Proposta de Metodologia de Homologação e Certificação de Produto de Defesa Cibernética: o caso dos equipamentos de videoconferência

Ariane C. B. Florentino, Sanderson C. M. Barbalho

Departamento de Engenharia Mecânica – Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – Brasília – DF – Brasil

arianecristin@hotmail.com, sandersoncesar@unb.br

Abstract. *The information security management brings procedures and processes based on international standards, such as ISO (International Standard Organization) standards, aimed at providing safety of the technology assets of an organization.This research will show the cyber defense and the videoconference system, its definition and a proposal for a homologation system and cyber defense product certification with the help of the Common Criteria.*

Resumo. *A gestão da segurança da informação traz procedimentos e processos baseados em normas internacionais, tais como a International Standard Organization ISO, que visa proporcionar segurança dos ativos de tecnologia de uma organização. Esta pesquisa irá expor a ciberdefesa e o sistema de videoconferência, a sua definição e uma proposta de sistema de homologação e certificação de produtos de defesa cibernética com o apoio do Common Criteria.*

1. Introdução

Segundo [Junior 2011], a utilização dos sistemas de informação pelas organizações tornou-se questão de sobrevivência em meados de 1990. Sejam elas públicas ou privadas, a informação é extremamente valiosa para essas entidades, considerando que é a base de suas tomadas de decisões.

A Tecnologia da Informação (TI) pode ser considerada a base para o modelo operacional de diversas entidades, além do que "A dependência frente à infraestrutura exige cada vez mais a participação dos gestores de TI no planejamento organizacional, bem como dos gestores de telecomunicações na formulação de políticas públicas" [Junior 2011].

Diversos dados sensíveis trafegam pelos sistemas de comunicações unificadas, sejam em reuniões virtuais, videoconferências ou web chats realizados entre as diferentes entidades da administração pública federal (APF). Qualquer falha de gestão de segurança pode impactar negativamente a organização, alterando sua disponibilidade de serviços, trazendo prejuízos financeiros e de imagem, e até mesmo multas e sanções administrativas aos envolvidos.

A pesquisa em tela analisa o aspecto da defesa cibernética nas homologações e certificações do produto mecatrônico "equipamento de videoconferência". Esse tipo de equipamento é muito difundido nas esfera pública e privada e objeto pelo qual transitam informações sensíveis das mais diversas categorias. O estudo parte de um modelo teórico para a homologação e certificação cibernética para esse tipo de produto e visa chegar à

 ©2016 SBC — Soc. Bras. de Computação

realização de testes em um equipamento específico de uma empresa de capital misto de grande porte.

As próximas seções deste artigo estão dispostas da seguinte forma: a 2ª seção aborda a revisão teórica, com conceitos de produto mecatrônico e videoconferência; enquanto que a seção 3 apresenta a metodologia usada. Na 4ª seção são tratados os resultados e as discussões, e na 5ª seção seguem as considerações finais.

2. Revisão Teórica

A cibernética compreende a utilização de distintos meios tecnológicos, envolvendo sistemas de informação e comunicações. O setor cibernético é considerado pelo governo brasileiro como de importância estratégica – ao lado dos setores nuclear e espacial.

Após o governo brasileiro estabelecer, em dezembro de 2008, o setor cibernético como de importância estratégica – ao lado dos setores nuclear e espacial - o Exército Brasileiro instituiu no ano seguinte o Setor Cibernético no âmbito da Força Terrestre sob determinação do Ministério da Defesa. Desde então, o Projeto Estratégico de Defesa Cibernética vem consolidando-se devido à necessidade da existência de uma entidade para liderar os intervenientes nessa empreitada [Brasil 2015a]. Com o objetivo de desenvolver medidas de proteção e mitigar ataques no campo cibernético, o Projeto Estratégico de Defesa Cibernética, estabelecido em 2009 pelo Exército Brasileiro, é composto por várias ações em nível operacional e estratégico [Brasil 2015a] dentre elas a criação do Comando de Defesa Cibernética (ComDCiber).

Considerando o risco à soberania do país, o ComDCiber possui em sua estrutura dois elementos importantes: a Escola Nacional de Defesa Cibernética (ENaDCiber) e o Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética (SHCDCiber). A primeira visa capacitar recursos humanos, permitindo dominar áreas multidisciplinares e implantar pesquisa científica voltada ao tema, dialogando com entidades civis corporativas e acadêmicas [Brasil 2015a]. Já o SHCDCiber objetiva se "constituir em um sistema nacional de homologação e certificação de produtos e serviços de defesa cibernética, que seja economicamente sustentável junto à Base Industrial de Defesa nacional, e em conformidade a padrões nacionais de segurança de equipamentos e serviços necessários à defesa do espaço cibernético" [Brasil 2015b].

A Fundação Universidade de Brasília (FUB) executou recentemente o projeto "Apoio ao Programa Defesa Cibernética na Defesa Nacional: Viabilidade e Concepção da Escola Nacional de Defesa Cibernética e do Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética - ENaDCiber-SHCDCIBER@DCDN", atestando a viabilidade de implantação da ENaDCiber e do SHCDCiber. Diversos dos aspectos metodológicos aqui referenciados são oriundos desse estudo.

2.1 Produto Mecatrônico e Videoconferência

Produto mecatrônico é um sistema com múltiplos componentes e domínios, envolvendo elementos mecânicos, eletrônicos, de controles e engenharia da computação [Behbahani e De Silva 2012].

A multidisciplinaridade possibilita integrar as características de cada um de seus componentes, otimizando-o sinergicamente."O entendimento da mecatrônica como aplicação da eletrônica na engenharia mecânica explica um número considerável de

 ©2016 SBC — Soc. Bras. de Computação

aplicações da mecatrônica" [Barbalho 2006]. Diversos produtos, como robôs, sistemas de manufatura automatizados, automação de produtos de consumo como automóveis e dispositivos iOT (*internet of things*) exemplificam tal definição. Outros produtos mecatrônicos têm origem em equipamentos eminentemente eletrônicos. Um exemplo dessas aplicações são os terminais de videoconferência.

Terminais de videoconferência são compostos basicamente por: um codec (codificador/decodificador de áudio e vídeo); microfones; uma (ou mais) câmeras de vídeo (fixas ou com PTZ - pan/tilt/zoom); um monitor de vídeo (ao mínimo, ou um projetor de grandes dimensões); câmara de documentos (opcional).

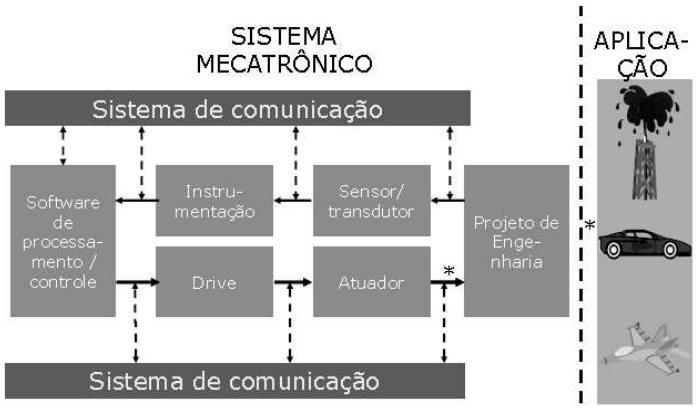

Figura 1 – Elementos de um Sistema Mecatrônico [Barbalho 2006]

A solução tecnológica utiliza redes convergentes, que encaminham e tratam voz, dados e vídeo em uma infraestrutura única de rede, através de uma única modalidade de equipamento. Com a videoconferência é possível a comunicação com voz e vídeo entre pessoas dispersas geograficamente, inclusive com compartilhamento de conteúdo. Os participantes podem acessar a conferência de qualquer lugar com acesso à Internet, usando seu próprio computador, com um microfone e uma webcam, ou seu dispositivo móvel.

O *Common Criteria for Information Technology Security Evaluation* (abreviado como *Common Criteria* ou CC) é um *framework* de Critérios Comuns de avaliação padronizada de Segurança da Informação voltada à segurança de computadores, padronizado na ISO/IEC 15048.O CC trata da proteção dos ativos com relação a três tipos de falhas de segurança: divulgação não-autorizada, modificação ou perda de uso. As categorias de proteção utilizadas são conhecidas por confidencialidade, integridade e disponibilidade, respectivamente.

Conforme suas necessidades, os usuários de sistemas computacionais especificam seus requisitos funcionais de garantia e de segurança [Common Criteria 2006]. Os fabricantes, ao seguirem esses requisitos na produção dos equipamentos de segurança computacional podem garantir que o fluxo de especificação, implementação e avaliação ocorreu conforme critérios determinados rigorosa e padronizadamente.

3. Metodologia

O estudo buscará identificar principalmente quais os riscos de segurança da informação envolvidos nos equipamentos de videoconferência e quais devem ser os parâmetros

 ©2016 SBC — Soc. Bras. de Computação

mínimos a serem exigidos nesses sistemas, quando de sua fabricação, aquisição e utilização.

A partir do levantamento inicial serão verificados os requisitos funcionais de garantia e de segurança, conforme especificados no CC, proporcionando o desenvolvimento de um *Protection Profile* (PP). Para auxiliar nessa tarefa o *Target Of Evaluation* (TOE) a ser considerado será o equipamento de videoconferência, sendo o objetivo da pesquisa o desenvolvimento de um PP para o TOE. A metodologia empregada neste trabalho está apresentada na figura 2.

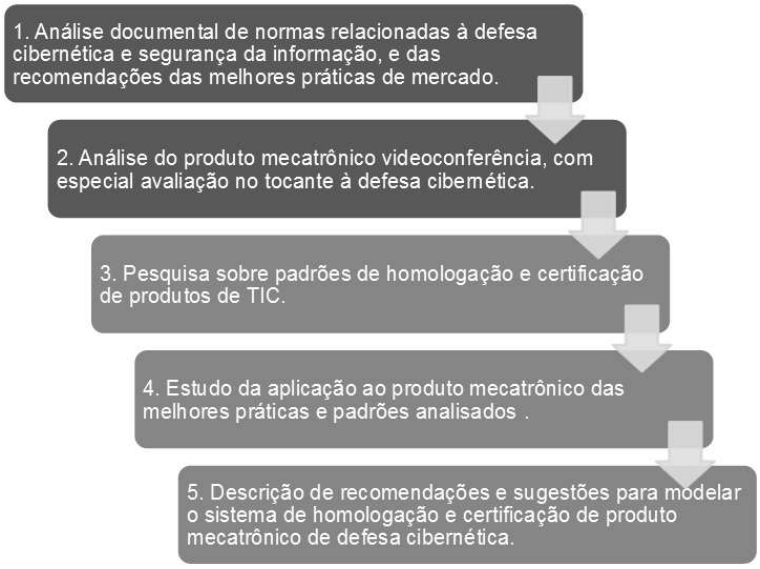

Figura 2 – Metodologia da pesquisa

Para fundamentação da pesquisa os seguintes conceitos serão analisados inicialmente: segurança cibernética; produto mecatrônico; sistema de videoconferência; segurança da informação e comunicações. Após o embasamento desses conceitos segue-se a análise do produto mecatrônico sob o ponto de vista da segurança, com vistas à elaboração de *protection profile* baseado no *Common Criteria*.

O trabalho acadêmico conclui com a análise do equipamento de videconferência utilizando o *protection profile* definido anteriormente. Tal análise permitirá descrever recomendações, propondo uma metodologia de homologação e certificação do produto de defesa cibernética.

4. Resultados e Discussões

Após a revisão bibliográfica dos conceitos fundamentais da pesquisa foram realizadas as análises estrutural e funcional do equipamento de videoconferência. Estruturalmente, o equipamento de videoconferência divide-se em: componentes ópticos, elétricos, eletroeletrônicos e de controle, conforme o esquema da figura 3.

Como componente óptico tem-se a câmera de vídeo. Em componentes elétricos agrupam-se: microfone, cabos de alimentação e de rede. O controle remoto e o decodificador de vídeo são considerados componentes eletroeletrônicos, enquanto que o software de controle é o componente de controle do produto mecatrônico.

 ©2016 SBC — Soc. Bras. de Computação

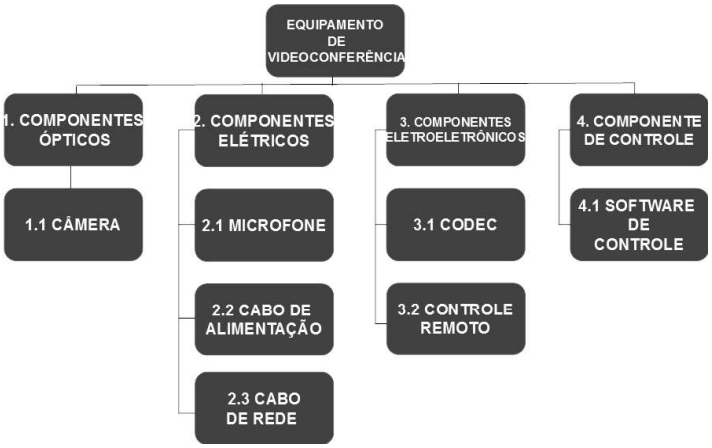

Figura 3 – Estrutura do Produto Mecatrônico Equipamento de Videoconferência

Conforme mostrado na figura 4, o produto mecatrônico apresenta dois sistemas principais: o sistema de alimentação e o sistema de controle.

O fluxo de energia entre esses sistemas e os componentes do equipamento estão representados pela linha tracejada. Dessa forma, estão diretamente associados ao sistema de controle o codec (codificador/decodificador) e o controle remoto. Ao sistema de alimentação relacionam-se diretamente: os cabos de alimentação e de rede, o microfone, a câmera e o monitor.

As setas de linha contínua representam o funcionamento essencial do sistema mecatrônico: os cabos de alimentação e de rede ligam-se diretamente ao microfone e câmera; o controle remoto direciona o software de controle do equipamento, que por sua vez controla o microfone, a câmera e o codec. Este último recebe instruções do software de controle, processando sinais de áudio e vídeo recebidos do microfone e da câmera e liberando-os ao monitor.

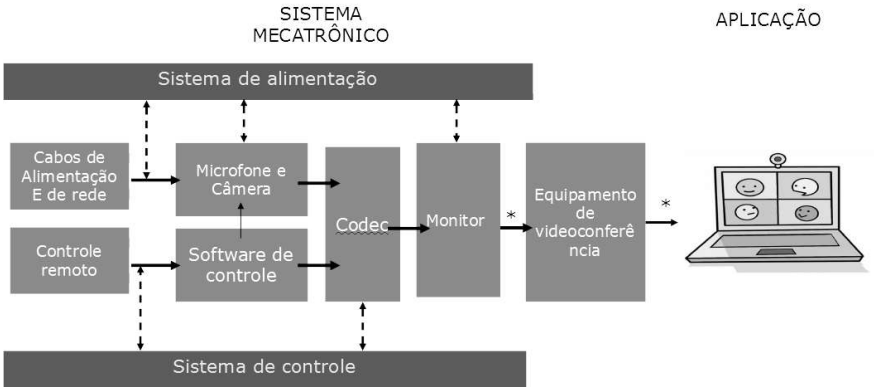

Figura 4 – Esquema Funcional do Equipamento de Videoconferência

Em sequência à análise do produto mecatrônico e de seu esquema funcional teve início o desenvolvimento do *protection profile,* com o objetivo de aplicar as melhores práticas de segurança da informação aos equipamentos de videoconferência, norteado pelo padrão *Common Criteria* de homologação e certificação de produtos de Tecnologia da Informação e Comunicações (TIC). Este é o estágio atual desta pesquisa acadêmica.

 ©2016 SBC — Soc. Bras. de Computação

5. Considerações Finais

O uso da videoconferência pelas organizações permite agilidade, qualidade e segurança nas tomadas de suas decisões colegiadas, garantindo maior dinamismo na realização das transações comerciais entre seus clientes internos (diversas instâncias administrativas) e externos (clientes finais), já que dispensa deslocamento físico entre os funcionários para participar de reuniões com seus parceiros comerciais, dispersos pelo mundo.

Alinhada ao conceito de defesa cibernética e soberania do país, é vital a realização de um sistema de certificação e homologação de produto de defesa cibernética.

É extremamente válida a utilização de *protection profiles (PP)* para avaliar os equipamentos de videoconferência, considerando que o *Common Criteria* é um padrão internacionalmente reconhecido. Os requisitos de segurança a serem levantados para a formação do PP dos equipamentos devem possuir relação direta com as funcionalidades conforme a necessidade de utilização dos usuários. Para auxiliar nessa tarefa o TOE a ser considerado é o equipamento de videoconferência, sendo que o desenvolvimento de um PP para o TOE é o objetivo da pesquisa. Para o desenvolvimento do PP, os requisitos de segurança serão relacionados considerando ainda os seguintes aspectos: disponibilidade, integridade e confidencialidade dos dados.

O fato de um produto ter sido avaliado significa somente que no contexto de propriedades de segurança, determinadas características foram avaliadas através de métodos específicos, não que o produto seja completamente seguro, do ponto de vista computacional. As autoridades certificadoras devem verificar os produtos, propriedades e métodos para determinar que uma avaliação irá fornecer resultados significativos. Já os consumidores dos produtos avaliados devem considerar esse contexto para determinar se aquele produto é útil e aplicável a situações específicas e segundo suas necessidades.

Referências

Barbalho, S. C. M. (2006) “Reference Model for Mechatronic Product Development: Proposal and Applications”, Universidade de São Paulo, Escola de Engenharia de São Carlos, São Carlos.

Behbahani S. e De Silva C. W. (2012) A design paradigm for mechatronic systems. In *Mechatronics Jounal, Elsevier*, Volume 23, Issue 8, Dezembro, páginas 960 – 966, http://dx.doi.org/10.1016/,Dezembro 2015.

Brasil. Ministério da Defesa. Exército Brasileiro. (2015a) http://www.epex.eb.mil.br/index.php/projetos/defesa-cibernetica.html>, Dezembro.

Brasil. Ministério da Defesa. Exército Brasileiro. (2015b) “Estudo de Viabilidade do SHCDCiber no Âmbito do Projeto EnaDCiber-SHCDCiber@DCDN”, Brasília: UnB.

Common Criteria (2006) Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 1.

Junior, C. C. (2011) Sistemas Integrados de Gestão – ERP: Uma abordagem gerencial, Curitiba, Ibpex, 4ª edição.

 ©2016 SBC — Soc. Bras. de Computação