Análise de Normas de Software Crítico Orientada pelo Processo de Requisitos do Guia Geral de Software do MPS.Br

Johnny Marques [1], Everton Machado [1], Sarasuaty Yelisetty [1], Rodrigo Souza Cardoso [1]

[1]Instituto Tecnológico de Aeronáutica (ITA)

johnny@ita.br, evertonmach@gmail.com

sarasuaty@ita.br, rodrigo.cardoso@ga.ita.br

Resumo. *Este estudo analisa a correspondência entre os Resultados Esperados do Processo de Engenharia de Requisitos do Guia Geral de Software do MPS.Br e as normas internacionais RTCA DO-178C, IEC 62279 e IEC 62304. A pesquisa revela que, embora todas as normas abordem a rastreabilidade de requisitos (REQ 4), nenhuma trata explicitamente do comprometimento da equipe técnica (REQ 3) ou da revisão integrada de planos e produtos (REQ 5) exigidos pelo MPS.Br.*

1. Introdução

O desenvolvimento de software crítico de segurança é geralmente realizado em ambientes onde normas regulamentadoras estabelecem padrões rigorosos, com exigências de certificação que devem ser atendidas para garantir a segurança dos sistemas. Normas publicadas por comitês, entidades técnicas internacionais ou agências reguladoras têm um papel crucial ao influenciar o desenvolvimento de software em ambientes regulamentados, fornecendo diretrizes que orientam tanto os processos, quanto os produtos de software. Estas diretrizes são essenciais para minimizar a ocorrência de erros no desenvolvimento de software. Ademais, é possível identificar várias semelhanças entre as normas aplicadas ao desenvolvimento de software em setores como aviação, ferroviário e saúde [Marques and Cunha 2019].

O MPS.Br é um programa estratégico, de longa duração, iniciado em dezembro de 2003, sob a coordenação da Associação para Promoção da Excelência do Software Brasileiro (SOFTEX). Considerando a existência do consolidado programa em Engenharia de Software, o MPS.Br, com mais de duas décadas de atuação, os autores deste trabalho buscam explorar possíveis similaridades entre o Guia de Software do MPS.Br, especificamente no Processo de Engenharia de Requisitos e as normas RTCA DO-178C [RTCA 2011], IEC 62279 [IEC 2015] e IEC 6230 [ISO 2015]. Neste contexto, a seguinte pergunta de pesquisa é delineada: **"Qual a correlação entre os Resultados Esperados do Processo de Engenharia de Requisitos do Guia Geral de Software do MPS.Br, e as cláusulas de Engenharia de Requisitos previstas nas normas RTCA DO-178C, IEC 62279 e ISO/IEC 62304?"**.

Com o intuito de abordar essa indagação, o objetivo deste estudo consiste em realizar um mapeamento dos Resultados Esperados do Processo de Engenharia de Requisitos do Guia de Software do MPS.Br para cláusulas que versam sobre Requisitos dessas três normas (RTCA DO-178C, IEC 62279 e iSO/IEC 62304). Este trabalho representa uma pesquisa em andamento no Instituto Tecnológico de Aeronáutica e engloba a elaboração

de um mapeamento abrangente, incluindo todos os Resultados Esperados do Guia Geral de Software do MPS.Br e as cláusulas das normas *Safety-Critical* de interesse.

2. Visão Geral das Normas Envolvidas

A RTCA DO-178C [RTCA 2011] é um padrão essencial para o desenvolvimento de software em sistemas embarcados em aeronaves, estabelecendo os critérios necessários para garantir a segurança e a confiabilidade desses sistemas. A RTCA DO-178C fornece uma estrutura rigorosa para todo o ciclo de vida do software, desde a definição de requisitos até a verificação, validação e certificação. A norma categoriza o software em diferentes níveis de criticidade, conforme o impacto que uma falha poderia ter na operação segura da aeronave, variando de "catastrophic" (nível A) a "no effect" (nível E). Esse sistema de classificação determina o rigor exigido em cada etapa do desenvolvimento.

A norma IEC 62279 [IEC 2015] é um padrão internacional que define os requisitos para o desenvolvimento de software para sistemas de controle e proteção ferroviários. O principal objetivo da IEC 62279 é garantir que o software utilizado em sistemas ferroviários críticos, como sinais, controle de trens e sistemas de proteção, seja desenvolvido de maneira a minimizar os riscos de falhas que poderiam comprometer a segurança operacional. A norma aborda todas as etapas do ciclo de vida do software, desde o conceito inicial e requisitos até a implementação, testes, validação e manutenção. Ela enfatiza a necessidade de processos rigorosos e metodologias formais para garantir que o software atenda aos mais altos padrões de segurança e confiabilidade.

A ISO/IEC 62304 [ISO 2015] é um padrão internacional que estabelece os requisitos para o ciclo de vida do desenvolvimento de software utilizado em dispositivos médicos. A norma fornece uma estrutura abrangente para o design, desenvolvimento, validação, manutenção e gestão de riscos do software, garantindo que ele atenda aos requisitos de segurança essenciais para dispositivos médicos. A ISO/IEC 62304 categoriza o software em três classes de segurança (A, B e C), dependendo do nível de risco que uma falha no software pode representar para os pacientes. Essa classificação orienta o rigor dos processos de desenvolvimento, desde a definição de requisitos até os testes e a documentação.

3. Análise

O propósito do Processo de Engenharia de Requisitos do Guia Geral de Software do MPS.Br é definir, gerenciar e manter atualizados os requisitos das partes interessadas e do produto. A Tabela 1 apresenta a lista dos Resultados Esperados do Guia Geral de Software do MPS.Br.

Tanto a RTCA DO-178C, quanto a IEC 62279 e a ISO/IEC 62304 são normas amplamente reconhecidas que estabelecem requisitos rigorosos para o desenvolvimento de software em setores críticos, como a aviação, sistemas ferroviários e dispositivos médicos, respectivamente. Apesar de sua abrangência e detalhamento, conforme apresentado na síntese da Tabela 2, essas normas não abordam explicitamente o Resultado Esperado REQ 3 do modelo MPS.Br, que exige que o compromisso da equipe técnica com a implementação dos requisitos seja obtido.

Enquanto essas normas focam fortemente em assegurar que o software desenvolvido atenda aos requisitos técnicos e de segurança, elas não especificam mecanismos

REQ 1	(A partir do nível G) As necessidades, expectativas e restrições das partes interessadas, tanto em relação ao produto quanto a suas interfaces, são identificadas e o entendimento dos requisitos é confirmado.
REQ 2+	(A partir do nível D) Os requisitos são especificados, priorizados, refinados, alocados para implementação e mantidos atualizados a partir das necessidades, expectativas e restrições identificadas, o que inclui a especificação de conceitos operacionais, cenários e interfaces internas e externas.
REQ 3	(A partir do nível G) O compromisso da equipe técnica com a implementação dos requisitos é obtido.
REQ 4	(A partir do nível G) A rastreabilidade bidirecional entre requisitos, atividades e produtos de trabalho do projeto é estabelecida e mantida.
REQ 5	(a partir do Nível G) Os planos, atividades e produtos de trabalho relacionados são revisados visando identificar e tratar inconsistência em relação aos requisitos
REQ 6	(A partir do nível D) Os requisitos são entendidos e analisados para garantir que sejam necessários e suficientes e para balancear as necessidades das partes interessadas com as restrições existentes.
REQ 7	(A partir do Nível D) Os requisitos são validados.

Tabela 1. Resultados Esperados do Processo de Engenharia de Requisitos do Guia de Software MPS.Br 2024 [Softex 2024]

Resultados Esperados	RTCA DO-178C	IEC 62279	ISO/IEC 62304
REQ 1	Completo	Completo	Completo
REQ 2+	Completo	Completo	Completo
REQ 3	Não explícito	Não explícito	Não explícito
REQ 4	Completo	Completo	Completo
REQ 5	Completo	Parcial	Parcial
REQ 6	Completo	Completo	Completo
REQ 7	Completo	Completo	Completo

Tabela 2. Síntese da Análise de Mapeamento

ou práticas destinadas a garantir que a equipe técnica esteja efetivamente comprometida com a implementação desses requisitos. O REQ 3 do MPS.Br vai além da conformidade técnica, enfatizando a importância do comprometimento da equipe em todo o processo de desenvolvimento, algo que não é diretamente tratado pelas normas mencionadas. Portanto, apesar de sua importância e rigor, as normas RTCA DO-178C, IEC 62279 e ISO/IEC 62304 não contemplam de forma explícita o aspecto humano e de engajamento da equipe técnica, conforme previsto pelo REQ 3 do Guia Geral de Software do MPS.Br.

Adicionalmente, como também apresentada na síntese da Tabela 2, nenhuma dessas normas aborda explicitamente a necessidade de garantir que os planos, atividades e produtos de trabalho sejam revisados visando identificar e tratar inconsistências em relação aos requisitos, conforme é solicitado pelo Resultado Esperado REQ 5 do Guia Geral de Software do MPS.Br.

A ISO/IEC 62304 e IEC 62279, embora detalhem a importância de revisões e verificações ao longo do ciclo de vida do software, focam em assegurar que os produtos de trabalho sejam revisados e validados contra os requisitos especificados. Elas não explicitam a necessidade de uma revisão integrada que também contemple a coerência e consistência entre planos, atividades e produtos de trabalho, conforme requerido pelo REQ 5 do MPS.Br. Esta lacuna implica que, embora estas normas garantam a conformidade dos produtos de trabalho com os requisitos, elas não garantem que todo o processo de desenvolvimento esteja sincronizado e livre de inconsistências, como preconiza o Guia

Geral de Software do MPS.Br.

Segundo Lauesen (2002), o rastreamento de requisitos é essencial para comparar esses requisitos com outras informações relacionadas. Gotel e Finkelstein (2014) definem a rastreabilidade de requisitos como "a capacidade de traçar os requisitos desde suas origens, passando por seu desenvolvimento e especificação, até sua implementação, uso subsequente e períodos de refinamento contínuo e iteração em qualquer fase".

Considerando que as três normas atendem completamente o REQ 4, sobre a rastreabilidade, é possível avaliarmos inclusive as diferenças nas rastreabilidades exigidas nas três normas. Na RTCA DO-178C, a rastreabilidade de requisitos ocorre em diversas direções. Os Requisitos de Software de Alto Nível devem manter rastreabilidade bidirecional com os Requisitos de Sistema, Requisitos de Software de Baixo Nível e casos de teste. Já os Requisitos de Software de Baixo Nível, que fazem parte do Design, precisam ter rastreabilidade bidirecional com os de Alto Nível, Código Fonte e Testes.

Na ISO/IEC 62304, a rastreabilidade de requisitos é menos abrangente do que na RTCA DO-178C. Os Requisitos de Software devem ter rastreabilidade bidirecional com os Requisitos de Sistema e Testes. Embora não seja mandatória, a norma sugere que a rastreabilidade entre a Arquitetura, parte do Design, e os Requisitos de Software pode ser útil para a verificação. Na IEC 62279, a rastreabilidade bidirecional dos requisitos é estabelecida entre os Requisitos de Software, os Requisitos de Sistema, o Design e os Testes. A Figura 1 apresenta uma síntese da rastreabilidade entre os Requisitos de Software e outros artefatos nas três normas de software analisadas.

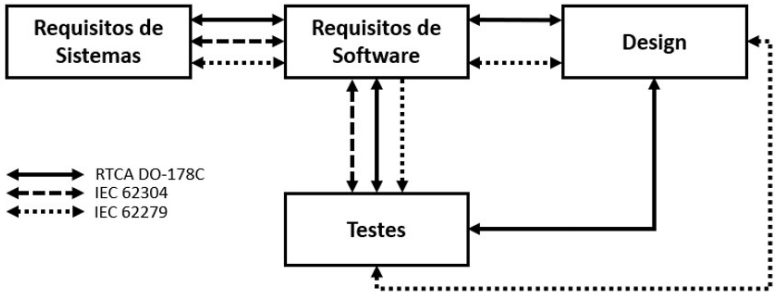

Figura 1. Síntese das rastreabilidades das Normas

4. Conclusão

Este trabalho apresentou um alto grau de alinhamento entre o Processo de Engenharia de Requisitos do Guia Geral de Software do MPS.Br de Software e as normas internacionais RTCA DO-178C, IEC 62279 e ISO/IEC 62304, especialmente no Processo de Engenharia de Requisitos. Todas as normas enfatizam a importância de requisitos claros, completos e rastreáveis. No entanto, o Guia Geral de Software do MPS.Br se destaca ao valorizar aspectos humanos e de processo, como o compromisso da equipe e revisões abrangentes, que complementam o rigor técnico das normas internacionais. Ao adotar o MPS.Br, as organizações podem enriquecer suas práticas de desenvolvimento de software e melhorar a qualidade de seus produtos.

A análise comparativa revelou que, embora o Guia Geral de Software do MPS.Br e as normas internacionais compartilhem objetivos comuns, o modelo brasileiro apresenta

características distintivas. O Guia Geral de Software do MPS.Br, além de atender aos requisitos técnicos exigidos pelas normas internacionais, incorpora elementos relacionados à gestão de pessoas e processos, como o compromisso da equipe e a revisão contínua dos requisitos. Essa abordagem mais holística faz com que os autores deste trabalho acreditem que isto contribui para um desenvolvimento de software mais eficaz e robusto. Embora já existam outros trabalhos dos autores que correlacionam a norma RTCA DO-178C e ISO/IEC 62304 ([Machado and Marques 2023] e [Marques and Machado 2024]) com o Guia de Software do MPS.Br, nenhum desses trabalhos anteriores abordavam um mapeamento dos Resultados Esperados para as normas e sim no caminho contrário.

Como trabalhos futuros planeja-se: (i) Avaliar os demais processos e Resultados Esperados do Guia de Software do MPS.Br em face das três normas; e (ii) Investigar outras normas de segurança crítica além da RTCA DO-178C, IEC 62279 e ISO/IEC 62304 para avaliar se elas abordam de maneira diferente os requisitos do MPS.Br, especialmente o compromisso da equipe técnica e a revisão de planos e atividades.

Referências

Gotel, O. C. Z. and Finkelstein, C. W. (1994). An analysis of requirements traceability problem. In *Proceedings of IEEE International Conference on Requirements Engineering*, Estados Unidos.

IEC (2015). Iec 62279:2015 railway applications - communication, signalling and processing systems - software for railway control and protection systems.

ISO (2015). Iso/iec 62304:2015 medical device software - software life-cycle processes – amendment 1. Technical report, International Electrotechnical Commission.

Lauesen, S. (2002). *Software Requirements – Styles and Techniques*. Pearson, Grã-Bretanha, 1st edn. edition.

Machado, E. and Marques, J. (2023). Me-mps: An mr-mps-sw extension model for critical software in regulated environments. In *Proceedings of the XXII Brazilian Symposium on Software Quality*, SBQS '23, page 52–61, New York, NY, USA. Association for Computing Machinery.

Marques, J. and Cunha, A. (2019). Ares: An agile requirements specification process for regulated environments. *International Journal of Software Engineering and Knowledge Engineering (IJSEKE)*, 29(10):1403–1438.

Marques, J. and Machado, E. (2024). Um mapeamento do mps.br para o desenvolvimento de dispositivos médicos com foco em engenharia de requisitos. In *Anais do XXVII Congresso Ibero-Americano em Engenharia de Software*, pages 241–255, Porto Alegre, RS, Brasil. SBC.

RTCA (2011). Do-178c software considerations in airborne systems and equipment certification.

Softex (2024). Guia geral mps de software.