PRODUÇÃO ONLINE
REVISTA CIENTÍFICA ELETRÔNICA DE ENGENHARIA DE PRODUÇÃO
ISSN 1676-1901

DIAGNÓSTICO DOS PROCESSOS DE HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS DE NATUREZA CIBERNÉTICA: PERSPECTIVAS PARA A CONSTRUÇÃO DE UM SISTEMA NACIONAL

DIAGNOSIS OF APPROVAL AND CERTIFICATION PROCESSES OF CYBER-NATURE PRODUCTS: PERSPECTIVES FOR THE CONSTRUCTION OF A NATIONAL SYSTEM

Sanderson Cesar Macedo Barbalho*E-mail: scmbbr@yahoo.com.br
Simone Borges Simão Monteiro* E-mail: simoneborges@unb.br
Ana Carla Bittencourt Reis* E-mail: anacarlabr@yahoo.com.br
Rhoxanna Crhistianth Farago Miranda** E-mail: rhoxanna@gmail.com
*Universidade de Brasília (UnB), Brasília, DF
**Força Aérea do Brasil, Brasília, DF

Resumo: O uso de computadores, tablets, smartphones, relógios inteligentes, smartmeters, sistemas GPS e assim por diante, traz um benefício comum a todos aqueles que acessam tais tecnologias, porém, ao mesmo tempo, tais sistemas têm uma influência fundamental no aspecto da privacidade do indivíduo. Desta forma, torna-se premente em nossa sociedade ter um sistema que permita homologar e certificar produtos de natureza cibernética. O presente artigo tem como objetivo retratar um diagnóstico dos processos de homologação e certificação de produtos de natureza cibernética que são usados por órgãos da administração central e pelas forças armadas, com vistas a desenvolver um Sistema Nacional de homologação e certificação desse tipo de produto. A fim de desenvolver o diagnóstico foram realizadas pesquisas documentais em órgãos responsáveis pela certificação de produtos tecnológicos e foram realizados estudos de caso em cinco organizações públicas e privadas. Os resultados desses estudos foram sistematizados para serem validados em grupo focal com especialistas. Demonstrou-se uma visão compartilhada pelas empresas e órgãos quanto ao aspecto da certificação de produtos, mas não houve um entendimento consensual sobre a homologação. Foram identificados ainda processos realizados por órgãos governamentais que fogem ao escopo tradicional da homologação de produtos na literatura científica.

Palavras-chave: Homologação de produtos. Certificação de produtos. Desenvolvimento de produtos. Cibernética. Mecatrônica.

Abstract: The use of computers, tablets, smartphones, smart clocks, smartmeters, GPS systems and so on bring a common benefit to all those who access such technologies, but at the same time such systems have a fundamental influence on the individual privacy. In this way, it becomes imperative in our society to have a system that allows homologating and certifying cyber-nature products. The present article aims to portray a diagnosis of the approval and certification processes for products of cybernetic nature by public agencies in Brazil with a view to developing a National System for approval and certification. In order to develop the diagnosis, document research was carried out in bodies responsible for certification of technological products and case studies were carried out in five public and private organizations. The results of these studies were systematized to be validated by a focal group of specialists. There was a shared view of companies and bodies regarding the aspect of product certification, but there was no consensus on the homologation procedures. Also were identified some processes performed by government agencies that are outside the traditional scope of homologation.

Keywords: Product homologation. Product certification. New Product Development. Cyber-physical Systems. Mechatronics.

1 INTRODUÇÃO

A dependência de tecnologias de informação e comunicação (TICs) tais como computadores, *tablets, smartphones,* relógios inteligentes, *smartmeters*, sistemas GPS, torna-se cada vez maior. Essas tecnologias podem apresentar vulnerabilidades que se não forem gerenciadas colocam em risco a segurança do indivíduo, da sociedade, ou até mesmo do sistema de Defesa Nacional. Portanto, torna-se fundamental ter um sistema que permita homologar e certificar esse tipo de produto, a fim de mitigar tais ameaças.

Adicionalmente, no contexto brasileiro – no qual todas as tecnologias envolvidas com o espaço cibernético, desde as aplicações mais próximas do usuário, como as acima citadas, até aplicações sem qualquer transparência ao indivíduo, como um sistema de guiamento de míssil – o controle permitido pelos sistemas de tecnologia cibernética não está a serviço do Governo Brasileiro, uma vez que tais tecnologias tem origem principalmente norte-americana, estando as empresas deste país sujeitas à legislação do Governo que impõe a disponibilização das informações geradas pelas tecnologias aos seus órgãos de inteligência, para serem usadas, especialmente em segurança e combate ao terrorismo.

Essa problemática não é exclusividade brasileira. A União Européia tem buscado regular o uso dos sistemas aqui discutidos. Mais recentemente, a questão foi retomada no continente europeu com uma tentativa de combate ao monopólio da busca na internet, baseado em Google. A questão cibernética, no âmbito das relações diplomáticas tem sido uma constante, desde a guerra fria. Atualmente, as relações diplomáticas estabelecidas entre americanos e chineses ou russos é fortemente influenciada pelos denominados ciberataques e influencia as principais economias a criarem programas voltados para o que tem sido denominado Defesa Cibernética.

O Brasil foi um dos principais alvos do escândalo Snowden, pelo fato de haver espionagem direta no e-mail e telefone da Presidenta. Desde então, passou-se a discutir a problemática da Defesa Cibernética. O Governo divulgou ações a serem tomadas nesse âmbito no qual são mencionados os programas vinculados a estabelecer uma Escola Nacional de Defesa Cibernética (ENADCiber) e um Sistema Nacional de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDCiber), ambos objetivos abrangidos por um projeto de pesquisa desenvolvido

entre os anos de 2014-2016 por uma Universidade Pública Federal junto ao Exército Brasileiro.

Este texto é originado da vertente do SHCDCiber no projeto acima mencionado. O objetivo final do projeto foi desenvolver um plano de implantação com a análise de viabilidade econômica e planejamento do projeto de implementação do sistema. Tais resultados foram entregues ao Exército Brasileiro, o qual é responsável na Estratégia Nacional de Defesa pela questão cibernética (BRASIL, 2008). Uma das etapas do projeto foi o diagnóstico dos processos de homologação e certificação que essa tipologia de produto segue atualmente, antes de ser adquirido pelos órgãos da administração central e especialmente, pelas Forças Armadas.

O objetivo deste artigo é apresentar diversos aspectos da problemática da homologação e certificação de produtos de natureza cibernética com enfoque na identificação dos principais processos, problemas encontrados e diretrizes que servirão de insumo para o posterior desenvolvimento e implementação do SHCDCiber. Visa também contribuir para aprofundar contingências às referências para o processo de desenvolvimento de produtos no Brasil, quando a tecnologia de produto incorpora elementos de diversos matizes tecnológicos (Pagan, Silva e Mello, 2013; Pinheiro, Santos e Cleto, 2015). Para isso, foram realizados estudos de múltiplos casos, além de entrevistas em grupo focal com profissionais, professores universitários e empresários envolvidos com a cibernética no Brasil.

A seção2 apresenta conceitos teóricos sobre o tema estudado, a seção 3 expõe a metodologia do trabalho, na seção 4 é retratado o diagnóstico dos processos de homologação e certificação realizados com produtos que tenham aplicação em defesa cibernética, e por fim, a seção 5 exibe as considerações finais.

2 DEFESA CIBERNÉTICA

O termo cibernética deriva do grego *kybernetikos* que significa governança ou arte de governar (COLARIK e JANCZEWSKI, 2011). A cibernética se preocupa em estudar a relação entre comando, controle, comunicação e fluxo de informações entre máquinas e seres vivos (WIENER, 1984).

Para Haeni (1997) e Neumann (2014), as infraestruturas críticas oferecidas à sociedade tais como energia elétrica, distribuição de água, transportes, finanças,

petróleo e gás, sistemas de saúde etc, são atividades que denotam uma grande dependência de TICs. As tecnologias cibernéticas ganharam um grande impulso nas últimas décadas, se tornando uma ameaça à estabilidade de redes que sustentam infraestruturas críticas de vários países.

A ciberguerra (*cyber war*) é concebida como uma ameaça real, uma ação intencional humana, emanada por um agente de ameaça cibernética, que provoca um incidente cibernético ou incidente de segurança cibernética, com efeitos potencialmente danosos. Os ataques cibernéticos podem ser conduzidos por meio de "armas" cibernéticas (vírus e *worms* projetados para desestabilizar), obtendo como consequência a danificação de computadores, invasão de sistemas ou redes de informação, destruição de redes críticas, danos físicos ou alteração de desempenho de sistemas cruciais, ações em geral vinculadas a espionagens e sabotagens (HAENI, 1997). Na ocorrência de um ataque cibernético, a depender de sua natureza, as Forças Armadas para preservar a soberania e o patrimônio nacional lidam com as vulnerabilidades decorrentes desses ataques, o que é realizado por meio da utilização de tecnologias adequadas sendo estas também de natureza cibernética.

Com o intuito de proteger a nação, a Defesa Cibernética atua com um conjunto de ações defensivas, exploratórias e ofensivas, no âmbito de um planejamento militar, ocorridas no espaço cibernético, com o propósito de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência, e agravar os sistemas de informação do oponente. A Segurança Cibernética, que faz parte do sistema de Defesa Cibernética, é responsável pela preservação da confidencialidade, da integridade e da disponibilidade da informação na Internet, incluindo não somente o *hardware, software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes (ISO/IEC 27032, 2012).

A falta de uma padronização em segurança cibernética assim como o compartilhamento de informações pertinentes às estratégias adotadas é um problema enfrentado por muitos países, conforme demonstra Shafqat e Massod (2016) que realizam uma comparação das estratégias nacionais de segurança cibernética em 20 países de diferentes regiões do mundo. Relatam ainda a Malásia como o país mais experiente em cibernética, porém, assim como o Irã e Israel, não compartilham suas estratégias de segurança cibernética.

Segundo os autores, o conceito de espaço cibernético para países como Nova Zelândia, Austrália, Alemanha, Espanha e Canadá refere-se apenas à internet e aos dispositivos de TIC pertinentes. Apesar de metas e objetivos semelhantes, a pesquisa revelou inúmeras diferenças no âmbito e na abordagem das 20 estratégias selecionadas para o estudo. Conclui-se que as estratégias do Reino Unido, EUA e Alemanha são particularmente mais efetivas em termos de desenvolvimento e execução de planos de ação alinhados às diretrizes estratégicas.

Min et. al. *(*2015) realizam um estudo comparativo internacional das estratégias de segurança cibernética adotadas pelos EUA, Japão e União Européia (UE). Nos EUA existe um conselho de segurança nacional que controla, dirige e implementa a política nacional de segurança cibernética. Porém, não foi definida até então uma lei específica para tratar do tema. Por outro lado, a União Européia (UE) possui planos de ação para a segurança cibernética tratados como prioridade.

Os autores relatam ainda que no ano de 2005, o Japão estabeleceu o Centro Nacional de Segurança da Informação (NISC), sob a autoridade do governo, e a criação de níveis de segurança para infraestruturas críticas. Em 2013 lançou a Estratégia de Segurança Cibernética, ampliando a área de Defesa para o espaço cibernético. Os autores relatam que os países analisados possuem estratégias de Segurança Cibernética, mas ainda é necessário reforçar a parceria público-privado, pois a maior parte do espaço cibernético é utilizado por empresas privadas.

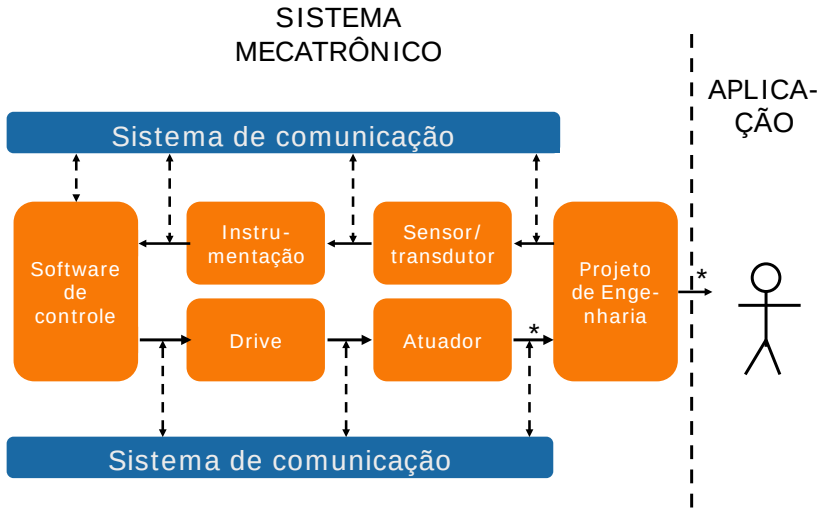
Assim, a experiência internacional aponta para a necessidade de consolidar um Sistema Nacional de Homologação e Certificação de Produtos para a Defesa Cibernética sendo este essencial para informar e proteger o adquirente dos produtos que serão utilizados para fins da Defesa Nacional, além de implicar em legislação para aquisições comuns, uma vez que qualquer produto de TIC que apresente vulnerabilidades, quando usado em locais de risco para as chamadas infra-estruturas críticas, pode se tornar uma arma cibernética, conforme o conceito de sistema cibernético físico (*cyber-physical system* - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2015) apresentado a seguir.

2.1 Produtos de Defesa Cibernética

Uma forma de compreender a tecnologia dos produtos de natureza cibernética

é por meio do conceito de mecatrônica: produtos cibernéticos podem ser considerados produtos mecatrônicos, para os quais devem-se considerar os componentes ilustrados na Figura 1.

Figura 1 - Elementos de um sistema mecatrônico



Fonte: Barbalho (2016)

Os elementos ilustrados na Figura 1 tem, segundo BRADLEY (1991), as seguintes definições:

- sensores e instrumentação: sistema de mensuração utilizado no produto para controlar condições de operação e/ou ambientais.
- *software* de processamento/controle: É o principal componente lógico do sistema. Nele são armazenadas e comandadas as principais funções e rotinas são executadas de maneira a comandar a operação do produto.
- atuadores e drives: os atuadores são componentes robustos utilizados para corrigir o funcionamento do sistema.
- projeto de engenharia: é o projeto básico do mecanismo ou solução de engenharia para o propósito ao qual o produto deve atender.

O produto mecatrônico é um dispositivo essencialmente cibernético, se considerarmos a definição do termo no conceito proposto por Wiener (1984), fundamento de todo o cabedal de conceitos e teorias de controle, as quais resultaram na conceituação dos dispositivos de sensoriamento e atuação, conforme já mencionado.

Atualmente, o produto mecatrônico pode ser conceituado como um *cyber-physical system* (CPS), basicamente um produto cibernético com capacidade de atuação sobre um sistema físico (WU, KAO e TSENG, 2011; LI, QING e BIN, 2013). O Governo Americano, por meio do *National Institute of Standards and Technology* (NIST), constituiu um comitê técnico para desenvolver um framework que no futuro possa ser usado para a regulação técnica de produtos baseados no conceito de CPS (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2015).

Mais especificamente, o padrão americano recomenda que o projeto de sistemas CPS seja orientado à confiança (*trustworthness*), cujos elementos componentes são: (1) segurança da informação (ou cibernética), privacidade, segurança no sentido de evitar catástrofes, confiabilidade e resiliência, esta última como capacidade de resistir e se recuperar de ataques, tendo estreita relação com a dependabilidade (DENKER et al., 2012). O conceito de certificação confiável (*trustiness certification*) de equipamentos de tecnologia da informação é abordado em Coelho e Silva (2013) em esforço similar ao projeto SHCDCiber, realizado em Portugal.

Alguns padrões da indústria como o *Payment Card Industry Data Security Standard* (PCI DSS), contribuem para a adoção de controles de segurança, porém o caminho ainda é árduo. Quando um produto é disponibilizado no mercado ou um serviço é prestado, é necessário que os mesmos tenham qualidade, assim como a segurança, que deve ser considerada como um pré-requisito para incorporação de CPS ao processo de negócio das organizações.

Em geral, a segurança dos produtos de natureza cibernética é uma discussão atual e implica em diversos desafios para homologação e certificação, o que é discutido na seção seguinte.

2.2 Os processos de homologação e certificação de produtos

A homologação e certificação de produtos é parte do processo de desenvolvimento do produto. Pesquisadores brasileiros têm investido na proposição de modelos de referência para o desenvolvimento de produtos (SALGADO et al., 2010) em que se destaca o modelo de referência unificado (ROZENFELD et al., 2006), no qual a homologação é tratada na fase de "preparação da produção" adotando um

enfoque muito próximo ao padrão *Advanced Product Quality Planning* (APQP), proposto pela norma ISO/TS 16949, sendo, portanto, adaptado a um modelo de produção em massa.

Ainda segundo (ROZENFELD et al., 2006), para a certificação do produto, que deve ocorrer na fase de "preparação da produção", são previstas as seguintes atividades: avaliação das exigências de regulamentação, submissão ao cliente do processo de aprovação, avaliação dos serviços associados ao produto e obtenção da documentação para a certificação. Para os autores, o processo de certificação não acontece somente na fase de preparação da produção, podendo ocorrer desde a fase de projeto informacional. O trabalho de Pinheiro, Santos e Cleto (2015) sugere que aspectos de certificação para a Comunidade Européia (CE) sejam incorporados aos processos de desenvolvimento de produtos desde as etapas de pré-desenvolvimento.

No presente trabalho, considera-se que ao buscar contemplar os processos de alto volume de "conceitos estáticos" (PUGH, 1990), como o automotivo, em que a homologação está muito vinculada à produção comercial envolvendo o *ramp up* (CLARK e FUJIMOTO, 1991) dos produtos, o Modelo Unificado acaba trazendo uma certa dificuldade de incorporação de elementos mais tecnológicos, envolvendo desafios técnicos que muitas vezes limitam sobremaneira a definição do próprio conceito do produto, como os imperativos da segurança de informação e de confiança do ponto de vista cibernético.

Por outro lado, o processo sugerido por Barbalho e Rozenfeld (2013), no modelo de referência mecatrônico (MRM), trata a homologação como uma fase do processo de desenvolvimento, e a certificação como etapa da fase de validação do produto. As duas fases são mais detalhadas que em outros processos de referência para desenvolvimento de produtos. Ambos os requisitos, de homologação e certificação, são incorporados no projeto nas fases intermediárias de "especificação" e de "planejamento técnico". Considera-se que tal proposta garante um fluxo mais efetivo de restrições técnicas para o projeto do produto propriamente dito. Assim, como o modelo MRM incorpora elementos de mecatrônica que estão mais próximos ao conceito de cibernética, passou-se a utilizá-lo como referência para a análise proposta neste trabalho.

Atividades de preparação da produção foram estudadas por Tarallo e Amaral (2008) com enfoque em empresas de bens de consumo não-duráveis de alto volume,

e por Varandas Jr e Cauchick (2012) analisando indústrias de processo de alto volume. O enfoque em alto volume incorpora elementos de homologação que se distanciam da tipologia de produto aqui analisado. Adicionalmente, ambos os trabalhos estudam empresas de processo contínuo, o que também difere consideravelmente dos produtos de natureza cibernética aqui analisados.

Mais alinhado ao escopo das homologações e certificações relacionadas a produtos de natureza cibernética, tem-se o trabalho de Tintinago, Trajano e Barbalho (2015) quanto à homologação e validação de produtos de controle de acesso. Para essa tipologia de produtos, os autores identificaram procedimentos de validação com o usuário e de homologação muito frágeis do ponto de vista documental e não ficou evidenciada a questão da submissão dos produtos a organismos de certificação.

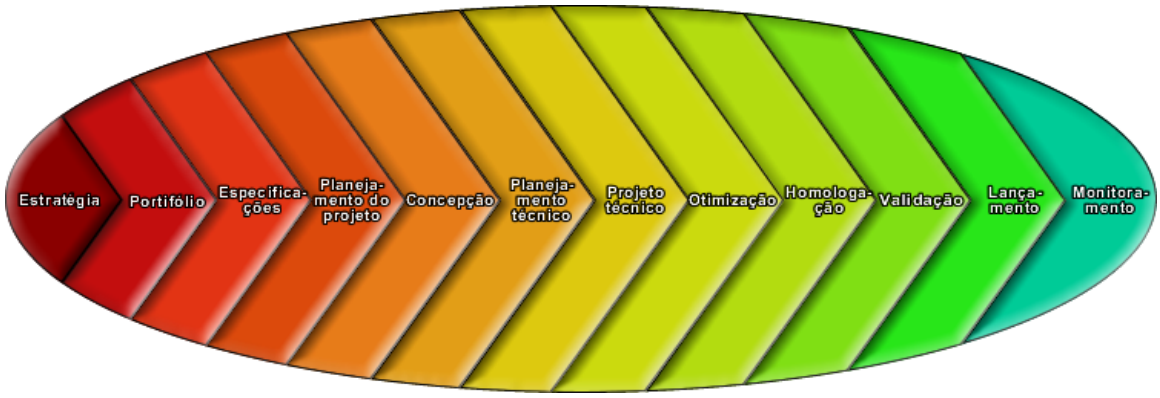
No trabalho de COELHO e SILVA (2013), é apresentada uma proposta para certificação de equipamentos de tecnologia da informação, permitindo prover um ambiente de segurança e confiabilidade. A proposta é baseada na existência de um laboratório de certificação baseado na norma ISO/IEC-17025 e os resultados desses testes e avaliações são incluídos em um relatório técnico, acreditado por organismos internacionais. A garantia do nível de confiabilidade obtida deve então assegurar que o equipamento esteja livre de quaisquer ameaças cibernéticas.

De uma maneira geral, observa-se que o conceito de homologação e certificação utilizado na literatura científica sumarizada acima, não incorpora elementos relativos à problemática enfrentada pelas forças armadas quanto aos produtos cibernéticos utilizados em defesa. De qualquer maneira foi possível identificar um ponto de partida para o estudo dos processos de homologação e certificação de produtos, o que é apresentado na seção seguinte.

2.3 Processo de referência para a homologação e certificação de produtos

A Figura 2 demonstra o fluxo de processo do desenvolvimento de um produto mecatrônico, de acordo com o denominado Modelo de Referência Mecatrônico (MRM). No MRM, um produto é certificado na fase de validação e só é validado depois de homologado.

Figura 2 - Fases do MRM



Fonte: Barbalho e Rozenfeld (2013)

A Figura 3 apresenta a fase de homologação do produto que tem uma relação com o processo mediante o qual o produto é produzido na empresa e/ou em seus fornecedores. Algumas atividades de homologação são mais operacionais, como o projeto de embalagem, por exemplo. Mas é na homologação que as soluções desenvolvidas para o produto passam por atividades cujo objetivo é detalhar a documentação técnica de fabricação e montagem: (1) a instalação e configuração de software e a eletrônica a ele vinculado; (2) uma revisão nas folhas de processo de fabricação utilizadas para produzir os protótipos alta e beta; (3) a confecção de desenhos de conjunto vinculados a listas de peças e procedimentos que detalhem a montagem e ajustes.

Na eletrônica, devem ser consolidados os arquivos de projeto de placas, com máscaras e listas de montagem. Detalhes de limpeza, isolação, crimpagem, soldas especiais e introdução de blindagem e dissipadores dos PCBs são demonstrados. O cabeamento utilizado nas interfaces entre os PCBs, assim como os conectores utilizados devem ser especificados. As formas de ancoramento, isolação, derivações etc. devem ser ilustradas. Especial atenção deve ser dada à integração entre as placas eletrônicas que implementam funções de controle e os dispositivos e placas de alimentação do sistema. Métodos de dissipação térmica, de redução da indutância de acoplamento e aumento das distâncias de separação e escoamento devem ser documentados.

A documentação de fabricação e montagem é analisada sob a ótica das possibilidades de redução de custos. Conceitos de projeto para a manufatura e montagem (*Design for manufacture and assembly* – DFMA) devem ser utilizados para

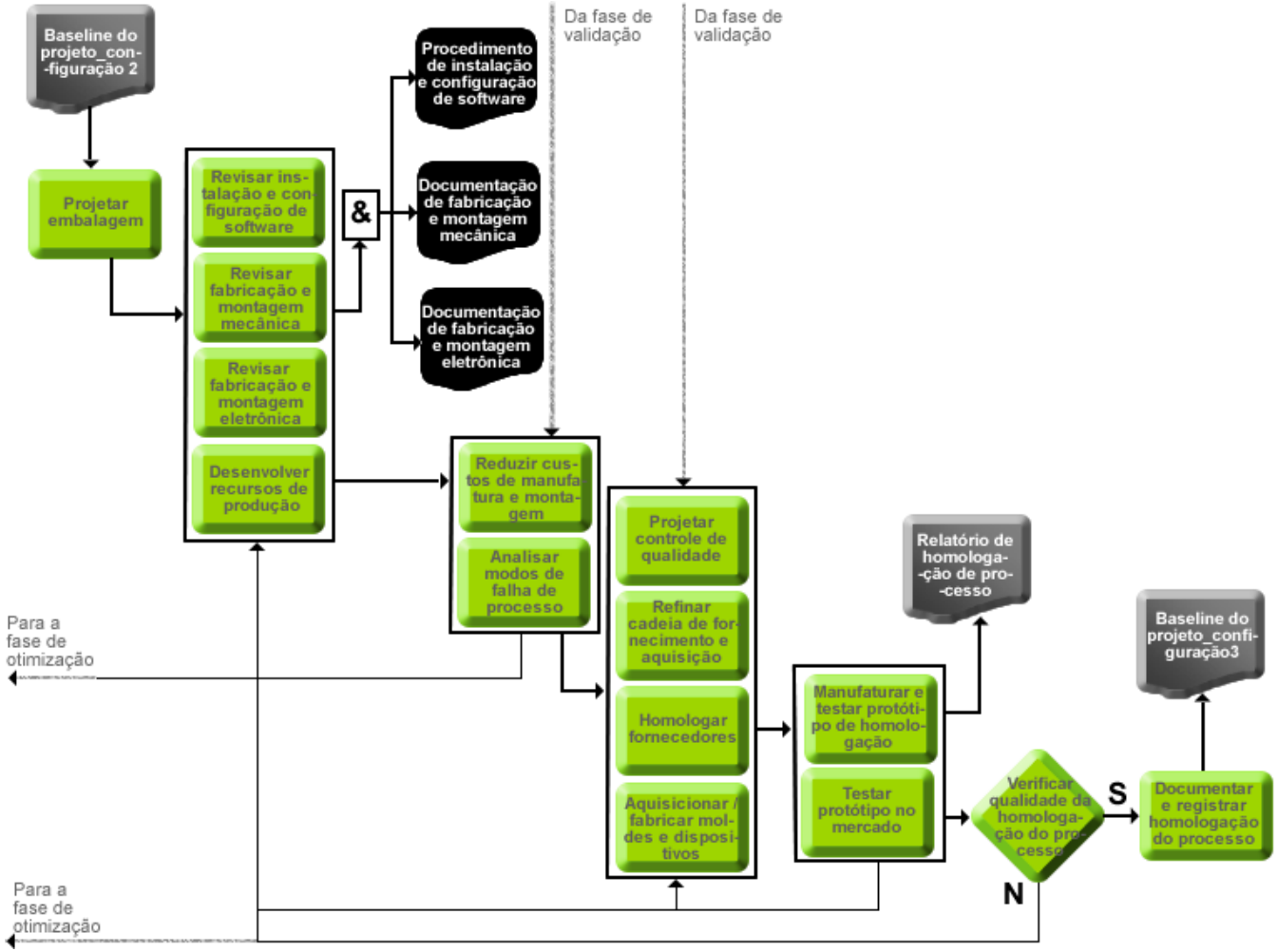
reduzir custos de manufatura e montagem, com materiais e componentes construtivos etc. A empresa deve implementar análises de modos de falha de processo (*process failure mode and effect* analysis – PFMEA). Assim, as alterações de projeto necessárias à redução dos custos de manufatura e montagem são analisadas quanto ao seu impacto no risco de falhas do processo antes que se determinem ações de revisão do projeto.

Conclui-se a fase quando todas as possibilidades de redução de custos de manufatura e montagem forem consideradas e os modos de falha do processo estiverem delimitados a valores de risco pré-definidos. Deve-se então refinar a cadeia de fornecimento e documentação da produção.

Essas atividades correm em paralelo com a aquisição ou fabricação de moldes e dispositivos necessários à fabricação, montagem e integração do produto.

Deve-se realizar o cálculo da capabilidade do processo. Em setores como os automotivo e eletro-eletrônico, em função do alto volume e rígidos requisitos de qualidade, esses valores são mais apertados, enquanto para baixo volume, como em produtos médicos, da área espacial, militar etc., ao invés de utilizar esses parâmetros, o processo deve ser orientado pelos métodos de “zero defeito”.

Figura 3 - Fase de homologação

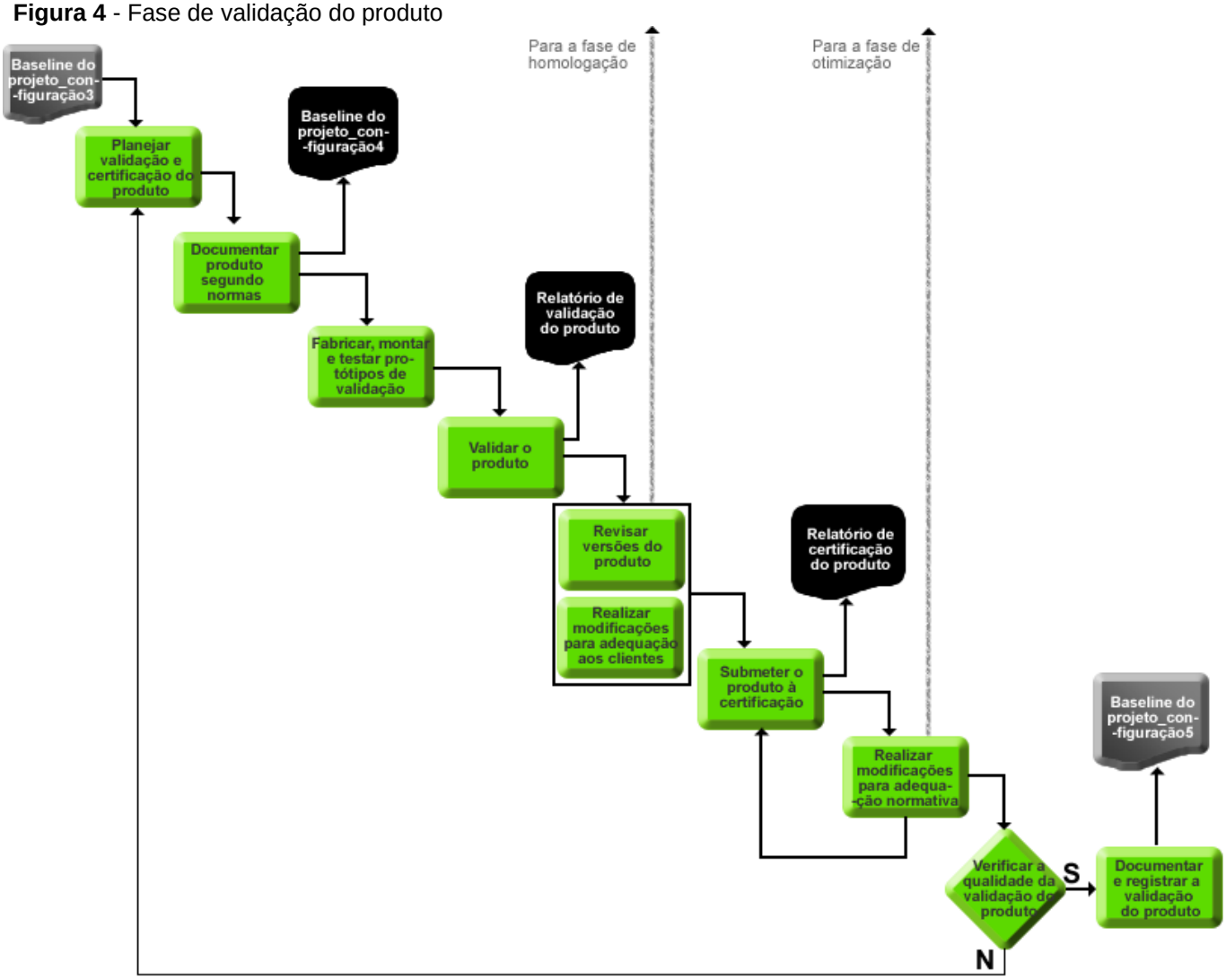


Fonte: Barbalho (2016)

Se os resultados da fase de homologação forem considerados satisfatórios, passa-se ao planejamento da fase de validação do produto. A Figura 4 apresenta a fase de validação em Barbalho (2016). Deve-se inicialmente planejar a validação e a certificação do produto. O produto é, então, documentado segundo as normas de processo e de segurança a ele aplicáveis.

Devem ser fabricados, montados e integrados os protótipos a serem utilizados para a validação do produto, sendo esta uma etapa prescrita na ISO 9001:2015, mas não diretamente relacionada com a certificação técnica do produto.

Figura 4 - Fase de validação do produto



Fonte: Barbalho (2016)

O processo de certificação é a submissão do produto a laboratórios credenciados para certificá-lo. O escopo dos testes aos quais o produto será submetido depende do mercado ao qual é destinado e do tipo de produto,

considerando as normas aplicáveis já previamente identificadas nas fases de "especificação" e "planejamento técnico".

Ao longo dos testes pode ser necessário realizar alterações incrementais no produto, tais como aumento de proteção elétrica em partes com sinais de entrada, introdução de filtros de linha, utilização de resinas e materiais isolantes em determinadas partes do circuito etc. Caso haja implicações na documentação de processo elas devem ser enviadas aos engenheiros de processo.

3 METODOLOGIA

Adotou-se como estratégia de pesquisa uma etapa de estudo de múltiplos casos e pesquisa documental realizadas em paralelo. O objetivo deles foi levantar elementos para a etapa seguinte da pesquisa que foi a submissão do diagnóstico inicial a um grupo focal formado por especialistas em segurança da informação, produtos de alta tecnologia e ainda em cibernética, no intuito de validá-lo.

Os estudos de caso múltiplos são utilizados quando se busca explorar determinadas situações cujo conteúdo científico não é conhecido detalhadamente (YIN, 2010). No trabalho em questão foram realizados cinco estudos de caso, na primeira etapa da pesquisa.

Nos estudos de caso foram pesquisadas duas empresas fornecedoras de produtos para a defesa nacional, tanto para as forças armadas quanto para órgãos da administração central; e ainda, foi realizado estudo de caso em órgão militar responsável pelo controle do espaço cibernético nacional, no âmbito da Copa do Mundo de 2014. Por fim, foram realizadas entrevistas com profissionais de dois centros de pesquisa em tecnologia da informação e comunicação, um de caráter público e outro privado. Os estudos foram realizados com base em um roteiro de pesquisa que buscava entender como a abordagem processual discutida na seção anterior ocorria de fato, se ocorriam as etapas propostas na literatura e caso contrário, como eram realizadas as atividades de homologação e certificação. A experiência das empresas com produtos de áreas que não a de defesa nacional, mas que caracterizavam produtos cibernéticos submetidos à rígida legislação de segurança, tais como equipamentos médicos, aeronáutica e espacial, foram também consideradas.

Para cada tipologia de produto para a qual o órgão ou empresa pesquisada realizava ações de homologação e certificação, solicitou-se a identificação de normas técnicas e laboratórios utilizados.

A pesquisa documental, conforme descrito em Gil (2008), foi realizada com o objetivo de identificar os conceitos de homologação e certificação utilizados por órgãos e empresas vinculadas à questão cibernética, conforme seus documentos de referência acessados na internet ou fornecidos pelos entrevistados nos estudos de caso, ou ainda as normas identificadas nos estudos de caso, as quais foram adquiridas pela equipe de projeto.

Os dados coletados nos estudos de caso foram analisados pela equipe de coordenação do projeto de maneira a preparar material para a segunda etapa da pesquisa, o grupo focal. Essa etapa foi operacionalizada em sessões grupais com especialistas da área, em formato presencial, com o intuito de discutir os aspectos relacionados aos processos de homologação e certificação de produtos cibernéticos diagnosticados na etapa anterior, a fim de fornecer contribuição para a pesquisa, conforme Gil (2008). O grupo focal foi realizado com um conjunto de oito especialistas em cibernética, produtos de defesa, segurança da informação e certificação de produtos. O grupo continha pessoal vinculado à Associação Brasileira de Indústrias de Defesa (ABINDE), ao Centro de Defesa Cibernética do Exército Brasileiro (CDCiber), ao INMETRO, ao Centro de Tecnologia de Informação (CTI) e profissionais de empresa e academia. As pessoas residentes em outras localidades que não a do Estado da federação onde a Universidade em tela se localiza tiveram suas custas de deslocamento pagas pelo projeto.

Buscou-se a participação de pessoal do INMETRO tanto pelo aspecto técnico do projeto, uma vez que o representante do órgão é responsável pelo laboratório de análise de produtos que utilizam criptografia, quanto pelo aspecto mais processual buscando identificar profissional com sólida vivência relativa ao sistema metrológico nacional.

Na condução do grupo focal houve uma apresentação inicial do diagnóstico realizado na etapa de estudos de caso, seguida por uma discussão em grupo realizada com questões a serem respondidas pelos participantes. Entre as questões discutidas, há: (1) dentre os processos de homologação e certificação apresentados, quais seriam mais críticos e porquê; (2) se haveriam outros processos necessários à

homologação e certificação de produtos cibernéticos usados em Defesa; (3) se haveriam níveis diferentes de homologação e/ou certificação para cada tipologia de produto; (4) adicionalmente às normas identificadas na etapa anterior e apresentadas inicialmente ao grupo focal, se haveriam outras normas aplicáveis aos produtos a serem submetidos ao SHCDCiber; (5) qual o grau de consenso sobre os conceitos de homologação e certificação apresentados ao grupo focal; e (6) se há outros órgãos envolvidos no processo de homologação e certificação de produtos cibernéticos além dos já identificados na etapa anterior da pesquisa. As sessões foram gravadas e posteriormente transcritas pela equipe de apoio do projeto.

Após tal atividade, a equipe de coordenação do projeto se debruçou sobre as transcrições de maneira a extrair elementos consensuais e questões em aberto com base nas discussões realizadas com os participantes do grupo focal. Os consensos e principais dissensos do grupo foram transformados em documento, por meio de uma análise de conteúdo (GIL, 2008) e disponibilizados para os participantes do grupo focal para eventuais críticas e alterações mediante uma plataforma digital. Enfim, o resultado desse processo foi transformado em documento de diagnóstico que foi enviado ao Exército Brasileiro.

O Quadro 1 sumariza a forma de condução da pesquisa, assim como caracteriza as organizações pesquisadas e pessoal envolvido no grupo focal.

Quadro 1 – Condução da Pesquisa

ESTRATÉGIA DA PESQUISA	ÓRGÃOS E ESPECIALIS-TAS	QUANTI-DADE	TÉCNICAS DA PESQUISA	CARACTERIZAÇÃO DA EMPRESA, ORGANIZAÇÃO OU PESSOAL ENTREVISTADO
Estudo de Caso	Empresas fornecedoras da Defesa Nacional	2	Entrevista semi estruturada / pesquisa documental	A primeira empresa pesquisada desenvolve e fornece produtos para as áreas de defesa, espaço e médica. A segunda empresa desenvolve e fornece produtos de criptografia para o Governo brasileiro. No primeiro caso, além das entrevistas houve acesso irrestrito à documentação dos produtos desenvolvidos. No segundo caso, entrevista com os proprietários que são também os principais desenvolvedores da empresa.
Estudo de Caso	Órgão Militar	1	Entrevista semi estruturada / pesquisa documental	O órgão pesquisado foi responsável pelo monitoramento do espaço cibernético para detectar incidentes nas copas das confederações e copa do mundo. O órgão é ligado ao exército e mantém profissionais das três forças armadas dedicados à implementação da política nacional de defesa cibernética.
Estudo de Caso	Centro de pesquisa TIC (privado)	1	Entrevista semi estruturada	O centro de pesquisa é referência nacional em tecnologias de informação e comunicação. A área de criptografia foi entrevistada. Os principais projetos relativos à segurança da informação, de redes e criptográfica foram discutidos com a equipe.
Estudo de Caso	Centro de pesquisa TIC (público)	1	Entrevista semi estruturada	Centro responsável pelo desenvolvimento de padrões de certificação de software no Brasil. Pesquisadores com ampla atuação em análise de produtos de software, assim como do processo de desenvolvimento de software foram entrevistados. Ocorreram duas visitas. Em uma delas a área de certificação de hardware foi entrevistada, especialmente discutindo os testes realizados em casos emblemáticos do desenvolvimento de produtos de software embarcado no Brasil.
Grupo Focal	Especialistas: (ABID), (CDCiber), INMETRO, (CTI)	8	Grupo Focal de 3,5 horas compreendendo: - Apresentação do diagnóstico - Entrevista semi estruturada - Discussão com os especialistas - Análise de conteúdo	Os profissionais envolvidos no grupo focal foram articulados por meio de uma rede nacional de profissionais de tecnologia da informação, envolvidos em desenvolvimento de produtos, na certificação e homologação de produtos fornecidos para o exército brasileiro e órgãos de regulação de chaves criptográficas utilizadas pelo Governo brasileiro. Os profissionais foram convidados à participação na pesquisa aqui descrita tendo como uma de suas atribuições a presença no grupo focal e a realização de comentários sobre os documentos desenvolvidos. Dentre os participantes do grupo focal estão profissionais responsáveis pelo projeto de sistemas criptográficos, pelo estabelecimento de padrões de certificação de software, pela operação de internet de alta velocidade no Brasil, pelo desenvolvimento de algoritmos de certificação de software para smartmeters, pela operação dos sistemas de segurança cibernética do exército brasileiro e pelo desenvolvimento de anti-virus e sistemas de computação na nuvem nacionais para uso das forças armadas.

Os resultados dos estudos de múltiplos casos nos órgãos e empresas entrevistadas e do estudo exploratório com os especialistas, possibilitou identificar as práticas usuais dos processos de homologação e certificação de produtos cibernéticos realizadas no Brasil, os quais são apresentados na seção 4.

4 CARACTERIZAÇÃO DA HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTO DE NATUREZA CIBERNÉTICA

Para apresentar os resultados da pesquisa inicialmente são discutidos os conceitos de homologação e certificação utilizados para os produtos cibernéticos, conforme os órgãos reguladores e empresas pesquisados. Posteriormente, uma visão consolidada dos processos de homologação e certificação desses produtos é apresentada e ao final uma lista com as principais referências normativas da área.

4.1 Conceitos de homologação e certificação de produtos de natureza cibernética

A figura 5 ilustra as responsabilidades de homologação e certificação de alguns produtos encontrados no mercado brasileiro, conforme as pesquisas documentais e estudos de caso realizados na etapa inicial da pesquisa.

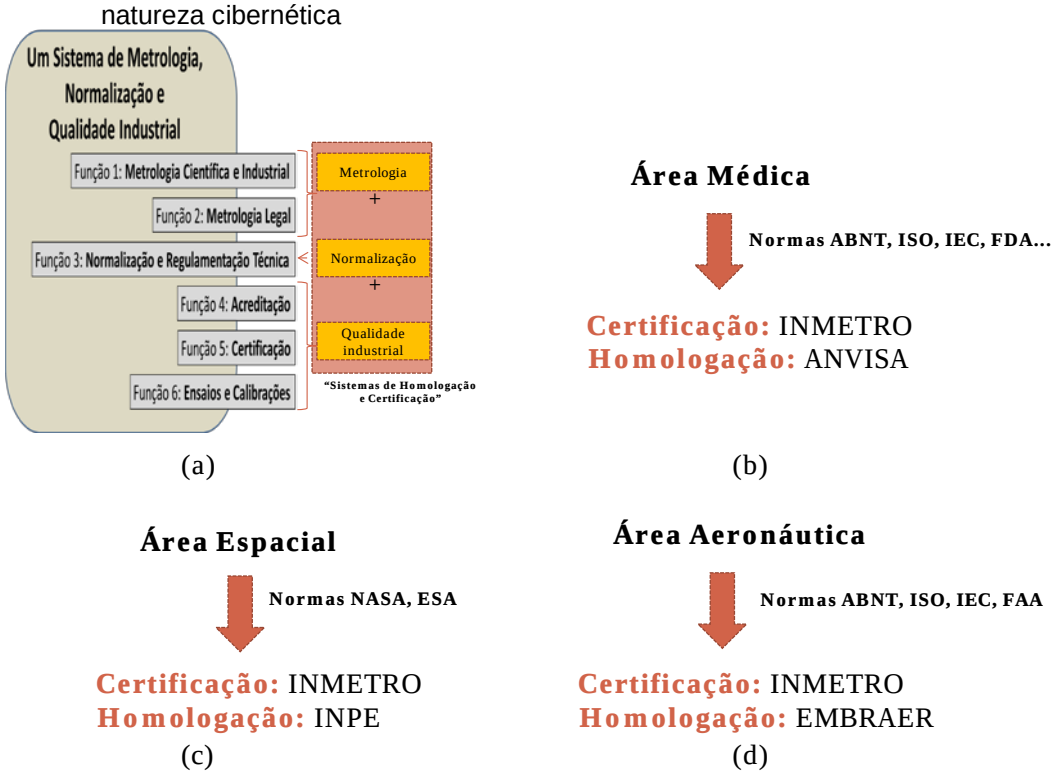
Na Figura 5 (a) é apresentada a estruturação do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (SINMETRO), operado pelo INMETRO, sendo o sistema que garante vinculação de produtos certificados no Brasil às normas internacionais de segurança e metrologia industrial. Dentro das funções do INMETRO estão a metrologia, nos seus aspectos científico, industrial e legal; o estabelecimento de normas técnicas para produtos das mais diversas áreas, o que é fortemente vinculado à Associação Brasileira de Normas Técnicas (ABNT); e a qualidade industrial, dividida em acreditação de laboratórios, certificação de produtos e ensaios e calibrações em geral.

Basicamente, como regra geral, um produto para ser certificado no Brasil precisa estar indexado em um dado Programa de Certificação, no qual consta uma norma de qualidade de produto e laboratórios acreditados, cujos instrumentos são

calibrados e realizam os ensaios capazes de testar os parâmetros previstos na normatização.

Uma vez submetido o produto aos ensaios e aprovado, é possível ao laboratório emitir um certificado, rastreável ao INMETRO.

Figura 5 - Ilustrativo das responsabilidades sobre a homologação e certificação de produtos de natureza cibernética



Fonte: Autores

Como ilustra a Figura 5, tanto na área médica (b), como espacial (c) e aeronáutica (d), a certificação do produto é baseada em normas rastreáveis ao sistema internacional por meio do INMETRO. A homologação, por outro lado, é algo mais específico de cada área. Na área médica, o produto certificado é homologado pela ANVISA (Agência Nacional de Vigilância Sanitária) por meio de um registro. Na área espacial, o produto é certificado mediante ensaios de suas partes e componentes, os quais devem ser ao máximo rastreáveis às normas do INMETRO - embora nesta área diversas tecnologias não são ainda abrangidas pelo sistema metrológico nacional -, e quem homologa o produto para uso espacial é o INPE (Instituto Nacional de Pesquisas Espaciais). Na aeronáutica, situação similar à espacial existe, em que há uma cadeia de fornecimento bastante extensa cuja

certificação deve ser rastreável ao INMETRO, mas quem homologa o produto junto ao CTA (Centro Tecnológico da Aeronáutica) é a OEM, no caso a EMBRAER.

Assim, observou-se empiricamente que enquanto a certificação do produto possui um significado similar nos diversos setores industriais pesquisados, quanto à homologação o termo não é utilizado em algumas áreas cujos produtos são cibernéticos, mas sua função de fato existe em todos.

Do ponto de vista documental foi levantada a terminografia de homologação e certificação de produtos junto órgãos ligados ao SINMETRO, chegando-se a:

> Certificação é a declaração formal de "ser verdade", emitida por quem tenha credibilidade e tenha autoridade legal ou moral. Ela deve ser formal, isto é, deve ser feita seguindo um ritual e ser corporificada em um documento. A certificação deve declarar ou dar a entender, explicitamente, que determinada coisa, *status* ou evento é verdadeiro. (ABNT NBR ISO/IEC 17025: 2005 - Requisitos gerais para competência de laboratórios de ensaio e calibração).

Já o termo homologação não foi encontrado em documentos do INMETRO, mas foi do ITI (Instituto de Tecnologia da Informação), órgão responsável pelas chaves criptográficas públicas no Brasil. O ITI, emite uma homologação para os produtos comercializados no Brasil, e a define da seguinte forma:

> Processo que consiste no conjunto de atos, realizados de acordo com um Regulamento e com as demais normas editadas ou adotadas pela ICPBrasil que, se plenamente atendido, resultará na expedição de ato pelo qual a entidade responsável pela condução do referido processo reconhecerá o laudo de conformidade. (GLOSSÁRIO ICPBRASIL Versão 1.2 03.10.2007).

Ou seja, para o ITI, a homologação é o reconhecimento do laudo de conformidade emitido por um laboratório que certifica o equipamento de chave criptográfica para uso no Brasil. Ainda, conforme as entrevistas realizadas e o grupo focal, há uma crítica da comunidade técnica vinculada às chaves públicas quanto à homologação realizada pelo ITI, compreendida como mera burocracia sem profundidade técnica, uma vez que todas as atividades técnicas, desde análise documental até os ensaios laboratoriais eram realizados pelo LEA (Laboratório de Ensaios e Auditorias) da Universidade de São Paulo.

Na tentativa de aprofundar a crítica quando da realização do grupo focal, observou-se que a comunidade considera que a homologação nesse formato abre a possibilidade de que um certificado técnico que ateste o funcionamento de um produto criptográfico não seja reconhecido pelo órgão homologador por motivos políticos

apenas ou questões subjetivas de maneira geral, o que inviabilizaria a comercialização de um produto que tecnicamente é adequado ao uso.

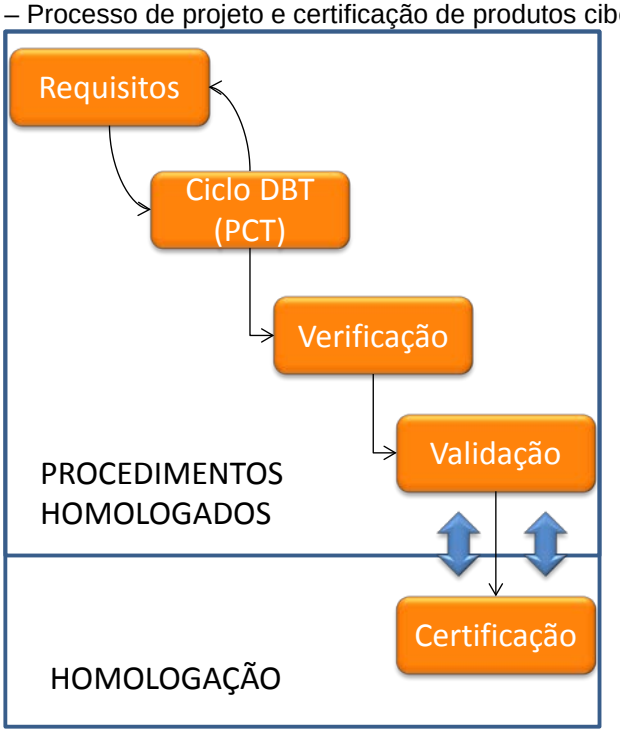
É importante salientar que nas demais áreas pesquisadas nesse trabalho, a homologação demanda uma submissão de documentos técnicos do produto e comprovação de boas práticas de fabricação (ANVISA), de relatórios de qualificação de processos e testes de ciclo de vida do produto (ESPACIAL) e de relatórios de vôo (AERONÁUTICA), conforme relatos das empresas de estudo de caso e dos especialistas. Ou seja, em todos esses casos a homologação não é apenas um ateste de um certificado de terceira parte.

4.1 Processo de homologação e certificação de produtos de natureza cibernética

Foi ainda sistematizada uma visão processual para o procedimento atual de homologação e certificação de produtos de natureza cibernética, considerando os casos, grupo focal e documentação analisada na pesquisa. A visão processual abrange um processo detalhado, similarmente ao apresentado em Barbalho, Nitzsche e Dantas (2017), sendo aqui suprimidos os mapas detalhados para efeito de apresentação. Basicamente, o produto de defesa cibernética seria certificado ao final de seu processo de desenvolvimento, cujos procedimentos devem ter sido previamente homologados. A homologação final do produto seria, entretanto, formalizada apenas com a apresentação do certificado à autoridade homologadora.

Tais procedimentos de construção do produto de defesa cibernética deveriam seguir um processo cujas etapas principais seriam as ilustradas na figura 6.

Figura 6 – Processo de projeto e certificação de produtos cibernéticos



Fonte: Autores

As etapas ilustradas na figura são:

- Uma etapa inicial de definição de requisitos. Esta etapa deve considerar as melhores práticas de levantamento, elucidação e gerenciamento de requisitos, já considerando os aspectos normativos. Essa etapa apareceu em todos os setores analisados na pesquisa.
- Os requisitos são insumo fundamental para uma etapa posterior que é, na verdade, um ciclo de projeto-construção-teste (PCT, do inglês *design-build-test* - DBT; WHELLWRIGHT e CLARK, 1992). Desse ciclo podem surgir novos requisitos a integrar a lista gerada inicialmente. Conforme, os casos estudados, na área espacial esse ciclo é documentado e reportado periodicamente ao órgão regulador. Nas demais áreas o ciclo é documentado através de registros de sistema de gestão, os quais são auditados por amostragem.
- De acordo com os estudos de caso e o grupo focal, uma vez que as soluções atendam aos requisitos de entrada do projeto, conforme testes realizados no ciclo PCT, passa-se a uma etapa de verificação. A etapa de verificação consiste na realização de testes formais que são registrados, reportados e objeto de apresentação formal ao contratante nas áreas espacial e aeronáutica, e são registrados e sujeitos à auditoria nos demais setores pesquisados.

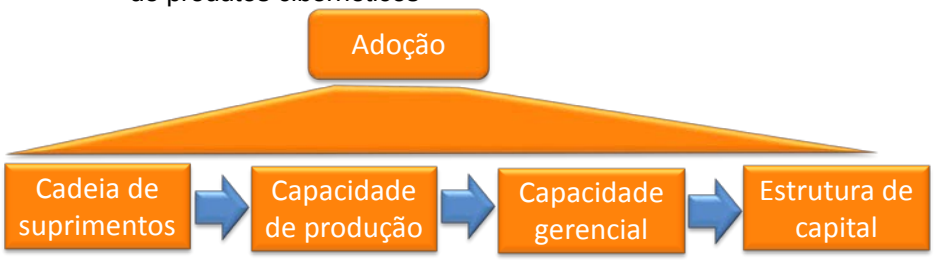
- A etapa seguinte é a validação do produto com o cliente que envolve sua demonstração para o cliente e o aceite deste. Essa etapa de validação pode ser compreendida como as apresentações formais consolidadas em revisões de projeto intermediárias e final na área espacial. Nas demais áreas a validação é realizada com o produto em estágio final de desenvolvimento, conforme dados coletados na pesquisa.
- O produto/serviço validado é submetido a um processo de certificação por meio do qual ele adquire o “certificado”, o qual atesta que o produto passou por alguns testes e verificações que permitem considerá-lo seguro para uma determinada aplicação. Essa certificação ocorre em todos os setores pesquisados. Nos setores médico, espacial e aeronáutico, a certificação demanda a documentação do produto, incluindo manuais de usuário e de serviço, assim como relatórios de análise de falhas utilizando *Failure Mode and Effect Analysis* (FMEA) de produto e de processo. As análises de falha documentadas não foram evidenciadas na pesquisa documental e entrevistas realizadas com profissionais envolvidos com produtos cibernéticos de defesa, tais como as chaves criptográficas anteriormente mencionadas.

Conforme ilustra a Figura 6, o processo de certificação pode implicar retorno a etapas anteriores do desenvolvimento do produto, considerando tanto o processo de validação e verificação como, especialmente, o ciclo de PCT e implicações nos requisitos do produto/serviço. O conceito de homologação é representado pelas áreas que delimitam os elementos ilustrados na Figura 6, o que foi diagnosticado como elemento mais crítico já que a ITI utiliza um conceito mais burocrático de homologação, enquanto que para os participantes do grupo focal e os entrevistados nos estudos de caso todos os processos pelos quais o produto de defesa cibernética deve seguir são processos que precisam estar homologados.

Adicionalmente, foi identificado para as aquisições de itens de natureza cibernética realizadas pelo exército brasileiro que, uma vez homologado, o produto de defesa passaria por uma etapa que envolve uma decisão de compra muito específica do órgão Governamental. Essa decisão seria a escolha, dentre o rol de produtos homologados, de qual seria adotado pelo órgão, o que foi aqui referido pelo conceito de adoção. Essa prática foi reportada pelo alto comando do Exército nos estudos de caso e reforçado no grupo focal.

Para a adoção seriam analisados aspectos de processo de produção, cadeia de suprimentos, capacidade operacional e de gestão da empresa e estrutura de capital, conforme a Figura 7.

Figura 7 – Elementos considerados no conceito de adoção no processo de desenvolvimento de produtos cibernéticos



Fonte: Autores

O aspecto da cadeia de suprimentos tem relação com o domínio da tecnologia de produto e de processo. O exército brasileiro leva em conta o país de origem da tecnologia em função da legislação local de propriedade intelectual, de disponibilização de informações e de privacidade, algo que precisa ser mapeado uma vez que há países em que o Governo têm poder sobre as informações geradas ou adquiridas pelas tecnologias, por exemplo, para manutenções e atualizações via internet.

Outro elemento é a capacidade de produção da empresa. Capacidade tem relação com a tecnologia de processamento disponível, no aspecto *hardware, software* e pessoal. Uma das questões é se a capacidade dos equipamentos disponíveis na empresa suprem as quantidades e padrão de qualidade exigido do produto. Observe-se que na etapa de projeto, até o processo de certificação e homologação exposto, está se trabalhando com um protótipo ou um lote piloto de algumas unidades. Na linha de produção, isso pode se tornar centenas e até milhares de unidades de produto a serem entregues. Há uma diferença considerável do ponto de vista de processo de produção nos dois casos e a etapa de homologação de produtos com características cibernéticas nos setores aqui pesquisados não demanda a produção de um grande lote piloto com testes de capabilidade de processo.

A tecnologia de processamento tem intrincada relação com o aspecto do domínio tecnológico. Não é apenas a empresa deter maquinário para produzir um determinado produto, mas ela detém a capacidade de manter esse maquinário produzindo? Ou qualquer quebra, descontinuidade ou perda de parâmetros exigirá

que ela acione o fornecedor do equipamento e esteja sujeita à legislação de propriedade intelectual de seu país de origem? Ou aos prazos de atendimento do serviço de pós-venda do fornecedor? Nesse sentido, o comprador militar considera tanto a tecnologia de *hardware* quanto de *software* necessárias à produção do produto.

A capacidade gerencial abrange aspectos relativos à saúde financeira da empresa ao longo de um determinado período de tempo, ao grau de profissionalização de sua estrutura decisória e à capacidade gerencial da empresa para reter seus talentos e manter o conhecimento que vai sendo gerado nos projetos, nos processos e no seu sistema de produção. Esse elemento, sutil, foi diagnosticado como preocupação dos entrevistados que ocupam funções de decisão nas forças armadas. Algo inusitado e não esperado na pesquisa.

Enfim, observou-se uma preocupação dos órgãos de defesa quanto ao aspecto da estrutura de capital da empresa fornecedora. O principal fator aqui é a nacionalidade do negócio. Países que exigem que suas empresas liberem informações para o Governo geram uma situação de claro conflito de interesses com o aspecto da defesa cibernética em geral e tem preocupado o comprador público desse tipo de tecnologia.

4.3 Base normativa para homologação e certificação de produtos de natureza cibernética

Durante as entrevistas e grupo focal foram identificados os principais padrões normativos utilizados especificamente em certificação de produtos de natureza cibernética, apresentados abaixo:

- O *Common Criteria*: um framework utilizado como padrão internacional que define critérios comuns de padrão de Avaliação da Segurança da Informação (série ISO/IEC15408) para a segurança de computadores.
- O FIPS PUB 140-2 define padrões de construção de hardware, requisitos de projeto, níveis para homologação de produtos, dentre outros.
- O FIPS PUB 199 é um documento editado pelo NIST que apresenta um padrão a ser usado por todos os órgãos federais dos EUA para categorizar todas as

informações e sistemas de informações coletadas e emitidas por ou em benefício de cada órgão.

- O FIPS PUB 200 é um documento editado pelo NIST que descreve, de forma sucinta um conjunto de requisitos mínimos de segurança para a informação e os sistemas de informação federais dos EUA.

As normas acima são usadas hoje pelas empresas e órgãos relacionados à segurança cibernética, e prevêem um fluxo de projeto similar ao apresentado na Figura 6. Elas foram posteriormente utilizadas pela equipe para o desenvolvimento de procedimentos mais detalhados de verificação dos processos de desenvolvimento dos produtos de natureza cibernética para compor o SHCDCiber. Tal detalhamento foge ao escopo do presente artigo.

5 CONSIDERAÇÕES FINAIS

Esse artigo aborda os processos de homologação e certificação de produtos utilizados em defesa cibernética. O Governo brasileiro tem como uma importante diretriz em sua estratégia tecnológica a confecção de um sistema que seja capaz de homologar e certificar os produtos utilizados pelos órgãos centrais e forças armadas de forma a garantir que não haja espionagem cibernética nos equipamentos por eles utilizados. Tais sistemas são também esforços atuais dos Estados Unidos e países da Europa e Ásia para construírem uma sistemática de segurança cibernética similar à preocupação brasileira.

Nesse sentido, um projeto realizado por uma Universidade pública federal visou diagnosticar os processos atualmente utilizados pelas empresas e órgãos de Governo para certificar e homologar os produtos de natureza cibernética por eles desenvolvidos e utilizados, respectivamente. O estudo foi realizado por uma equipe de pesquisadores e envolveu uma etapa de estudos de múltiplos casos e análise documental e uma outra de grupo focal com especialistas.

Os resultados demonstraram uma visão compartilhada pelas empresas e órgãos quanto ao aspecto da certificação de produtos, mas demonstrou haver um entendimento não consensual sobre o aspecto da homologação. Algumas áreas utilizam a homologação apenas como mero reconhecimento de certificados emitidos por laboratórios, o que gera desconforto com a comunidade técnica envolvida na área.

As experiências das áreas de equipamentos médicos, espacial e aeronáutica podem servir como referência para o desenvolvimento de metodologias de homologação mais robustas. No texto em tela foi apresentado um processo de homologação e certificação que contempla todos os elementos identificados nas diversas áreas pesquisadas no trabalho.

Foram identificados ainda processos realizados por órgãos governamentais que fogem ao escopo tradicional da homologação, conforme a literatura analisada no texto. Observou-se que tais processos, aqui denominados de adoção, consistem em uma análise mais estratégica para o desenvolvimento de uma política industrial de defesa considerando o domínio tecnológico, as cadeias de suprimento e a origem da tecnologia, e a capacidade de resposta da empresa em termos gerenciais e de produção. Essas são preocupações identificadas pelo comprador militar, mas que não foram identificadas nos demais setores estudados.

Enfim, foram identificadas as principais normas e padrões da área, especialmente utilizadas por empresas que desenvolvem produtos de natureza cibernética para o mercado externo. Tais padrões são da área de segurança de informação e criptografia. Ressalta-se, entretanto, a necessidade de sua incorporação aos requisitos de outras tipologias de produto, como as aqui pesquisadas - médica, espacial e aeronáutica. Considerando que atualmente todos esses equipamentos podem ser considerados ou utilizam sobremaneira tecnologias de sistemas cibernéticos físicos, o aspecto da segurança da informação e da possibilidade de sua utilização como arma tecnológica é algo real.

Considerando o referencial de homologação e certificação utilizado como ponto de partida para o estudo, observou-se que as práticas de certificação utilizadas pelos setores pesquisados são bem próximas ao referencial de processos descrito na Figura 4 em que uma documentação é gerada e submetida a laboratórios acreditados pelo INMETRO. Entretanto, o referencial utilizado para homologação (Figura 3) precisa incorporar outros elementos, como a adoção, para refletir as demandas do mercado de produtos de defesa cibernética, um nicho com base em compras públicas e de uso militar. O referencial da figura 3 precisa ainda incorporar elementos de segurança da informação. Por outro lado, observou-se que diversos elementos mais operacionais ligados a processos de manufatura não eram considerados pela comunidade vinculada a produtos de natureza cibernética, algo necessário e que pode gerar a

insegurança que o comprador militar busca dirimir pela incorporação do processo de adoção aqui diagnosticado.

Como trabalhos futuros sugere-se a proposição de um processo que possa ser utilizado por organizações vinculadas à questão cibernética e que permitam atender a requisitos tanto de empresas, para as quais é importante que os certificados e homologações abranjam o acesso ao mercado externo, quanto para órgãos de Governo que demandam segurança e atendimento de requisitos específicos de fornecimento. Sugere-se ainda detalhar o processo de adoção aqui identificado no sentido de estudar mais apropriadamente como ele se efetiva para uma dada tecnologia, assim como relacioná-lo com o processo de homologação que é mais consolidado na bibliografia de desenvolvimento de produtos como um todo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17025:2005 Versão Corrigida 2:2006**: Requisitos gerais para competência de laboratórios de ensaio e calibração. Rio de Janeiro: ABNT, 2005. 38 p.

BARBALHO, S. C. M. **Modelo de referência para o desenvolvimento de produtos mecatrônicos**: conceitos e aplicações práticas. 1. ed. Düsseldorf: Nova Edições Acadêmicas, 2016. v. 1. 225p.

BARBALHO, S. C. M.; NITZSCHE, M. C. M.; DANTAS, A. S. Melhoria de processos na gestão pública: uma pesquisa-ação com foco nas atividades administrativas de um programa de intercâmbio estudantil de uma universidade pública. **Revista Produção Online**, v. 17, p. 406-439, 2017. http://dx.doi.org/10.14488/1676-1901.v17i2.2314.

BARBALHO, S. C. M.; ROZENFELD, H. Modelo de referência para o processo de desenvolvimento de produtos mecatrônicos (MRM): validação e resultados de uso. **Gestão & Produção (UFSCAR. Impresso)**, v. 20, p. 162-179, 2013. http://dx.doi.org/10.1590/S0104-530X2013000100012

BRADLEY, D.A. et al. **Mechatronics**: electronics in products and processes. London, United Kingdom, Chapman and Hall, 1991.

BRASIL. **Estratégia nacional de defesa**. Brasília: MD, 18 dez. 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>.

CLARK, K. B.; FUJIMOTO, T. **Product development performance**: strategy, organization and management in the world auto industry. Harvard Business School Press, Boston, Massachussets, United States, 1991.

COELHO, Manuel; SILVA, Rui. Trustiness Certification of Information Technology Equipment. **International Journal of Computer Science and Network Security(IJCSNS)**, v.13, n. 1, p.35-42, 2013.

COLARIK, A.; JANCZEWSKI, L. **Developing a grand strategy for cyber war**. Proceedings of the 17th International Conference on Information Assurance and Security, 2011. http://dx.doi.org/10.1109/ISIAS.2011.6122794.

DENKER G. et al. Resilient dependable cyber-physical systems: a middleware Perspective, **Journal of Internet Service Appliances**, n. 3, p. 41–49, 2012. http://dx.doi.org/10.1007/s13174-011-0057-4

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

GLOSSÁRIO ICPBRASIL, Versão 1.2, 03.10.2007. Disponível: http://www.ipc.org/ContentPage.aspx?pageid=Standards

HAENI, R.E. **Information warfare**: an introduction. Washington DC, 1997.

INTERNATIONAL ORGANIZATION FOR STARDATIZATION. **ISO/IEC 27032:2012:** information technology - security techniques - guidelines for cybersecurity.50 p. ISO, 2012.

LI, Z.; QING, W.; BIN, T. Security threats and measures for the cyber-physical systems. **The Journal of China Universities of Posts and Telecommunications**, v. 20, n.1, p. 25-29, 2013. http://dx.doi.org/10.1016/S1005-8885(13)60254-X

LOBATO, L.; KENKEL, K. M. A Ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, PUC, v.37, nº2, p.629-660, 2015. DOI: http://dx.doi.org/10.1590/S0102-85292015000200010.

MIN, K.; CHAI. S.; HAN, M. An International Comparative Study on Cyber Security Strategy. **International Journal of Security and Its Applications.** v. 9, n. 2, p. 13-20, 2015. http://dx.doi.org/10.14257/ijsia.2015.9.2.02

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **CPS PWG Draft Framework Cyber-Physical Systems.** Release 0.8. Cyber Physical Systems Public Working Group, Washington, DC. 2015

NEUMANN, P. G.**The Risks Digest: Forum on Risks to the Public in Computers and Related Systems [Internet]**. 2014. Disponível: http://catless.ncl.ac.uk/Risks/

PAGAN, R.P.; SILVA, C.E.S.; MELLO, C.H.P. Projeto conceitual no processo de desenvolvimento de produtos eletroeletrônicos: estudo de caso em empresas incubadas. **Revista Produção Online**, Florianópolis, SC, v.13, n. 3, p. 1089-1117, 2013. DOI: http://dx.doi.org/10.14488/1676-1901.v13i3.1402

PINHEIRO, N.M.G.; SANTOS, A.P.L.; CLETO, M.G. Proposta de modelo de desenvolvimento de produtos focada na metodologia de certificação CE. **Revista Produção Online**, v.15, p.972-979, 2015. DOI: http://dx.doi.org/10.14488/1676-1901.v15i3.1942

PUGH, S. **Total design**: integrated methods for successful product engineering. Addison Wesley, London, United Kingdom, 1990.

ROZENFELD, H. et al. **Gestão de desenvolvimento de produtos**. São Paulo/SP: Editora Saraiva, 2006.

SALGADO, E.G.; SALOMON, V.A.P.; MELLO, C.H.P.; FASS, F.M.D.; XAVIER, A.F. Modelos de referência para o desenvolvimento de produtos: classificação, análise e sugestões para pesquisas futuras. **Revista Produção Online**, v.10, n.4, p. 886-911, 2010. http://dx.doi.org/10.14488/1676-1901.v10i4.520.

SHAFQAT, N.; MASSOD, A. Comparative Analysis of Various National Cyber Security Strategies. **International Journal of Computer Science and Information Security**. v. 14, n. 1, p. 129-136, 2016. http://dx.*doi*.org/ security/ 10.1787/5k8zq92vdgtl-em

TARALLO, F. B.; AMARAL D. C. Práticas e desafios na preparação da produção em projetos de novos produtos de higiene pessoal. **Produção**, v. 18, n. 3, set./dez. 2008, p. 556-568. http://dx.doi.org/10.1590/S0103-65132008000300011.

TINTINAGO, D. A. I.; TRAJANO, J. P. G.; BARBALHO, S. C. M. Aplicação das fases de otimização e de homologação do modelo de referência mecatrônico a um sistema de controle automático de acesso. In: CONGRESSO BRASILEIRO DE GESTÃO DA INOVAÇÃO E DESENVOLVIMENTO DE PRODUTOS, 10., 2015. **Anais...** Itajubá, 2015.

VARANDAS JR. A.; MIGUEL. P. A. C.; Análise do processo de preparação da produção no desenvolvimento de novos produtos por meio de um estudo de caso em uma empresa do setor siderúrgico**. Produção**, v. 22, n. 2, p. 185-200, 2012. DOI: http://dx.doi.org/10.1590/S0103-65132012005000012.

WHEELWRIGHT, S. C.; CLARK, K. B. **Revolutionizing product development process: quantum leaps in speed, efficiency, and quality**. New York, United States, The Free Press, 1992.

WIENER, Norbert. **Cibernética e sociedade:** o uso humano dos seres humanos. 3. ed. São Paulo: Cultrix, 1984.

WU, F.; KAO, Y.; TSENG, Y. From wireless sensor networks towards cyber- physical systems. **Pervasive and Mobile Computing**, v.7, p.397-413, 2011. http://dx.doi.org/10.1016/j.pmcj.2011.03.003

YIN, R. K. **Estudo de caso**: planejamento e métodos. Porto Alegre: Bookmann, 2010.

Artigo recebido em 04/03/2017 e aceito para publicação em 19/08/2017
DOI: http://dx.doi.org/10.14488/1676-1901.v18i2.2789