25º SEMANA DE TECNOLOGIA METROFERROVIÁRIA

6º PRÊMIO TECNOLOGIA & DESENVOLVIMENTO METROFERROVIÁRIOS

CATEGORIA 3

INOVAÇÃO, INTEGRAÇÃO E AUTOMAÇÃO DE UMA LINHA DE METRÔ UTILIZANDO CENÁRIOS OPERACIONAIS

Introdução

De acordo com informações da <u>Comissão Permanente do Observatório de Metrôs Automatizados da UITP</u>, a extensão de linhas de metrô automatizadas no mundo atingiu em 2018 o marco quilométrico de 1000 km distribuídos em 63 linhas totalmente automáticas em 42 cidades de 19 países. Segundo dados históricos da Comissão, levou cerca de 30 anos para atingir o marco de 500 km a partir da operação comercial da 1ª linha de metrô totalmente automatizada do mundo em Kobe, no Japão, mas somente 8 anos para duplicá-lo graças a pujante expansão de linhas automatizadas na China.

A Figura 1 seguinte, extraída do <u>Relatório Mundial sobre Linhas Automáticas (julho de 2016)</u>, também de autoria da UITP, retrata melhor a aceleração deste avanço na automação de linhas de metrôs no mundo nas últimas quatro décadas e projeta um crescimento exponencial com perspectivas de superar o marco de 2000 km de linhas totalmente automáticas nos próximos anos.



Figura 1 – Crescimento total de linhas totalmente automáticas (em km de linha)

O aumento do grau de automatismo de uma linha permite obter um conjunto de vantagens aos gestores das operadoras, cujos benefícios se estendem às autoridades e aos passageiros por meio da oferta de um melhor serviço de transporte, pois a experiência operacional demonstra que uma solução, consolidada e automatizada do sistema, provê mais segurança, confiabilidade, disponibilidade e flexibilidade em relação as linhas convencionais, enquanto que o custo operacional é menor, aumentando a atratividade do transporte público.

A Figura 2 a seguir mostra a correlação inversa entre os níveis de automação de uma linha com suas despesas operacionais (OPEX). Embora o investimento inicial (CAPEX), para implantar uma linha totalmente automatizada, seja maior em relação às linhas com graus menores de automação, seu custo operacional é menor ao longo do tempo, possibilitando obter o retorno deste investimento adicional depois de um determinado período de operação.

Tal ganho nas despesas operacionais é obtido graças a maior eficiência na operação e na manutenção do empreendimento, sem contar com o diferencial de menor tempo de resposta em se adequar com os diferentes níveis de carregamento da linha ao longo

do dia e de desenvolver perfis de profissionais mais qualificados e com mais tempo disponível para atender necessidades dos passageiros de maneira mais plena e humana, uma vez que o operador deixa de estar confinado em uma cabine de trem, contribuindo para a excelência nos transportes e consequentemente melhoria na qualidade de vida urbana.

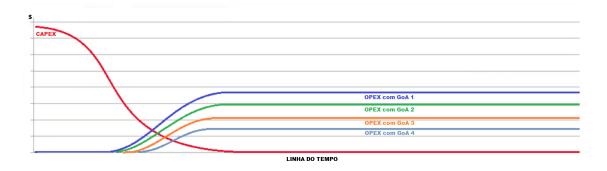


Figura 2 – Relação entre grau de automação de uma linha de metrô e despesas operacionais

Atualmente no Brasil existem duas linhas automáticas que já operam com trens sem cabine e com a via comercial totalmente segregada aos passageiros por meio de portas de plataforma (PSD): a Linha 4 - Amarela (inaugurada em 2010), e a Linha 15 – Prata (1º monotrilho brasileiro de média capacidade com operação comercial iniciada em 2015), sendo que ambas as linhas fazem parte da rede metroferroviária da cidade de São Paulo.

Para empreendimentos futuros de linhas de metrôs em São Paulo ou para a compra de novas frotas de trens, diversas áreas da CMSP, destacando-se a engenharia de projetos de sistemas, tem como premissa básica a concepção de sistemas que permita que uma nova linha, ou aquisição de nova frota de material rodante, opere no grau máximo de automação para metrôs.

Para as linhas existentes na companhia, atualmente operando com níveis de automação intermediários como a Linha 1-Azul, Linha 2-Verde e Linha 3-Vermelha,

cogita-se a modernização da maioria das frotas existentes e parte do sistema de sinalização visando o aumento do grau de automação para permitir a operação em GoA4, ou *Unattended Train Operation* (UTO), uma vez que o processo de instalação de portas de plataforma para estações dessas linhas já se encontra em andamento.

A Figura 3 a seguir mostra resumidamente as características de condução dos trens para os distintos níveis de automação para sistemas metroferroviários conforme a classificação da norma IEC 62267, com a possibilidade de algumas linhas incorporarem parte das características funcionais de níveis de automação adjacentes.

| Nível de automação | | Tipo de operação do trem | Trem em movimento | Parada do trem | Portas de plataforma | Operação em caso de emergência |
|-----------------------|---|-----------------------------|----------------------|-------------------|-------------------------|-----------------------------------|
| GoA1 | | ATP com condutor | Condutor | Condutor | Condutor | Condutor |
| GoA2 | | ATP e ATO com condutor | Automático | Automático | Condutor | Condutor |
| GoA3 | J | Driverless | Automático | Automático | Assistente | Assistente |
| GoA4 | | UTO | Automático | Automático | Assistente | Automático |

Figura 3 – Classificação do grau de automação segundo a norma IEC 62267

Geralmente em uma operação convencional, os trens operam de acordo com uma programação escalonada de oferta de trens, basicamente não existem agentes circulantes dentro do salão dos trens com foco no atendimento dos passageiros, as regras e procedimentos aos operadores e agentes são restritas e repetitivas, existe um potencial de erro humano, e a mitigação de falhas no material rodante, que surge durante a operação, necessita da intervenção humana a bordo.

Já os modelos de operação automática GoA3 e GoA4, a oferta de trens pode mais flexível e alinhada com a capacidade de carregamento necessária em determinado período em decorrência de não necessitar mais deslocar um operador até o trem para

despachá-lo, a percepção pelos passageiros da presença de agentes circulantes de prontidão no interior dos trens é maior, existe mais flexibilidade e dinamismo no papel de cada agente, o maior grau de automação remove riscos de erros humanos e, por fim, é possível mitigar algumas falhas no material rodante remotamente.

Segundo a experiência de algumas operadoras de linhas de metrôs completamente automáticas, e que fazem parte do <u>Grupo de Benchmarking e Comunidade de Metrôs (CoMET/Nova)</u>, os fatores que podem pesar contra a operação automática são problemas de interface entre sistemas e mão de obra especializada durante a sua implementação, resgate em situações de emergência, maior tempo de recuperação após um incidente, tratamento do comportamento dos passageiros em situações de superlotação, incertezas na relação custo/benefício no modelo de negócios, maior investimento inicial, e finalmente maior sensibilidade a defeitos técnicos e riscos ocultos.

Em termos de confiabilidade, de acordo com informações da <u>Keolis</u> no 4° Seminário da UITP de Metrôs Automáticos, empresa francesa subsidiária da SNCF que projeta e opera sistemas de transporte público em uma escala global, a disponibilidade de sistemas de transporte com a presença humana do operador no trem é de 96-98% comparada com 99% a 99,99% de sistemas sem operadores ou assistentes embarcados.

Embora os sistemas GoA1 e GoA2 colecionam mais incidentes em relação aos novos sistemas que já operam com grau de automação GoA4, seja em razão da maior suscetibilidade de ocorrência de falhas humanas, acidentes com passageiros na plataforma ou de seu longo histórico de operação, o tempo de resposta na

recuperação é menor com a presença de operadores no local. Já linhas GoA4 configuradas como GoA3⁺, onde se prevê a presença de agente no salão do trem para agir prontamente na normalização da operação em casos de emergência, tem um nível de confiabilidade maior e pode ser uma estratégia a ser aplicada, se necessário.

Dependendo do tipo de cenário degradado, existe também a flexibilidade de combinar um grau de automação diferente ao GoA4 na condução de trens com falhas em um mesmo carrossel, desde que analisada a criticidade de cada falha, e que a decisão de mitigação, durante a operação comercial, seja a presença de um assistente embarcado para supervisionar e atuar localmente quando necessário, minimizando assim incertezas que possam demandar ações pontuais remotas e riscos de evacuação de passageiros ao longo da via em regiões de interestação.

Segundo informações do Conselho Permanente para Análise de Segurança de Incidentes com os Sistemas Operacionais (COPESE) da CMSP, e também dados estatísticos da *Federal Railroad Administration* (FRA), indicam que uma parte relevante das questões relacionadas as falhas e incidentes foram provocadas por ações equivocadas do ser humano. Existe também uma relação direta entre a ocorrência de falhas humanas com uma baixa qualidade da documentação ao longo do ciclo de vida de um projeto, com gaps originados desde as fases iniciais de concepção e que se estendem até os processos de operação e de manutenção da linha.

Somente como definição, entende-se como o ciclo de vida de um projeto um conjunto de tarefas e recursos necessários para atingir um determinado objetivo, que possui escopo, custo e prazo definidos. Também agrega processos de manutenção e operação, com tarefas e recursos rotineiros, bem como seus respectivos indicadores,

visando o atendimento pleno do objetivo durante um período predeterminado de tempo.

Nos registros históricos da COPESE, existem erros operacionais causados por decisões equivocadas pelos operadores durante o modo condução manual em regiões de intertravamentos, na via comercial ou no pátio, por exemplo em uma situação degradada devido a falha no equipamento de sinalização, onde o trem passa pelo aparelho de mudança de via (AMV) sem rota alinhada, mesmo que exista um sinaleiro fechado e um procedimento operacional claro para este tipo de cenário.

Em outros casos, também caracterizados como erros operacionais ou operações indevidas, as recomendações da COPESE resultam em ajustes em procedimentos, manuais e treinamentos. As demais possíveis causas de falhas são manutenção indevida, procedimento ou documentação inadequados, falhas de equipamentos ou sistemas, erros de projetos, e até mesmo ocorrências com causa caracterizada como desconhecida após o período de investigação.

A tomada de decisão, para aumento do grau de automação no transporte metroferroviário, considera basicamente três importantes aspectos inter-relacionados:

- Incremento da capacidade de transporte
- Maior assertividade, garantida pela automação e padronização de operação
- Otimização e economia no uso da energia e recursos

O nível de automação UTO possui uma relação direta com a integração entre os Sistemas de Sinalização e Controle, Material Rodante, Sistema de Controle Centralizado, Telecomunicações e as Redes de Comunicação, mas também com o Sistemas de Energia, Fluxo de Passageiros e Auxiliares de uma Linha, de forma que

todos os requisitos necessários de projeto, de operação e de manutenção, bem como na aplicação de inovações que visam, por exemplo, obter ganhos em padronização e na otimização de recursos, sejam plenamente atendidos.

Para a concepção de projetos de sistemas críticos, tais como sinalização e material rodante, que se destacam pelo seu alto nível de complexidade funcional, principalmente para a implantação ou modernização de linhas de Metrô totalmente automáticas, ou seja, sem a necessidade de operadores ou assistentes no interior dos trens, é primordial que seja feita a análise dos diversos cenários operacionais de linhas existentes (análise reativa), assim como a análise preliminar de riscos (análise proativa) para o novo empreendimento, que identifica riscos já na etapa inicial do projeto para o devido monitoramento e controle ao longo de seu ciclo de vida.

Ao se avaliar a dinâmica dos cenários operacionais atuais, cria-se uma base de conhecimento sólida para rever e retroalimentar os registros dos riscos, requisitos e especificações de sistemas, visando o atendimento das exigências recomendadas para o nível máximo de automação requerido em empreendimentos futuros.

O propósito deste trabalho é apresentar uma metodologia que mapeia e estrutura possíveis cenários operacionais partindo de uma base de conhecimento de macroprocessos de operação, existentes na CMSP, correlacionando-os com premissas e critérios de gerenciamento de riscos, visando o aumento do grau de automação de um empreendimento metroferroviário segundo normas internacionais, e de estar alinhado com as melhores práticas e lições aprendidas em questões fundamentais que afetam a operação automática dos metrôs.

A partir desta correlação entre os macroprocessos existentes de operação com as premissas e critérios segundo normas internacionais, tais como IEEE 1474, IEC 62290-1 e IEC_PAS 62267_DTO_UTO, abre-se espaço para propor melhorias em projetos de sistemas que, somadas com o expertise técnico interno de operação e manutenção, permite também a automação de processos, testes de sistemas e verificação das condições operacionais, revisitando e aferindo então os registros dos riscos e requisitos especificados nos projetos de sistemas para as novas linhas de metrô com uma visão sistêmica, global e consolidada através da análise crítica requerida para o grau de automação UTO.

Além de propor melhorias e inovações nos sistemas e processos existentes, o resultado final deste trabalho será um <u>BOOK de Cenários</u>, que irá compor parte do Edital de Contratação para as novas linhas.

Descrição

Uma vez que sistemas com a filosofia UTO também são passíveis de falhar durante a operação, a análise de cenários operacionais ou *Operational Safety Hazard Analysis* (OSHA) é um instrumento vital para a garantia da segurança (*Safety and Security*) em um sistema de transporte.

Os macroprocessos operacionais existentes são resultados da análise das ocorrências que afetaram a operação comercial ao longo dos anos, visando otimizar a redução do tempo de paralisação na circulação de trens, e por consequência, manter o intervalo entre trens aderente com a programação horária. Considerando que o Centro de Controle tem a visão geral dos sistemas, tomar uma decisão que afete qualquer um

dos sistemas controlados, se baseando em informações remotas e provenientes de operadores do sistema em campo, pode gerar efeitos colaterais comprometedores para a operação comercial.

O nível de automação GoA4 – UTO, com a inserção dos cenários operacionais, deve contemplar uma miríade de ações e mitigações necessárias, identificadas e consolidadas, nas análises de maneira tal que o sistema seja capaz de interagir, com a ajuda da ação humana, na tomada de decisão mais adequada.

Uma vez que o sistema de automação detecta uma ocorrência, informa a situação ao Centro de Controle e, de acordo com o contexto geral, verificado pela ação humana, a interação entre ambos, contextual e cartesiana, determina a tomada de decisão mais precisa e assertiva.

Se for analisado os índices de confiabilidade dos sistemas, pode-se afirmar que os mesmos possuem um nível de assertividade mais "determinístico" se comparado com as ações humanas, as quais sofrem influências "não determinísticas" que podem afetar a confiabilidade da mitigação dos riscos. Dessa forma, recomenda-se uma interação equilibrada entre o ser humano e o resultado das funções do sistema, de forma que a confiabilidade na tomada de decisão seja mais assertiva, garantindo maior precisão nas atuações humanas nas ocorrências.

A integração dos sistemas é uma condição primordial e essencial no nível de automação GoA4 – UTO, pois, toda função de segurança, necessária para a mitigação de um determinado risco, deve ser automática e concebida com o nível de segurança (SIL) adequado ao risco a ser mitigado. Quanto a automação de alguns processos, é preciso realizar a análise de valor agregado com base nas taxas de falha dos elementos

do sistema, ponderando os ganhos obtidos, uma vez que o ser humano pode corroborar em decisões que envolvam análises contextuais e subjetivas.

Metodologia

Visando dar início ao estudo de mapeamento de cenários operacionais, no começo de abril de 2019 foi criado um plano de trabalho preliminar com propostas de metas de entregas dos cenários por sistemas e unidades construtivas em uma linha de tempo, que posteriormente foi ajustado pelo grupo de trabalho, composto por representantes das áreas de projeto, operação e manutenção, adequando-o para as demandas e prioridades da empresa.

A Figura 4 a seguir mostra a linha de base das entregas de cenários deste estudo, previstas até julho de 2020, bem como os produtos que serão gerados ao final do trabalho. É importante destacar para este processo que as funções de sistemas serão ponderadas, validadas e especificadas sobre uma análise sistêmica de riscos para cada cenário, e que *gaps* de mitigação de riscos e em automação dos sistemas existentes, que poderão surgir nesse estudo, irão pavimentar a introdução de inovações tecnológicas, desde que justificadas, na especificação de sistemas de novas linhas de metrôs.

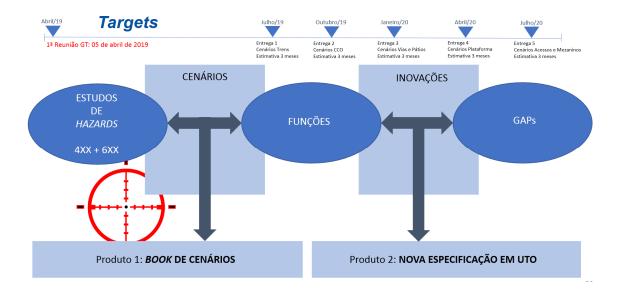


Figura 4 – Entregas de cenários e produtos previstos neste estudo

Visando obter matéria prima e subsídios para o levantamento de informações e discussões sobre cenários operacionais, primeiramente acessou-se a base de conhecimento de 50 anos de operação da CMSP e foi feita uma análise preliminar da documentação da área operacional da empresa através de consultas ao Sistema de Gestão de Documentação (SGD) da Gerência de Operações (GOP) hospedado na intranet. Foram então mapeados todos os procedimentos operacionais (PO), manuais operacionais (MO) e comunicados (COM) existentes, sejam estes implantados, em implantação, revisados ou cancelados pela área operacional da empresa.

Com o auxílio de planilhas, o material foi classificado por categoria, macroprocesso, posto, linha, dentre outras informações com o propósito de identificar procedimentos operacionais relacionados aos cenários em condições nominais e degradadas. Em linhas gerais, na empresa existem 489 procedimentos operacionais implantados ou válidos (levantamento realizado em 18/03/2019) classificados conforme a Tabela 1 a seguir:

| CLASSIFICAÇÃO DO PO | QTY DE PO |
|--|-----------|
| VIA E SALA TÉCNICA | 54 |
| PÁTIO | 51 |
| ADMINISTRAÇÃO DO POSTO | 43 |
| SUBESTAÇÃO GERAL | 36 |
| ESTRATÉGIAS OPERACIONAIS | 35 |
| TERCEIRO TRILHO E REDE AÉREA | 28 |
| ROTINAS DE SEGURANÇA | 22 |
| PA | 19 |
| TREM-VIA | 17 |
| ARRECADAÇÃO | 13 |
| EQUIPAMENTOS AUXILIARES | 10 |
| SUBESTAÇÃO RETIFICADORA | 10 |
| SUBESTAÇÃO AUXILIAR | 9 |
| TREM-GERAL | 9 |
| ADMINISTRAÇÃO DE PESSOAL | 7 |
| cco | 7 |
| COMPUTADORES - EQUIPAMENTOS | 7 |
| CONTROLE DE FLUXO NA ESTAÇÃO | 7 |
| DETECÇÃO DE INCÊNDIO | 7 |
| OCORRÊNCIAS OPERACIONAIS | 7 |
| SUBESTAÇÃO PRIMÁRIA | 7 |
| SUBESTAÇÕES RETIFICADORAS E AUXILIARES | 7 |

| | _ |
|--|-----|
| COMUNICAÇÃO FORMAL | 6 |
| SISTEMA DE FALHAS | 6 |
| TREM-PÁTIO | 6 |
| "SOFTWARE" | 5 |
| EQUIPAMENTOS DE FLUXO | 5 |
| TELEFONIA E SINALIZAÇÃO | 5 |
| "NO BREAK" | 4 |
| ATENDIMENTO AO USUÁRIO | 4 |
| CAMPANHAS | 4 |
| FLUXO DE USUÁRIOS | 4 |
| HIDRÁULICA | 4 |
| RÁDIO | 4 |
| SISTEMA DE GESTÃO DA QUALIDADE | 4 |
| VENTILAÇÃO | 4 |
| CONVIVÊNCIA OPERACIONAL ENTRE EMPRESAS | 2 |
| FISCALIZAÇÃO DE BILHETES | 2 |
| ILUMINAÇÃO | 2 |
| ÁREAS AJARDINADAS | 1 |
| DTS / STD | 1 |
| EVENTOS | 1 |
| INTEGRAÇÃO | 1 |
| LIMPEZA | 1 |
| PUBLICIDADE | 1 |
| QUANTIDADE TOTAL DE PO | 489 |

Tabela 1 – Classificação dos procedimentos operacionais implantados na CMSP

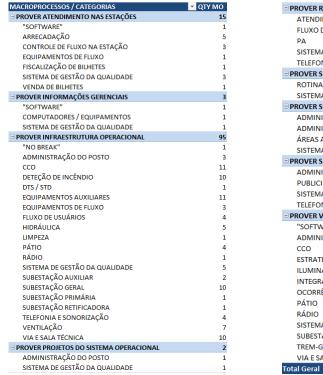
Quanto ao histórico de procedimentos revisados nas últimas décadas, destaca-se um grande número de revisões relacionadas a programação de oferta de trens e a emissão de PA nos empreendimentos mais recentes como a Linha 15-Prata, a extensão da Linha 5-Lilás, obras na Linha 4-Amarela e implantação do CBTC na Linha 2-Verde, conforme listado na Tabela 2 a seguir.

| DESCRIÇÃO DO PO | N° REVISÕES |
|--|-------------|
| PROGRAMAÇÃO DA OFERTA DE TRENS | 266 |
| EMISSÃO DE PA - TESTES NO SISTEMA NA LINHA 15-PRATA | 105 |
| ALTERAÇÃO DE TARIFAS | 44 |
| EMISSÃO DE PA - TESTES DE CBTC NA LINHA 5- LILÁS | 44 |
| EMISSÃO DE PA - OBRAS NA LINHA 4 - AMARELA | 40 |
| EMISSÃO DE PA - MODERNIZAÇÃO - IMPLANTAÇÃO DE CBTC NA LINHA 2-VERDE | 32 |
| EMISSÃO DE PA - TESTES NO SISTEMA DA LINHA 15-PRATA | 29 |
| UTILIZAÇÃO DOS EQUIPAMENTOS DE SINALIZAÇÃO E VIA PERMANENTE DA L15 - PRATA | 29 |
| ESTRATÉGIA DE OPERAÇÃO DA LINHA 1-AZUL | 27 |
| RETIRADA DE OBJETO DA VIA | 27 |
| BILHETES | 26 |
| ESTRATÉGIA PARA EMBARQUE DE USUÁRIOS PREFERENCIAIS | 25 |
| EMISSÃO DE PA - INSTALAÇÃO DE PORTAS DE PLATAFORMA EM VTD | 24 |
| SEGURANÇA ELÉTRICA PARA SERVIÇOS DE INSPEÇÃO E MANUTENÇÃO NAS VIAS DA LINHA 1-AZUL | 24 |
| OPERAÇÃO DOS TRENS EM CONDIÇÕES ADVERSAS NA VIA PRINCIPAL | 23 |
| ATENDIMENTO EM PRIMEIROS SOCORROS | 22 |
| ATUAÇÃO EM SITUAÇÕES DE EMERGÊNCIA | 22 |
| EMISSÃO DE PA - FIO DE CONTATO DA REDE AÉREA NA LINHA 5-LILÁS | 21 |
| INSPEÇÃO DE ROTINA NAS VIAS, SAÍDAS DE EMERGÊNCIA E DE VENTILAÇÃO | 21 |
| ANÁLISE DE INCIDENTES NOTÁVEIS | 20 |

Tabela 2 – Ranking de revisões de procedimentos operacionais

Dentro do contexto desse levantamento apresentado nas Tabelas 1 e 2, deve ser analisado se o aumento no grau de automação de uma linha pode ter influência na quantidade de procedimentos operacionais e na frequência de suas revisões.

Além dos procedimentos operacionais, no momento a empresa possui 193 manuais operacionais (MO) implantados que abrangem 9 macroprocessos, que visam prover o Atendimento nas Estações; Informações Gerenciais; Infraestrutura Operacional; Projetos do Sistema Operacional; Relacionamento e Informação do Cliente; Segurança Pública; Suporte Administrativo e Operacional, Suporte Gerencial; e Viagem. A Tabela 3 a seguir detalha as categorias de manuais por macroprocesso.



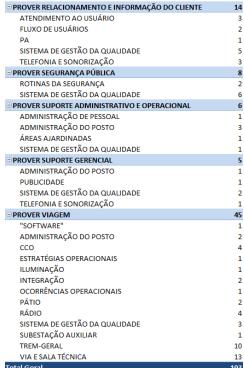


Tabela 3 – Relação categorizada de manuais operacionais vigentes na CMSP

Utilizando o material das listas de procedimentos e manuais operacionais da empresa em conjunto com a documentação de avaliação preliminar de riscos da Linha 6-Laranja, em comum acordo nas reuniões do grupo ficou consolidado <u>4 modos distintos</u>

de operação para a análise de cenários na perda de determinada função e que pode potencialmente comprometer a operação segura do sistema:

Modo de Operação Normal: operação quando todos os sistemas e subsistemas estão operando normalmente conforme projeto, não havendo a ocorrência de nenhum tipo de falha ou desastre natural.

Modo de Operação Degradado: operação durante períodos quando alguns sistemas ou subsistemas não estão operando conforme projeto, ou quando falhas humanas, desastres naturais ou outros fatores exigem uma ação operacional, mas sem representar ameaça à segurança das pessoas ou a graves danos materiais.

Modo de Operação de Emergência: operação após a ocorrência de uma emergência. Define-se como "incidente" uma ocorrência operacional anormal que resulta em danos a equipamentos e/ou à saúde e segurança humana. Incidentes muito graves podem ser chamados de "emergência", que ocorre quando um evento inesperado, geralmente, provoca riscos de vida ou implicações de perda extrema, requerendo atenção imediata.

Modo de Manutenção: manutenção preventiva ou operação durante o período de implantação dos sistemas.

Uma vez que o mapeamento e identificação dos riscos em cenários com perdas de função é a espinha dorsal deste trabalho, faz-se necessário também o agrupamento e comparação de parte da documentação existente dos projetos das linhas automáticas em operação e qualquer outro material já desenvolvido sobre o assunto, tal como informações de projeto básico da Linha 6-Laranja, de forma a identificar *gaps* entre

sistemas e/ou com recomendações de normas internacionais. A Figura 5 a seguir busca ilustrar a base de conhecimento disponível atualmente ao grupo de trabalho:

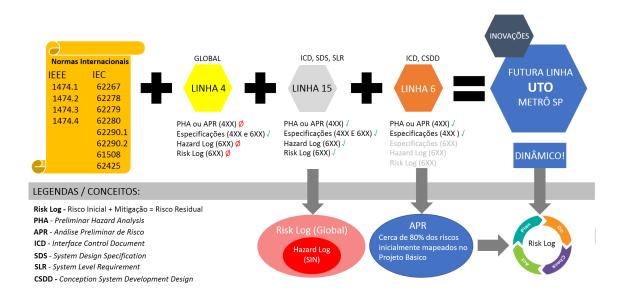


Figura 5 – Base de conhecimento

A análise preliminar de risco (APR) é um documento elaborado na etapa de projeto básico e que visa o mapeamento inicial de cerca de 80% dos riscos do empreendimento. Já o *Risk Log* e o *Hazard Log* são bancos de dados elaborados ao longo do ciclo de vida do projeto e que consideram todos os riscos do empreendimento de uma forma global, abrangendo todos os riscos iniciais e suas mitigações, bem como os riscos residuais e riscos secundários que possam surgir no plano de resposta ao risco.

No relatório de 2015 de Análise Preliminar de Riscos (APR) para a Linha 6 – Laranja, elaborado pelo Consórcio Move 6 São Paulo (AN-6.89.XX.XX/4XX-050), foram identificados 106 riscos relacionados aos sistemas e foram mapeadas 331 funções, ações ou requisitos para a mitigação dos riscos de sistemas, enquanto que foram identificados 121 riscos relacionados a infraestrutura civil e foram mapeadas 412 funções, ações ou requisitos para a mitigação dos riscos de civil.

Sistemas

| Cenário | Riscos |
|------------------------|--------|
| Normal | 47 |
| Emergência | 27 |
| Degradado | 18 |
| Manutenção | 12 |
| Normal / Degradado | 1 |
| Degradado / Emergência | 1 |

Civil

| Cenário | Riscos |
|------------------------|--------|
| Normal | 48 |
| Emergência | 38 |
| Manutenção | 29 |
| Degradado | 6 |
| Degradado / Emergência | 1 |
| | 122 |

106

Tabela 4 – Cenários de riscos para sistemas e para civil por modo de operação do APR da L6

A metodologia deste trabalho visa a realização de uma estimativa análoga do quantitativo de cenários operacionais, identificados nas bases de conhecimentos da empresa por meio dos procedimentos operacionais (PO), assim como na realização de uma estimativa paramétrica, associando o quantitativo de cenários operacionais multiplicado por um fator conhecido e determinado pelos estudos do APR.

Ao se iniciar qualquer projeto de linha de Metrô, uma das principais atividades preliminares, antes mesmo do escopo estar completamente definido, é a identificação dos perigos e a estimativa dos riscos, porém a plenitude no mapeamento na identificação dos perigos só será atingida com a caracterização precisa do sistema, ou produto, e do contexto de seu ambiente operacional, de forma a estimar os riscos associados bem como introduzir margens de segurança no projeto. Já os riscos precisam ser estimados corretamente a partir dos perigos, de forma que seja possível tomar as medidas adequadas para eliminá-los ou controlá-los.

Grande parte de um projeto metroferroviário está associada ao gerenciamento dos perigos, ou seja, estimar o potencial de ter consequências danosas aos sistemas de transporte e prejuízos às pessoas, com o grau de gravidade das ocorrências variando entre insignificantes a catastróficos, mas que geralmente os riscos podem ser reduzidos até um nivel aceitável, desde que aderentes a uma análise de custos

associada. Além do grau de gravidade, a probabilidade de ocorrência também faz parte análise sistemática do risco que deve ser estimado durante todo o ciclo de vida de um sistema ou produto, tanto para a mitigação quanto para o *feedback* sobre seu sucesso. Como exemplo, a seguir são mostrados os critérios adotados de classificação dos riscos para uma avaliação preliminar de um empreendimento metroferroviário:

- Frequência: (A- Frequente, B- Provável, C- Ocasional, D- Remota, E- Improvável e F-Incrível)
- Gravidade: (I- Catastrófico, II- Crítico, III- Marginal ou IV- Insignificante)
- Classificação de Controle: (INT- Intolerável, IND- Indesejável, TOL- Tolerável ou DES-Desprezível)

A partir da compreensão da causa e da classificação de um determinado do risco, é possível delinear a melhor estratégia de mitigação, seja ela uma ação operacional humana mais assertiva e documentada em um procedimento operacional, manuais com informações mais claras e estruturadas, treinamentos periódicos, alarmes de sistemas para o CCO em tempo real, *log* de falhas de sistemas para a manutenção preventiva, testes periódicos durante a inicialização de sistemas, recomendações para planos de manutenção pelos fornecedores, procedimentos rotineiros de manutenção, rotinas de restabelecimento, normalização de dispositivos após testes ou manutenção, requisitos e funções para projetos de sistemas, requisitos de arquitetura, civil e via permanente, dentre outros.

Em relação aos requisitos e funções de projetos de sistemas para a mitigação de riscos, a Figura 6 a seguir ilustra o variado contingente de sistemas comumente envolvidos na operação e manutenção de uma linha metroferroviária. Na especificação de um

projeto de sistemas, quando requisitos técnico-funcionais estão claramente relacionados com a segurança dos passageiros e/ou integridade do sistema, ou safety/security, mitigando riscos para determinados cenários operacionais, tais requisitos podem ser denominados também como requisitos de segurança.



Figura 6 – Exemplos de sistemas metroferroviários

A definição dos requisitos de segurança tem o propósito de vigorar medidas de controle de riscos e podem ser originadas por obrigações de segurança, de metas estabelecidas no início do processo de desenvolvimento ou de novos requisitos que venham a surgir a partir de uma atividade de risco, visando reduzi-la a um nível aceitável.

Os requisitos de segurança podem especificar:

- funções ou características específicas de um produto metroferroviário ou uma parte do setor metroferroviário;
- recursos de design e construção de processos;

- ações para controle de risco;
- características de práticas de manutenção ou operação;
- tolerâncias dentro das quais algo deve ser mantido.

Os requisitos de segurança podem existir com níveis de detalhes distintos quando se especifica o projeto de um sistema ou produto. É possível definir metas globais para riscos dentro de determinada área de responsabilidade e, em seguida, definir requisitos técnicos para peças individuais de equipamentos. Um ponto importante é certificar de que os requisitos de segurança são realistas, claros, abrangentes e precisos e que seja possível confirmar se foram atendidos.

Outro ponto importante em relação a segurança é a distinção clara da forma e razão comportamental de erros humanos que são cometidos por algumas pessoas em determinados papéis nas empresas, sejam eles decorrentes de violações deliberadas de regras e resultantes de um raciocínio errôneo, até simples lapsos, conforme recomendações nas práticas de prevenção no gerenciamento de risco de acidentes organizacionais, descritas pelo especialista britânico em fatores humanos, Prof. *James T. Reason*.

Algumas formas de prevenção ou controle de erros humanos são conhecidas, logo requisitos de segurança com o propósito de ajudar pessoas a evitar tais erros devem ser previstos. Como definição, um requisito de segurança é qualquer compromisso escrito que implemente uma medida de controle cuja conclusão possa ser rastreada, não importando como esses compromissos sejam nomeados, pois uma determinada ação em um registro de riscos pode servir também como uma função que atenda um requisito de segurança.

Os requisitos de segurança, quantitativos ou qualitativos, podem ser divididos em categorias distintas e a norma EN 50126 considera a seguinte classificação:

- Requisitos funcionais: executam funções que são fundamentais para o sistema ou produto, incluindo requisitos associados com confiabilidade e com atributos de desempenho;
- Requisitos contextuais: relacionam o sistema com seu meio ambiente;
- Requisitos técnicos: são derivados da forma pela qual um sistema é construído.

Também pode ser útil categorizar os requisitos de acordo com aspectos restritos a determinado sistema ou produto. A EN 50126 exige que os requisitos sejam definidos para as seguintes categorias:

- requisitos funcionais e suporte aos requisitos de desempenho, incluindo segurança;
- requisitos funcionais e requisitos de integridade de segurança para cada função;
- requisitos de suporte logístico;
- interfaces;
- ambiente de aplicativos e perfil de missão;
- consequências decorrentes de perigos identificados para níveis de risco toleráveis;
- medidas externas necessárias para atingir os requisitos;
- requisitos de suporte do sistema;
- detalhes dos limites da análise;
- detalhes de quaisquer suposições feitas;
- identificação de padrões relacionados à tecnologia;

• escopo de diagnóstico e monitoramento.

Na medida que se aumenta a complexidade de um determinado projeto, aumenta-se proporcionalmente o risco de falhas sistemáticas. Para o *software*, onde todas as falhas são sistemáticas e que cada falha sistemática é um problema específico a ser tratado, a prática de engenharia para atender aos requisitos de integridade é aplicar níveis de integridade de segurança (SIL).

Algumas outras áreas, onde os projetos podem ser particularmente complexos, como o projeto da eletrônica, também se aplica o SIL, que é uma definição padronizada e amplamente utilizada e recomendada pelas normas EN 50126 e IEC 61508 para sistemas ou partes onde o padrão for aplicável, caso contrário, recomenda-se a verificação rigorosa para controle do risco decorrente de uma falha sistemática.

Mesmo em sistemas complexos, atender um padrão SIL não é a única forma de controle de falhas, pois algumas podem ser controladas por meio de recursos na arquitetura do projeto. Os 5 níveis distintos de SIL representam o grau de rigor em um processo de desenvolvimento e estão relacionados a probabilidade aproximada de atingir metas de integridade, que variam desde o nível mais rigoroso (SIL 4) até o seu nível mínimo (SIL 0), e onde cada nível é preenchido com processos e técnicas cada vez mais rígidos. Cada nível de integridade está associado a uma taxa alvo de ocorrência de falha, conforme mostra a Tabela 5 a seguir extraída da norma EN 50126. As funções que não possuem confiabilidade no controle de risco não possuem SIL, embora se possa aplicar medidas de controle.

| Taxa alvo de ocorrência de falha (por hora) | Nível de integridade de segurança (SIL) | |
|---|---|--|
| 10 ⁻⁹ 10 ⁻⁸ | 4 | |
| 10 ⁻⁸ 10 ⁻⁷ | 3 | |
| 10 ⁻⁷ 10 ⁻⁶ | 2 | |
| 10 ⁻⁶ 10 ⁻⁵ | 1 | |
| >= 10 ⁻⁵ | 0 | |

Tabela 5 – Taxa de falhas por níveis de integridade de segurança

Diagnóstico

Necessidade de estabelecer um método de trabalho para análise crítica nos processos de coleta de requisitos para definição de um escopo de projeto de uma linha UTO, de forma a identificar e garantir que as necessidades da maioria das partes interessadas sejam realmente mapeadas, justificadas e devidamente incluídas na especificação.

O método deve ser também efetivo na identificação de possíveis desejos de algumas partes interessadas que não geram valor na solução, mais que podem demandar em maiores custos, aumento da complexidade e do tempo de implantação do projeto quando são solicitados nas etapas iniciais, mas podem impactar também em retrabalhos futuros quando as solicitações de mudanças são feitas com o projeto em fase avançadas.

O mapeamento deficitário de riscos durante a fase inicial de um projeto de sistemas pode gerar aditivos em contratos e retrabalhos durante o projeto executivo e sua implantação conforme registros do histórico de aditivos da empresa.

Desde 2018, a empresa definiu um Plano de Negócios a ser revisto anualmente e uma Estratégia de Longo Prazo como compromissos para o tratamento de 4 grandes

objetivos estratégicos e que abrange cerca de 20 iniciativas e metas a serem alcançadas.

O gerenciamento e governança de expansão visa melhorar os processos de expansão tornando-os mais previsíveis e confiáveis, reduzindo as incertezas e garantindo os resultados previstos, sendo um dos objetivos do Plano de Negócios da CMSP. Entendese que a adoção de métodos que permitam obter um maior grau de maturidade na concepção e elaboração de projetos básicos de sistemas, considerando a maior complexidade no projeto de uma linha UTO, está alinhada também com este objetivo, pois segundo o histórico de aditivos de contratos para empreendimentos nas linhas L1, L2, L3, L4, L5, L15 e L17, uma parcela de 22% do total do número de aditivos está relacionada somente com a implantação de sistemas, enquanto outra parcela de 19% está relacionada com a somatória de aditivos de projeto básico e executivo de sistemas, material rodante e a análise de segurança.

Conforme apresentado na introdução, existe uma pressão crescente oriunda das necessidades de mercado para o aumento no grau de automação das linhas existentes, que demandam um *upgrade* do SIL, transferindo tarefas envolvidas pelo fator comportamental humano para funções determinísticas pelo sistema, delegando ao homem tarefas menos repetitivas, contextuais e mais nobres.

Análise dos resultados

Embora o trabalho tenha sido iniciado há poucos meses, já é possível antecipar benefícios com a rica combinação entre a análise de cenários e riscos com as lições aprendidas, sejam elas extraídas da vivência operacional da empresa por meio da

análise de seus manuais e procedimentos, histórico das ocorrências e recomendações da COPESE e análise dos aditivos de contrato.

A meta é a obtenção de ganhos em qualidade na especificação de projetos de sistemas quando se atingir uma combinação harmônica e assertiva na interação entre o processo de identificação dos perigos, as estimativas e controles de riscos em conjunto com o mapeamento e a análise de cenários operacionais.

Baseando-se nas informações sobre cenários do relatório APR em conjunto com os procedimentos operacionais, estima-se a elaboração de cerca de 130 cenários operacionais para uma nova linha UTO.

Como um breve exemplo de estudo de análise de cenários, onde se cogita a possibilidade de criação de uma função remota em um posto do CCO para abertura de portas dos trens, tal função precisa ser validada, não somente para atender um contexto de cenário degradado ou de emergência, de modo que um simples comando remoto errôneo, de abertura de portas, não seja executado para um trem parado na região de interestação em um cenário nominal. No caso de um cenário crítico de descarrilamento, desenergização do trem e falhas na comunicação trem-terra, recomenda-se manter os manípulos de emergência em algumas portas de forma que os passageiros tenham uma opção de evacuar o trem. Ao se permitir comandar remotamente a abertura de todas as portas de um lado do trem na região de interestação, mesmo aplicando o comando no lado correto da passarela de emergência, deve ser avaliada se a passarela comporta a evacuação dos passageiros na condição de carregamento máximo e com todas as portas abertas. Em um cenário de emergência, limitar e permitir a abertura de somente duas portas por carro pelos

passageiros via manípulo de emergência, e com a devida orientação remota do CCO por PA, uma melhor organização e fluidez de passageiros na passarela de emergência durante a evacuação pode gerar menos pânico.

A grande vantagem de convergir potenciais riscos com os cenários operacionais é permitir prever como os sistemas poderão se comportar em situações variadas, justificando determinadas funções e possibilitando ajustes nos requisitos técnicosfuncionais.

Outra grande oportunidade, visando o aumento do grau de automação de uma linha, é estabelecer uma convivência harmoniosa e agregadora na combinação de funções de sistemas com tarefas de seres humanos. É custoso e desnecessário, em termos de OPEX e CAPEX, automatizar tarefas que demandam uma análise contextual tais como check-list de inspeções periódicas realizadas por agentes circulantes no interior dos trens e estações, tais como a detecção de bancos sujos, quebrados, adesivos de comunicação visual ilegíveis nos trens ou sancas e armários elétricos abertos, já que este mesmo agente possui outras diversas tarefas a serem desempenhadas em outras localidades, seja na normalização de sistemas como no atendimento aos passageiros.

Por outro lado, sanados os ajustes nos requisitos técnicos de sistemas para funções conhecidas de mitigação de riscos, também é possível automatizar alguns testes de verificação de desempenho de alguns sistemas nos trens. criando requisitos funcionais de *softwares* para dispositivos que já existem, por exemplo, aplicando periodicamente um ruído branco, ruído rosa ou uma varredura por frequências audíveis nos altofalantes do sistema de sonorização do salão dos trens, fazendo então a medição e análise deste ruído através da captação do som no salão pelos microfones dos

intercomunicadores dos passageiros com o propósito de identificar automaticamente distorções geradas por algum alto-falante danificado.

Outra inovação a ser desenvolvida, e que pode somar na concepção de um sistema UTO, é a criação de uma plataforma colaborativa de serviços georeferenciada que também permita aos passageiros contribuir, por exemplo, na inspeção do salão dos trens, identificando adesivos de comunicação visual danificados, piso molhado, vômitos, mal súbito, dentre outras ocorrências, contribuindo com os processos periódicos de inspeção dinâmica nos trens para manutenção e limpeza.

Entende-se que tal estratégia pode colaborar com a percepção positiva da qualidade de serviço, uma vez que passageiro pode identificar lâmpadas queimadas, ar condicionado (VAC) desligado, carros com o VAC no máximo em dias frios, falhas nos mapas de linhas dinâmicos, no sistema de sonorização, nos monitores da TV minuto e eventuais consequências de vandalismo tais como bancos quebrados e vidros riscados, com a vantagem da identificação automática do número do trem, número carro e localidade dentro do salão de passageiros, repassando informações estruturadas do tipo de ocorrência e localidade para as equipes de operação, manutenção, segurança e limpeza e possibilitando melhorar o tempo de resposta na gestão de tais ocorrências.

Conclusões

Com base nos estudos, será elaborado um *Book* de cenários operacionais & riscos a ser utilizado na elaboração de projetos básicos e executivos de sistemas.

Com base nos cenários operacionais, será possível ter maior previsibilidade para a tomada de decisão, mais maturidade na avaliação custo/benefício na automação dos

processos e possibilitar agregar inteligência embarcada para atuar na mitigação automática de falhas de sistemas e riscos, enquanto que funções são disponibilizadas ao CCO para inibir falsas atuações dentro de intervalo de tempo.

A decisão na aplicação de inovações em requisitos para a automação de sistemas deve ser ponderada pela relação custo/benefício, avaliando se cada nova função visa atender necessidades justificadas que demandam análises determinísticas.

Referências bibliográficas

- 1- iESM International Engineering Safety Management Good Practice Handbook Vol. 2
- 2- Norma CENELEC EN 50126.
- 3- Norma IEC 62267.
- 4- Strategic Implications of Unattended Train Operation CoMET 2013 Case Study CEO Day, Annual Meeting, Santiago.
- 5- Relatório Mundial sobre Linhas Automáticas julho 2016 Statistics Brief UITP.
- 6- Press Release: UITP Celebrates Rail Achievement as Automated Metro Reaches 1000km Milestone - Brussels, 9 May 2018.
- 7- 18º AEAMESP A análise de riscos envolvendo segurança baseada em cenários operacionais OSHA.
- 8- 19º AEAMESP Integração dos sistemas Filosofia e concepção de projeto UTO para monotrilhos (CBTC/UTO da Linha 15-Prata).
- 9- 19º AEAMESP Critérios de seleção de sistemas de sinalização CBTC.

- 10-22º AEAMESP Diagnóstico do sistema metroferroviário utilizando tecnologia embarcada de *smartphones*.
- 11- 24º AEAMESP Integrar sistemas começa com "P".