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

Rubens Navas Borloni – Companhia do Metropolitano de São Paulo
José Sabariego Ruiz Filho – Companhia do Metropolitano de São Paulo
George Eduardo Gomes de Faria – EGIS Engenharia e Consultoria

22ª Semana de Tecnologia Metroferroviária

22ª Semana de Tecnologia Metroferroviária 2016
AEAMESP
3º PRÊMIO TECNOLOGIA & DESENVOLVIMENTO METROFERROVIÁRIOS
ANPTrilhos
CBTU Companhia Brasileira de Trens Urbanos

Relevância

Os Sistemas PSD, "Platform Screen Doors" ou Portas de Plataforma, são cada vez mais presentes em novas linhas de metrô e em modernizações de linhas existentes.

No caso de linhas sem condutor ("Driverless“) ou, ainda, UTO, o sistema PSD torna-se obrigatório por requisitos de segurança.

O estudo dos níveis de segurança do PSD é de alta relevância para a garantia da segurança do sistema metroviário.

Objetivos do Trabalho

Determinar os conceitos, critérios e metodologia utilizados para a identificação, dos níveis de integridade de segurança - SIL - necessários às funções do PSD.

Conceito de Risco

O conceito de risco é a combinação de dois elementos:

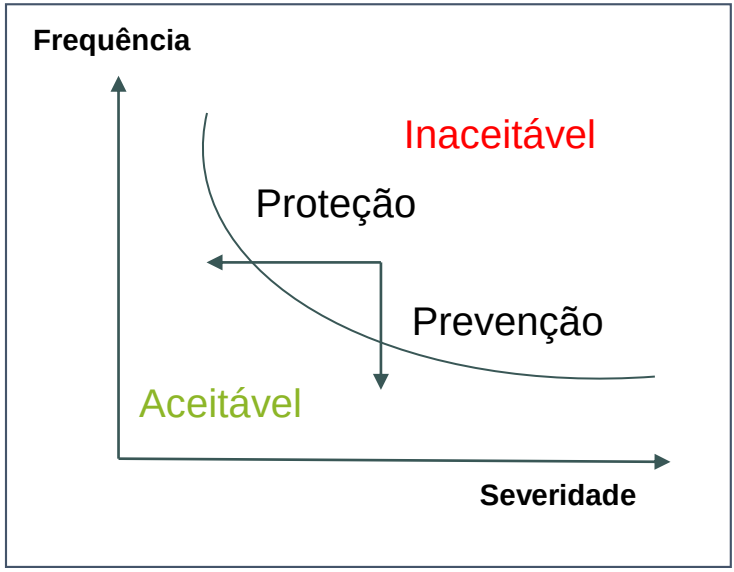
- A probabilidade de ocorrência de um evento ou combinação de eventos levando a um perigo, ou a frequência de tais ocorrências.
- As consequências de um perigo.

As normas CENELEC / IEC definem categorias qualitativas de frequências e consequências para elaboração da avaliação de riscos

Avaliação/Aceitação de Riscos (Norma EN 50126)

Frequência de ocorrência de um evento perigoso	**Níveis de Risco**			
Frequente	Indesejável	Intolerável	Intolerável	Intolerável
Provável	Tolerável	Indesejável	Intolerável	Intolerável
Ocasional	Tolerável	Indesejável	Indesejável	Intolerável
Remoto	Negligenciável	Tolerável	Indesejável	Indesejável
Improvável	Negligenciável	Negligenciável	Tolerável	Tolerável
Inacreditável	Negligenciável	Negligenciável	Negligenciável	Negligenciável
	Insignificante	**Marginal**	**Crítico**	**Catastrófico**
	Níveis de Severidade das Consequências de Perigos			

Objetivos do processo de segurança: Redução do Risco



2 tipos de medidas de redução de risco:

- Medidas de Prevenção:

Medidas que permitem a redução da frequência do acidente

- Medidas de Proteção:

Medidas que permitem a redução da gravidade das consequências do acidente

Exemplo de Redução de Risco: Queda de passageiros na via

Prevenção: Pisos táteis nas plataformas

Proteção: Poço de Segurança

Perigo / Acidente / Consequências

Nível de exposição	Probabilidade adotada (E)
Frequente ou permanente.	1
Rara ou excepcional.	10^{-1}
Muito rara.	10^{-2}

Probabilidade de Exposição ao Perigo (E)

Meios de redução do acidente	Probabilidade adotada (P)
Nenhuma barreira adicional.	1
Uma barreira.	10^{-1}
Duas barreiras.	10^{-2}

Probabilidade de Redução do Acidente (P)

Possibilidade de evitar a consequência	Probabilidade adotada (C)
Impossível para as pessoas evitarem.	1
Existe um meio possível para evitar.	10^{-1}
Existem dois meios independentes possíveis para evitar.	10^{-2}

Probabilidade de Redução da Consequência (C)

Referência : [32] DEL-D4.1_UITP_WP4_100318_V2.1-2010: WP4 – D4.1 – State of Art Analysis and Review of Results from Previous Projects – European Commission – Seventh Framework Programme – MODSafe Modular Urban Transport Safety and Security Analysis

Taxa tolerável de perigo e nível de severidade

THRm = THRn / (E.P.C)

Onde: THRn: taxa tolerável de perigo inicial (nível de severidade inicial)
THRm: taxa tolerável de perigo final (Nível de Segurança final)

Severidade da consequência/acidente	Faixa do THR (THR/hora/função)	THR inicial adotado (THRn)	Nível de Severidade (SLn)
4: Catastrófica: várias fatalidades	$10^{-9} \leq THR < 10^{-8}$	$THR_4 = 10^{-9}$	SL4
3: Crítica: ferimentos ou uma fatalidade	$10^{-8} \leq THR < 10^{-7}$	$THR_3 = 10^{-8}$	SL3
2: Marginal: pequeno ferimento	$10^{-7} \leq THR < 10^{-6}$	$THR_2 = 10^{-7}$	SL2
1: Insignificante	$10^{-6} \leq THR < 10^{-5}$	$THR_1 = 10^{-6}$	SL1

Referência : [25] DEL-D4.1_UITP_WP4_100318_V2.1-2010: WP4 – D4.1 – State of Art Analysis and Review of Results from Previous Projects – European Commission – Seventh Framework Programme – MODSafe Modular Urban Transport Safety and Security Analysis

O que é Nível de Integridade de Segurança - SIL

SIL – sigla em Inglês para "Safety Integrity Level" é um número que indica o grau necessário de confiança com que um sistema deve atender aos requisitos das suas funções de segurança especificadas em relação às falhas sistemáticas

O que é Nível de Integridade de Segurança - SIL

Table 3 — Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in high demand or continuous mode of operation

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE See notes 3 to 9 below for details on interpreting this table.	

Referência da IEC 61508 – Tabela 3

Table A.5.1: SIL-table

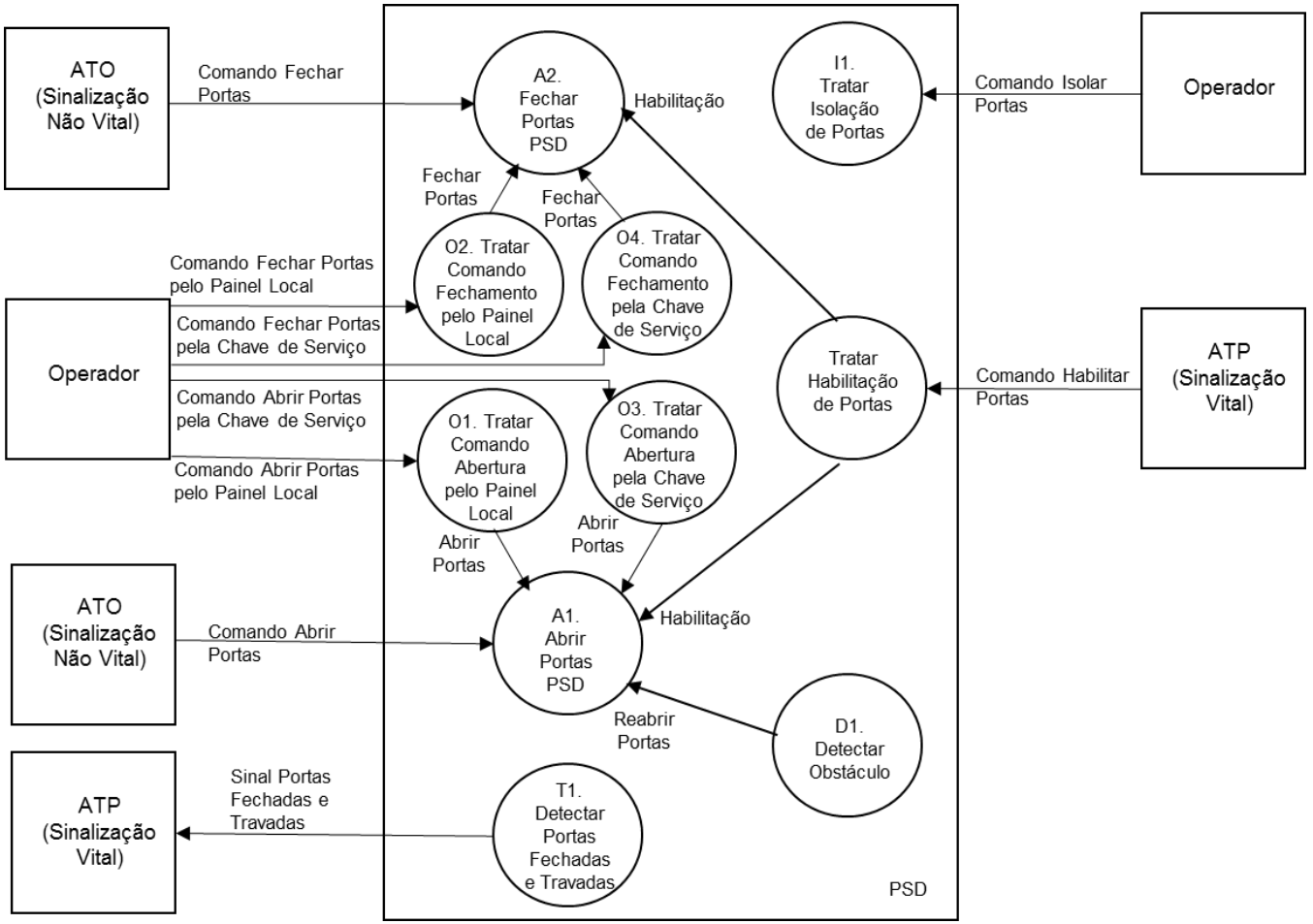
Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Referência da CENELEC – EN 50129– Tabela A.5.1

Metodologia do Processo de Segurança do PSD

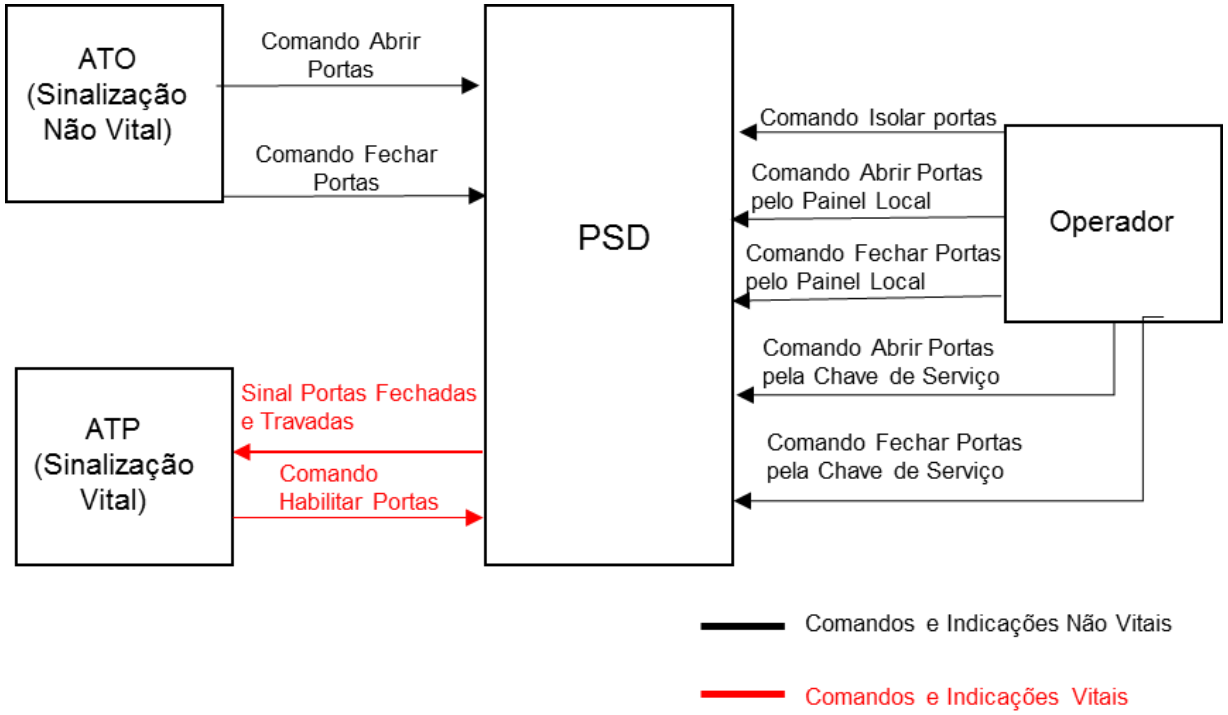
1. Decomposição funcional do Sistema PSD;
2. Análise de Contexto;
3. Avaliação de causa e efeito para cada perda de função;
4. Integração e associação de duas ou mais funções para a realização de uma determinada tarefa;
5. Avaliação das interferências externas às funções;
6. Avisos ou alertas quando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

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



Avaliação de causa e efeito para cada perda de função

As técnicas de Árvore de Falhas (FTA),
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.

Integração e associação de 2 ou mais 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.

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.

Alocação dos Níveis de Segurança SIL às funções do PSD – Técnicas utilizadas pela CSMP

- PHA - Análise Preliminar de Perigos;
- SHA - Análise de Perigos do Sistema;
- SSHA – Análise de Perigos do Subsistema;
- IHA - Análise de Perigos de Interface.
- O&SHA - Análise de Perigos de Operação e Suporte.
- FTA - Árvore de Falhas.
- FMECA - Modo de Falha e Análise de Efeitos Críticos.
- HAZOP - (Estudo de Perigos e Operabilidade.
- ALARP - Limite Aceitável de Risco.

Alocação dos Níveis de Segurança SIL às funções do PSD – Resultados

				Análise de Risco			THRn - **Taxa inicial** Tolerável do Perigo		THRm - **Taxa final** Tolerável do Perigo				
Função Principal	Perigo	Efeito	Causa	Gravidade	Probabilidade	Categoria de Risco	THRn	**SLn**	E	P	C	**SIL**	Função de Segurança
Permitir ao passageiro se movimentar entre o trem e a plataforma com segurança.	Queda de passageiros na via	Mortes, atropelamentos e eletrocussões	Abertura indevida das portas deslizantes de plataforma sem trem alinhado	Catastrófica	Ocasional	Intolerável	10^{-9}	**4**	1	10^{-1}	1	**3**	Habilitar de forma segura o comando de abertura
			Sinalização indevida de portas deslizantes de plataforma fechadas	Catastrófica	Ocasional	Intolerável	10^{-9}	**4**	1	10^{-1}	1	**3**	Indicar de forma segura portas fechadas e travadas
	Queda de um passageiro na via	Morte, atropelamento e eletrocussão	Abertura indevida de uma porta deslizante de plataforma sem trem alinhado	Crítico	Ocasional	Indesejável	10^{-8}	**3**	1	10^{-1}	1	**2**	Alimentar o Motor a partir de dois sinais da lógica de portas (2oo2)
Detectar um Obstáculo	Ferimento dos passageiros durante o processo de fechamento das portas deslizantes de platforma	O passageiro pode se ferir.	A porta pode fechar com força ou velocidade excessiva.	Marginal	Remoto	Tolerável	10^{-7}	**2**	1	10^{-1}	1	**1**	Movimentar a porta deslizante com limite de força e velocidade das folhas (controle de corrente).
	Esmagamento do passageiro entre a porta deslizante de plataforma e o trem ou queda de passageiro na via	Morte, atropelamento e eletrocussão	Área suficiente entre o trem e a fachada da porta de plataforma	Crítico	Ocasional	Indesejável	10^{-8}	**3**	1	10^{-2}	1	**1**	Evitar que o passageiro possa situar-se entre a PDM e o trem. Manter a distância entre o PDM e o gabarito do trem inferior a 200 mm.

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

Rubens Navas Borloni – rborloni@metrosp.com.br
José Sabariego Ruiz Filho – jsruiz@metrosp.com.br
George Eduardo Gomes de Faria – george.faria@egis-brasil.com.br

22ª Semana de Tecnologia Metroferroviária

22ª Semana de Tecnologia Metroferroviária 2016
AEAMESP
3º PRÊMIO TECNOLOGIA & DESENVOLVIMENTO METROFERROVIÁRIOS
ANPTrilhos
CBTU Companhia Brasileira de Trens Urbanos