas descritas pela norma, destaca-se o travamento de desvio, o qual faz menção ao fato da obrigatoriedade de o desvio permanecer estático antes da chegada do veículo e continuar assim até que a travessia de todo o veículo seja executada.

Ainda, o mecanismo de troca de trilho deve ser capaz de executar o movimento completo de troca de trilhos antes de sinalizar para a central que o sentido do trilho foi alterado. Em caso de exceção ou falha, cabe ao sistema de controle detectar que não houve a correta operação do sistema de desvio (via algum mecanismo de redundância por exemplo) e impedir que o veículo continue o trajeto, de modo a evitar um eventual descarrilamento. Além dessas diretivas que a norma traz, há outras que são internas ao funcionamento do mecanismo de troca de trilho ou auxiliares a esse que não fazem parte do escopo do estudo, como por exemplo, a resistência a queda de energia durante o translado do veículo sobre o trecho.

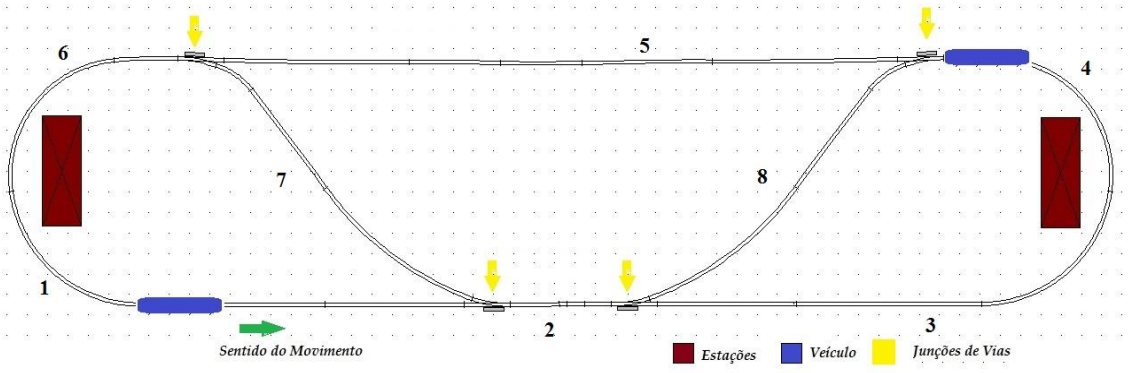
De modo a facilitar a análise desse item e das premissas necessárias para o correto funcionamento do sistema APM, será dividido esse item em dois subitens, um a respeito da operação normal do veículo e outro quando há impedimentos para a operação normal do sistema, ou seja, casos de falha no sistema, e o mesmo faz uso dos desvios de trilho para contornar tais impedimentos. Dessa forma, as premissas de operação serão separadas em caso normal de operação e para casos de falha, fazendo com que as premissas fiquem mais enxutas e de fácil entendimento. Vale ressaltar que não são dois sistemas distintos, e sim um único sistema baseado em dois conjuntos distintos de premissas referentes ao estado de operação que o sistema se encontra.

4.3.1 Operação em Condições Normais

Feitas as considerações referentes ao aspecto físico da topologia, é necessário estabelecer algumas premissas de funcionamento desse sistema para casos de operação normal. Assim como na primeira premissa do item 4.1, a garantia de direito exclusivo de via ainda é mantida para o veículo em uso daquele trecho, porém agora o trecho de trilho passa a ser definido como o trecho presente entre duas estações consecutivas, ou entre uma estação e um desvio, ou entre dois desvios consecutivos (desde que extenso o suficiente para que um veículo caiba por inteiro no trecho entre desvios). Dessa forma, entre duas estações, é possível que haja *N* veículos, desde que cada veículo esteja em um trecho distinto, e não venham a concorrer pelo direito de uso de um trecho comum no futuro. Assim, utilizando como base o esboço apresentado na figura 4.8 abaixo, vê-se que entre as duas estações há oito trechos para os veículos trafegarem (sendo dois deles,

desvios, utilizados somente em casos de falha), quatro trechos situados entre uma estação e um desvio e quatro trechos entre desvios consecutivos.

Figura 4.8 – Trechos enumerados da Topologia com Intersecções



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Como pode-se ver, a quantidade de trechos aumentou consideravelmente em relação a topologia circular sem intersecções (onde havia somente um trecho entre estações), e com isso os cuidados necessários também crescem na mesma proporção. Assim, supondo que o veículo operando no trecho *#1* só possa seguir sua operação pelos trechos #2 e #3, respectivamente, se o trecho *#2* estiver livre (e não for parte do trajeto do veículo situado no trecho #4) e o trecho #3, no momento que o veículo APM ingressar no trecho #2, esteja liberado (note que é possível que haja um veículo no trecho #3 no instante do ingresso do veículo no trecho #1 sem ferir a primeira premissa do sistema). Ainda, veículos parados nas estações não se configuram como ocupantes de trecho da topologia, somente quando ingressarem na via. Assim, uma análise rápida permite mostrar que o sistema de controle dessa topologia cresce em complexidade ao mesmo passo que a topologia cresce fisicamente. Ou seja, quanto maior o número de desvios, veículos e trechos disponíveis, ocorrerá um maior número de requisições para acesso a trechos e por eventuais desvios e consequentemente uma escalada na complexidade e no "timing" dos veículos por parte da central de controle.

A premissa relativa as estações ainda é a mesma, ou seja, as estações são capazes de receber no máximo dois veículos ao mesmo tempo, sendo o primeiro veículo parado da fila o primeiro também a sair da estação (filas FIFO). Já a terceira premissa que estabelecia que a estação poderia liberar somente um veículo para entrar no trecho precisa ser estendida, uma vez que há mais de um trecho entre duas estações, podendo, assim,

despachar um segundo veículo uma vez que se tenha confirmação que o primeiro veículo liberado já tenha desocupado o trecho e que nenhum outro esteja concorrendo pelo trecho em questão.

Porém, para uma topologia maior, com mais desvios e estações, é preciso que o controle dos trechos, e consequentemente, de desvios, por parte da central do sistema APM, seja mais rigoroso. Isso se dá pela presença de mais veículos no sistema, os quais requerem trafegar em trechos que possam ser comuns a diversos veículos. Nesses casos, caso o sistema não respeite as premissas, podem vir a ocorrer "*deadlocks*", ocasionado por vários veículos que precisam utilizar um determinado trecho, que está sendo ocupado no momento por um veículo e o mesmo não consiga sair por não haver trechos livres para ingressar.

Além disso, o controle de partidas e chegadas da central de controle em relação a uma determinada estação precisa ser robusto para que não ocorra a situação onde a estação em questão, cuja capacidade é de dois veículos, possua três ou mais veículos a caminho em virtude da existência de mais trechos passíveis de possuírem veículos trafegando. Isso violaria a segunda premissa e causaria uma situação de falha no sistema, pois não teria lugar na estação para um dos veículos excedentes parar, uma vez que a estação de destino já possui dois veículos parados, restando ao veículo parar fora da estação, ou seja, parar fora de local apropriado, resultando em falha de operação.

Vale lembrar que a presença de veículos em desvios nesse trabalho é resultado de falha em algum ponto da topologia. Em outras palavras, os desvios presentes não são considerados caminhos de operação, e sim vias secundárias, cujo objetivo é aumentar a robustez do sistema em caso de falhas em pontos físicos específicos do trajeto, permitindo que ainda haja operação no sistema mesmo com a falha. Tais situações serão explicadas e cobertas no item seguinte, como previamente explicado.

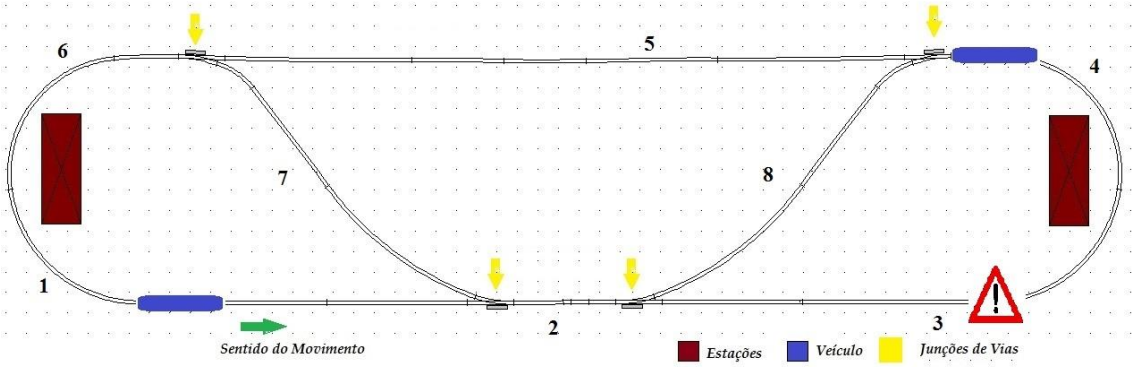
4.3.2 Operação na Presença de Falhas

Como explicado anteriormente, na presença de falhas que resultem em um impedimento sobre uma parte relativa da via, a topologia com desvios possibilita ao sistema de controle alterar o curso dos veículos e seu funcionamento para que o sistema continue operando por caminhos alternativos, evitando o local onde foi constatado problema. Cabe atenção que certos trechos da via, como o trecho #2 da figura 4.8, é

considerado um trecho crítico, uma vez que a presença de defeitos sobre esse trecho impossibilita o uso dos desvios. Porém, se a eficiência é um aspecto desejado mesmo em casos de falha em trechos críticos, o sistema pode permitir a troca de sentido de movimento de um dos veículos, não cessando, assim a operação. Assim, ainda é possível que o veículo circule utilizando os trechos #4, #5 e #6 da topologia para efetuar o translado, com inversão de sentido de movimento ao chegar nas estações, recaindo na operação de somente um veículo entre duas estações, em outras palavras, o caso 4.1 desse trabalho.

Embora existam trechos considerados críticos e meios de contorná-los sem utilizar desvios, não é o escopo desse item, cujo objetivo é explicitar como um sistema opera utilizando os desvios disponíveis para contornar casos de falhas. Assim, será utilizado como base a figura 4.9, apresentada abaixo, para desenvolver o funcionamento desse sistema na presença de falhas.

Figura 4.9 – Presença de falha na topologia circular com intersecções



Fonte: SCARM – Simple Computer Aided Raillway Modeller

Assim, utilizando a figura 4.9, é possível notar que há um sinal, ilustrativo, de alerta sobre o trecho #3. Tal sinal indica que naquele local, ou trecho, existe algum impedimento na via de natureza arbitrária, podendo ser um veículo parado por falha, uma rachadura na viga de sustentação do trilho ou mesmo uma falha elétrica. O motivo/natureza do impedimento não é importante, mas sim que existe um problema na topologia que impossibilite sua operação normal.

Dado que o sentido de movimento dos veículos no sistema é no sentido anti-horário, pode-se concluir que o veículo presente no trecho #1 não chegará a estação de destino “B” (entende-se que a estação da esquerda da figura 4.9 é denominada de “A” e a da direita, de “B”) em sua operação normal, pois ao chegar no trecho #2, o veículo não

poderá ingressar no trecho #3 para concluir o translado. Porém, como dito anteriormente, o sistema de controle opera sobre um segundo conjunto de premissas, além do conjunto de operação, que são as premissas específicas para casos de falhas no sistema, onde a utilização dos desvios é coberta pelas premissas.

Assim, o veículo que partiu da estação "A" em direção à estação "B", será desviado, ao chegar no trecho #2, para o trecho #8, um desvio, e posteriormente para o trecho #4, dessa vez operando no sentido horário sobre o trecho em questão, para concluir seu percurso. Já o segundo veículo, que partiu da estação "B" em direção à "A", que está trafegando no trecho #4, continuará sua operação normal, prosseguindo, respectivamente, pelos trechos #5 e #6 até a estação "A".

Alguns desses aspectos de operação do APM poderiam causar uma certa dúvida se o sistema ainda segue os conceitos da norma ASCE previamente apresentados, como o subitem "L" do item 2.3.4 desse trabalho, onde é abordado o travamento de direção reversa de operação imposto pela norma ASCE. Cabe enfatizar, a fim de esclarecer essa eventual dúvida, que o subitem "L" faz menção ao bloqueio de troca de sentido de movimento do veículo e não a troca de sentido de operação dos trilhos. Ou seja, se o veículo está indo para, por exemplo, o norte, ele somente poderia se mover para o sul, sobre o mesmo trilho, após atingir velocidade zero, inverter o sentido dos propulsores e aí reiniciar o movimento. No caso do exemplo, o veículo não muda o sentido de operação, ele somente passa a trafegar sobre um outro trilho que, anteriormente ao caso de falha, o sistema somente permitia um sentido de movimento.

Observando essa descrição de operação, nota-se aspectos de funcionamento diferentes dos previamente apresentados, como o uso de desvios, de sistemas de troca de trilho, o uso de um trilho em sentido contrário ao de operação normal e a chegada em uma das estações pelo lado que seria a extremidade de saída de veículos. A respeito das estações ou uso de desvios, a norma ASCE não faz proibições nem impedimentos quanto ao modo que é feito, desde que seja mantido o sistema, como um todo, em um estado seguro. Assim, o sistema descrito não infringe aspectos da norma ASCE, porém é preciso que esse tipo de caso de operação seja previsto e permitido pelo sistema de controle.

Referente as premissas em caso de falha, a primeira delas faz menção ao uso dos desvios. Assim, ao utilizar um desvio, é imperativo que o trecho a seguir do desvio também esteja livre e não haja outro veículo concorrendo pelo trecho. Essa premissa é considerada uma extensão da primeira premissa do caso de operação normal, onde o

direito de via exclusiva e obrigatoriedade do trecho seguinte (nesse caso, o desvio) estar desimpedido. Ou seja, dada a necessidade de utilizar um desvio de trilho, é preciso que exista um caminho completo até a estação de destino sem que haja impedimentos ao veículo. Assim o sistema de controle precisa monitorar tanto os trechos futuros no sentido de operação nominal quanto os trechos no sentido oposto para permitir a entrada do veículo em um desvio. O motivo real da extensão da premissa é por ser possível que a estação "B" libere um veículo com destino a "A", fato que implicaria numa competição por um trecho de operação exclusiva, não previsto no subitem 4.3.1.

A segunda premissa é relativa ao funcionamento das estações finais dos veículos. O número de veículos parados simultaneamente continua o mesmo nas estações, porém o funcionamento de uma das estações (a outra se mantém sem alterações) precisa ser revisto para que seja possível o ingresso de veículos pelo lado utilizado, anteriormente, como partida de veículos. Assim, o modelo FIFO da estação já não é mais obedecido, uma vez que a entrada e saída de veículos ocorre pelo mesmo lado, sendo assim, o último veículo a chegar na estação também será o primeiro a sair.

Além disso, a estação que estiver sobre o funcionamento alternativo, ficará com um de seus veículos estacionados sem operação até que o impedimento da via seja resolvido, para que a questão de "timing" não impacte na análise em questão. Por exemplo, o trecho #4 da topologia anterior será um trecho de alta frequência de uso, pois tanto os veículos que possuírem a estação "B" como destino ou origem passarão por esse trecho, transformando o trecho #4 num recurso muito requisitado e, consequentemente, pouco disponível. Assim, a retirada de operação de um dos veículos dessa estação melhora a performance do sistema como um todo.

E por último, a terceira premissa é referente ao controle de partida de veículos das estações. Similarmente, ao item anterior, a estação só pode liberar um veículo por vez, por trecho da via. Como há mais trechos na via devido a nova classificação de trecho feita na seção 4.3.1, é possível a liberação de mais de um veículo de uma mesma estação como explicando anteriormente.

Porém, para liberar um veículo é preciso não ter somente confirmação de que o trecho está livre, mas também que os veículos que estão em circulação não possuem esse trecho como trecho futuro imediato (primeira premissa). Ou seja, como existe a chance de veículos em sentidos opostos de movimento requisitarem o mesmo trilho, a central precisa saber, com precisão, o trajeto dos veículos que irão requisitar tal trecho e a posição

que cada um se encontra, para então analisar a possibilidade ou não de outro veículo ingressar na via.

Feito essas considerações em relação a topologia, partiremos para a análise, no próximo item, de alguns casos simples onde ocorram algumas falhas em uma topologia com desvios, de como o sistema reage a elas e em quais situações essas falhas podem levar o sistema a um perigo real.

4.3.3 Análise de Falhas

Uma vez que a topologia com desvios é a topologia mais complexa apresentada nesse trabalho, nota-se que todas as falhas previamente citadas são possíveis de acontecer nesse sistema. Nos casos já estudados, têm-se falhas de comunicação que obriguem um veículo a frenar a ponto de não colidir com uma estação ou outro veículo parado, ou ainda, um veículo necessitar frenar devido ao veículo que está em um trecho, a sua frente, apresentando defeitos. Essas situações acontecem devido a esta topologia possuir características em comum às demais apresentadas, como retas, curvaturas, presença de mais de um veículo circulando e, com isso, seus cenários de falhas.

Como os demais cenários de falha já foram investigados em seus respectivos itens, cabe, agora, a análise de situações onde as falhas afetem veículos operando sobre os desvios e suas imediações. Assim, supondo um veículo que partiu da estação “A”, definida anteriormente, em direção a estação “B”, tenha ingressado no desvio. No momento de ingresso no desvio, o veículo já possuía confirmação, por parte da central de controle, que o trecho seguinte ao desvio estava reservado para usufruto dele. Além disso, um sinal de abertura do desvio já havia sido emitido por parte da própria central, garantindo, assim, a primeira premissa. Ou seja, a garantia de via exclusiva e a garantia de um caminho completo sem impedimentos (necessário ao se utilizar um desvio) até a estação de destino.

Porém, esse sinal de abertura de desvio não foi recebido pelo mecanismo ou foi recebido e não executado por algum motivo, como por exemplo, uma falha mecânica do mesmo. Assim, o mecanismo de desvio permanece fechado para o veículo dentro do trecho de desvio, levando o sistema a um estado de falha, pois com um desvio fechado não há como o veículo ingressar no trecho final de seu trajeto. Esse cenário, com uma

análise breve, é similar ao cenário apresentado no caso 4.1 do trabalho, da topologia retilínea, pois temos um final de via, de caráter lógico, e o veículo trafegando em direção ao final de via. A questão de como a central detectará que o desvio está fechado não é escopo desse trabalho, mas em caso de detecção, as análises temporais feitas no item 4.1 serão suficientes para determinar se o veículo conseguirá parar (se haverá trilho suficiente para efetuar a frenagem) ou ocorrerá um sinistro.

Ainda há outro cenário de falha possível de acontecer, diferente do exemplo anterior, que é a inserção de um segundo veículo em funcionamento, mas partindo o segundo da estação "B" em direção a estação "A". Se, com esse segundo veículo trafegando, o mecanismo de troca de trilhos apresentar problemas e emitir um sinal falso-positivo, pode fazer com que o trajeto do veículo que estaria indo para a estação "A" acabe sendo alterado, colocando-o em curso de colisão com o outro veículo.

Assim, supondo que haja dois veículos no sistema, um que partiu da estação "A" em direção a estação "B", e está próximo do acesso ao desvio, trecho #8, e outro que partiu da "B" para a estação "A", estando também na iminência de atravessar o desvio que liga os trechos #4 e #5, vide figura 4.9. Nota-se que a primeira premissa ainda é válida pois, para a central, um veículo seguirá do trecho #4 para o trecho #5, enquanto o outro ainda irá ingressar no trecho #8.

Porém, como citado antes, acontece uma falha com o desvio que liga os trechos #4 e #5, que resultou na emissão de um sinal falso-positivo para a central. Dessa forma, o desvio informou à central que o desvio estava fechado, ou seja, dando passagem para o veículo da estação "B" seguir seu rumo normalmente para o trecho #5. Mas na verdade o desvio estava aberto, fazendo com o que o veículo que saiu da estação "B" ingressasse, erroneamente, no desvio em direção ao trecho #2.

Agora, o cenário em questão se caracteriza pela presença de dois veículos sobre o mesmo trecho de trilho, sem saberem da existência um do outro, trafegando em curso de colisão. Ainda, se não houver qualquer tipo de redundância de localização espacial dos veículos em funcionamento, essa falha não será detectada pela central de controle dos veículos, ocasionando a omissão da mesma no momento em que deveria sinalizar para que ambos iniciem as frenagens. Em relação as premissas de emergência, já houve o não cumprimento da primeira premissa a respeito do direito exclusivo de via, o qual foi violado no momento em que o mecanismo de desvio falhou e permitiu o ingresso do outro veículo.

Como a detecção de presença é exigida pela norma, a central deverá reconhecer, que um dos veículos ingressou no desvio impropriamente, seja pela sua localização através de sensores ou outro mecanismo. Porém, agora que se tem conhecimento da falha do mecanismo de troca de trilhos, cabe à central de controle administrar a situação de modo a manter o sistema em um estado seguro. Caso a central consiga, além de localizá-los também se comunicar com os veículos (caso contrário não acionarão os freios por desconhecerem a falha), resta agora saber se ainda há espaço suficiente entre os veículos para pará-los. Para isso, será adotado os mesmos valores de velocidade nominal e aceleração/desaceleração para os veículos dos itens anteriores, considerando que a aceleração seja em termos dos ocupantes em pé no veículo, utilizados no início do capítulo 4 e reapresentados na tabela 4.3.1 a seguir:

Tabela 4.3.1 – Grandezas Físicas dos Veículos APM

Uma vez que os valores de aceleração e desaceleração são idênticos ao do item 4.1, os cálculos realizados anteriormente são suficientes para descobrir a distância que cada veículo leva para parar, e consequentemente, o tempo para tal. Assim, do item 4.1 temos que a distância necessária para um veículo parar é de:

$$\Delta x = 103{,}88m$$

Para casos normais e, para casos emergenciais, é de:

$$\Delta x = 51{,}94m$$

Porém, como os dois veículos estão indo um ao encontro do outro, a distância mínima entre eles para que possam parar é, logicamente, o dobro da distância que um requer, já que as acelerações/desacelerações são imutáveis. Isso vale tanto para o quesito de distância para frenagem normal ou emergencial. Salienta-se ainda que nesse caso de falha, a norma ASCE não faz menção a utilização de frenagem emergencial

obrigatoriamente, ou seja, como a falha é aquém dos veículos, eles ainda estão sobre operação normal, podendo, dependendo da distância, e dos comandos da central, utilizar frenagem de operação ou emergencial.

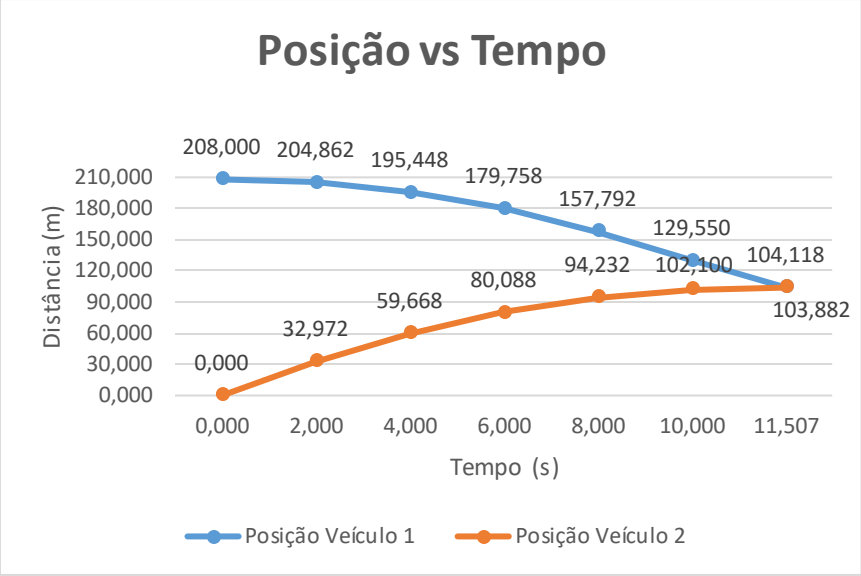
Tendo conhecimento disso, será abordado ambos os casos de frenagem e suas variações. Assim, para melhor visualizar, segue a tabela 4.3.2, com os valores referentes ao comportamento de ambos os veículos, em uma relação entre posição e tempo, sobre frenagem normal e o gráfico referente representado pela figura 4.10.

Tabela 4.3.2 – Valores referentes a Frenagem de Operação

Tempo (s)	**Posição Veículo 1 (m)**	**Posição Veículo 2 (m)**
0	208,000	0,000
1	207,216	17,271
2	204,862	32,972
3	200,940	47,105
4	195,448	59,668
5	188,388	70,663
6	179,758	80,088
7	169,560	87,945
8	157,792	94,232
9	144,456	98,951
10	129,550	102,100
11	113,076	103,681
11,50732951	104,118	103,882

Nota-se que esse é o caso limite considerando que dois veículos não podem estar sobre o mesmo ponto físico quando pararem, por isso o arredondamento da distância mínima (originais 207,764m).

Figura 4.10 – Gráfico de Frenagem de Operação



Ao analisar o gráfico, algumas coisas precisam de destaque, como por exemplo, o comprimento do desvio. Essa distância tem importância pois, para um cenário onde cada veículo opera em uma velocidade de, aproximadamente, 18m/s, e estão em sentidos opostos, em 10 segundos eles percorrem, juntos, 360 metros de trilho. Cabe salientar que, normalmente, os desvios não são extensos, uma vez que os próprios APMs também não o são. Assim, se houver qualquer demora, por parte da central, em detectar que o sistema está operando sobre falha ou emitir os respectivos sinais de frenagem para os veículos iniciarem a frenagem, pode ser que a frenagem operacional já não seja suficiente para para-los. Uma vez que somente o ato de frenagem demoraria, aproximadamente, 11,5 segundos.

Porém, se houver espaço suficiente entre eles, vale destacar aqui que se a central conseguir se comunicar com os veículos, e os mesmos iniciem a frenagem no instante $t=0$ segundos, a frenagem de operação será capaz de parar ambos os veículos (velocidade zero), apesar do sistema estar apresentando falhas externas aos veículos.

Em relação as variações deste cenário de falhas, além da falha do sistema de troca de trilho, podem haver situações onde algum dos veículos perca o sinal de controle de início de frenagem, ou mesmo ambos venham a perder seus respectivos sinais. Lembrando que uma vez perdido a comunicação com a central de controle, a norma exige que a frenagem seja obrigatoriamente emergencial, independente da distância ou da possibilidade de parar com os freios de operação. Assim, será abordado o pior caso proposto para esse cenário, onde a central reconhece a falha do sistema de troca de trilhos com um certo atraso, ocasionando que ambos estejam próximos da distância limite para

frenagem de operação quando for emitido o sinal de frenagem, e esse sinal, por uma falha de transmissão, seja incapaz de chegar aos dois veículos.

Dessa forma, o cenário é caracterizado com ambos os veículos trafegando no mesmo trilho (desvio), com velocidade nominal e em sentidos opostos de movimentação. E, em dado momento, o sinal da central é perdido por ambos. Como a detecção de perda de sinal por parte dos veículos faz com que o sistema entre em um estado de falha, cabe identificar, se ainda for possível, quão rápido o sistema de proteção dos veículos e suas funções de segurança precisam atuar para evitar a colisão.

Devido aos cálculos feitos no capítulo 4.1, é conhecida a distância mínima para frenagem emergencial de um veículo APM de maneira que os limites impostos pela norma ASCE sejam respeitados. Assim, como feito no exemplo anterior de frenagem normal, sabe-se que a distância mínima para ambos pararem deve ser o dobro da distância que um dos veículos precisa para parar, uma vez que ambos trafegam na mesma velocidade e em sentidos opostos. Assim, como ambos os veículos requerem, aproximadamente, 52 metros de trilho para frenar, temos que 104 metros seja a distância mínima entre eles para o acionamento dos freios de emergência de modo a pararem

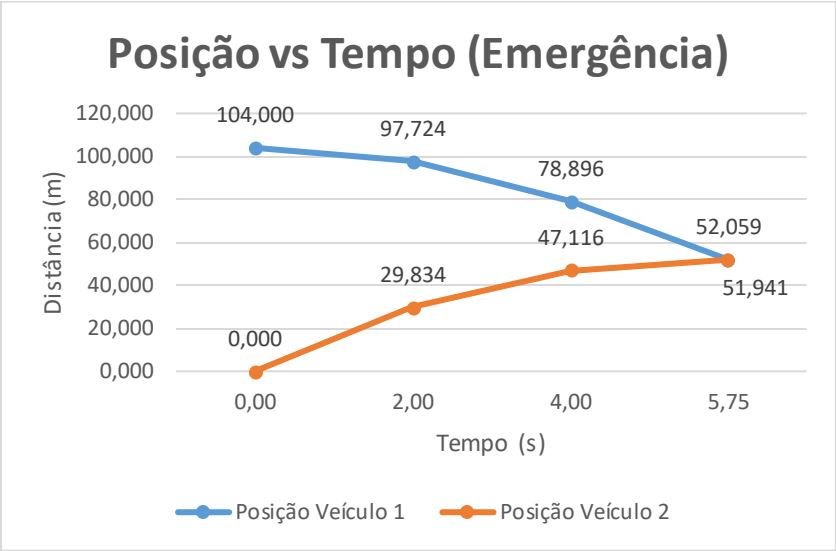
A tabela 4.3.3 a seguir mostra o resultado em valores derivados do acionamento dos freios emergenciais, e para auxílio visual, o gráfico referente a esses valores é representado pela figura 4.11. Esses valores são uma relação entre posição e tempo dos veículos APM.

Tabela 4.3.3 – Valores referentes a Frenagem de Emergência

Tempo (s)	**Posição Veículo 1 (m)**	**Posição Veículo 2 (m)**
0	104,000	0,000
1	102,431	16,486
2	97,724	29,834
3	89,879	40,044
4	78,896	47,116
5	64,775	51,050
5,753664755	52,059	51,941

Lembrando que essa distância é relativa, podendo ser maior ou menor, em função do tempo necessário para a central de controle confirmar a falha do mecanismo de troca de trilhos e contatar os veículos para iniciarem suas frenagens.

Figura 4.11 – Gráfico de Frenagem de Emergência



Analisando o gráfico, nota-se que se o comando de início de frenagem for perdido pelos veículos em algum momento e os mesmos somente iniciarem a frenagem no instante $t=0$, ou seja, na distância mínima requerida para pararem em caso de emergência, ainda é possível efetuar a frenagem obedecendo os requisitos da norma em termos de limites de aceleração/desaceleração emergenciais. Assim, os veículos serão capazes de estarem devidamente parados (velocidade zero), mesmo estando em uma situação de falha tanto interna quanto externa aos veículos. Vale lembrar que esse é pior caso possível, qualquer atraso para início de frenagem nessa situação resultará em uma frenagem mais brusca, podendo ocasionar lesões aos ocupantes do veículo ou mesmo uma colisão frontal.

5 CONCLUSÃO

O projeto e concepção de movimentadores automatizados de pessoas é um fato pouco conhecido quando comparados a outros meios de transporte de pessoas, embora existam exemplares em funcionamento deste tipo de sistema desde a década de 70. Ainda, além da pouca disseminação desses sistemas, as pesquisas na área de automação de veículos sobre trilhos automatizados também são escassas, trazendo dificuldades ao estudo desse tópico, bem como das normas referentes ao domínio e as exigências impostas pelos diversos padrões aplicados a projetos. Assim, o desenvolvimento desse estudo teve como objetivo a análise das normas e padrões de segurança do domínio APM através da modelagem de um sistema idealizado, almejando um esclarecimento das exigências das normas, a completude das mesmas e da eficácia da implementação delas no aspecto de segurança funcional de um projeto APM.

Ao término do estudo, atingiram-se os objetivos iniciais planejados para esse trabalho. Com o estudo das funções de segurança, níveis de integridade de sistemas, padrões aplicados à projetos, como o IEC61508, e da norma ASCE para o domínio APM, e a respectiva aplicação dos resultados desse estudo na modelagem feita de um sistema APM foi possível atender as expectativas desse trabalho. Com o encerramento da modelagem feita sobre aspectos da norma, os resultados obtidos mostraram que a aplicação de padrões de projeto traz benefícios significativos em termos de segurança funcional e robustez de um projeto APM. E em relação ao uso de protocolos seguros na comunicação, é aconselhável, porém não obrigatório, uma vez que o protocolo utilizado precisa atender aos requisitos de segurança do sistema em questão, podendo ser nativo ao protocolo ou ser implementado, posteriormente, de acordo com a necessidade da aplicação.

Embora os resultados tenham sido positivos em relação ao entendimento e esclarecimento dos padrões e normas através da aplicação de conceitos sobre um modelo de sistema APM em funcionamento, este trabalho é de cunho, exclusivamente, conceitual e não tem por objetivo servir de base para um projeto real. Todas as premissas, modelos, e cenários de falhas aqui escritos e desenvolvidos não tem uma correspondência precisa com a realidade por simplificações feitas. Assim, para pretensões futuras, pode-se buscar aprimorar esse estudo através da realização de uma análise prática de um sistema, considerando variáveis locais e físicas de uma determinada região para trazer uma maior

exatidão aos cálculos bem como um maior aprofundamento dos mesmos. Ainda, uma eventual simulação desses resultados afim de comprovar a viabilidade do desenvolvimento de um projeto seria de grande valia.

REFERÊNCIAS

1474.1-1999 **IEEE Standard for Communication Based Train Control Performance Requirements and Functional Requirements.** Piscataway: IEEE, .

AMERICAN SOCIETY OF CIVIL ENGINEERS (Org.). **Automated people mover standards**. Reston, VA: American Society of Civil Engineers, 2006a.

AMERICAN SOCIETY OF CIVIL ENGINEERS (Org.). **Automated people mover standards**. Reston, VA: American Society of Civil Engineers, 2006b.

AMERICAN SOCIETY OF CIVIL ENGINEERS (Org.). **Automated people mover standards**. Reston, VA: American Society of Civil Engineers, 2006c.

BAUFRETON, P. et al. **Multi-domain comparison of safety standards**. [S.l.]: [s.n.], 2010.

BELL, R. **Introduction to IEC 61508**. [S.l.]: Australian Computer Society, Inc., 2006. p. 3–12.

Brown, 2000 **- Overview of IEC 61508 Design of electricalelectro.pdf**.

Conexão metrô-aeroporto - Trensurb - Empresa de Trens Urbanos de Porto Alegre S.A. [S.l.], [s.d.].

DALE, C.; ANDERSON, T. (Org.). **Advances in Systems Safety**. London: Springer London, 2011.

Demanda | Portal da Transparência. [S.l.], [s.d.]. Disponível em: <https://transparencia.metrosp.com.br/dataset/demanda>. Acesso em: 4 jul. 2017.

(OpenSAFETY Manual)

GAJ, P.; JASPERNEITE, J.; FELSER, M. **Computer Communication Within Industrial Distributed Environment—a Survey**. IEEE Transactions on Industrial Informatics, fev. 2013. v. 9, n. 1, p. 182–189.

GALL, H. **Functional safety IEC 61508/IEC 61511 the impact to certification and the user**. [S.l.]: IEEE, 2008. p. 1027–1031.

HALLIDAY, RESNICK, WALKER; **Fundamentos da Física**, Vol. 1, 8a Edição, LTC, 2009.

JOANNOU, P.; WASSYNG, A. **Understanding integrity level concepts**. Computer, 2014. v. 47, n. 11, p. 99–101.

KUNZ, G. De O. **Metodologia para o desenvolvimento de sistemas de controle de APM (Automated People Movers) com aplicação ao sistema aeromovel de transporte de passageiros**. 2012.

KUNZ, G.; PERONDI, E.; MACHADO, J. **Modeling and simulating the controller behavior of an Automated People Mover using IEC 61850 communication requirements**. [S.l.]: IEEE, 2011. p. 603–608.

MORAR, S. **Evolution of communication based train control worldwide**. 2010.

NBR 16074-4_(sistema APM_) Parte 4_Requisitos do veículo e sistema de propulsão e frenagem.pdf.

NBR 16074-5_(sistema APM_) Parte 4_Requisitos dos equipamentos Elétricos.pdf.

NBR16074-1_ Sistema Movimentador Automático de Pessoas _(Sistema APM_) - Parte 1_ Terminologia e abreviaturas.pdf.

NEUMANN, P. **Communication in industrial automation—What is going on?** Control Engineering Practice, nov. 2007. Special Issue on Manufacturing Plant Control: Challenges and IssuesINCOM 200411th IFAC INCOM'04 Symposium on Information Control Problems in Manufacturing. v. 15, n. 11, p. 1332–1347.

OHARA, T. **Anatomia aplicada ao Yoga**. Ser Yoga, [S.l.], [s.d.].

RANEY, S.; YOUNG, S. E. **Morgantown people mover–updated description,** 2000. v. 785, p. 296–6959.

ROXANNE, W. **Automated People-Movers**, 2000. [s.d.]. Disponível em: <http://onlinepubs.trb.org/onlinepubs/millennium/00008.pdf>. Acesso em: 3 jul. 2017.

SCHERER, M.; WICHSER, J.; VENCKAUSKAITE, J. **Alternatives to automated people-mover systems for small but dense populated areas**. Technological and Economic Development of Economy, jan. 2009. v. 15, n. 1, p. 90–101.

VEHICULAR TECHNOLOGY SOCIETY *et al.* **IEEE standard for communication-based train control (CBTC) performance and functional requirements**. New York, N.Y.: Institute of Electrical and Electronics Engineers, 1999.

VUCHIC, V. R. **Urban public transportation systems**. University of Pennsylvania, Philadelphia, PA, USA, 2002.

WASSYNG, A. et al. **Software certification: Is there a case against safety cases?** [S.l.]: Springer, 2010. p. 206–227.

ZHIVICH, M.; CUNNINGHAM, R. K. **The Real Cost of Software Errors**. IEEE Security & Privacy Magazine, mar. 2009. v. 7, n. 2, p. 87–90.