3º PRÊMIO TECNOLOGIA E DESENVOLVIMENTO METROFERROVIÁRIOS

CATEGORIA 3

NÍVEL DE SEGURANÇA SIL - ESTUDOS PRÁTICOS DO SISTEMA DE PORTAS DE PLATAFORMAS – PSD

INTRODUÇÃO

Os Sistemas PSD - sigla em Inglês para "Platform Screen Doors" ou Portas de Plataforma - estão cada vez mais presentes nos projetos de novas linhas e, também, nos projetos de modernização de linhas existentes. No caso de linhas de metrô com Sistemas de Sinalização e Material Rodante sem condutor ("Driverless") ou UTO (sigla em Inglês para "Unmanned Train Operation" ou Operação de Trem sem Intervenção Humana), a utilização do sistema PSD torna-se obrigatória pela imposição dos requisitos de segurança. Neste contexto, o estudo dos níveis de segurança necessários às funções deste sistema é de alta relevância para a garantia da segurança do sistema metroviário como um todo.

Neste trabalho são apresentados os conceitos, critérios e a metodologia utilizados para a identificação, determinação e avaliação dos níveis de integridade de segurança SIL – sigla em Inglês para "Safety Integrity Level" ou Nível de Integridade de Segurança - necessários às

funções de um sistema PSD, a fim de que se possa aferir e realimentar os requisitos especificados pelos projetos deste sistema.

Segundo os conceitos de “Safety System” e “Safety Analysis” apresentados em “A. John Wiley & Sons, Inc. Publication - Hazard Analysis Techniques for System Safety” e o conceito trazido pela norma MIL-STD-882, um sistema é uma composição, em qualquer nível de complexidade, de pessoas, procedimentos, materiais, ferramentas, equipamentos, instalações e software. Os elementos constituintes desta entidade são utilizados em conjunto no ambiente operacional ou de apoio e, são destinados a desempenhar uma determinada tarefa ou atingir um propósito específico, definido pelos requisitos da missão.

Os sistemas têm muitos atributos diferentes necessários à sua segurança. Projetar e compreender os principais atributos de um sistema é necessário, pois estes fornecem o quadro para a sua concepção, construção, operação e análise.

As principais categorias de atributos de um sistema são apresentadas abaixo e, estão relacionadas à riscos e considerações de segurança do sistema que foram analisados em algum momento de seu plano de desenvolvimento:

- Equipamentos: modos de falha, fontes de energia perigosas;
- Software: erros de projeto, incompatibilidades de design;
- Pessoal: Erro humano, ferimentos, Interface Homem-Máquina;
- Ambiente: Tempo, equipamento externo, interferências;
- Procedimentos: instruções, tarefas, notas de advertência;
- Interfaces: erros de entrada / saída, complexidades inesperadas;

- Funções: não executadas, executadas erroneamente;
- Instalações: falhas de construção, compatibilidade de armazenamento, falhas de transporte.

Processo de Segurança

O processo de segurança é um conjunto de atividades relacionadas que visam dotar um sistema do nível de integridade de segurança, especificado pelos seus requisitos de projeto, durante a execução de suas missões determinadas.

A fim de se aplicar um processo de segurança a um sistema, faz-se necessário entender completamente este sistema e todas as suas ramificações (interfaces e decomposições). Isto inclui o entendimento do que compreende este sistema, como ele opera, quais são suas ferramentas de análise, seu ciclo de vida e seu processo de desenvolvimento.

O processo de segurança proativo e preventivo só pode ser eficaz se as tarefas de segurança forem orientadas ao sistema e realizadas adequadamente durante as fases do ciclo de vida deste, em conjunto com a utilização de ferramentas apropriadas de engenharia de sistemas. O calendário e o conteúdo das tarefas de segurança devem coincidir com determinadas fases do desenvolvimento do sistema para que se garanta o sucesso de sua segurança.

Todos os elementos do sistema, suas inter-relações, suas apreciações e avaliações devem ser considerados para garantir-se a real análise de segurança do sistema. Por exemplo, é possível que cada fase de operação ou modo operacional tenha diferentes impactos sobre a segurança do sistema.

A análise de segurança envolve duas atividades fundamentais para a garantia de segurança de um sistema: a análise de perigos e a análise de riscos.

Análises de perigos são realizadas para identificar os perigos, seus efeitos e fatores causais. Análises de riscos são utilizadas para determinar a probabilidade e severidade de cada perigo aos quais o sistema está exposto e, estabelecer medidas de concepção de segurança para eliminar ou mitigar estes riscos. Estas análises são realizadas de forma sistemática, em várias fases de desenvolvimento do projeto, avaliando os perigos e riscos com foco nos subsistemas, instalações, componentes, software, pessoal e suas inter-relações.

O entendimento do tipo do sistema e seu escopo são importantes para a garantia de segurança deste e para a análise de perigos e riscos. O tipo de sistema pode ser uma indicação da criticidade da segurança envolvida. O âmbito da aplicação dos limites do sistema estabelece o tamanho e a profundidade deste. As limitações do sistema descrevem basicamente o que este pode e o que não pode fazer com relação à segurança. Algumas limitações podem exigir a inclusão de um projeto especial que assegure dotá-lo das características de segurança necessárias.

Cada sistema funciona dentro de um ou mais ambientes diferentes. O ambiente específico estabelece qual o potencial de risco que o sistema poderá estar exposto. Uma análise de contexto ao qual o sistema está inserido e as interfaces externas deste são necessárias para o estudo de sua segurança.

Por fim, a criticidade de um sistema estabelece a classificação global da segurança para este sistema.

Níveis de integridade de segurança SIL

A análise de perigos e de riscos podem ser realizadas qualitativamente, quantitativamente ou semi-quantitativamente. Os resultados finais das análises de perigos e de riscos podem ser um conjunto de problemas com elevado risco potencial que tem que ser reduzido.

Pode-se escolher qualquer abordagem sobre a forma de se reduzir os riscos, desde que estes fiquem reduzidos a um nível aceitável.

O número SIL significa a ordem de grandeza (a potência de dez) para a redução do risco de que a função de segurança necessita para alcançar a confiança desejada. SIL 1 é uma redução de dez vezes ou mais; SIL 2 é uma redução do risco de cem vezes ou mais; SIL 3 é de mil vezes ou mais e SIL 4 é um fator de redução de risco de dez mil vezes ou mais. Quando se percebe o significado dos números SIL, percebe-se, também, porque todos os atores de um sistema, incluindo os órgãos regulamentadores de segurança, possuem muito interesse nos níveis de segurança das funções.

A tabela a seguir ilustra os significados dos Níveis de Integridade de Segurança SIL:

Tabela 1- "IEC 61508 define quantitativamente os níveis de segurança (SIL) em função da probabilidade de falhas e o fator de redução do risco, os quais serão utilizados na classificação das funções pelos projetistas e fornecedores de sistemas de segurança".

Probabilidade de Falha	**Probabilidade de Falha em Potência de 10**	**SIL**	**Fator de Redução de Risco**
1 a 0,1	**10E0 – 10E-1**	**SIL 0**	**1 a 10**
0,1 a 0,01	**10E-1 – 10E-2**	**SIL 1**	**10 a 100**
0,01 a 0,001	**10E-2 – 10E-3**	**SIL 2**	**100 a 1.000**
0,001 a 0,0001	**10E-3 – 10E-4**	**SIL 3**	**1.000 a 10.000**
0,0001 a 0,00001	**10E-4 – 10E-5**	**SIL 4**	**10.000 a 100.000**

DIAGNÓSTICO

Descrição da Metodologia Adotada

Os sistemas PSD realizam funções que implementam os requisitos referentes ao embarque/desembarque seguro dos usuários entre o trem e a plataforma, à proteção de acesso à via, à proteção de queda dos passageiros na via, à operação em modos normal e degradado e ao seu próprio monitoramento.

Nem todas as funções de um sistema PSD são críticas em respeito à segurança. A análise, inicialmente, deve identificar quais funções serão alocadas a um Nível de Segurança mais elevado (SIL 2, 3 ou 4) e quais não dizem respeito à segurança e, portanto, serão tratadas como sem SIL (SIL 0). Esta análise e alocação do nível de segurança das funções devem obedecer às seguintes etapas do processo de segurança:

1. Decomposição funcional do Sistema PSD;
2. Análise de Contexto;
3. Avaliação de causa e efeito para cada perda de função;
4. Integração e associação de duas ou mais funções para a realização de uma determinada tarefa;
5. Avaliação das interferências externas às funções;
6. Avisos ou alertas quando de um provável desvio funcional;
7. Alocação dos Níveis de Segurança SIL às funções do Sistema PSD.

Decomposição Funcional do Sistema PSD

O Sistema PSD pode ser decomposto, construtivamente, da seguinte forma:

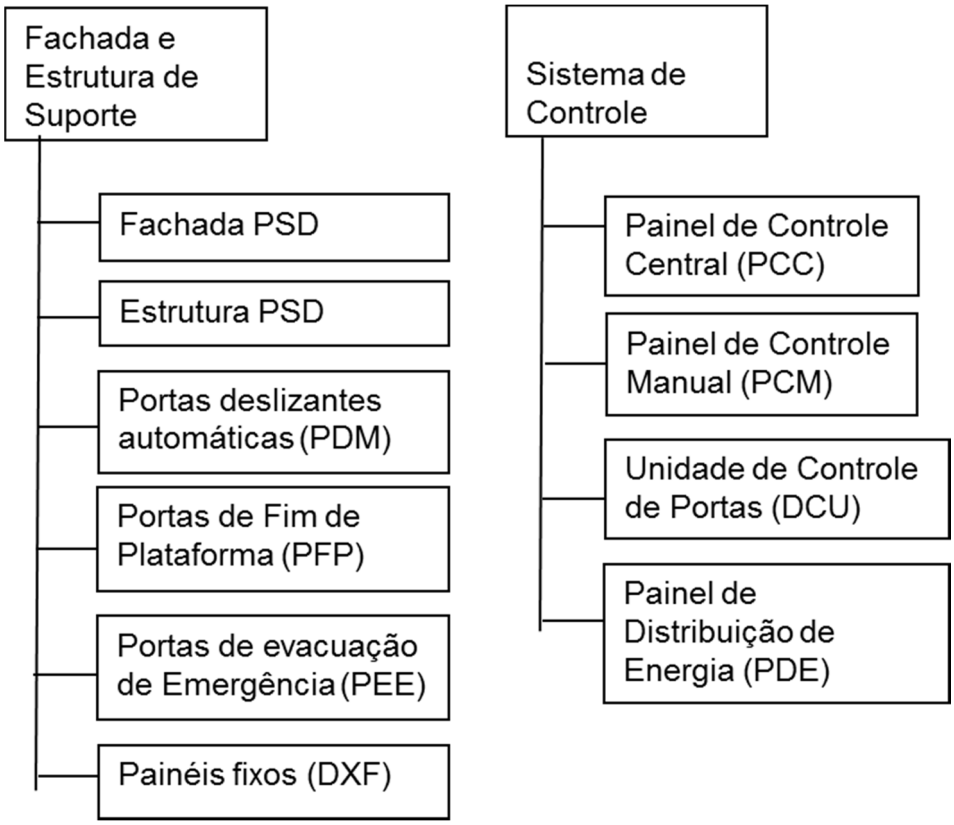

Figura 1 – Decomposição Construtiva do Sistema PSD

Funcionalmente, entretanto, o sistema PSD apresenta a seguinte forma:

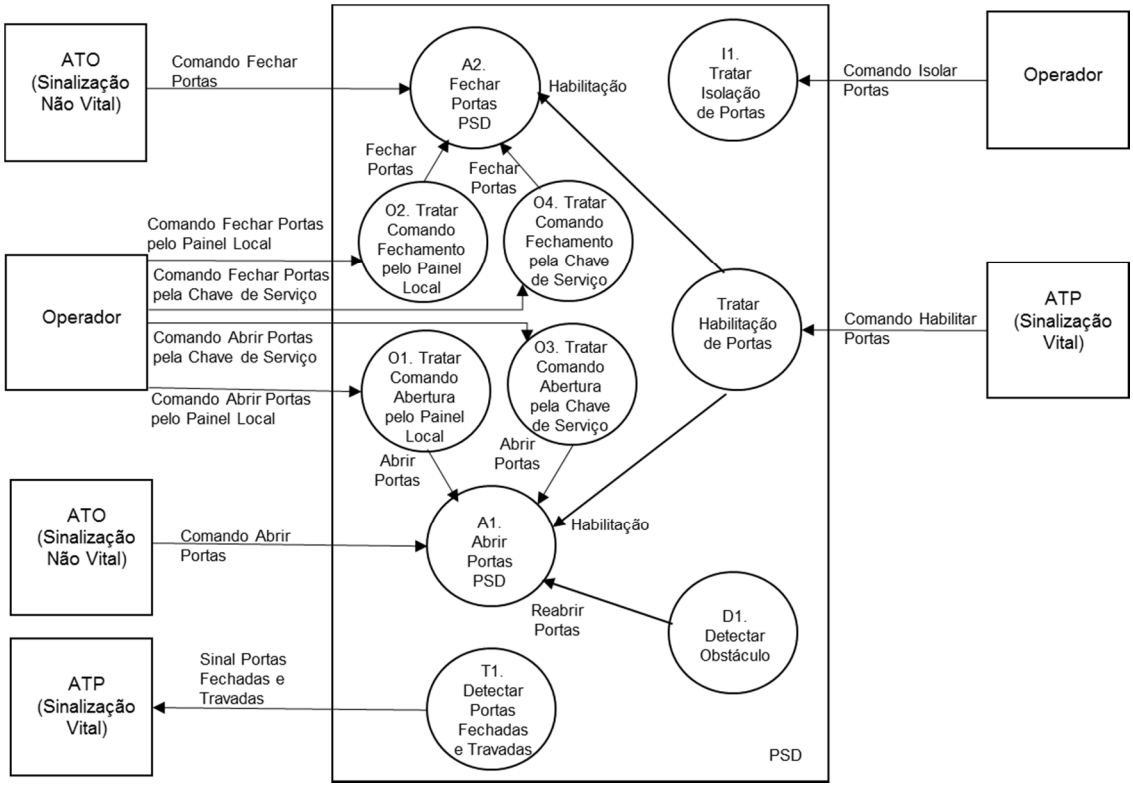

Figura 2 – Decomposição Funcional do Sistema PSD

Análise de Contexto

Na análise de contexto, identificam-se todos os sistemas externos, subsistemas, equipamentos e atores que interagem com o Sistema PSD. As técnicas OHSA (Occupational Health and Safety Act) e HAZOP (Hazard and Operability Study) ajudam a identificar os atributos e artefatos do sistema e suas interfaces, contextualizando-os de uma forma global, assim como, podem definir alguns modelos de cenários operacionais que podem realimentar as análises de perigos e de riscos. A figura a seguir ilustra o contexto do sistema PSD.

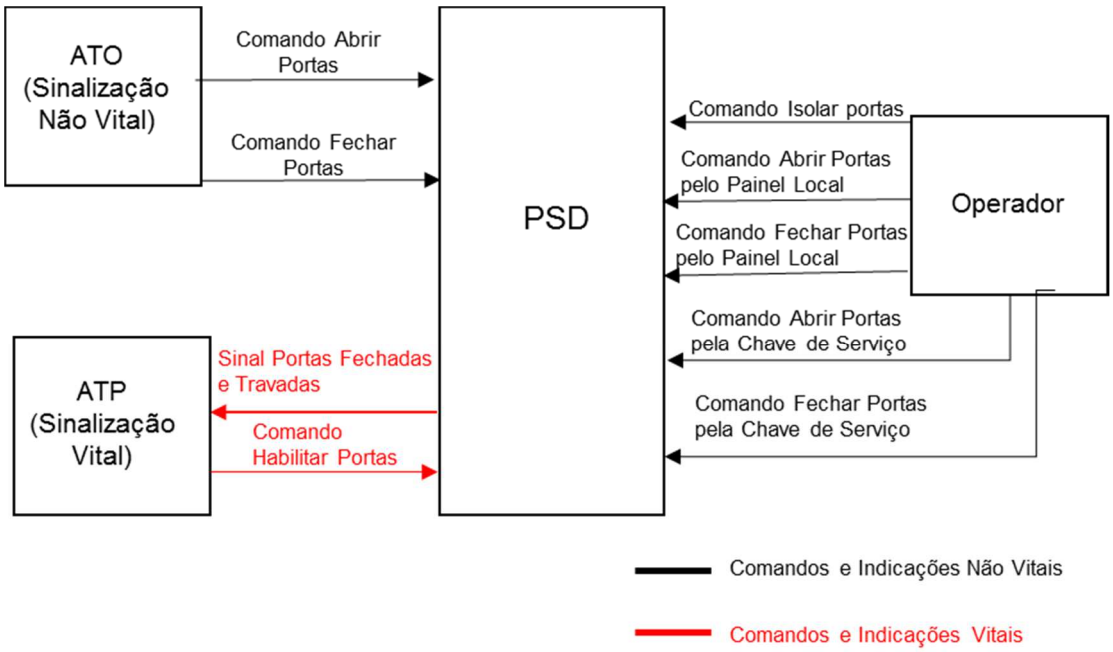

Figura 3 – Contexto do Sistema PSD

Como mostrado na figura, o Sistema PSD interage com o subsistema ATP, que é um dos subsistemas vitais do Sistema de Sinalização, por meio de comandos e indicações vitais.

Sua interação com o subsistema ATO, que é não vital e, com o Operador é, entretanto, efetuada por meio de comandos e indicações não vitais.

Ao se estudar o contexto entre os sistemas PSD, Sinalização e Material Rodante, tem-se o resultado mostrado na figura a seguir:

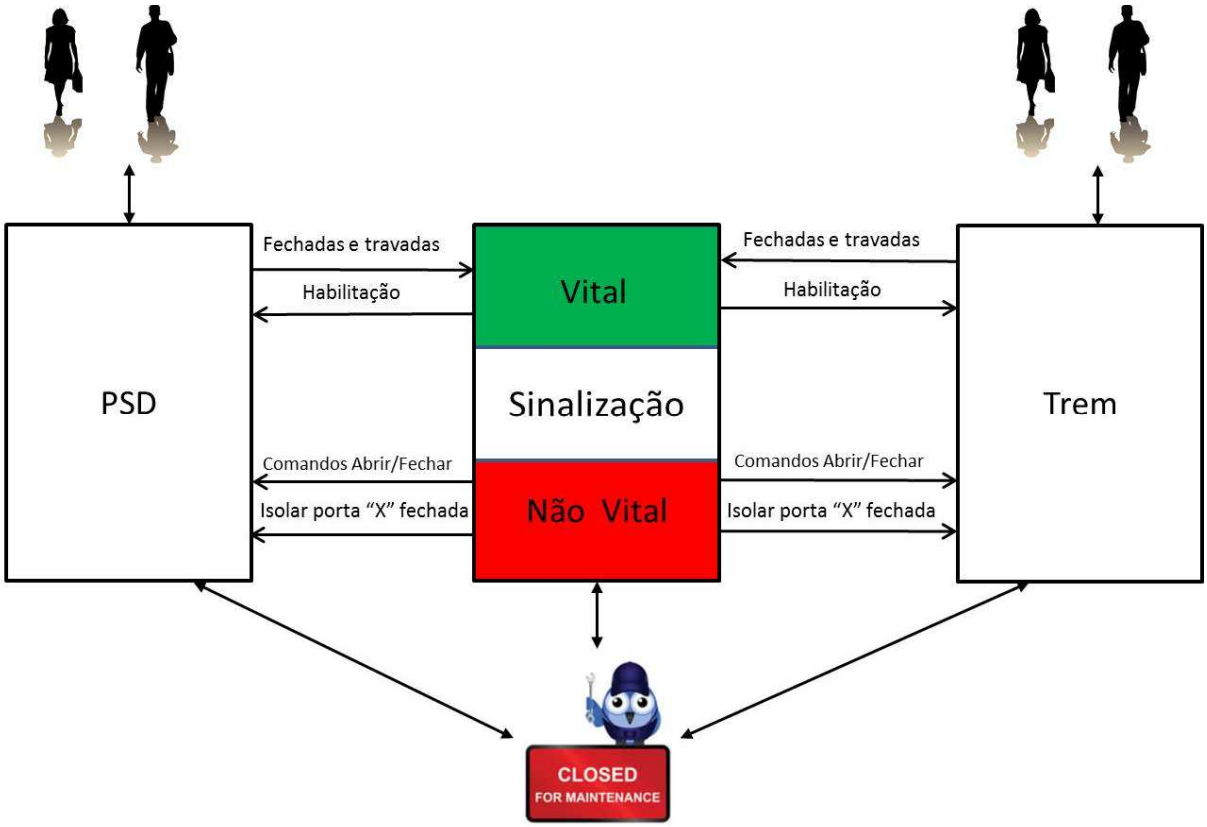

Figura 4 – Diagrama de Contexto dos Sistemas PSD, Sinalização e Material Rodante

Avaliação de causa e efeito para cada perda de função

As técnicas de Árvore de Falhas (FTA) e Modo de Falha e Análise de Efeitos Críticos (FMECA) contribuem nos estudos para se identificar os modos de falha potencialmente correlacionados com perdas integrais ou parciais das funções do Sistema PSD. Estas técnicas caracterizam as causas raízes e seus efeitos, determinando a probabilidade de cada evento de perda de função ocorrer, identificando inclusive o evento gatilho, o qual poderá ser criteriosamente analisado, eliminado ou mitigado.

Integração e associação de funções para a realização de uma determinada tarefa

Diante das correlações das funções de um sistema para executar uma determinada missão ou tarefa, faz-se necessário, neste estudo, não só identificar, analisar e classificar as funções de modo isolado, mas também avaliar a integração e associação das funções visando a identificação de alguma vulnerabilidade no nível de segurança da função quando incorporada a outras funções. O resultado deste tipo de avaliação pode delinear a arquitetura do sistema em dois grandes blocos: funções vitais e funções não vitais.

Avaliação das interferências externas às funções

Esta avaliação deve levar em conta todos os possíveis agentes externos que podem, de alguma forma, interferir no resultado de uma determinada função. Como exemplo, pode-se citar o estudo de interferências eletromagnéticas no sistema PSD.

Avisos ou alertas quando de um provável desvio funcional

A forma preditiva de um aviso ou um alerta antes da ocorrência de um evento indesejável pode colaborar para que o Sistema PSD não fique exposto a um perigo. Porém tal fato depende de um agente externo ao sistema, ou seja, que tal aviso ou alerta tenha sido corretamente disparado pelo sistema, mas, não se tem a garantia de que a ação preditiva tenha sido corretamente aplicada antes da ocorrência do evento indesejável. Este caso pode ser caracterizado como uma mitigação e uma exportação de uma determinada ação para o agente externo, o qual deve ou não aceitar este tipo de intervenção.

Alocação dos Níveis de segurança SIL às funções do Sistema PSD.

O critério adotado para analisar, classificar e eleger as funções do Sistema PSD, que exigem um maior nível de segurança SIL está baseado na utilização de uma metodologia de boas práticas dos estudos de segurança. Estas boas práticas são técnicas de análise de perigos e de riscos que orientam a identificação das funções do sistema PSD que devem possuir um SIL mais elevado, em razão da criticidade da funcionalidade a ser desempenhada, bem como a sua missão a ser executada.

A tabela 2 a seguir relaciona as principais funções estudadas.

Tabela 2 - Principais funções do sistema PSD

Função Principal	Index	Função de Segurança
Permitir ao usuário movimentar-se entre o trem e a plataforma com segurança.	**A1**	**Abertura automática das portas de acordo com o Sistema**
	A2	**Fechamento automático das portas de acordo com o Sistema**
Permitir ao pessoal operativo controlar o sistema PSD (modo degradado)	**O1**	**Abertura das portas através do painel Local**
	O2	**Fechamento das portas através do painel Local**
	O3	**Abertura da porta pela chave de serviço**
	O4	**Fechamento da porta pela chave de serviço**
Transferência de dados para a partida do trem	**T1**	**Enviar o estado das portas fechadas e travadas para o Sistema**
	T2	**Enviar o estado de portas fechadas e travadas para a Operação degradada**
Permitir o desembarque dos usuários do trem na plataforma	**P1**	**Permitir a saída dos usuários do trem para a plataforma**
Habilitar portas	**H1**	**Habilitar portas**
Detectar um obstáculo	**D1**	**Detectar um obstáculo**
Isolar uma porta	**I1**	**Isolar uma porta**
Assegurar a integridade do PSD	**N1**	**Manter as portas na condição fechada e travada sem a presença de um trem alinhado na plataforma**

As técnicas de análise de perigos utilizadas, segundo as boas práticas utilizadas na Companhia do Metrô de São Paulo, são listadas a seguir:

- Análise de Perigos, compreendendo:
- PHA – Análise Preliminar de Perigos;
- SHA – Análise de Perigos do Sistema;
- SSHA – Análise de Perigos do Subsistema;
- IHA – Análise de Perigos de Interface.
- OHSA (Occupational Health and Safety Act).
- Árvore de Falhas (FTA).
- Modo de Falha e Análise de Efeitos Críticos (FMECA).
- HAZOP (Hazard and Operability Study).
- ALARP (As Low As Reasonably Practicable).

Os estudos de Hazard, OHSA e HAZOP ajudam na identificação dos perigos e cenários operacionais, sendo que, as fontes de ideias deste estudo foram as recomendações Europeias - MOD SAFE e as experiências e lições apreendidas em projetos anteriores do estudo de caso do sistema PSD.

Já os estudos FTA e FMECA contribuíram para determinar as causas raiz e as probabilidades de ocorrência de eventos indesejados, bem como avaliar os efeitos e consequências dos modos de falha potenciais.

O ALARP foi utilizado para classificar e selecionar os itens dos estudos anteriores mais relevantes segundo a premissa adotada de um maior número de pessoas expostas aos perigos identificados.

Para este estudo foram, também, seguidas as práticas e diretivas da norma IEC 62425, norma equivalente à norma CENELEC EN 50129, que trata da segurança de um produto ou sistema em um Caso de Segurança (em Inglês "Safety Case").

As práticas e diretivas de outras duas normas correlatas foram, também, tomadas como base para este estudo: a norma IEC 62278, equivalente à norma CENELEC 50126, que trata do Sistema de Gerenciamento da Segurança em projetos metroferroviários e a norma IEC 62279, equivalente à CENELEC EN 50128, que trata do gerenciamento de software de segurança.

ANÁLISE DOS RESULTADOS

A aplicação das técnicas descritas acima permitiu avaliar a criticidade (vital e não vital) de cada função do Sistema PSD e alocá-las ao nível de segurança SIL necessário. Os resultados são mostrados na tabela 3, que traz as principais funções deste sistema elencadas pela sua criticidade e classificadas pelos níveis de segurança SIL adequados.

Tabela 3 - Funções do sistema PSD listadas pela criticidade e alocadas ao Nível SIL adequados

Index	Função de Segurança	Evento indesejado / vulnerabilidade de segurança	SIL exigido
A1, O1, O3, H1	Abertura das portas de acordo com o Sistema, Painel Local ou Chave de Serviço	Abertura espúria de uma ou várias portas quando o trem não está corretamente estacionado. Passageiro pode cair na via (evento crítico)	SIL 3
A2, O2, O4, H1	Fechamento das portas de acordo com o Sistema, Painel Local ou Chave de Serviço	Não há questão de segurança, apenas consequência na operação (retardo) devido ao circuito de segurança.	Não há SIL (SIL 0)
T1, T2	Enviar o estado das portas fechadas e travadas	Uma porta pode não estar no estado fechada e travada e não ser detectada. A partida do trem é autorizada e um passageiro pode cair na via (evento crítico)	SIL 3
P1	Permitir o desembarque dos usuários do trem na plataforma	Não há abertura manual da porta. Passageiro não consegue sair do trem. Em caso de emergência, esta situação é catastrófica.	SIL 2
D1	Detectar um obstáculo	Prensar um passageiro entre as folhas de porta durante o processo de fechamento (evento marginal)	SIL 2
		Prensar um passageiro entre o PSD e o trem (evento crítico)	SIL 3
I1	Isolar uma porta	Não há questão de segurança, apenas consequência e indisponibilidade da porta isolada para a Operação	Não há SIL (SIL 0)
N1	Manter as portas na condição fechadas e travadas sem a presença de um trem alinhado na plataforma	Abertura espúria de uma porta quando o trem não está corretamente estacionado na estação. Passageiro pode cair na via (evento crítico)	SIL 2

CONCLUSÕES

Em função de todas as premissas e estudos realizados neste trabalho, conclui-se que um Sistema PSD pode ter funções caracterizadas como vitais, as quais devem ser tratadas durante todo o ciclo de desenvolvimento deste sistema em conformidade com as regras e os processos necessários para se atingir um nível de segurança elevado.

Porém, existem outras funções do Sistema PSD que podem ser caracterizadas como não vitais, as quais não necessitam de todo um rigor de processo, pois, pela sua própria missão, ficou definida e categorizada nos estudos como uma função que não exige um nível de segurança elevado.

Diante destas abordagens, as quais estão baseadas em estudos e técnicas já consagradas, entende-se que o Sistema PSD pode, também, ser caracterizado como sendo um sistema crítico em relação à segurança. Suas funções eleitas com um nível de segurança elevado devem ser tratadas com todo o rigor para que as missões pertinentes à estas funções críticas sejam realizadas com sucesso, ou seja, para que os riscos associados às funções projetadas sejam reduzidos ou até mesmo eliminados, nas devidas proporções definidas em normas, tornando-os passíveis de serem aceitos no Sistema PSD.

REFERÊNCIAS BIBLIOGRÁFICAS

- A John Wiley & Sons, Inc. Publication - Hazard Analysis Techniques for System Safety
- Dr Michael J.M. Houtermans "SIL and functional safety in a Nutshell"
- Clive De Salis "Using Risk Graphs for SIL Assessment"
- Norma MIL-STD-882
- Norma IEC 62425 (CENELEC EN 50129)
- Norma IEC 62278 (CENELEC EN 50126)
- Norma IEC 62279 (CENELEC EN 50128)
- Norma IEC 61508