

PROPOSTA DE UMA ABORDAGEM INTEGRADA PARA O GERENCIAMENTO DE RISCOS DE SOFTWARES E SISTEMAS PROGRAMÁVEIS DE EQUIPAMENTOS ELETROMÉDICOS

Marcelo de Moraes Antunes¹

¹Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A. – IPT
Laboratório de Equipamentos Elétricos e Ópticos - LEO
São Paulo – Brasil
e-mail: mantunes@ipt.br

Resumo: O presente artigo baseia-se em Normas vigentes para propor uma abordagem integrada para o gerenciamento de riscos de softwares e sistemas programáveis de equipamentos eletromédicos. A proposta leva em consideração a integração das Normas para software e para o próprio equipamento eletromédico, visando aglutinar os requisitos de ambas em um processo único de modo a agilizar o processo e preencher as lacunas entre ambos. A metodologia baseia-se nas Normas ABNT NBR IEC 60601-1-4 e ABNT NBR ISO 14971. O resultado do trabalho é uma metodologia otimizada que pode ser utilizada por fabricantes como maneira de demonstrar a conformidade aos requisitos para a segurança de softwares implementando um processo mais atual que o encontrado na Norma específica para softwares. Essa contribuição está inclusive em consonância com as propostas de harmonização global para as regulamentações de produtos para a saúde.

Palavras chave: gerenciamento de riscos, equipamento eletromédico, software

1. INTRODUÇÃO

O desenvolvimento de equipamentos médicos foi beneficiado pelo rápido desenvolvimento da informática. Atualmente, softwares embarcados e outros sistemas programáveis são responsáveis por funções e garantem a segurança dos equipamentos, substituindo ou controlando comandos e dispositivos mecânicos. A utilização de tais sistemas programáveis traz suas próprias situações de risco. Um exemplo clássico é o caso do Therac-25 [1], um acelerador linear que entre junho de 1985 e janeiro de 1987 provocou situações de sobre-dosagem em seis pacientes que utilizaram o equipamento para tratamento. Após diversas investigações, constatou-se que os problemas deviam-se à falta de um desenvolvimento criterioso e voltado à segurança do software de controle; a partir disso diversas iniciativas foram desenvolvidas para validar esses softwares de maneira a garantir a segurança.

Atualmente tal validação é realizada através da aplicação da Norma ABNT NBR IEC 60601-1-4 [2], a partir daqui chamada apenas de 60601-1-4, que prescreve a utilização de gerenciamento de riscos do sistema programável através do ciclo de vida de desenvolvimento do mesmo. Uma outra Norma, ABNT NBR ISO 14971 [3], a

partir daqui chamada apenas de 14971, prescreve a aplicação de gerenciamento de risco em produtos para a saúde, incluindo os equipamentos eletromédicos. Embora os processos de ambas as Normas sejam parecidos há diferenças em diversas prescrições em ambos os casos. Muitas empresas possuem processos de gerenciamento de riscos separados tanto do sistema de qualidade (por exemplo, a NBR ISO 9001 ou a NBR ISO 13485) quanto entre si (por exemplo, um processo para o software baseado na 60601-1-4 e um processo para o equipamento baseado na 14971).

Este trabalho tem como objetivo propor uma abordagem integrada para a avaliação de segurança dos sistemas programáveis, utilizando as duas Normas citadas em conjunto e, portanto, incluindo o gerenciamento de riscos do sistema programável no processo de gerenciamento de riscos do equipamento como um todo. As diferenças que devem ser levadas em consideração são abordadas e os principais problemas são comentados.

Tal proposta visa a uma integração das necessidades impostas pela introdução do gerenciamento de riscos no desenvolvimento de equipamentos médicos, seja por imposição legal (por exemplo, a Diretiva de Produtos para a Saúde Européia – Medical Devices Directive [4] obriga os fabricantes a implementarem um processo de gerenciamento de riscos para seus produtos; além disso, a nova versão da Norma geral IEC 60601-1 [5] a ser publicada em 2006 irá conter prescrições que obrigam os fabricantes a apresentarem um processo de gerenciamento de riscos de acordo com a ISO 14971 para garantir a conformidade com a Norma geral) ou seja por imposições de melhoria da qualidade do produto (por exemplo, para diminuir a incidência de falhas que poderiam ser razoavelmente previstas).

2. MÉTODOS

A metodologia de trabalho foi dividida em duas etapas:

- leitura crítica das Normas em questão: foi dado ênfase à 14971, pois a mesma é a visão atual do estado da arte do gerenciamento de risco de produtos para a saúde. Quando a Norma IEC 60601-1-4 foi produzida em 1996, não existiam Normas de gerenciamento de risco na área, e, portanto, a mesma possui a descrição de um processo de gerenciamento de riscos como visto na época. O processo é

bastante parecido com o produzido alguns anos depois para 14971 (em 2000), mas possui algumas diferenças significativas. A principal delas é a falta de um requisito, na 60601-1-4, para a implementação de um processo sistemático para análise crítica do sistema programável na fase de pós-produção, de maneira a realimentar o processo realizado durante o ciclo de vida de desenvolvimento e minimizar/mitigar os riscos que forem reportados pelo clientes. Portanto a 14971 foi utilizada pelo autor como a base para o desenvolvimento do processo deste trabalho.

- verificação das diferenças entre as Normas e revisão e agrupamento dos itens específicos da 60601-1-4 que devem ser adicionados às prescrições da 14971 de maneira a garantir a conformidade com ambas as Normas: uma diferença importante na abordagem das duas Normas é o fato de que a 60601-1-4 prescreve que os documentos produzidos pela aplicação da mesma façam parte dos registros da qualidade; a 14971 deixa em aberto a possibilidade ou não de se colocar o arquivo de gerenciamento de riscos atrelado ao sistema da qualidade. Para estar em conformidade com a primeira, é necessário que se atrele o processo de gerenciamento de riscos ao sistema da qualidade. Conforme já dito, muitas empresas possuem esses sistemas em separado. Contudo, é da opinião do autor que tal junção não só seja desejável como melhore a aplicação de ambas; essa tendência pode ser comprovada pela publicação, pela Força-tarefa para a Harmonização Global – Global Harmonization Task Force (GHTF) - organização que tem por iniciativa a harmonização dos requisitos regulatórios de produtos para a saúde, do documento “Implementation of Risk Management Principles and Activities Within a Quality Management System” [6].

3. RESULTADOS E DISCUSSÃO

Foram analisados os 62 itens da 60601-1-4 e os 21 itens da 14971. A diferença no número de itens se dá pelo fato de que a 14971 agrupa diversas prescrições em cada item, enquanto a 60601-1-4 separa as mesmas. Dos 62 itens da 60601-1-4, chegou-se à conclusão que 23 itens são cobertos pelas prescrições da 14971, e os outros 39 devem ser adicionados à um processo que abranja as duas Normas.

Tabela 1 – Itens das Normas

| Número total de itens da 60601-1-4 | Número total de itens da 14971 | Número de itens 60601-1-4 que são cobertos pela 14971 | Número de itens da 60601-1-4 que não são cobertos pela 14971 |
|------------------------------------|--------------------------------|---|--|
| 62 | 21 | 23 | 39 |

Os 39 itens a serem incluídos são relacionados principalmente à implementação sistemática de um ciclo de vida de desenvolvimento de sistemas programáveis imposto pela 60601-1-4, a aspectos específicos de um sistema programável (especificação de prescrições e arquitetura), à verificação de fases do ciclo de vida e validação do produto final e à manutenção de um sumário de gerenciamento de riscos que faz um resumo dos riscos encontrados e procedimentos de segurança implementados.

Durante a escolha de itens levou-se em consideração o fato de que a 14971 é uma Norma de âmbito mais geral para gerenciamento de riscos, possuindo portanto pontos menos específicos que a Norma de sistemas programáveis.

Os itens iniciais de documentação da 60601-1-4 (52.201) não são cobertos pela 14971 pois são os itens que exigem a inclusão da documentação no sistema da qualidade conforme já comentado anteriormente. O último sub-item (52.201.3) prescreve o desenvolvimento de um documento conhecido como “Sumário de gerenciamento de risco”, que deve possuir a cadeia perigo-causas-estimação de risco-controle de risco-eficácia do controle-verificação-validação, ou seja, todas as informações principais da aplicação da Norma. A 14971 possui uma prescrição parecida no item 8, “Relatório de gerenciamento de risco”. A diferença é que no Relatório é necessário apenas o fornecimento de rastreabilidade de cada perigo para a análise, avaliação implementação e verificação do risco, sendo que esses últimos podem estar em documentos separados. É da opinião do autor que um Sumário conforme prescrito pela 60601-1-4 é mais prático por conter todas as informações, facilitando inclusive a verificação da Norma por laboratórios independentes.

O item 52.202 da 60601-1-4, Plano de gerenciamento de risco, não é completamente coberto pelo item 3. 5 da 14971, de mesmo nome. A única adição é a necessidade de inclusão de um plano de validação, termo que designa o processo de avaliação para determinar se o produto final atende às prescrições iniciais, geralmente feito no final de um ciclo de vida de desenvolvimento. O termo “validação” não é utilizado na 14971.

O item sobre “Ciclo de vida de desenvolvimento” (52.203 da 60601-1-4) não possui equivalente na 14971. Embora esta última deva ser aplicada no ciclo de vida de um produto, ela não possui a necessidade de uma especificação de um ciclo de vida específico, até por não ser possível planejar um ciclo de vida que tem uma componente temporal longa e fora do controle do fabricante (por exemplo, o ciclo pós-produção, quando o equipamentos já foi comercializado). No caso da Norma de sistemas programáveis, há a necessidade de se especificar um ciclo de vida dentro da fase de desenvolvimento a ser seguido, e reside aí a principal preocupação da Norma: uma vez que um software nem sempre pode ser ensaiado como um hardware, com ensaios do tipo passa/falha, a única maneira de garantir a segurança do mesmo é através da aplicação sistemática de um processo que minimize ou mitigue os perigos relacionados ao mesmo. Esse ciclo de vida de desenvolvimento deve possuir algumas características, como por exemplo a divisão entre fases e tarefas, com entradas, saídas e atividades bem definidas para cada fase de forma que possa ser feita uma verificação de que as saídas satisfazem os requisitos de entradas. Além disso, deve-se definir um sistema de resoluções de problemas, que pode possuir diversas características dependendo do escopo do mesmo, mas que deve se preocupar em resolver os problemas dentro do ciclo de vida de desenvolvimento que surjam (por exemplo, quando é verificado que a saída de uma fase não atende aos requisitos de entrada da mesma). A Norma 60601-1-4 não prescreve um modelo específico de ciclo de vida de desenvolvimento (ela possui apenas um exemplo gráfico na figura DDD.1) e portanto o fabricante

pode utilizar qualquer ciclo que preferir. Uma vez que o conceito foi retirado da literatura de engenharia de software, uma opção é utilizar um dos ciclos que podem ser pinçados de tal literatura (para exemplo de literatura de engenharia de software, pode ser consultada a referência [7]). Contudo, existe uma Norma em desenvolvimento que abrange um ciclo de vida de desenvolvimento completo para softwares de equipamentos médicos, e é a opinião do autor que, se possível, tal Norma deva ser utilizada quando publicada principalmente porque a mesma já leva em consideração toda a normalização já existente.[8].

Com relação à análise de risco (52.204.3 da 60601-1-4 e 4 da 14971) as prescrições são muito parecidas pois fazem parte do conceito geral de gerenciamento de risco. Os únicos pontos da 60601-1-4 que devem ser levados em consideração são:

- item 52.204.3.1.5, que possui causas iniciadoras de perigos específicas para sistemas programáveis que devem ser consideradas (por exemplo, erros de integração);
- item 52.204.3.1.6, que possui assuntos específicos a serem considerados na análise (por exemplo, softwares de terceira parte).

No quesito qualificação de pessoal, vale lembrar que a Norma 60601-1-4 enfatiza, inclusive nas justificativas dos itens, a necessidade da utilização e implementação da Norma por pessoas qualificadas, uma vez que a literatura da área de engenharia de software é muito extensa e cresce em um ritmo frenético. Um especialista saberá quais as melhores ferramentas para empregar em determinadas situações, onde uma pessoa que não possui tal qualificação pode não conhecer todas as possibilidades a serem empregadas.

As especificações de prescrições são itens do campo de engenharia de software e, portanto, não cobertos pela 14971, assim como a parte de arquitetura de software.

Uma definição para “especificação de prescrição” é: “um documento que especifica as prescrições para um sistema ou componente. São incluídas tipicamente prescrições funcionais, de desempenho, de interface e de projeto, e também Normas para o desenvolvimento” [9]. Tais especificações, portanto, traduzem em um documento tudo que o é esperado do sistema programável dentro de sua utilização destinada. A 60601-1-4 indica, ainda, a necessidade de se detalhar as funções que são relacionadas com os riscos, e as informações necessárias para assegurar que os procedimentos implementados de controle de risco reduzam os riscos identificados à um nível aceitável. Deve-se ter em mente que as especificações de prescrições devem ser escritas de forma a poderem ser verificadas e validadas, sendo portanto necessário elaborá-las já tendo em mente quais critérios serão utilizados para verificar se o produto final está de acordo com as mesmas. Diversos métodos existem na literatura para se derivar especificações de prescrições. Sugere-se um estudo atento de tais métodos para se escolher o melhor a ser utilizado em cada caso, dependendo também dos conhecimentos dos especialistas envolvidos.

Arquitetura é definida como “a estrutura organizacional de um sistema ou componente” [8], [9]. O projeto de uma arquitetura está relacionado com o processo de definição de componentes de hardware e software e suas interfaces para que possa ser estabelecida uma estrutura para o desenvolvimento do produto. A 60601-1-4 explicita que a

arquitetura deve satisfazer a especificação de prescrições, significando que, uma vez feita a especificação de componentes separados, sua interface deve ser montada para que se possa ter uma visão geral do sistema. O sistema programável e cada subsistema devem possuir uma especificação de arquitetura. Tal especificação deve possuir prescrições para o controle dos riscos presentes, reduzindo a probabilidade do perigo ou a severidade do perigo ou ambos. Tal conceito é inerente à definição de risco. A Norma cita também alguns métodos específicos que podem ser utilizados para se reduzir a probabilidade do perigo (por exemplo, componentes altamente confiáveis, ou seja, componentes que são construídos de tal maneira – geralmente certificados por suas Normas específicas – que não existe a possibilidade de falha dos mesmos).

A 60601-1-4 prescreve também que, onde apropriado, o projeto deve ser decomposto em subsistemas, de modo a simplificar a abordagem de sistemas mais complexos. Cada um desses subsistemas deve ter sua própria especificação de projetos e de ensaios.

Embora o conceito de “verificação” seja o mesmo para as Normas (verificação da implementação das prescrições de segurança), no caso da 60601-1-4 ele é melhor explicado, e também torna necessário realizar verificações entre cada fase do ciclo de vida de desenvolvimento do sistema. O plano de verificação da Norma de sistemas programáveis explicita a necessidade do mesmo conter uma seleção e documentação de estratégias, atividades e técnicas de verificação, ferramentas de verificação e critérios para a verificação. A 14971 apenas prescreve a necessidade de um plano de verificação, sem mencionar seu conteúdo.

Não há o conceito de “validação” na 14971. Conforme já mencionado, a validação está relacionada ao atendimento das prescrições iniciais (ou especificações de prescrições). A 60601-1-4 preocupa-se em validar o equipamento dentro de sua condição de utilização destinada e saber se as prescrições de segurança corretas foram implementadas. Uma outra preocupação da Norma é a separação da equipe de validação e projeto, de modo que uma pessoa não valide seu próprio projeto.

Pelo fato da 60601-1-4 exigir um desenvolvimento sistemático que garanta a segurança, modificações no projeto devem ser validadas de maneira a garantir que a introdução das mesmas não degrade a segurança. Outra opção, se a mudança for muito complexa, é aplicar novamente o conteúdo total da Norma.

Finalmente, é necessária uma auditoria (que pode ser uma auditoria interna mas que deve ser de um grupo separado) de maneira a assegurar que o sistema foi desenvolvido de acordo com a 60601-1-4. No caso da abordagem integrada, a auditoria deverá garantir que o sistema foi desenvolvido de acordo com as duas Normas.

Para ajudar na implementação da abordagem integrada, a Tabela 2 foi compilada com as prescrições da 60601-1-4 a serem adicionadas às prescrições da 14971.

Tabela 2. Itens da 60601-1-4 a serem incluídos em um processo integrado e descrição resumida

| Itens da 60601-1-4 | Descrição resumida |
|--------------------|---|
| 6.8.202 | Identificação nos documentos acompanhantes |
| 52.201.1 | Documentação sendo parte dos registros da qualidade |
| 52.201.2 | Arquivo de gerenciamento de risco dentro de sistema de gerenciamento formal |
| 52.201.3 | Sumário de gerenciamento de risco |
| 52.202.2 b) | Plano de validação dentro do plano de gerenciamento de risco |
| 52.203.1 | Ciclo de vida de desenvolvimento para sistemas programáveis |
| 52.203.2 | Ciclo de vida dividido em fases e tarefas com entrada, saída e atividade |
| 52.203.3 | Inclusão de processos de gerenciamento de risco no ciclo |
| 52.203.4 | Prescrições para documentação no ciclo |
| 52.203.5 | Gerenciamento de risco aplicado ao longo do ciclo |
| 52.203.6 | Sistema definido de resoluções de problemas no ciclo |
| 52.204.3.1.5 | Causas iniciadoras de perigos |
| 52.204.3.1.6 | Assuntos específicos a serem considerados na análise de perigo |
| 52.204.3.1.10 | Inclusão dos perigos e causas iniciadoras no sumário de gerenciamento de riscos |
| 52.205 | Qualificação de pessoal |
| 52.206.1 | Especificação de prescrições para cada sistema programável e subsistemas |
| 52.206.2 | Especificação deve detalhar funções relacionadas a riscos |
| 52.206.3 | Especificação deve incluir informações sobre redução de risco |
| 52.207.1 | Arquitetura deve satisfazer a especificação |
| 52.207.2 | Deve ser especificada uma arquitetura para o sistema programável e subsistemas |
| 52.207.3 | Especificação da arquitetura deve endereçar as prescrições para controle de risco |
| 52.207.4 | Utilização de estratégias para reduzir a probabilidade do perigo |

| Itens da 60601-1-4 | Descrição resumida |
|--------------------|--|
| 52.207.5 | Considerações a serem levadas em consideração na especificação da arquitetura |
| 52.208.1 | Projeto deve ser decomposto em subsistemas onde apropriado |
| 52.208.2 | Dados do ambiente de projeto devem constar no arquivo de gerenciamento de riscos |
| 52.209.1 | Deve ser executada verificação das prescrições de segurança |
| 52.209.2 | Desenvolvimento de um plano de verificação para cada fase do ciclo |
| 52.209.3 | Verificação deve ser realizada conforme o plano e resultados devem ser documentados, analisados e avaliados |
| 52.209.4 | Referência aos métodos, técnicas e resultados da verificação deve ser incluída no sumário |
| 52.210.1 | Validação deve ser realizada sob as condições de utilização destinadas |
| 52.210.2 | Desenvolvimento de um plano de validação para mostrar que as prescrições de segurança corretas foram implementadas |
| 52.210.3 | Validação deve ser realizada de acordo com o plano Resultados documentados, analisados e avaliados |
| 52.210.4 | Líder do grupo de validação deve ser independente do grupo de projeto |
| 52.210.5 | Relacionamentos profissionais entre grupo de validação e projeto devem ser documentados no arquivo |
| 52.210.6 | Nenhum membro do grupo de validação deve validar seu próprio projeto |
| 52.210.7 | Referências aos métodos de validação e resultados deve ser incluído no arquivo |
| 52.211.1 | Modificações no projeto |
| 52.211.2 | Documentos do ciclo de vida devem ser mantidos de acordo com um sistema de gerenciamento formal |
| 52.212.1 | Deve ser executada uma avaliação para assegurar o desenvolvimento de acordo com esta Norma |

Conforme já mencionado, uma vantagem da proposta é a integração das necessidades de gerenciamento de riscos, e além disso, em um nível superior, dos sistemas de gerenciamento de riscos e sistemas de qualidade. Tal proposta pode ser facilmente implementada em uma organização em estágios iniciais de implementação de processos de gerenciamento de riscos. Uma limitação pode estar em organizações que já possuem sistemas separados e onde a reestruturação em um só sistema pode ser muito trabalhosa ou dispendiosa.

Contudo, vale à pena lembrar um ponto: a nova versão da Norma geral de equipamentos eletromédicos, além de possuir a necessidade de um processo de gerenciamento de riscos de acordo com a 14971, incorpora os requisitos da 60601-1-4 em seu corpo (a Norma 60601-1-4 deixará de existir individualmente). Embora tal mudança tardará a chegar nas regulamentações nacionais, os fabricantes que fazem exportação de equipamentos terão necessidade de se adequar a essa Norma geral em pouco tempo (o prazo de mudança deverá ser de 5 anos no exterior). Portanto, quanto antes tal integração for implementada, mais preparados os fabricantes estarão para a competição no mercado externo.

5. CONCLUSÃO

Foi proposta uma abordagem integrada de processos de gerenciamento de riscos de equipamentos eletromédicos e seus sistemas programáveis. Tal proposta tem vantagens e desvantagens dependendo de quão inserido está o processo de gerenciamento de riscos na organização. Espera-se que o trabalho seja utilizado como uma ponte entre os diversos sistemas de gerenciamento que existem dentro das organizações, e que possa ser utilizado como idéia inicial para outros tipos de integração. Um exemplo seria a integração de um processo de gerenciamento de fatores humanos e usabilidade, conforme exemplificado pela Norma IEC 60601-1-6 [10].

REFERÊNCIAS

- [1] N. G. Leveson, "Safeware – System safety and computers", Addison-Wesley Professional, Boston, 1995.
- [2] Associação Brasileira de Normas Técnicas, "ABNT NBR IEC 60601-1-4 – Equipamentos Eletromédico Parte 1-4 – Prescrições gerais para segurança – Norma colateral: Sistemas eletromédicos programáveis", Segunda edição, ABNT, Rio de Janeiro, 2004.
- [3] Associação Brasileira de Normas Técnicas, "ABNT NBR ISO 14971 – Produtos para a saúde – Aplicação de gerenciamento de risco em produtos para a saúde", Primeira edição, ABNT, Rio de Janeiro, 2004.
- [4] European Commission, "Council Directive 93/42/EEC of 14 June 1993 Concerning Medical Devices - Medical Device Directive (MDD)", *Official Journal of the European Communities*, vol 36, 1993.
- [5] International Electrotechnical Commission, "IEC 60601-1 Ed. 3 – Medical Electrical Equipment – Part 1: General requirements for basic safety and essential performance", documento 62A/505/FDIS, IEC, Suíça, 2005.
- [6] Global Harmonization Task Force, "Implementation of Risk Management Principles and Activities Within a Quality Management System", www.ghtf.org – acessado em 19 de setembro de 2005, 2005..
- [7] R. S. Pressman, "Software Engineering – A practitioner's approach – International Edition", McGraw-Hill Book Co., Cingapura, 2001.
- [8] International Electrotechnical Commission, "IEC 62304 Ed. 1 – Medical device software – software life-cycle processes", documento 62A/474/CDV, IEC, Suíça, 2005.
- [9] Institute of Electrical and Electronics Engineers, "IEEE Std 610.12 – IEEE Standard Glossary of Software Engineering Terminology", IEEE, Nova Iorque, 1990.
- [10] International Electrotechnical Commission, "IEC 60601-1-6 Ed. 1 – Medical Electrical Equipment – Part 1-6: Collateral standard - Usability", IEC, Suíça, 2004.