ESCOLA DE GUERRA NAVAL

CMG MARCO EUGÊNIO MADEIRA DI BENEDITTO

DEFESA CIBERNÉTICA: PROPOSTA DE ESTRUTURA PARA O ÂMBITO DA MB.

Defesa dos sistemas ciber-físicos dos meios operativos de superfície da MB.

Rio de Janeiro

2016

CMG MARCO EUGÊNIO MADEIRA DI BENEDITTO

DEFESA CIBERNÉTICA: PROPOSTA DE ESTRUTURA PARA O ÂMBITO DA MB.

Defesa dos sistemas ciber-físicos dos meios operativos de superfície da MB.

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CF (RM1) Ohara Barbosa Nagashima

Rio de Janeiro

Escola de Guerra Naval

RESUMO

Este trabalho pretende evidenciar vulnerabilidades potenciais em sistemas ciber-físicos em uso nos meios operativos de superfície da MB e, em seguida, propor uma forma de redução dessas mesmas vulnerabilidades. Para isso analisa uma série de incidentes em sistemas ciber-físicos que foram desencadeados por ações iniciadas no meio cibernético, e acabaram por gerar variados efeitos cinéticos nos respectivos processos físicos sob seu controle. Sua relevância deriva da ausência, no presente momento, de qualquer ferramenta sistêmica na MB capaz de minimizar os efeitos indesejados de ações adversas contra os sistemas ciber-físicos em uso nos meios operativos de superfície. Na pesquisa bibliográfica são revisados os conceitos e práticas, relacionadas à proteção de sistemas ciber-físicos, já publicados em diversas normas internacionais para sistemas de controle industriais. A partir disso, propõe-se utilizá-los numa estrutura que servirá para incrementar a proteção de sistemas deste tipo, atualmente empregados nos meios operativos de superfície existentes na Marinha. Esta estrutura será formada por meio de um programa de implantação baseado nos conceitos e práticas revisados e em procedimentos já consolidados na Marinha e aplicáveis neste novo domínio. As soluções apresentadas indicam um caminho para a questão da proteção dos sistemas ciber-físicos empregados nos meios operativos da Marinha, melhorando a sua proteção e gerando uma visão de mais alto nível dos riscos ao cumprimento das missões.

Palavras-chave: sistemas ciber-físicos, cibernética, defesa cibernética, sistemas de controle industriais.

ABSTRACT

This work aims to highlight potential vulnerabilities in cyber-physical systems in use in the Brazilian Navy surface ships and then propose a way of reducing these same vulnerabilities. For this it analysis a series of incidents in cyber-physical systems that were triggered by actions initiated in the cyber environment, and have generated various kinetic effects on their physical processes under their control. Its relevance stems from the lack, at present, of any systemic tool in Brazilian Navy able to minimize the unwanted effects of adverse actions against cyber-physical systems in use in the operating surface means. In the literature are reviewed the concepts and practices related to the protection of cyber-physical systems, already published in several international standards for industrial control systems. From this, it is proposed to use them in a structure that will serve to enhance the protection of this type of systems currently used in surface ships in the navy. This structure is formed by an implementation program based on concepts and revised practices and procedures already established in the Navy and applicable in this new domain. The solutions indicate a path to the issue of protection of cyber-physical systems used in surface ships, improving their protection and creating a vision of higher level of risk to the discharge of their duties.

Keywords: cyber-physical systems, cyber, cyber defense, industrial control systems.

AGRADECIMENTOS

À minha querida esposa e a minha filha, que contribuíram para a boa execução deste trabalho, agradeço pelas seguidas demonstrações de compreensão e apoio.

Ao meu orientador, Ilustríssimo Senhor Capitão de Fragata (RM1) Ohara Barbosa Nagashima, que proporcionou a constante troca de ideias e uma profícua posição crítica, registro aqui o meu muito obrigado. Ainda, agradeço pela sua disponibilidade, profissionalismo e incentivo ao longo do desenvolvimento do trabalho.

À todos os Professores e Palestrantes que tive durante o curso, sou muito grato pela valorosa apresentação de novas informações que trarão uma contribuição positiva para as minhas futuras decisões.

À todos os oficiais integrantes da turma C-PEM 2016 por esse ano de convívio acadêmico e de intenso fluxo de ideias.

Por fim, agradeço à todo o pessoal servindo presentemente na Escola de Guerra Naval pelo apoio recebido ao longo do ano, decorrente do correto cumprimento das suas atividades profissionais.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANSI	American National Standards Institute
CLP	Controladores Lógicos Programáveis
DCS	Distributed Control Systems
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PLC	Programmable Logic Controllers
SCADA	Supervisory Control and Data Acquisition
SCF	Sistemas Ciber-Físicos

SUMÁRIO

1 INTRODUÇÃO

Sistemas ciber-físicos (SCF) são sistemas em que ocorre a integração de computação e processos físicos (LEE, 2008). Em termos gerais, esses sistemas servem para supervisionar e controlar processos físicos. Eles são compostos por:

a) sensores de aquisição de dados, que observam o processo;

b) computadores embarcados, que perfazem o controle; e

c) atuadores, que executam as ações de controle.

Assim, o sistema ciber-físico é um sistema de malha fechada de sensores e atuadores em rede, em que os dados coletados pelos sensores são enviados aos controladores que ajustam a operação do sistema por meio dos atuadores.

O uso de SCF é crescente, seja devido ao desempenho que ele pode prover, ou pela possibilidade de redução de pessoal necessário para a execução de um conjunto de tarefas, redução essa decorrente da automação provida por um SCF. Olhando-se para a Marinha do Brasil, um exemplo típico de SCF são os sistemas de armas empregados em navios de superfície, como os das Fragatas da Classe Niterói e da Corveta Barroso. Além dos sistemas de armas, outros podem ser listados como o Sistema de Controle e Monitoração da Propulsão e Auxiliares das Fragatas da Classe Niterói (SCMPA), desenvolvido pelo Centro Tecnológico da Marinha em São Paulo (CTMSP).

Um ataque a este tipo de sistema pode resultar em diferentes efeitos, desde a parada do sistema físico, deixando-o indisponível, até mesmo o seu controle por um agente adverso, onde este agente passa a controlar o respectivo processo físico. Segundo Loukas (2015, p. 12) “um ataque ciber-físico é uma brecha de segurança no ciberespaço que afeta um espaço físico de modo adverso”. Seguindo essa definição, o ataque a um SCF envolve uma ação não

autorizada no espaço cibernético, aproveitando-se de uma brecha de segurança, que terá como consequência um efeito no espaço físico. Essa brecha na segurança significa o comprometimento de um ou mais dos objetivos da segurança da informação, que são: confidencialidade, integridade e disponibilidade (CONKLIN; WHITE, 2014).

Além do crescente uso de sistemas ciber-físicos em navios, e a consequente dependência deles no emprego destes meios, ao longo do seu ciclo de vida, esses sistemas sofrem um aumento na probabilidade de possuírem alguma vulnerabilidade. Este aumento decorre principalmente de dois aspectos. O primeiro é o emprego de tecnologias, seja software ou hardware, cada vez mais difundidas no mercado para o desenvolvimento dos sistemas ciber-físicos. Isso traz a reboque um conjunto de ferramentas de exploração e ataque já existentes, bem como facilita a implantação de um laboratório que permita o desenvolvimento de artefatos maliciosos contra esta infraestrutura. Além disso, a lista de vulnerabilidades já conhecidas para estes componentes de software e hardware também passa a ser imediatamente possível de ser empregada. Em segundo é o software que permeia esses sistemas pois, em alguns casos, esse software é derivado de uma linha de produto de software[1]. Este é o caso do Sistema de Controle Tático (SICONTA) empregado nas Fragatas da Classe Niterói modernizada (SICONTA Mk II), na Corveta Barroso (SICONTA Mk III) e no NAe São Paulo (SICONTA Mk IV). Numa linha de produto de software, uma vulnerabilidade num componente de software pode acarretar uma vulnerabilidade que também seja comum a todos os itens da linha, ou seja, no caso do SICONTA todas as versões podem possuir uma mesma vulnerabilidade desde que eles utilizem um mesmo componente de software.

Ao longo do ciclo de vida, um meio pode ter alguns sistemas removidos, outros

1 Uma linha de produto de software é um conjunto de sistemas que usam software intensivamente, compartilhando um conjunto de características comuns e gerenciadas, que satisfazem as necessidades de um segmento particular de mercado ou missão, e que são desenvolvidos a partir de um conjunto comum de ativos (CLEMENTS; NORTHROP, 2001).

substituídos ou mesmo receber novos sistemas. Uma substituição ou o recebimento de um novo sistema pode trazer consigo novas vulnerabilidades decorrentes das tecnologias que compõem esse sistema, como uma antena de comunicação por satélite. Ao ser instalada esta antena, ela virá com todo o mecanismo de controle de seu fabricante e a respectiva interface de controle, seja ela por hardware ou por software. Numa rápida consulta a sítios de fabricantes dessas antenas, pode-se observar algumas das funcionalidades providas para facilitar a sua operação, como por exemplo[2]: "O sistema tem excelente software remoto, permitindo que a antena seja monitorada e controlada por meio do protocolo internet a partir de qualquer computador na rede do navio ou mesmo, se necessário, a partir de um computador com acesso à rede do navio em terra.". O texto acima descreve a interface homem-máquina de software, executada num computador, para uma antena de comunicação por satélite nas bandas Ku, Ka e X. A possibilidade de controlar a antena de dentro ou de fora do navio por meio do protocolo internet já aumenta o risco deste equipamento sofrer ações maliciosas.

Cabe ressaltar que ataques a sistemas com tecnologia proprietária tendem a ser mais difíceis pois alguns componentes, sejam de software ou hardware, podem ser de uso pouco comum. Entretanto, a convergência de tecnologias já consagradas e de ampla difusão no mercado e o seu respectivo uso nestes mesmos componentes reduz esse grau de dificuldade.

A motivação deste estudo decorre da alta dependência entre SCF e um meio operativo. Como visto acima, os sistemas ciber-físicos empregados em meios operativos são uma parte essencial na relação entre o meio e o respectivo desempenho. Com o passar do tempo, estes sistemas tendem a ser mais vulneráveis e, por isso, sua segurança deve ser planejada e executada permanentemente. Atualmente, no âmbito da MB, estes sistemas não possuem uma

2 *Orbit VSAT Antennas*. Sítio localizado em: http://www.marinesatellitesystems.com/index.php?page_id=811#511, Acesso em: 30 Jul. 2016.

política dedicada para a sua segurança. As medidas de segurança, atualmente em vigor, na MB tem como principal norma a Doutrina de Tecnologia da Informação da Marinha (EMA-416). Esta norma trata dos objetivos da segurança da informação, com aplicação direta nos sistemas de Tecnologia da Informação, e deixa de considerar os seus efeitos nos processos físicos relacionados aos sistemas ciber-físicos.

Um outro aspecto interessante a destacar é o efeito desejado de ações no domínio cibernético definidos tanto na Doutrina Militar de Defesa Cibernética (MD31-M-07) quanto na Doutrina Básica da Marinha (EMA-305). Em ambas as normas, as ações de guerra cibernética têm efeito no nível informacional e respectivos sistemas de informação, e não consideram que estas ações também poderiam ter efeitos diretamente no nível de processos físicos. Vê-se que ainda não está amadurecida a visão da cibernética para possíveis efeitos cinéticos, além do nível informacional previsto e, consequentemente, isso afeta a percepção de que os SCF das forças amigas também devem ser protegidos.

Desse modo, o objetivo principal desse trabalho é gerar e apresentar uma estrutura que aprimore a segurança de SCF existentes na MB, em especial, naqueles sistemas utilizados nos meios operativos de superfície atualmente incorporados e em uso. O principal aspecto desta estrutura serão as atividades a serem desenvolvidas e uma abordagem para a implantação das atividades, sem tratar da estrutura organizacional na MB que se responsabilizará por estas atividades.

Nesse sentido, o restante deste trabalho está organizado da seguinte forma. No Capítulo 2 são descritos alguns casos reais de ataques a SCF, que alertam para a real possibilidade de situações análogas nos meios operativos de superfície da MB. No Capítulo 3 são tratados a fundamentação de segurança para SCF e respectivos trabalhos que visam promover a segurança destes sistemas. No Capítulo 4 é apresentada a estrutura proposta.

Finalmente, no Capítulo 5 são discutidas a aplicação desta estrutura e trabalhos futuros.

2 VALIDAÇÃO EM CASOS REAIS

A tecnologia de SCF tem sido empregada por um amplo espectro de setores industriais e foram projetados para terem efeitos nos processos físicos, ou seja, efeitos cinéticos. Esses sistemas podem ser encontrados em inúmeras áreas, por exemplo, na distribuição e geração de energia, controle ambiental, aviônica, automóveis, instrumentação, controle de infraestruturas , manufatura e sistemas de defesa. Infelizmente, como outras tecnologias baseadas na informação, muitos SCF foram originalmente projetados com pouca ou nenhuma segurança, ou mesmo após o reconhecimento dessa falta, nenhuma segurança foi adicionada. Desse modo, a segurança de muitos destes sistemas se baseia na ocultação do sistema em si, em vez da segurança ter sido desenvolvida dentro do processo de projeto (APPLEGATE, 2013).

Em princípio, estas vulnerabilidades apontadas poderiam ser consideradas potenciais, ou seja, com capacidade de serem exploradas. Porém, nos dias de hoje, já há casos que tiram proveito dessas vulnerabilidades e os efeitos são os mais diversos possíveis. Desse modo, a motivação para tratá-las assume uma prioridade elevada em especial quando se observa o estado dos SCF hoje empregados na MB.

Para se contrapor a isso, uma série de medidas foram descritas com o propósito de aumentar a segurança desses sistemas. Aqui, segurança é entendida como a união de três macroatividades que são: prevenção, detecção e resposta. Segundo Conklin e White (2014), por muito tempo o foco da segurança foi na prevenção, assumindo que, se é possível prevenir que alguém tenha acesso a um sistema, então ele está seguro. Entretanto, com o passar do tempo, foi visto que, não importa o quanto se consiga prevenir o acesso a um sistema, basta haver uma violação ao mesmo que esta hipótese assumida se torna falsa. Assim, é preciso agregar aos métodos de prevenção os mecanismos que indiquem quando eles falharem, de

modo a permitir que os meios para se resolver o problema possam ser adequadamente empregados. Logo, adaptando-se de Conklin e White (2014), a segurança para sistemas de informação pode ser vista como a seguinte equação operacional:

Segurança = Prevenção + (Detecção + Resposta)

Cada técnica de segurança ou tecnologia aplicada à segurança pode ser vista em um dos elementos da equação operacional dada acima.

Este capítulo mostra casos reais de ataques a SCF. A Seção 2.1 revisa uma série de ataques a SCF com efeitos cinéticos, seja em ambiente controlado ou em ambiente operacional, que validam esse tipo de ataque, e na Seção 2.2, é feita uma análise desses ataques perante os meios considerados neste estudo.

2.1 Validação dos efeitos cinéticos

Os ataques cibernéticos são frequentemente ataques não-violentos e não-cinéticos, sem efeitos físicos. Entretanto há uma grande probabilidade de ataques cibernéticos serem usados para se conseguir efeitos cinéticos por meio dos SCF. Esses tipos de ataques foram validados em ambiente de laboratório, através da experimentação, e também no ambiente real, empregados por agentes maliciosos para sabotar dispositivos físicos.

A seguir será revisada uma série de ataques já efetuados e descritos na literatura. Essa lista de ataques está dividida em três grupos. No primeiro serão tratados os ataques feitos em ambiente controlado, mas empregando métodos e itens reais. No segundo, os ataques listados foram efetuados no ambiente real e desencadeados por atores maliciosos com o intuito de causar algum dano ou prejuízo decorrente dos efeitos cinéticos da ação. No terceiro e último será descrito um ataque de cunho operacional e, possivelmente, financiado por governos de países e perpetrado por agentes interestatais.

Projeto Aurora (MESERVE, 2007) – O *Department of Homeland Security* (DHS), um órgão governamental dos Estados Unidos da América, conduziu um experimento para mostrar que um ataque cibernético pode destruir componentes físicos de um equipamento pertencente a rede de geração de energia elétrica daquele país, mais especificamente um diesel gerador de energia elétrica de 2 MW. No experimento os pesquisadores, por meio de uma ação cibernética, abriram e fecharam os disjuntores do gerador fora de sincronia, para maximizar o estresse decorrente da variação de carga. Ao final, essas variações geraram vibrações tão intensas que o gerador foi perdendo uma série de suas partes, causando um dano catastrófico em três minutos.

Os resultados do experimento alarmaram o governo norte-americano e a indústria elétrica sobre o que poderia acontecer se um tal ataque fosse realizado numa escala maior e a geradores em uso na rede de geração de energia elétrica.

O experimento mostra que, caso um agente malicioso consiga chegar no sistema de controle ele poderia ter o controle virtual da abertura física e fechamento de dispositivos de proteção associados, contribuindo para uma condição igual ao experimento.

Apesar de o projeto deste gerador considerar uma série de seguranças, a situação descrita no experimento não foi prevista e por isso, esse risco não foi mitigado, apesar de ser possível fazê-lo por meios de equipamentos adicionais, como um Dispositivo de Isolamento de Equipamento Rotativo[3].

Assim a aquisição e uso de novos equipamentos de geração de energia, e também para propulsão, devem ser avaliados do ponto de vista cibernético para serem tomadas as medidas necessárias a sua proteção a estes novos riscos.

---

3 *What You Need to Know (and Don't) About the AURORA Vulnerability.* Disponível em: <http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?pagenum=3>. Acesso em: 30 Jul. 2016.

Implantes Médicos (GREENEMEIER, 2008) – Em 2008, pesquisadores da Escola de Medicina Beth Israel Deaconess, em Boston, da Universidade de Massachusetts Amherst e da Universidade de Washington em Seattle levantaram uma série de alertas sobre as vulnerabilidades que implantes cardíacos, em especial o marca-passo, possuíam a ataques cibernéticos e as respectivas consequências. Nessa investigação foi mostrado que um implante cardíaco: a) é potencialmente susceptível a ataques maliciosos que violam a privacidade das informações do paciente e da telemetria médica; e b) podem sofrer alteração maliciosa da integridade das informações ou do estado, incluindo os dados do paciente e configurações da terapia para quando e como os choques são administrados.

A funcionalidade de comunicação sem fio com o implante é importante, para permitir ajustes até então difíceis de serem realizados, mas traz como consequência as vulnerabilidades apresentadas. Desse modo, a cada nova utilidade inserida num equipamento, cabe avaliar os riscos que ela trará, por meio de uma avaliação de riscos sistemática.

Carro Comercial (SCHNEIDER, 2015) – Em julho de 2015, dois pesquisadores de segurança, Charlie Miller e Chris Valasek, foram capazes de controlar, por meio de uma conexão sem fio, um carro do modelo Jeep Cherokee estando o carro em movimento. Essa conexão sem fio era provida por meio da funcionalidade "*wi-fi*" e também por uma conexão baseada em telefonia celular, ambas disponibilizadas pela central multimídia do carro.

A entrada, a partir da central multimídia, foi conseguida por meio de força bruta na obtenção da senha dessa central. Os pesquisadores reduziram as possibilidades de combinações de senha, devido à descoberta de uma fraqueza no método de geração de senhas empregado pela central multimídia. Inicialmente os pesquisadores tomaram o controle do sistema de entretenimento provido pela central multimídia e do limpador de pára-brisas. Em seguida, eles conseguiram controlar o ar condicionado, desativar o acelerador – inibindo os

comandos do motorista via pedal do carro – e acionar os freios do carro.

No exemplo, fica claro que a interligação da central multimídia aos componentes de controle principais do carro, sem a devida proteção, permitiu aos pesquisadores atuar nos movimentos do carro. O aumento da conectividade externa do veículo, por meio da central multimídia com uma rede de dados sem fio, e da conectividade interna do veículo, devido à interligação da central multimídia com os controles do veículo, implica em adotar novas abordagens para reduzir os riscos à segurança decorrentes. Uma dessas abordagens é defesa em profundidade[4], que aumenta a prevenção e não se limita a tratar apenas as exposições óbvias, mas também as vulnerabilidades de segunda ordem que se tornam visíveis apenas por meio de ligações entre vários componentes do sistema.

Após esses três exemplos experimentais, serão descritas ações efetuadas por pessoas maliciosas, com o intuito de causar algum prejuízo, de forma deliberada, a partir dos efeitos cinéticos decorrentes destas ações.

Sistema de Águas e Esgoto na Austrália (CRAWFORD, 2006) – Em janeiro de 2000, um ex-empregado da firma *Maroochy* Sistema de Serviços de Água, localizada em Queensland, Austrália, foi o responsável pelo vazamento de milhões de litros de esgoto nos cursos de água, jardins de hotéis e canais ao redor do subúrbio de *Sunshine Coast*.

Inicialmente, os funcionários da empresa pensavam que se tratava de um mau funcionamento dos sistemas de bombeamento. Porém, esses mesmos funcionários, num dia de manutenção, perceberam que após reprogramarem os sistemas de bombeamento, esse era alterado. Após contratar uma firma de detetives e contatar a polícia sobre o ocorrido, o ex-empregado foi capturado pela polícia e, com ele, encontraram um computador portátil do qual ele enviava os comandos para o sistema supervisor da companhia de esgotos, comprovando a

4 Um mecanismo de segurança em camadas que minimiza o impacto de uma falha nos demais componentes.

sua ação maliciosa.

Os danos causados pelo ataque à firma *Maroochy* levaram os especialistas a concluírem que o projeto não possuía proteção cibernética ou políticas de segurança cibernética em vigor. Possivelmente, o mais importante foi o contato com um ente externo sem as devidas medidas adequadas de segurança pessoal.

O conhecimento especializado do ex-empregado o transformou numa ameaça interna, pois ele sabia como se conectar às estações de bombeamento e compreendia os procedimentos envolvidos na gestão do SCF de controle de águas residuais daquela empresa.

Sinais de Trânsito em Los Angeles, EUA (BERNSTEIN, BLANKSTEIN, 2007) – Em agosto de 2006, dois engenheiros invadiram o sistema de semáforos de Los Angeles, EUA e escolheram uma série de cruzamentos, de grande movimento, para alterar o tempo de duração dos sinais. Essa alteração consistia no aumento do tempo de sinal vermelho nas vias de maior fluxo e no aumento do tempo de sinal verde nas vias de menor fluxo. Como consequência foram causados grandes congestionamentos na cidade, em especial na chegada do aeroporto. A alteração na duração do semáforo foi feita de modo a não permitir que outros pudessem alterá-la, ou seja, a empresa de tráfego não conseguia reprogramar os semáforos.

Um dos dois engenheiros se fez passar por um alto funcionário da empresa de controle de tráfego e conseguiu entrar da rede de computadores. A partir daí, ele obteve os códigos necessários para desbloquear os computadores que controlavam semáforos.

Embora não tenha ocorrido acidentes entre veículos atribuídos a esse incidente e, portanto, nenhum dano físico ou ferimentos, ele poderia facilmente resultar em efeitos cinéticos. Basta imaginar, num cruzamento, os semáforos abertos para todas as vias simultaneamente.

A possibilidade de acesso externo às redes da empresa de controle de tráfego acrescido

do conhecimento específico dos agentes maliciosos, permitiu que os mesmos fizessem todas as alterações por eles desejadas, concretizando a sabotagem ao sistema.

Alto Forno na Alemanha (COBB, 2015) – Em dezembro de 2014, o Escritório Federal Alemão para a Segurança da Informação (BSI) revelou, por meio de um relatório, um ataque cibernético a uma usina de aço que resultou em grandes danos ao alto forno. De acordo com esse relatório, o ataque usou engenharia social e técnicas de "spear-phishing[5]" para convencer o destinatário das mensagens a abrir um anexo malicioso ou visitar um site malicioso em que um código malicioso ("malware") era baixado para o seu computador. Uma vez obtido o controle de uma máquina da rede pelos atacantes, eles foram capazes de explorar outros ativos da rede e chegar aos componentes industriais conectados à rede de produção da usina. Isso ocasionou falhas em partes da planta e um alto-forno não pode ser desligado corretamente.

Embora não explicitamente declarado no relatório, pode-se inferir que o atacante era alguém de dentro ou um profundo conhecedor da empresa e das respectivas redes. A conexão da rede corporativa com a rede da planta de fabricação deu a oportunidade ao invasor e danificar os sistemas. Se esse tipo de ligação for necessário, deve-se tomar medidas de prevenção para se evitar o acesso, bem como as respectivas medidas para a detecção de um acesso desse tipo. Uma arquitetura adequada permite aos analistas de segurança limitar o acesso, identificar movimentos suspeitos numa rede de computadores e coletar os dados necessários a uma detecção, seja ela imediata ou num momento posterior.

Após esses exemplos, tanto os experimentais como os utilizados por pessoas maliciosas, será descrito um dos mais famosos, se não o mais famoso, ataque cibernético de efeitos

5 "Spear-phishing" é um tipo de engenharia social no qual um indivíduo tenta obter informações sensíveis de um usuário, como senhas, dados financeiros e outros dados pessoais, se fazendo passar por uma pessoa ou entidade confiável enviando uma comunicação eletrônica ou mensagem oficial a esse usuário. Os usuários destinatários são pertencentes a grupos específicos, possuindo algo em comum como pertencer a um mesmo departamento numa empresa (CONKLIN; WHITE, 2014).

cinéticos que se tem conhecimento confirmado.

Usina de Enriquecimento de Urânio no Irã (FALCO, 2012) – Em 2010, começaram a surgir na mídia as histórias de um novo *worm* que ainda não havia sido descrito. Um *worm* de computador é um programa de computador malicioso que tenta penetrar redes e sistemas de computadores. Quando ele consegue entrar o *worm* se replica, a fim de se espalhar para outros computadores (CONKLIN; WHITE, 2014).

Esse *worm* fez uso de seis vulnerabilidades, tanto do sistema operacional quanto de aplicações, até então desconhecidas da comunidade de segurança, também denominadas *zero-day* ou *dia-zero*[6], e foi descoberto em 17 de junho de 2010 por uma firma de segurança da Bielorússia.

O Stuxnet era capaz de se propagar por meio da porta USB, da rede de computadores e de vulnerabilidades do sistema operacional Windows em diversas versões desse. Ele foi o primeiro artefato malicioso a incluir um mecanismo de acesso privilegiado a Controladores Lógicos Programáveis (CLP). Foi por meio desse acesso privilegiado que o Stuxnet causou os efeitos que levaram a destruição das instalações. Ele alterava a frequência dos conversores entre 1410Hz, depois 2Hz e 1064Hz enquanto mascarava os dados para o sistema de controle, ou seja, tudo parecia dentro da normalidade. Essa variação de frequência causou o estresse mecânico das centrífugas levando-as à falha e comprometendo a qualidade do urânio enriquecido.

Quanto às ações de mitigação, a maneira mais eficaz de prevenir que o *worm* Stuxnet se espalhe é fazer o uso de defesa baseadas em zonas, como descritos em normas como a IEC-

6 Uma vulnerabilidade é denominada de *zero-day* ou "dia-zero" porque uma vez que ela se torne conhecida, o autor do software tem zero dias para planejar e anunciar um plano de mitigação contra a exploração da vulnerabilidade.

62443[7]. Esse conceito separa uma rede de computadores em áreas seguras e, entre as áreas são instalados *firewalls*[8] com regras para bloquear protocolos desnecessários ou suspeitos. Entretanto, o Stuxnet cuidadosamente também empregava protocolos usados pelo software executado nas máquinas e o bloqueio de um destes protocolos, também bloquearia a comunicação e, consequentemente o funcionamento normal. Nesse caso, uma solução melhor seria instalar *firewalls* pessoais em cada máquina para permitir apenas que processos selecionados possam enviar dados por meio dos protocolos indicados.

O Stuxnet foi cuidadosamente desenvolvido e é um malware especificamente orientado, com a intenção de, sutilmente, causar dano significativo numa infra-estrutura chave (BRIGHT, 2010). O ataque efetuado por meio do "*malware*" Stuxnet, contra a usina de enriquecimento de urânio de Natanz, no Irã em 2010, serve como exemplo operacional do uso de armas cibernéticas cinéticas e, seu sucesso, pode ter dado início a uma nova corrida armamentista, ou melhor, ciber-armamentista entre os programas de desenvolvimento de guerra cibernética dos Estados.

2.2 Considerações

Os ataques revisados anteriormente ilustram que os efeitos cinéticos são uma ameaça válida e crível. Considerando os sistemas hoje empregados na MB, a possibilidade de que essas vulnerabilidades ocorram e que ameaças façam uso delas só aumenta com o tempo.

O projeto AURORA mostra que os equipamentos de geração de energia, e consequentemente, os motores de combustão associados precisam ter o seu risco avaliado do

7 Esta norma será abordada no Capítulo 3.

8 Um *firewall* é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

ponto de vista cibernético. Novos mecanismos de controle, agora empregando sistemas cibernéticos, podem apresentar novas vulnerabilidades até então inexistentes e que precisam ser avaliadas a fim de serem tratadas adequadamente. Para a MB, isso tem relação direta nos futuros motores e turbinas de propulsão, motores e geradores de energia, e respectivos mecanismos de controle.

Apesar de o experimento do implante médico mostrar vulnerabilidades que afetam apenas a pessoa que o usa, sem demonstrar um efeito cinético, pessoas chaves da organização não podem estar submetidas a este risco de maneira desnecessária. Assim, além do implante em si, cabe uma avaliação de risco de acordo com a pessoa que o receberá.

As lições decorrentes do experimento com o carro, o que permitiu um controle elevado do mesmo, e do controle de tráfego em Los Angeles, mostram que o aumento da conectividade de sistemas bem como a sua integração com demais componentes internos deve ser acompanhada de uma avaliação de riscos sistemática, bem como do emprego de princípios de segurança já consagrados. A conectividade abre brechas que vão além do contato físico com o carro ou sistema de tráfego, ou seja, ele pode ser explorado à distância, e a integração sem a devida proteção, traz novas vulnerabilidades, como o controle de pontos críticos do automóvel.

Nesse sentido, pode-se identificar alguns possíveis pontos a serem tratados na MB. Com a introdução do canal satélite para comunicação de dados, os navios no mar podem empregar esse canal para a troca de dados entre sistemas, devido à ampla cobertura provida por este canal bem como pela sua capacidade. Esses sistemas podem estar localizados num outro navio ou num órgão de terra e, devido ao necessário dos dados que podem ser trafegados, como o posicionamento dos meios no mar, essa troca de dados deve ser protegida a fim de

evitar a possibilidade de que usuários que não tenham a necessidade de conhecer ou o respectivo grau de sigilo venham a entrar em contato com esses dados.

Num futuro breve, o submarino convencional e os novos navios disporão de sistemas de gestão da plataforma com alta integração entre os diversos subsistemas componentes do meio. Essa integração de SCF deverá ser cuidadosamente planejada, do ponto de vista da segurança, desde o projeto até as demais etapas ao longo do ciclo de vida[9].

Os exemplos do alto forno na Alemanha e do *Stuxnet*, mostram que as redes de controle precisam de proteção intra-rede e inter-rede. As ligações da rede de um SCF com a rede administrativa devem ter seu risco avaliado e as devidas ações tomadas para se mitigar os riscos identificados.

Trazendo para os dias de hoje, ao longo do ciclo de vida, novos componentes são adicionados a SCF já existentes e, considerando que estes componentes utilizam cada vez mais tecnologia de uso comum, ou seja, não-proprietárias, eles podem trazer as respectivas vulnerabilidades, sejam de software ou hardware, utilizadas na sua produção bem como criar novas vulnerabilidades que podem ser exploradas com um maior grau de facilidade. Por exemplo, um sistema de armas cujo barramento de dados utilize uma tecnologia de uso comercial e que, ao longo do tempo, receba um novo componente ao seu barramento para coletar dados relacionados a sua manutenção quando, esse componente é baseado num computador pessoal executando uma distribuição Linux como sistema operacional.

Cada vez mais os equipamentos de propulsão e geração de energia se apoiarão em SCF para o seu controle e difusão de informações. A complexidade desses mesmos equipamentos pode levar a dependência de manutenção de terceiros, que terão acesso privilegiado aos SCF

9 Planejar a segurança desde o projeto é muito importante pois permitirá soluções que deixam ser possíveis depois da construção, sendo uma área importante a ser tratada em trabalhos futuros.

responsáveis pelo controle do equipamento o que leva a necessidade de uma política de contratação de pessoal para executar este tipo de manutenção[10]. Como ilustrado no caso do Sistema de Águas e Esgoto na Austrália, será necessário gerar uma política de pessoal voltada para terceiros, envolvidos na manutenção destes itens devido aos riscos que podem ser identificados.

Por fim, vê-se que a MB está exposta a inúmeros dos riscos já identificados e relatados na literatura e o impacto dos mesmos pode afetar a disponibilidade dos meios, bem como o seu efetivo emprego e desempenho nas diferentes tarefas.

10 A segurança de pessoal é um dos controles de segurança empregados para tratar o risco e compreende aspectos de seleção, treinamento, transferência e encerramento. Ela corresponde a uma importante área da segurança e é recomendada para trabalhos futuros.

3 FUNDAMENTOS DE SEGURANÇA PARA SISTEMAS CIBER-FÍSICOS

Inicialmente, os SCF tinham pouca semelhança com os sistemas de tecnologia da informação (TI) tradicionais pois, em geral, SCF foram sistemas isolados que executavam protocolos de controle e comunicação proprietários, utilizando hardware e software especializados. Fisicamente, os componentes dos SCF foram posicionados em áreas com segurança física e os componentes não foram conectados a redes ou sistemas de TI.

Nos dias atuais, há uma ampla disponibilidade de dispositivos de baixo custo empregando o Protocolo Internet (IP) e que agora estão substituindo as soluções proprietárias antes utilizadas no SCF, o que aumenta a possibilidade de vulnerabilidades de segurança cibernética e incidentes. Além disso, os SCF estão adotando soluções de TI para permitir a conexão aos sistemas de negócios corporativos e a capacidade de acesso remoto, e estão sendo projetados e implementados utilizando-se de computadores, sistemas operacionais e protocolos de rede padrão da indústria. Dessa forma, os SCF estão começando a possuir similaridades com os sistemas de TI. Essa integração provê novos recursos de TI, mas leva a um decréscimo significativo no isolamento de um SCF do mundo exterior, criando uma maior necessidade de proteger esses sistemas. Aliado a esse quadro, há um crescente uso de redes sem fio colocando alguns SCF em maior risco pois permite que adversários possam acessá-lo à alguma distância, sem ter acesso físico direto ao equipamento. Enquanto as soluções de segurança foram projetadas para lidar com essas questões em sistemas de TI típicos, precauções especiais devem ser tomadas quando da introdução dessas mesmas soluções aos ambientes de SCF.

Apesar dessas características semelhantes a sistemas de TI tradicionais, que vieram a se incorporar ao longo do tempo, os SCF também têm características que os diferem desses sistemas. Muitas dessas distinções decorrem da lógica de execução que, num SCF, possui um efeito direto sobre o mundo físico. Essas características podem acarretar num risco significativo para a saúde, segurança de vidas, danos graves ao ambiente e, no caso de SCF em meios operativos, no seu emprego e desempenho. Os SCF possuem requisitos de desempenho e confiabilidade singulares e, muitas vezes, os objetivos de segurança e eficiência podem entrar em conflito com a segurança e a operação desses mesmos sistemas.

Para lidar com isso, algumas normas já foram publicadas ao longo do tempo para fornecer orientações sobre como proteger alguns tipos de SCF. Mais especificamente, dentro dessa categoria de sistemas, as normas visam os Sistemas de Controle Industrial (ICS), os Sistema de Supervisão e Aquisição de Dados (SCADA), os Sistemas de Controle Distribuído (DCS) e outras configurações de sistemas de controle, tais como as que incorporam CLP.

Segundo a norma IEC 61131, um CLP é uma solução proprietária de hardware e software para aquisição de dados e controle de processos. O CLP é um computador digital industrial que foi reforçado e adaptado para o controle de processos de manufatura, linhas de montagem, dispositivos robóticos ou qualquer atividade que necessite da facilidade de programação, de alta confiabilidade e de um processo de diagnóstico de falhas.

Apesar das especificidades desses sistemas com relação ao fim a que se destinam como manufatura, distribuição de água ou controle de motores, os componentes empregados na sua implementação e respectiva programação – software – têm forte similaridade com os SCF utilizados em meios operativos de superfície, como o controle da propulsão executado pelo SCAMPA. Assim, serão revistas as normas publicadas que tratam da segurança de SCF para

se extrair os aspectos aplicáveis aos sistemas objeto deste trabalho. As duas principais normas existentes na literatura, com o título traduzido, são:

a) Guia para Segurança de Sistemas de Controle Industrial – NIST Special Publication 800-82 Revision 2[11] ; e

b) Padrões de Segurança em Automação Industrial e Sistemas de Controle – ISA/IEC 62443[12].

Ambas as normas são extensas e cobrem detalhes de especificações, projetos e protocolos, descendo até o nível da informação que trafega nesse tipo de sistema, ou seja, um nível técnico. A norma NIST 800-82 é editada pelo N*ational Institute of Standards and Technology* (NIST) do Departamento de Comércio dos Estados Unidos da América. Já a norma ISA/IEC 62443 é editada pela *International Electrotechnical Commission* (IEC), uma organização de padrões internacionais que prepara e publica padrões internacionais para todas as tecnologias elétricas, eletrônicas e afins, sendo a Associação Brasileira de Normas Técnicas (ABNT) um membro dessa organização.

Considerando uma organização como a MB, e aderente à sua estrutura organizacional hoje vigente, este trabalho tratará de aspectos relacionados a uma estrutura para o gerenciamento da segurança de sistemas ciber-físicos, a partir de uma visão de mais alto nível. Desse ponto de vista, a estrutura poderá ser instanciada e especializada nos meios operativos, quando deverão ser empregados detalhes mais técnicos também previstos nessas normas e em outras mais especializadas.

A seguir serão revistos os principais conceitos a serem considerados nesta estrutura. Na Seção 3.1 é feita uma comparação entre a segurança de SCF e sistemas de TI. Em seguida, a

11 do original: *Guide for Industrial Control Systems Security*.
12 do original: *Security for Industrial Automation and Control System*s.

Seção 3.2 trata dos conceitos de gerenciamento de riscos e na Seção 3.3 são trazidos os controles de segurança para tratar esses riscos. Na Seção 3.4 são descritas as especificidades dos SCF. A Seção 3.5 combina os conceitos das seções anteriores e descreve o desenvolvimento de um programa de segurança para SCF. Por fim, a Seção 3.6 faz as considerações sobre como desenvolver esse programa no âmbito da MB.

3.1 Comparação entre a Proteção de SCF e de Sistemas de TI

Um SCF controla o mundo físico enquanto sistemas de TI gerenciam dados. As características que o diferem incluem os riscos e prioridades, como o risco à vida humana, o meio ambiente e às questões financeiras, decorrentes de perdas numa produção fabril ou industrial. A partir da norma NIST-SP-800-82, pode-se destacar uma série de aspectos comparativos entre SCF e sistemas de TI que serão destacados a seguir.

Em geral, SCF possuem requisitos de desempenho e são sistemas de tempo real críticos, quando o prazo para execução de uma tarefa não pode ser violado. Alguns sistemas requerem respostas determinísticas, confiáveis e nem sempre com alta taxa de transferência. Em contraste, sistemas de TI requerem alta taxa de transferência e são mais resistentes a algum nível de atraso. Em alguns SCF, o tempo de resposta a interações humanas pode ser crítico e, em geral, são desenvolvidos em sistemas operacionais de tempo real.

Muitos dos processos controlados por SCF são de natureza contínua ao longo do tempo e interrupções inesperadas não são aceitáveis. Os requisitos de disponibilidade em SCF são elevados e sua parada e reinicialização comprometem o meio físico em que atuam. Por isso nesses sistemas são encontrados componentes redundantes, em geral em execução paralela, para prover continuidade de funcionamento mesmo na falha do componente principal.

As preocupações primárias dos dados em sistemas de TI são a confidencialidade e a integridade. Para SCF são segurança da vida humana, perda de equipamento, perda de produtos e produção, tolerância a falha para prevenir danos e aderência as normas de segurança. Desse modo os requisitos para o gerenciamento de riscos são diferentes, e o pessoal que opera, mantém e protege um SCF deve entender a relação entre proteção do sistema e a segurança do meio físico.

Alguns dos componentes de um SCF são os responsáveis pelo efetivo controle dos processos físicos. As interações desse sistema com o mundo físico podem ser bem complexas e as suas consequências se manifestam como eventos físicos. O entendimento dos efeitos desses eventos pode requerer a comunicação entre os especialistas do domínio físico e dos mecanismos de controle.

O sistema operacional e as redes de controle de um SCF são bem diferentes dos respectivos componentes no âmbito da TI, requerendo outras habilidades, experiência e maturidade para a sua operação. Em geral, as redes de controle não são operadas por profissionais de TI e sim por engenheiros de controle, e essas diferenças devem ser consideradas, com o risco de consequências desastrosas.

A característica de trabalhar em tempo real e com dispositivos de capacidade de processamento variável tornam os SCF um tipo de sistema com recursos restritos, e por isso não permitem incorporar algumas capacidades de segurança existentes em sistemas de TI. Por exemplo, encriptação, registro de erros (*logging*) e proteção de senhas. O uso indiscriminado de capacidades de TI em SCF pode comprometer os requisitos de tempo e disponibilidade e pode não ser possível atualizar os dispositivos de um SCF para apresentarem tais capacidades.

Os protocolos de comunicação empregados em dispositivos de um SCF são diferentes

dos empregados em sistemas de TI, sendo em geral proprietários ou atendendo a protocolos muito específicos.

A gerência de mudanças é importante para manter a integridade de um sistema, seja ele de TI ou um SCF. Um software desatualizado representa uma das maiores vulnerabilidades a um sistema. Para um sistema de TI, as atualizações são aplicadas em tempo hábil e seguindo alguma política e procedimentos de segurança. Para SCF essas atualizações nem sempre podem ser feitas em tempo hábil, pois elas precisam ser testadas tanto pelo fabricante do produto como pelo usuário final da aplicação de controle. Adicionalmente, o agendamento de uma atualização pode precisar ser feito com antecedência a fim não comprometer o processo físico devido à uma parada. Uma outra particularidade é que alguns produtos podem utilizar um software sem manutenção do fabricante, por ter sido descontinuado, e por isso sem possibilidade de correção de alguma vulnerabilidade descoberta.

A assistência técnica em sistemas de TI permite diversas modalidades de prestação de serviço. Para SCF em geral a assistência técnica é feita por apenas um provedor, que pode não dispor de soluções variadas para o serviço. Além disso, soluções de segurança de terceiros podem não ser permitidas devido à licença de uso e acordos de serviço, e a perda da assistência pode ocorrer caso um produto de terceiro seja instalado sem a anuência ou conhecimento do vendedor.

O tempo de vida de um componente de TI típico é da ordem de 3 a 5 anos, podendo ser menor devido a rápida evolução tecnológica. Para SCF onde a tecnologia é desenvolvida para atender a requisitos bem específicos de uso e implementação, o tempo de vida dos itens pode ser da ordem de 10 a 15 anos.

Muitos dos componentes de TI e alguns de SCF são localizados nos respectivos locais

de negócio, sendo acessíveis fisicamente, mesmo que por meio de transporte. Locais remotos podem ser empregados como instalações de reserva (*backup*). Já em alguns SCF, seus componentes podem estar distribuídos, em locais remotos e isolados. Além da distância, estes componentes podem ter que considerar as medidas de segurança ambiental e físicas necessárias para poderem operar nesses ambientes.

3.2 Gerenciamento de Riscos

As organizações gerenciam o seu risco diariamente para cumprirem os seus objetivos de negócio. Elas devem desenvolver um processo de gerenciamento de riscos que pode ser descrito, de maneira simplificada, como um processo de tomada de decisão, em que: é determinado o que pode ocorrer ao negócio, avaliado o impacto caso venha a ocorrer e decidido o que poderá ser feito para controlar esse impacto e responder a ele. Os principais conceitos dessa área a serem utilizados neste trabalho seguirão as definições encontradas em Conklin e White (2014). Segundo os autores, **risco** é a possibilidade de sofrer uma perda ou prejuízo. O **gerenciamento de risco** é o processo completo de tomada de decisão de identificar ameaças e vulnerabilidades e seus potenciais impactos, determinar o custo para mitigar tais eventos, e decidir quais as ações de melhor custo benefício para controlar esses riscos. A **ameaça** é qualquer circunstância ou evento com o potencial de causar dano a um ativo. Um **ativo** é uma entidade sobre o qual alguém, ou organização, estabelece um valor. A **vulnerabilidade** é a característica de um ativo que pode ser explorada por uma ameaça para causar um dano. O **impacto** é a perda em decorrência da exploração, por uma ameaça, de uma vulnerabilidade. A **avaliação de risco** ou **análise de risco** é o processo de analisar um ambiente para identificar os riscos (ameaças e vulnerabilidades), e determinar o impacto de

um evento (de modo qualitativo ou quantitativo) que possa afetar um negócio ou projeto. Um **controle de segurança** é uma medida tomada para detectar, prevenir ou mitigar o risco associado a uma ameaça.

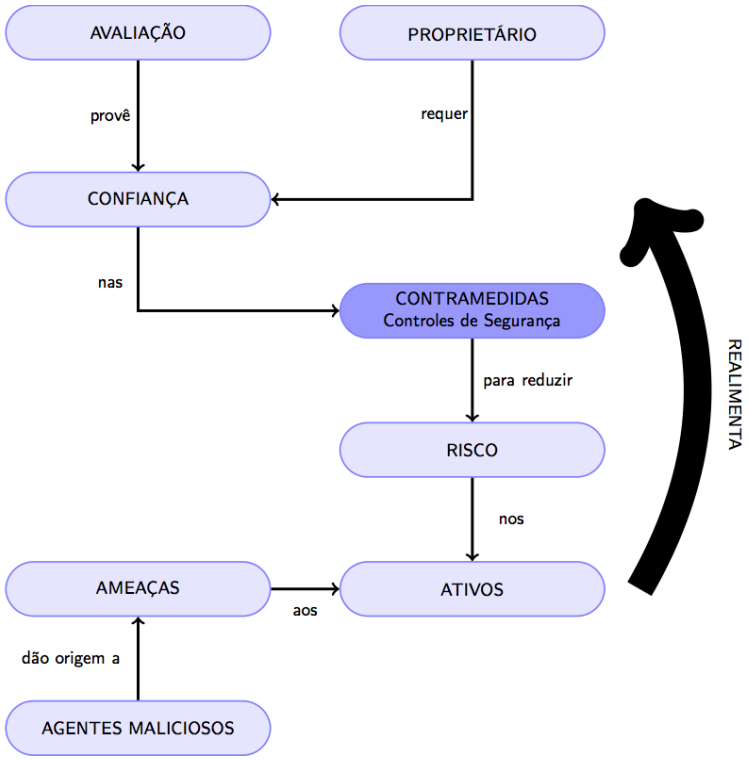

Figura 1: Conceitos de alto nível e relações entre si (adaptado da norma ISO/IEC 15408).

Segundo a norma ISO/IEC 15408, que trata sobre a Avaliação de Segurança de Tecnologia da Informação, estes conceitos podem ser vistos e relacionados como ilustrado na Figura 1. A seta no lado direito indica que novos agentes, ameaças ou vulnerabilidades, realimentam o processo de avaliação, pois agora este processo deverá considerar estas novas ameaças, incorporando-as. A segurança trata da proteção de ativos. Os proprietários desses ativos devem identificar seus requisitos de segurança, por meio de um método de avaliação de riscos. Essa avaliação irá resultar na determinação e condução das ações de gerenciamento apropriadas, na priorização do gerenciamento de risco e na implementação dos respectivos

controles de segurança, ou contramedidas, para se proteger destes riscos. Como ocorre um contínuo surgimento de novas ameaças ao longo do tempo, a avaliação de riscos é uma atividade periódica.

Agentes maliciosos podem ter interesse ou dar valor a ativos e buscar explorá-los de forma contrária aos interesses de seus proprietários. Como exemplos de agentes maliciosos pode-se citar *hackers*, usuários mal intencionados, usuários não maliciosos (que eventualmente cometem erros) e acidentes. As ameaças decorrentes dos agentes maliciosos são percebidas pelos proprietários como possibilidades de comprometimento dos seus ativos, reduzindo o seu valor. Consequentemente, essas ameaças dão origem aos riscos para os ativos, com base na probabilidade da ameaça e o seu respectivo impacto sobre o ativo ao se realizar o risco. Para se reduzir os riscos das ameaças empregam-se as contramedidas ou controles de segurança.

Gerenciar risco é uma atividade complexa que requer o envolvimento de toda a organização, desde o mais alto nível gerencial, provendo a visão estratégica e os objetivos estratégicos, passando pelos profissionais no nível médio gerencial, planejando, executando e gerenciando projetos, até os indivíduos na linha de frente que operam os sistemas de informação. Esse gerenciamento é um processo que requer:

a) uma concepção de riscos – que estabelece uma base para decisões;

b) uma avaliação de riscos;

c) uma resposta ao risco quando determinado; e

d) a monitoração do risco de forma contínua utilizando um mecanismo de realimentação para a melhoria contínua.

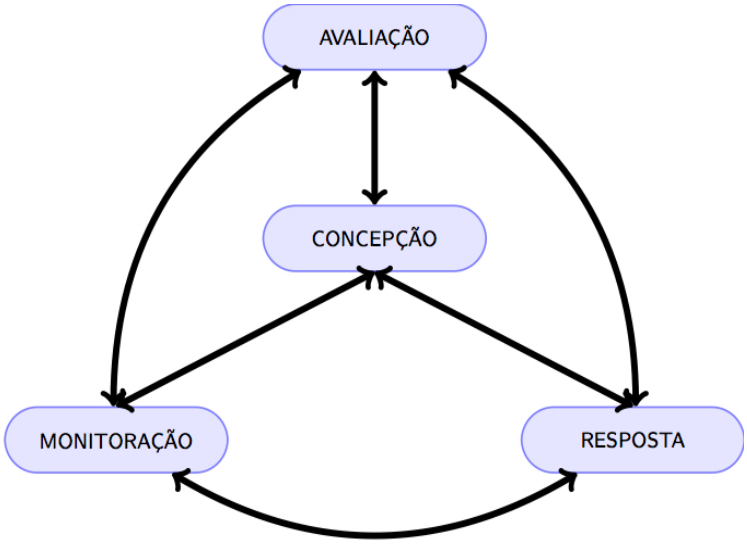

Figura 2: Os componentes do processo de gerenciamento de riscos (adaptado da norma NIST 800-39).

Na Figura 2 este processo de gerenciamento de risco está ilustrado, e as setas representam os fluxos de informação e comunicação entre os componentes.

O componente de **Concepção** consiste no desenvolvimento de um arcabouço para a tomada de decisões no gerenciamento de risco, bem como o nível de risco que a organização tolera aceitar. Ele também inclui as atividades de revisão de documentos e possui atividades relacionadas a um planejamento de desastres mais amplo, pois eventos em SCF podem impactar os requisitos contidos na avaliação de risco de outros planos. Por exemplo, os acidentes com o alto-forno na Alemanha e o sistema de controle de esgotos na Austrália, que no segundo caso, provocou um dano ambiental ao vazar esgoto em áreas não permitidas, devem ter desencadeado outros planos de segurança relacionados a esses efeitos.

O componente de **Avaliação** requer que as organizações identifiquem suas ameaças e vulnerabilidades, os impactos que elas podem causar à organização e a possibilidade de que

ocorram outros eventos adversos a partir dessas ameaças e vulnerabilidades.

O componente de **Resposta** é baseado no conceito de uma resposta consistente, por toda a organização, à identificação de risco. Diferentemente da resposta a incidentes, a resposta à identificação de riscos requer que a organização primeiro identifique as possíveis linhas de ação para tratar um risco, depois avalie essas linhas em relação a tolerância ao risco definido pela organização e às outras considerações determinadas no componente de concepção e, por fim, escolha a melhor alternativa para a organização. Esse componente também inclui a implementação da linha de ação escolhida para tratar o risco que pode ser: aceitar, evitar, mitigar, compartilhar, transferir ou alguma combinação destas opções.

O quarto e último componente, a **Monitoração**, trata do acompanhamento contínuo. As organizações devem monitorar o risco de maneira contínua incluindo: a implementação das estratégias de gerenciamento de risco escolhidas, as mudanças no ambiente que possam afetar o cálculo do risco e a efetividade e eficiência das atividades de redução de risco. Esse componente é responsável por realimentar todo o processo de gerenciamento de risco proposto na norma NIST 800-39, afetando todos os demais componentes desse processo.

Para integrar esse processo de gerenciamento por toda a organização, a norma NIST 800-39 propõe empregar uma abordagem em camadas para tratar o risco. Essa abordagem em camadas ou níveis, cobre os riscos nos três níveis organizacionais sugeridos pela publicação que, do mais elevado ao mais baixo, são:

1) nível organização;

2) nível de missão e processo de negócio; e

3) nível do sistema de informação.

O processo deve ser conduzido através das três camadas e contém o objetivo global de melhoria contínua nas atividades organizacionais relacionadas ao risco. O nível organização fornece o contexto para todas as atividades de gestão de riscos desenvolvidas na organização nas camadas abaixo. Esse nível ainda provê a priorização de missões e funções que por sua vez leva às estratégias de recuperação de sistemas críticos.

No nível de missão, as atividades incluem a definição de quais missões e processos que apoiam o nível de organização, a priorização desses processos de acordo com os objetivos estratégicos da organização, a definição dos sistemas e respectiva informação necessárias à execução com sucesso das missões e processos, bem como o seu fluxo na organização.

Por fim, no nível do sistema de informação os riscos são guiados pelo contexto e pelas decisões das camadas superiores. Na norma NIST 800-37 é proposto um arcabouço de gerenciamento de riscos para o nível do sistema de informação. Esse arcabouço é um processo que integra uma sequência de atividades e que se realimenta.

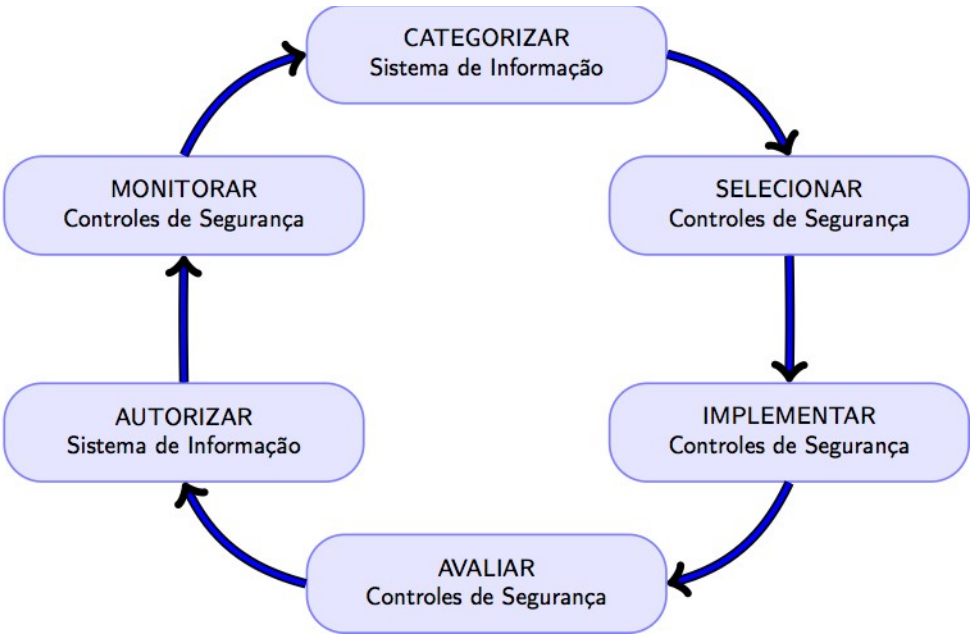

Figura 3: O arcabouço de gerenciamento de riscos (adaptado da norma NIST 800-37)

Na Figura 3 está ilustrada a sequência das atividades do arcabouço de gerenciamento de riscos. Esse processo começa na atividade de **categorizar**, em que os sistemas de informação e as informações processadas, armazenadas e enviadas por eles são categorizadas baseando-se numa análise de impacto. Em seguida é **selecionado** o conjunto base de controles de segurança para os sistemas de informação, fundamentado na categorização anterior. Uma revisão e refinamento desse conjunto base pode ser necessária baseando-se na avaliação de riscos da organização e condições locais. Escolhidos os controles de segurança eles serão **implementados** e também deverá ser descrito como se dará o seu emprego com os sistemas de informação e o ambiente de operação. Os controles de segurança são **avaliados** usando-se procedimentos de avaliação apropriados para determinar a extensão com que os controles estão implementados corretamente, se são operados como planejado e produzindo os resultados esperados em relação aos requisitos de segurança para o sistema. **Autorizar** a operação dos sistemas de informação baseado na determinação dos riscos à operação da organização, indivíduos e ativos e na decisão de que os riscos são aceitáveis. **Monitorar** os controles de segurança dos sistemas de informação de modo contínuo, documentar mudanças no sistema, inclusive no ambiente de operação, conduzir análises de impacto de segurança das mudanças e relatar o estado de segurança do sistema aos responsáveis.

3.3 Controles de Segurança

Um controle de segurança, ou contramedida, é uma medida tomada para detectar, prevenir ou mitigar o risco. Há diversos tipos de controles e a publicação NIST-SP-800-53 estabelece dezoito áreas nas quais pode-se agrupar os controles de segurança. Apesar desses controles terem sido gerados para sistemas de informação, as áreas estabelecidas servem

como uma base para a atividade de Selecionar do arcabouço de gerenciamento de riscos e, em alguns casos, pode ser necessário interpretá-los do ponto de vista de um SCF. Essas interpretações podem ser obtidas da norma ISA/IEC 62443, já citada anteriormente.

As dezoito áreas de segurança, ou famílias de controles de segurança, de acordo com a norma NIST-SP-800-53 são as seguintes:

1) Controle de acesso: o processo de garantir ou negar requisições específicas para obter e usar informação e serviços de processamento de informação relacionada para acesso físico às áreas dentro do ambiente do sistema de informação.

2) Avaliação e Treinamento: políticas e procedimentos para assegurar que todos os usuários do sistema de informação recebam o apropriado treinamento de segurança relativo ao seu uso do sistema e que registros de treinamento sejam executados e mantidos.

3) Auditoria e Prestação de Contas: revisão independente e verificação de registros e atividades para avaliar a adequação de controles, assegurar a aderência às políticas estabelecidas e procedimentos operacionais, e recomendar mudanças necessárias em controles, políticas e procedimentos.

4) Avaliação de Segurança e Autorização: assegura que os controles especificados são implementados corretamente, operam como pretendido e produzem o resultado desejado.

5) Plano de Contingência: políticas e procedimentos projetados para manter ou restaurar operações de negócio, incluindo operações de computador, possivelmente num local alternativo, em caso de emergência, falhas de sistemas ou desastres.

6) Gerência de Configuração: políticas e procedimentos para o controle de modificações em hardware, firmware, software e documentação para assegurar que o sistema de informação

é protegido contra modificações inapropriadas antes, durante e depois de sua implementação.

7) Identificação e Autenticação: o processo de verificar a identidade de um usuário, de um processo ou de um dispositivo, por meio do uso de credenciais específicas como, senhas, *tokens* e biometria, como um pré-requisito para garantir o acesso a recursos num sistema de TI.

8) Resposta a Incidente: políticas e procedimentos pertencentes a resposta a incidentes como treinamento, teste, manuseio, monitoração, relatórios e serviços de apoio.

9) Manutenção: políticas e procedimentos para gerenciar todos os aspectos de manutenção de um sistema de informação.

10) Proteção de Mídia: políticas e procedimentos para assegurar o manuseio seguro de uma mídia. Os controles devem cobrir acesso, identificação, armazenamento, transporte, desinfecção, destruição e descarte.

11) Proteção Física e Ambiental: políticas e procedimentos tratando da transmissão, da exibição de controle de acesso bem com controles ambientais para condicionamento (e.g., temperatura, umidade) e provisões de emergência (e.g., desligamento, força, descargas elétricas atmosféricas e proteção contra incêndio).

12) Planejamento: desenvolvimento e manutenção de um plano para tratar da segurança de sistemas de informação por meio da avaliação, especificação e implementação de controles de segurança, atribuição de níveis de segurança e resposta a incidentes.

13) Segurança de Pessoal: políticas e procedimentos para a categorização da posição funcional de pessoal, triagem, transferência, penalidade e encerramento. Também trata da segurança de pessoal terceirizado.

14) Avaliação de Risco: o processo de identificar riscos às operações, a ativos ou a indivíduos pela determinação da probabilidade de ocorrência, o impacto resultante e controles de segurança adicionais que podem mitigar este impacto.

15) Aquisição de Sistemas e Serviços: alocação de recursos para a segurança de sistemas de informação para serem mantidos por todo o ciclo de vida, e o desenvolvimento de políticas de aquisição baseadas no resultado da avaliação de risco, incluindo requisitos, critérios de projeto, procedimentos de teste e documentação associada.

16) Proteção de Sistema e Comunicações: mecanismos para proteção do sistema e de seus componentes de transmissão de dados.

17) Integridade de Informação e de Sistema: políticas e procedimentos para proteger sistemas de informação e seus dados de falhas de projeto e modificação de dados usando verificação de funcionalidade, de integridade de dados, detecção de intrusão, detecção de código malicioso, alerta de segurança e controles de alerta.

18) Gerência de Programa: provê controles de segurança em níveis mais elevados que o nível do sistema de informação.

Esses controles podem ser empregados para tratar os riscos em SCF. Entretanto cabe ressaltar as particularidades de um sistema decorrentes do processo físico sob seu controle, que serão tratadas na próxima seção.

3.4 Aspectos Específicos para SCF

Devido à característica de um SCF atuar no meio físico, os efeitos decorrentes de uma falha neste tipo de sistema podem acarretar danos no meio físico. Empregando um conceito

de segurança mais genérico e que abrange aspectos além da segurança do sistema de informação, como a definição vista no início do Capítulo 2, segundo a norma MIL-STD882E (2012), Segurança é a ausência de condições que possam causar morte, lesões, doenças ocupacionais, danos ou perda de equipamentos ou propriedade, ou danos ao meio ambiente. Esse conceito de segurança é o principal fator que afeta as decisões em como os sistemas são projetados e operados. Essas considerações precisam interagir com as boas práticas de segurança da informação e devem ser determinados pela organização pois, poderá haver um conflito entre esses dois aspectos, conforme mencionado na Seção 3.1, e esses devem ser localizados no componente concepção do processo anteriormente descrito.

Desta forma, na avaliação de riscos os impactos num SCF devem incorporar:

a) o efeito no processo físico controlado;

b) os efeitos em sistemas/processos dependentes (efeito cascata); e

c) os efeitos no ambiente físico.

Devido à integração de sistemas digitais a sistemas físicos existentes num SCF, as avaliações de risco de segurança da informação tratam do mundo digital e são complementares às avaliações de risco relacionados ao mundo físico, visto que um risco no meio digital pode acarretar um risco no meio físico. Seguindo a norma NIST 800-82, a avaliação de dano potencial decorrente de um incidente num SCF deve incorporar:

a) como um incidente pode manipular a operação de sensores e atuadores para impactar o ambiente físico;

b) que controles redundantes existem num SCF para prevenir um impacto; e

c) como um incidente físico pode surgir baseado nessas condições.

O foco dessa avaliação deve ser na segurança da vida humana, no meio ambiente e em outras infraestruturas críticas. Na segurança da vida humana os impactos devem considerar se eles causam alguma lesão, doença ou a morte decorrente do mal funcionamento do SCF. Impactos no meio ambiente podem ser necessários de serem tratados na avaliação, e provavelmente há uma série de regulamentações e normas legais já estabelecidas e que devem ser obrigatoriamente observadas. Por fim, um SCF pode ser distribuído por uma área, em vez de ser pontualmente localizado, e exposto a ambientes não controlados.

Um outro aspecto importante para os SCF é a disponibilidade do serviço provido por ele. Um SCF pode ser parte de uma infraestrutura crítica em que há uma significativa necessidade de operação contínua e confiável. Como consequência, estes sistemas podem ter requisitos rigorosos de disponibilidade e de recuperação em caso de falha. Além desses aspectos inerentes a um SCF, o ambiente no qual ele operará é mais um item a ser considerado no componente de concepção e que a organização deve considerar. Dependendo do domínio onde um SCF é empregado, eles devem atender a requisitos impostos por esse domínio ficando fortemente relacionados a ele e restritos. Com isso, esses requisitos devem ser claramente definidos e os riscos advindos disso devem ser identificados e considerados.

Dentre as abordagens propostas na literatura para a análise de segurança de SCF destacam-se a Análise do Modo e Efeito de Falha, ou simplesmente FMEA (do inglês *Failure Mode and Effect Analysis*), a Análise de Árvore de Falhas, ou simplesmente FTA (do inglês *Fault Tree Analysis*) e *Sneak Path Analysis* (SPA) (BAYBUTT, 2004). Esses tipos de análises empregam dados de projeto dos sistemas em questão.

Resumidamente, estes três tipos de análises são assim descritos por Azevedo (2010):

FMEA – Contém cinco elementos básicos, a seguir:

1) Qual o projeto ou processo;

2) Como ele pode falhar, Por que ele falha; e O que acontece quando falha;

3) Identificar os modos de falha mais importantes;

4) Priorizar os modos de falha; e

5) Acompanhar se as intervenções atendem aos objetivos e realizar auditorias de manutenção.

FTA – A análise envolve cinco etapas:

1) Definir o evento indesejado para estudar;

2) Obter o entendimento do problema;

3) Construir a árvore de falhas;

4) Avaliar a árvore de falhas; e

5) Controlar os riscos identificados.

SPA – Tem como principal objetivo identificar caminhos inesperados que sob certas condições podem produzir resultados indesejados ou mesmo impedir o funcionamento do sistema. Na aplicação para segurança cibernética, a SPA permite identificar caminhos inesperados que um agente malicioso possa vir a percorrer para penetrar um sistema.

Seja qual o método de análise, eles fornecem diferentes resultados e demandam uma série de informações sobre os sistemas analisados, incluindo dados de projeto e especificações, bem como profissionais qualificados e com conhecimento do domínio em que o SCF é empregado.

3.5 Programa de Segurança para SCF

Dados os conceitos para o gerenciamento de riscos, tratados na Seção 3.2 e 3.3, e as particularidades a serem consideradas para este gerenciamento, no que tange a SCF, tratados na Seção 3.4, nesta Seção serão revistos os principais aspectos no desenvolvimento de um programa para a segurança de SCF que irão apoiar esse processo de gerenciamento de riscos e consideram as particularidades de SCF.

As normas NIST 800-82 e ISA/IEC 62443, já mencionadas anteriormente, tratam do desenvolvimento desse tipo de programa. Aqui serão tratados os passos previstos na norma NIST 800-82 que se situam num nível mais elevado e permitem o seu aproveitamento para a proposta da estrutura, enquanto na norma ISA/IEC 62443 são abordados aspectos mais detalhados e específicos, situados no nível do sistema de informação.

O primeiro passo do programa é motivar a alta administração organizacional da importância de um programa de segurança para SCF. Essa motivação é obtida por meio de um Caso de Negócio para Segurança, que deve alinhar as preocupações da alta gerência com o negócio e os riscos identificados e fundamentados por especialistas. Além desses riscos, devem ser delineados os benefícios de se criar este programa, uma priorização dos cenários de danos identificados, uma visão de alto nível desse programa e respectivos custos envolvidos.

A segunda atividade é formar um grupo de pessoas multidisciplinar voltado para a segurança, ou seja, um time de segurança, que envolverá, pelo menos, pessoal da área de TI, engenheiros de controle, especialistas de segurança e profissionais de gestão de risco corporativo.

Em terceiro, deve-se definir um guia com os papéis a serem desempenhados, respectivas responsabilidades, gerentes de processos e usuários. Este guia também definirá o

escopo do programa de segurança, que conterá seus objetivos, as partes da organização que serão afetadas por ele, os sistemas de informação e SCF envolvidos e os recursos necessários, sejam financeiros e materiais.

No quarto passo, são definidas as políticas e procedimentos que devem ser integrados a outras políticas já existentes na organização. Estas políticas devem considerar a análise de risco de segurança da organização para estarem aderentes na gestão dos riscos identificados, permitir a proteção atual e às evoluções das ameaças e definir os objetivos de segurança e respectivas prioridades. Em decorrência das políticas serão desenvolvidos os procedimentos para implementá-las. Esses procedimentos devem ser documentados, testados e atualizados periodicamente em resposta a alterações que ocorram ao longo do tempo, tanto nas políticas nas quais eles se orientam, quanto nas tecnologias e novas ameaças.

Como quinto e último passo, o programa deve implementar um arcabouço para o gerenciamento do risco de segurança em SCF, como o ilustrado na Figura 3 e descrito na Seção 3.2.

3.6 Considerações

Um produto de segurança ou uma tecnologia não podem proteger adequadamente um SCF. A proteção deste tipo de sistema é calcada na combinação de políticas de segurança e a respectiva implementação, nos quais estarão incluídos os produtos e tecnologias.

Como visto neste capítulo, os documentos anteriores procuram tratar da segurança de SCF olhando para a organização como um todo e nos seus diferentes níveis decisórios. As normas descrevem uma série de medidas a serem tomadas com o intuito de executar um gerenciamento de riscos que cubra toda a organização, de maneira sistemática e contínua e

contendo um mecanismo de realimentação capaz de contribuir para a melhoria contínua do próprio gerenciamento de riscos para SCF e com isso aperfeiçoar o gerenciamento de riscos de toda a organização. Por fim, são colocadas as etapas para a implantação do gerenciamento de riscos para SCF numa organização, considerando as particularidades da organização e de seus SCF em questão.

A partir do "o quê" deve ser feito, obtido da revisão das normas enumeradas, cabe questionar como fazer isso. Considerando o estado atual da MB, algumas questões que poderiam ser feitas são:

– como iniciar um programa numa organização que ainda não trata a segurança desse tipo de sistema ?

– como alinhar o nível do sistema de informação com um nível superior ?

– que contramedidas são mais apropriadas para mitigar os riscos em sistemas já em produção e sem capacidade de mudança ?

– dado que a quantidade de riscos é enorme, como priorizá-los ?

Diante disso, no próximo capítulo será apresentada a proposta de implantação da estrutura a ser empregada na proteção de SCF embarcados em meios operativos, considerando os conceitos e aspectos revisados neste capítulo.

4 PROPOSTA DE UMA ESTRUTURA PARA A GESTÃO DO RISCO EM MEIOS OPERATIVOS

Como já mencionado, os SCF são fundamentais para o emprego e o desempenho de meios de combate e, ao longo do tempo, esses sistemas tendem a ser mais vulneráveis. Entretanto, no âmbito da MB, apenas os sistemas de TI possuem normas dedicadas à sua segurança, as quais tratam apenas dos objetivos da segurança da informação, sem considerar os SCF.

No capítulo anterior foram descritos os principais conceitos sobre segurança e gerenciamento de riscos, atividade fundamental em qualquer processo organizacional que venha a tratar da segurança de seus ativos. Também foram ressaltados aspectos particulares no que tange a SCF e sua segurança e, por fim, um Programa de Segurança para se implantar um processo de gerenciamento de riscos para SCF.

Considerando o problema definido neste trabalho e a revisão dos conceitos para a proteção de SCF, neste capítulo será proposta uma estrutura de proteção de SCF para meios operativos da MB. Cabe relembrar que e o principal aspecto desta estrutura serão as atividades a serem executadas e uma abordagem para a implantação das atividades, sem tratar da estrutura organizacional na MB que se responsabilizará por estas atividades. Na formação dessa estrutura, foi considerada uma série de condicionantes, decorrentes do estado atual, e que serão agora descritos:

a) os meios a serem protegidos já estão em operação, ou seja, numa fase do ciclo de vida posterior ao seu projeto, o que pode levar a soluções que não considerem alterações em

componentes físicos já existentes; e

b) a falta de um processo sistematizado de proteção destes sistemas, bem como da visão, em qualquer nível organizacional, dos riscos ao cumprimento dos objetivos e missões atribuídos aos meios.

O processo de gerenciamento de riscos, revisado na Seção 3.2, prevê que ele englobe toda a organização e que possa ser visto em três camadas gerenciais e hierárquicas distintas. O nível mais baixo é o informacional e, consequentemente, muito técnico e distante das tarefas a serem cumpridas por um meio. Porém ele é fundamental nesse processo pois é a partir dele que são identificados os primeiros riscos, bem como é nesse nível que se situa um grande número dos controles de segurança.

Esse nível informacional necessita ser alinhado com o nível de missão. Neste alinhamento ficará mais claro como subsistemas interagem para entregar um resultado de maior valor, que são as tarefas que um meio deve cumprir. Também nesse nível mais elevado, os respectivos riscos ao desempenho das missões e tarefas decorrentes poderão ser melhores visualizados pelo comando do navio.

O nível mais alto é o organizacional e que possui um alto grau de abstração. Mesmo na área de segurança para sistemas de TI, já existente na MB, ele não fica claramente definido, ou seja, não há indicadores que permitam avaliar o risco da MB no nível organização. Desse modo, no momento atual não se considera tratar dos riscos neste nível e espera-se que o mesmo aconteça num momento posterior, após os níveis de missão e informacional tiverem sido estabelecidos.

Assim considera-se que, num primeiro momento, a estrutura proposta cubra os níveis informacional e de missão para, num momento posterior e após a consolidação desses dois

níveis, ela possa vir a evoluir e cobrir a visão no nível da organização.

Para instanciar a visão no nível de missão, este trabalho sugere empregar a Sistemática para Avaliação Operacional (AO) na Marinha do Brasil, descrita na publicação EMA-333 (BRASIL, 2004), e descrita na próxima seção.

Um outro aspecto que o emprego da Sistemática para AO no gerenciamento de riscos pode contribuir é na consideração de requisitos de desempenho, com sistemas de tempo real crítico e cujo prazo para execução de uma tarefa não pode ser violado. Em geral, o foco da avaliação de riscos de SCF é a segurança da vida humana, o meio ambiente e infraestruturas críticas. Todavia em SCF relacionados ao emprego de meios operativos, a avaliação também deve levar em conta a disponibilidade dos serviços providos e o seu desempenho, pois esses serviços podem representar a proteção do próprio meio e a sua sobrevivência. Por exemplo, um armamento de defesa de ponto deve estar pronto e não pode ter o seu desempenho afetado ao ser empregado contra um míssil que venha em direção ao navio do qual ele faz parte.

Por fim, cabe ressaltar que a composição de sistemas leva a riscos derivados dessa ligação entre eles e que não poderiam ser vistos olhando-se para cada sistema individualmente. Num sistema de armas, uma série de subsistemas pode ser empregado para se obter um resultado, como diferentes sensores, consoles de processamento da informação para o cálculo da pontaria, envio de dados e controle do armamento a ser lançado, até mesmo durante a sua fase de vôo. Esse caso também corrobora o emprego da Sistemática de AO no gerenciamento de riscos.

4.1 Sistemática para Avaliação Operacional

A AO consiste no conjunto de procedimentos necessários para o fornecimento de

subsídios ou elementos de informação, em sua maioria quantitativos, que possam auxiliar no processo de tomada de decisões quanto à obtenção, ao emprego, ao apoio logístico e às modificações do sistema avaliado.

A AO procura estimar a eficácia e a adequabilidade operacional do sistema por meio de experimentos controlados, onde se busca o maior realismo possível (BRASIL, 2004). Uma AO é composta das seguintes fases:

1) Definição do problema;

2) Planejamento;

3) Execução;

4) Apresentação dos Resultados; e

5) Projeto de Exercícios Operativos.

A fase que interessa a este trabalho é a primeira, a Definição do Problema, quando uma série de documentos relativos a um meio são considerados para se entender o problema e formular um plano de avaliação. Esses documentos são compostos pelos Requisitos de Estado-Maior (REM), os Requisitos de Alto Nível dos Sistemas (RANS), as Especificações de Alto Nível dos Sistemas (EANS) e os Requisitos Táticos Operativos (RTO). Após o entendimento do problema, é delineado o Plano Mestre da Avaliação, em que se descreve a forma pela qual será conduzido o processo de avaliação. Um elemento fundamental desse Plano é a definição da(s) tarefa(s), ameaça(s), cenário(s) e função(ões), prevista(s) para o emprego do sistema a avaliar.

No entender deste trabalho, o método empregado para se delinear o Plano Mestre de Avaliação permite colocar o gerenciamento de riscos no nível da missão dos meios.

4.2 Gerenciamento de Riscos

Os componentes indicados na Seção 3.2 ficariam instanciados da forma a seguir. A **Concepção** irá estabelecer uma base para a gestão de risco estabelecendo os limites de decisão e o escopo dentro da organização. Devido à ausência de um gerenciamento de riscos anterior, num primeiro momento não se considera possível determinar a tolerância ao risco.

As premissas quanto ao risco, que inclui as suposições sobre as ameaças, vulnerabilidades, seus impactos e probabilidade de ocorrência, podem ser simples e pouco numerosas no início do gerenciamento e guiadas pela Sistemática proposta na Seção 4.1. Essa Sistemática também poderá ajudar na definição das prioridades e compromissos como, a importância relativa das tarefas, as compensações entre diferentes riscos e prazos que a organização tenha para tratar os riscos. As premissas também podem fazer o uso de revisões sobre casos que já tenham ocorrido para orientar a identificação de riscos mais prementes e com alguma abordagem já proposta para a sua mitigação.

A **Avaliação** é o segundo componente da gestão de risco e aborda como as organizações avaliarão o risco no contexto da Concepção. Ela identifica as vulnerabilidades internas e externas, as ameaças, o impacto para a organização caso uma ameaça explore uma vulnerabilidade e a probabilidade de ocorrência dessa ameaça. Como as possibilidades de identificação de riscos podem ser grandes, a visão no nível de missão, proporcionada pelo emprego da sistemática de AO, e uma priorização por meio de casos já ocorridos e da escolha de quais tarefas são as mais importantes a um meio, ajudarão a reduzir o espaço de possibilidades na identificação desses riscos.

A **Avaliação** também estabelecerá a frequência e a sistemática de coleta de informações para a avaliação de risco, o seu processamento e comunicação. Os riscos identificados podem

ser informações classificadas e por isso devem possuir o devido grau de sigilo. É importante um registro de dados sistematizado das tarefas que serão feitas nesse componente, para permitir avaliar o intervalo de tempo para se identificar um risco e propor uma ação correspondente. Isso irá determinar o tamanho das equipes de avaliação, no futuro, bem como planejar futuras avaliações de meios estabelecendo um cronograma exequível.

O terceiro componente da gestão de risco, a **Resposta**, trata de como as organizações respondem ao risco determinado nos resultados das avaliações de riscos. É nele que são desenvolvidas as linhas de ação para responder ao risco, bem como são implementadas as respostas a partir destas linhas de ação. Ela também identifica ferramentas, técnicas e metodologias para responder ao risco, e pode ser necessário treinamento especializado, aquisição de equipamentos ou mesmo contar com consultorias para lidar com isso.

No quarto componente da gestão de risco, a **Monitoração**, haverá a verificação se as respostas estão alinhadas com as tarefas dos meios, e determinada a eficácia das medidas de resposta. Também identificará alterações no ambiente previamente delineado e que possam vir a comprometer uma resposta, demandando uma revisão do risco pelos demais componentes de gerenciamento. Um aspecto importante é a rastreabilidade entre um risco e a respectiva monitoração. Devido ao número de riscos possíveis de serem identificáveis, esta rastreabilidade deverá ser feita com o apoio de algum software e dispondo de mecanismos de visualização com diferentes formas de apresentação.

Uma atividade importante a ser desenvolvida desde o início é o mecanismo de realimentação existente nos processos de gerenciamento de risco. Como ilustrado na Figura 1, ao longo do tempo novas vulnerabilidades e ameaças surgirão, e a realimentação é fundamental para que o grau de risco, seja qual for o nível da organização, possa ser gerido de

maneira adequada.

Um outro aspecto a ser considerado num segundo momento do processo de gerenciamento de riscos é a troca de informações com outros organismos, sejam eles governamentais ou não, que também cuidam de segurança cibernética de SCF. Essa troca deve se fundamentar numa relação de confiança e permitirá tomar conhecimento de novas vulnerabilidades ou ameaças e se antecipar na proteção dos SCF envolvidos.

4.3 O Programa de Implantação

A formação da estrutura proposta será feita por meio das recomendações descritas na Seção 3.5 que trata de um programa de segurança para SCF.

Inicialmente, o programa sugere iniciar com a motivação. O Capítulo 2 deste trabalho procurou mostrar que incidentes em SCF são uma realidade, podendo comprometer os processos físicos controlados por eles e causar efeitos danosos. A partir disso, escolhe-se um Caso de Negócio para Segurança alinhado com o emprego de algum meio, mostrando-se os efeitos que poderiam advir caso alguma vulnerabilidade seja explorada, ou seja, o impacto do risco.

O foco de Caso de Negócio não é identificar vulnerabilidades e sim estabelecer um senso de urgência, algo crucial para se obter a cooperação necessária a gerar uma mudança organizacional (KOTTER, 1997). A mudança pretendida é a implantação de um processo de gerenciamento de riscos para SCF voltado para meios operativos de superfície. Esse Caso deve ser feito em caráter experimental, com o intuito de demonstrar a aplicabilidade dos casos reais num sistema pertencente a um meio da MB. Devido ao grau técnico apresentado, este Caso requererá, além de pessoal do setor operativo, um grupo formado por especialistas

envolvendo pessoal de centros de manutenção e diretorias especializadas com conhecimento sobre o domínio a ser utilizado, bem como dos sistemas envolvidos.

Obtido o aval de prosseguir na implantação de um programa de gerenciamento de riscos para SCF, faz-se necessário designar o respectivo pessoal que irá planejar esse programa com o intuito de colocá-lo em execução. Apesar de não ser objeto desta pesquisa gerar uma nova organização responsável por desempenhar as atividades aqui propostas na estrutura da MB, e como ainda não existe tal organização, esta pesquisa sugere a formação de um núcleo no nível do Comando – em – Chefe da Esquadra, pois as experiências obtidas neste núcleo poderão, no futuro, serem disseminadas a outros meios de superfície e meios submarinos. Quanto ao pessoal que irá compor este núcleo, como os profissionais com capacidade técnica estão distribuídos por diversas organizações, caberia decidir colocá-los com dedicação exclusiva nesse núcleo para produzir os artefatos necessários ao programa. Também poderá ser necessário capacitar esse pessoal bem como visitar outros órgãos governamentais que já possuam programas similares.

Dentre os artefatos deste programa, destacam-se o escopo do programa, seus objetivos e as partes afetadas por ele. Apesar da necessidade desse programa cobrir a organização e se integrar a outros, no primeiro momento não se vislumbra um escopo muito grande para diminuir o próprio risco do programa. Assim, recomenda-se que o escopo do programa trate das Fragatas Classe Niterói, pois elas possuem uma gama de SCF, já fizeram dois ciclos de AO (um no recebimento e outro na modernização), e devido ao número de meios na classe, a execução das etapas do gerenciamento de riscos em cada navio da classe irá gerar aprendizado para os demais, permitindo formar uma base de conhecimento mais madura ao final.

A integração do programa deverá ser feita, principalmente, às normas já existentes sobre segurança de sistemas de informação, cuja principal norma é o EMA-416 – Doutrina de Tecnologia da Informação da Marinha (BRASIL, 2007).

No primeiro momento, os riscos estarão alinhados no nível da missão, obtido pela aplicação de alguns conceitos provenientes da sistemática de AO. Entretanto, num segundo momento esses riscos devem se alinhar ao nível de organização. Um aspecto importante é a documentação dos procedimentos de avaliação de riscos, respectivo registro dos dados coletados e estabelecimento de um mecanismo de revisão e atualização dos artefatos gerados.

Por fim, o programa irá gerar e implantar um arcabouço para o gerenciamento do risco de segurança em SCF, como descrito na Seção 4.2. Conforme proposto no escopo, esse arcabouço é limitado a um tipo de classe, mas precisará ser revisado para ampliar a sua aplicabilidade às demais classes de meios. Os controles de segurança a serem implementados, seguindo as recomendações previstas em normas já editadas, como NIST-SP-800-53 e IEC 62443, também serão revistos para cada classe de meio a ser incorporado nesse arcabouço.

4.4 Considerações

Neste capítulo, é definida a estrutura de gerenciamento de riscos que será instanciada por um programa de implantação. Este programa está descrito em alto nível e demandará a participação de diversos atores pertencentes a setores distintos da MB.

O programa proposto é um ciclo que, após executado, demandará outros que irão aumentar o nível do gerenciamento de risco, elevando-o para o nível organização, bem como ampliará o seu escopo cobrindo outros meios operativos.

Também vislumbra-se a parceria com órgãos de pesquisa e desenvolvimento na busca de soluções inovadoras e muitas vezes nacionais, a fim de reduzir uma possível dependência de produtos e serviços importados.

Como resultados futuros, pode-se considerar que os riscos serão utilizados em simuladores ora existentes, permitindo aos operadores vivenciarem os efeitos de uma ação maliciosa e o treinamento dos componentes de monitoração e resposta.

5 CONCLUSÕES

Os sistemas ciber-físicos empregados em meios operativos são uma parte essencial na relação entre o meio e seu desempenho. Ao longo do tempo, esses sistemas tendem a ser mais vulneráveis e, por isso, o risco aos meios também cresce, podendo afetar o cumprimento das tarefas a ele atribuídas. Para se contrapor às vulnerabilidades, a segurança desses sistemas deve ser planejada e executada permanentemente, integrando-a a outras políticas ora em vigor na MB.

Atualmente, no âmbito da MB, esses sistemas não possuem uma política dedicada para a sua segurança, bem como as suas especificidades não permitem empregar as normas existentes para a segurança de sistemas de TI. Entretanto, já há na literatura uma série de normas que consolidam a segurança de sistemas ciber-físicos e, em algumas dessas normas, há a participação de órgãos normativos brasileiros.

As normas indicam uma série de procedimentos e atividades que devem ser cumpridas com o intuito de planejar, implantar e executar um processo de gerenciamento de riscos contínuo. Todavia esses procedimentos devem ser instanciados na MB considerando as suas singularidades. Para isso, este trabalho sugere o emprego da sistemática de avaliação operacional como forma de:

– iniciar pelo nível de missão, em alinhamento com o nível da informação.

– permitir a priorização dos riscos que mais afetem ao cumprimento das tarefas dos meios.

– avaliar riscos decorrentes da interligação de sistemas e subsistemas.

– trazer uma sistemática de avaliação já em curso e madura na MB para ser empregada numa nova atividade da organização, com o intuito de diminuir o risco da implantação dessa nova atividade.

Para a MB, os reflexos da implantação de um processo de gerenciamento nesse nível permitirão compreender como os riscos, nos sistemas que compõem um meio, afetam a execução das suas tarefas, permitindo ao comando do meio ou mesmo de escalões mais elevados ter conhecimento do grau de vulnerabilidade de um conjunto de meios.

No longo prazo, um programa sistemático de gerenciamento de riscos permitirá avaliar os custos de sua manutenção e respectivo retorno e, num futuro, gerar uma base de conhecimento para a especificação de requisitos de segurança para novos meios, considerando a segurança desde a fase de projeto.

Para trabalhos futuros, prevê-se que a estrutura aqui proposta deverá evoluir a fim de definir requisitos de segurança para SCF a serem cumpridos por futuros meios operativos, ou seja, ainda na fase de projeto, o que permitirá empregar um maior número de soluções bem como integrar futuros meios na arquitetura de gerenciamento de riscos já utilizada. Ela também irá aumentar o seu escopo e incluir outros meios como submarinos, meios aeronavais e de fuzileiros navais.

REFERÊNCIAS

APPLEGATE, Scott D., **The Dawn of Kinetic Cyber** (CyCon), 5th International Conference on Cyber Conflict, Tallinn, Estônia, 2013, pp. 1-15.

AZEVEDO, Marcelo Teixeira. **Cibersegurança em sistemas de automação em plantas de tratamento de água**. São Paulo, 2010. 155 p. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos, Universidade de São Paulo, 2010.

BAYBUTT, Paul. **Sneak Path Security Analysis (SPSA) for Industrial Cyber Security**, Intech, p. 56, Vol. 51, Issue 9, Set. 2004.
. Disponível em:
<http://www.primatech.com/images/docs/paper_sneak_path_security_analysis_spsa_for_industrial_cyber_security.pdf>. Acesso em: 30 Jul. 2016.

BERNSTEIN, Sharon; BLANKSTEIN, Andrew. **Key signals targeted,** Times Staff Writers, 9 Jan. 2007. [Online]. Disponível em: <http://articles.latimes.com/2007/jan/09/local/me-trafficlights9>. Acesso em: 29 Jul. 2016.

BRASIL. Estado Maior da Armada. **Sistemática para Avaliação Operacional na Marinha do Brasil**: EMA-333, Brasília, DF, 2004.

BRASIL. Estado Maior da Armada. **Doutrina Básica da Marinha.** EMA-305 - 2ª revisão, Brasília, DF, 2014.

_____. Estado Maior da Armada. **Doutrina de Tecnologia da Informação da Marinha.** EMA-416 - 2ª revisão, Brasília, DF, 2007.

_____. Estado Maior da Armada. **Sistemática para Avaliação Operacional na Marinha do Brasil**: EMA-333, Brasília, DF, 2004.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**: MD31-M-07, Brasília, DF, 2014.

BRIGHT, Peter. **Stuxnet apparently as effective as a military strik,** ARS Technica Staff, 16 Dez. 2010. [Online]. Disponível em: <http://arstechnica.com/tech-policy/2010/12/stuxnet-apparently-as-effective-as-a-military-strike/>. Acesso em: 29 Jul. 2016.

CLEMENTS, Paul; NORTHROP, Linda. **Software Product Lines: Practices and Patterns**, 3 ed., Editora Addison-Wesley, 2001.

COBB, Pamela. **German Steel Mill Meltdown: Rising Stakes in the Internet of Things,** Security Intelligence, 14 Jan. 2015. [Online]. Disponível em: <https://securityintelligence.com/german-steel-mill-meltdown-rising-stakes-in-the-internet-of-things/>. Acesso em: 29 Jul. 2016.

CONKLIN, Arthur; WHITE, Greg. **CompTIA Security+**, 4 ed., Editora McGraw-Hill Education Group, 2014.

CRAWFORD, Michael. **Utility hack led to security overhaul,** Computerworld Australia, 16 Fev. 2006. [Online]. Disponível em: <http://www.computerworld.com/article/2561484/security0/utility-hack-led-to-security-overhaul.html>. Acesso em: 29 Jul. 2016.

EUA. **Cyber-Attack Against Ukrainian Critical Infrastructure,** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Department of Homeland Security. [Online]. Disponível em: <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01/>. Acesso em: 29 Jul. 2016.

FALCO, Marco De. **Stuxnet Facts Report: A Technical and Strategic Analysis**, CCDCOE, Tallinn, Estônia, 2012.

GREENEMEIER, Larry. **Heart-Stopper: Could Hackers Hit Pacemakers, Other Medical Implants?,** Cable News Network (CNN), 14 Mar. 2008. [Online]. Disponível em: <http://www.scientificamerican.com/article/heart-stopper-med-device-hack/>. Acesso em: 29 Jul. 2016.

ISO/IEC 15408 - **Common Criteria for Information Technology Security Evaluation**. Version 3.1 Revision 4. 2012.

IEC 62443-2-2 - **Security for Industrial Automation and Control Systems**. EUA, North Carolina, 2009.

KOTTER, John P. **Liderando Mudança**, 18 ed., Rio de Janeiro: Campus, 1997.

LEE, Edward A., **Cyber Physical Systems: Design Challenges, Object Oriented Real-Time Distributed Computing** (ISORC), 2008 11th IEEE International Symposium on Real-Time Computing, Orlando, FL, 2008, pp. 363-369.

LOUKAS, George. **Cyber-Physical Attacks: A Growing Invisible Threat**, Editora Butterworth-Heinemann, 2015.

MESERVE, Jeanne. **US Sources: Staged cyber attack reveals vulnerability in power grid**, Cable News Network (CNN), 26 Set. 2007. [Online]. Disponível em: <http://www.cnn.com/2007/US/09/26/power.at.risk>. Acesso em: 29 Jul. 2016.

MIL-STD 882E. **Standard practice for System Safety,** Departamento de Defesa dos EUA, EUA, Virginia, 2012.

NIST-SP-800-37 Rev. 1. **Guide for Applying the Risk Management Framework to Federal Information System,** Departamento de Comércio dos EUA, Maryland, EUA. Fev. 2010.

NIST-SP-800-39. **Managing Information Security Risk,** Departamento de Comércio dos EUA, Maryland, EUA. Abr. 2011.

NIST-SP-800-53 Rev. 4. **Security and Privacy Controls for Federal Information Systems and Organizations,** Departamento de Comércio dos EUA, Maryland, EUA. Abr. 2013.

NIST-SP-800-82 Rev. 2. **Guide for Industrial Control Systems Security,** Departamento de Comércio dos EUA, Maryland, EUA. Mai. 2015.

SCHNEIDER, David. **Jeep Hacking 101**, IEEE Spectrum, 6 Ago. 2015. [Online]. Disponível em: <http://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101>. Acesso em: 29 Jul. 2016.