

4º PRÊMIO TECNOLOGIA E DESENVOLVIMENTO METROFERROVIÁRIOS

CATEGORIA (3)

PROJETO ABNT-CB006 - NORMAS NBR IEC (EN5012X) -

SEGURANÇA EM SISTEMAS METROFERROVIÁRIOS -

EXPERIÊNCIA E EXPECTATIVAS

AUTOR

(Josafá A. Neves)

INTRODUÇÃO

Segurança é tema crítico para ferrovias, pessoas ou carga, quaisquer tipos.

Panorama técnico sofrendo mudanças rápidas devido aos avanços tecnológicos de grande impacto na implementação dos sistemas, exigindo avanços também nos métodos e recursos para garantir o mesmo nível de segurança tradicional, ou melhor. Os métodos e recursos tradicionais apresentam dificuldades de aplicação.

Esta questão é mundial. Assim, na busca de solução, as normas IEC 62278, IEC 62279 e IEC 62425, baseadas nas normas europeias EN 50126, EN 50128 e EN 50129, por sua vez derivadas da IEC 61508 em adaptação para aplicações metroferroviárias, apresentam o consenso internacional, estado-da-arte, como a metodologia considerada mais eficaz para o tratamento da segurança.

Um projeto atual da ABNT, CB006, CE – Sinalização, trata dos títulos NBR ‘por adoção’ das três normas IEC acima citadas, considerando que o Brasil é membro da IEC.

Observação geral: embora as normas façam referência a “RAMS”, este trabalho está focando especificamente em “S” – Segurança – Safety.

DIAGNÓSTICO

O QUE SÃO ESTAS NORMAS?

O que não são: normas de ‘comprovação’, ‘análise’, ‘verificação’, ‘auditoria’ da ‘segurança’, embora incluam tais atividades.

São normas abrangentes que abordam atividades de todas as fases do ciclo de vida de um sistema metroferroviário, garantindo a realização do grau de segurança necessário e sua comprovação evidente.

Estas atividades são principalmente de duas classes: de ‘realização’ do sistema, tais como especificações, projeto, desenvolvimento, fabricação, instalação, operação, manutenção, modificações, e atividades de verificação e comprovação do atendimento aos requisitos, especialmente os requisitos de segurança.

Os sistemas críticos nas aplicações metroferroviárias sempre tiveram tratamento especializado para que a segurança estivesse sempre privilegiada e garantida. Os métodos e processos para atingir estes objetivos foram adequados às tecnologias ao longo da evolução dos sistemas.

No entanto, nas décadas recentes, a tecnologia da implementação dos sistemas metroferroviários tem evoluído com transformações continuamente aceleradas, incorporando novos paradigmas e aumentando muito a complexidade dos sistemas. Os desafios para manter níveis satisfatórios de segurança também têm crescido, e têm exigido evolução intensa nos métodos e recursos para se continuar a atingir o grau de segurança elevado típico destas aplicações, e também gerar evidências desta segurança.

Como exemplo das dificuldades enfrentadas pode ser mencionada a observação na IEC 62279, norma específica para software, como segue:

O estado-da-arte corrente é tal que nem a aplicação de métodos de garantia da qualidade (as chamadas medidas de prevenção de falhas e medidas de detecção de falhas) nem a aplicação de abordagens de software tolerante a falhas podem garantir a segurança absoluta do software. Não é conhecido nenhum modo de provar a ausência de falhas em software relacionado à segurança razoavelmente complexo, especialmente a ausência de falhas de especificação e de projeto/desenvolvimento.

A percepção destas condições tem sido notável no âmbito internacional, resultando na criação das normas objeto desta apresentação, registrando o consenso atual do meio profissional especializado, quanto à abordagem mais eficaz para assegurar os resultados exigidos.

Os requisitos prescritos pelas normas estabelecem, desde o início, processos de trabalho estruturados, documentados, focados na segurança do sistema ou produto final. Há atividades específicas para a determinação dos requisitos de segurança, decisão da

arquitetura da implementação, transformação dos requisitos de segurança gerais em requisitos específicos para cada elemento da arquitetura, assegurando a rastreabilidade tal que o respeito a estes requisitos garanta o atendimento ao requisito global, e resulte, ao final do desenvolvimento, um sistema ou produto final seguro.

Em cada fase, para cada parte do sistema que esteja sendo abordada, são estabelecidos o objetivo, os elementos de entrada e os requisitos, incluindo tudo que, uma vez atendido, implica em que o resultado estabelecido para esta fase e parte do sistema esteja realizado e seja documentado nos elementos de saída. Finalmente, são realizadas atividades de verificação, incluindo, sempre que aplicável, análises de segurança para confirmar, documentar e evidenciar que esta parte do sistema, nesta fase do ciclo de vida, terá realizado o resultado adequado quanto à segurança.

A efetividade deste processo é afetada por condições operacionais tais como independência entre as equipes que projetam e desenvolvem o sistema, e as equipes que verificam os resultados da primeira, especialmente quanto à segurança. Estas condições também são abordadas nestas normas.

As normas estabelecem que, especialmente para os requisitos de segurança, todo o processo e documentação sejam avaliados – ‘assessed’, por profissional especializado – o ISA – Independent Safety Assessor, habilitado na área técnica envolvida, independente – livre de quaisquer conflitos de interesse, respeito à confidencialidade, através de exame de documentos técnicos e gerenciais, auditorias, testemunho de testes, e quaisquer questionamentos que julgue necessários para confirmar que as atividades e documentos estabelecidos pelas normas foram realizados satisfatoriamente, inclusive as verificações em

todas as fases, especialmente as verificações do cumprimento dos requisitos de segurança, que incluem análises de segurança onde aplicável.

A prática atualmente adotada é que o ISA cumpra um processo conforme a normas de inspeção ISO/IEC 17020 e ISO/IEC 17065.

Organismos oficiais 'Acreditadores' têm a responsabilidade de avaliar organismos e profissionais que se disponham a prestar serviços como 'ISA' e atendidas as qualificações normalizadas, os 'acreditam' como 'certificadores'. Após acreditado, o organismo é continuamente auditado para confirmar a manutenção do cumprimento aos requisitos estabelecidos.

As prescrições destas normas e a prática atual para confirmação do cumprimento a estas prescrições – a 'certificação', constituem a solução mais avançada reconhecida atualmente para cumprir os objetivos com eficácia.

As normas estabelecem processo verificável, de modo padronizado, controlado, assegurando critérios uniformes para qualquer aplicação.

PORQUE GERAR AS NBRs DESTAS NORMAS?

De modo geral, os países membros das organizações normalizadoras internacionais e regionais, uma vez emitidas as normas, emitem normas nacionais que, sempre que não haja conflitos importantes tais como na área legal, são versões equivalentes às normas originais. Isto é praticado mesmo quando o idioma original é o mesmo do país, tal como as normas

IEC, com originais em inglês e francês, e tanto o Reino Unido como a França emitem suas normas nacionais equivalentes às normas da IEC.

Do ponto de vista oficial, especialmente na área da segurança, ter as normas NBR torna suas prescrições acessíveis a quaisquer áreas e organismos públicos e privados, governamentais e jurídicos, facilitando amplamente o esclarecimentos de quaisquer questões nos assuntos abordados pelas normas. Em particular, esclarecimentos de questões em licitações podem ser processados em melhores condições a partir da referência à NBR.

COMO ESTÁ SENDO REALIZADO ESTE PROJETO

A participação é aberta a todos os profissionais que têm alguma relação com sistemas e equipamentos metroferroviários relacionados à segurança, em qualquer 'papel' nesta área.

A NBR IEC 62278 está em fase de ajustes formais após verificação pela ABNT, com previsão de apresentação ao GT e CE na reunião em 2017.10.03.

A NBR IEC 62425 está em discussão.

O processo é apresentar ao GT minutas de trechos, enviando por email a todos os participantes arquivo em pdf (formatação correta), e disponibilizando para comentários no GoogleDocs (que introduz problemas de formatação, a desprezar). Está sendo perquisada a disponibilidade de alternativas melhores em relação ao GoogleDocs. Minuta de cada trecho em 1ª revisão, 15 dias (mínimo) para comentários, consolidados na reunião seguinte; minuta na 2ª revisão, 8 dias (mínimo) para comentários, consolidados idem; minuta 3ª revisão, aberta para comentários até se completar a norma, repetindo as 3 revisões da mesma

forma, com o texto completo. Previsão último trecho, minuta em 1ª revisão, antes da reunião em 2017.11.07, última de 2017.

ANÁLISE DOS RESULTADOS

CONCLUSÕES

A elaboração do texto destas normas IEC, praticamente equivalentes às normas EN correspondentes, torna amplamente acessíveis à utilização e referência a quaisquer organismos públicos e privados, assim como aos profissionais, estes documentos que representam o estado-da-arte para o tratamento da segurança nos sistemas metroferroviários.

O próprio processo de elaboração tem tornado o Grupo de Trabalho responsável, um forum de esclarecimentos aos participantes, entre os próprios participantes, para entendimento preciso de quaisquer pontos mais difíceis destas normas.

Lembrando que a participação nestes trabalhos da ABNT é aberto aos profissionais relacionados aos temas tratados nas normas em questão.

Nota

REFERÊNCIAS BIBLIOGRÁFICAS

IEC 62278, 1ª ed, 2002.09 – Railways applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)

IEC 62279, ed.2.0, 2015.06 – Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems

IEC 62425, ed.1.0, 2007.09 – Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

EN 50126, 1999.09 – Railways applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

EN 50128, 2011.06 – Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems

EN 50129, 2003.02 – Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

Nota: textos originais em inglês e francês.