DEFESA CIBERNÉTICA – SEGURANÇA PARA OS SISTEMAS CIBERFÍSICOS DOS MEIOS OPERATIVOS DE SUPERFÍCIE*

MARCO EUGÊNIO MADEIRA **DI BENEDITTO****
Capitão de Mar e Guerra (RM1)

SUMÁRIO

INTRODUÇÃO

Sistemas ciberfísicos (SCF) são sistemas em que ocorre a integração de computação e processos físicos (LEE, 2008). Em termos gerais, são sistemas que atuam na tarefa de controle de um processo físico e, de acordo com a teoria de controle, esses sistemas devem escolher as ações ao longo do tempo para influenciar o processo sob seu controle. Se a escolha dessas ações depende do processo a ser controlado, um SCF observa esse processo por meio de sensores de aquisição de dados, perfaz o controle empregando computadores para escolher as ações e, por meio de atuadores, efetiva as ações de controle sobre esse processo físico.

---

* Adaptação da monografia apresentada à Escola de Guerra Naval em 2016, com o título "Defesa cibernética: proposta de estrutura para o âmbito da MB".

** Doutor em Ciência da Computação na área de Engenharia de Software pela Universidade Federal do Rio de Janeiro. Mestre em Ciência da Computação na área de Engenharia de Sistemas pela Universidade de São Paulo. Comandou o Aviso de Instrução *Guarda-Marinha Brito*.

O uso de SCF é crescente, seja devido aos ganhos e 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 (MB), 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*. Em adição a esses, outros sistemas 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), e o Sistema de Controle e Monitoração das Corvetas da Classe *Inhaúma* (SCM), desenvolvido pelo Instituto de Pesquisas da Marinha (IPqM).

Segundo a Doutrina Militar de Defesa Cibernética (MD31-M-07), o espaço cibernético é o espaço virtual composto por dispositivos computacionais conectados em redes ou não, em que as informações digitais transitam, são processadas e/ou armazenadas. Num SCF, o espaço cibernético em questão pode conter as conexões internas e externas de um SCF, bem como o seu mecanismo de aquisição de dados, controle e respectivos atuadores. Um ataque a um SCF pode resultar em efeitos no respectivo processo físico. Segundo Loukas (2015, p. 12), "um ataque ciberfísico é uma brecha de segurança no espaço cibernético 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 vulnerabilidade, que terá como consequência um efeito no espaço físico.

Ao longo do seu ciclo de vida, para um SCF há um aumento na probabilidade de ele possuir alguma vulnerabilidade, e esse aumento decorre, principalmente, dos aspectos abaixo listados:

a) Emprego de tecnologias cada vez mais difundidas no mercado, sejam *softwares* ou *hardwares*, para o desenvolvimento dos sistemas ciberfísicos. 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 a serem empregados contra um SCF alvo. Alem disso, a lista de vulnerabilidades já conhecidas para estes componentes de *software* e *hardware* também passa a ser imediatamente possível de ser empregada.

b) O *software*, que permeia esses sistemas, pode ser 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 Navio-Aeródromo *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 esse mesmo componente de *software*. Um exemplo de componente de *software* que deve ser comum a esses sistemas é o responsável pelo enlace automático de dados (EAD) ou *link* de dados.

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 às necessidades de um segmento particular de mercado ou missão e que são desenvolvidos a partir de um conjunto comum de ativos (CLEMENTS; NORTHROP, 2001).

c) Ao longo do ciclo de vida, um meio pode ter alguns sistemas removidos, outros 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 ou de como ele seja instalado. Usando como exemplo uma antena de comunicação por satélite nas bandas Ku, Ka e X, numa rápida consulta a *sites* 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 de 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. A possibilidade de controlar a antena de dentro ou de fora do navio por meio do protocolo de internet aumenta o espaço cibernético e o risco de este equipamento sofrer ações maliciosas.

d) Devido à crescente necessidade de informações para a tomada de decisão, ao crescente emprego de sistemas de informação e SCF e à convergência tecnológica entre eles, tem-se o aumento da interconectividade entre esses sistemas. Essas interconexões formam redes e permitem a transferência de dados e o acesso de usuários. Assim o espaço cibernético onde os SCF e os Sistemas de Tecnologia da Informação (TI) estão contidos é alargado com o passar do tempo.

Atualmente, no âmbito da MB, os SCF não possuem uma política dedicada à sua segurança. As medidas de segurança atualmente em vigor na MB têm 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 TI, e deixa de considerar os seus efeitos nos processos físicos relacionados aos sistemas ciberfísicos.

Com o passar do tempo, os sistemas tendem a ser mais vulneráveis e, por isso, sua segurança deve ser planejada e executada permanentemente

Um outro aspecto interessante a destacar é o efeito desejado de ações no domínio cibernético definido tanto na Doutrina Militar de Defesa Cibernética (MD31-7) 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. Essas normas não consideram que as referidas ações também poderiam ter efeitos diretos no nível de processos físicos. Vê-se que, no domínio cibernético, ainda não está amadurecida a visão de possíveis efeitos cinéticos e, consequentemente, isso afeta a percepção de que os SCF também devem ser protegidos.

Como visto acima, os sistemas ciberfísicos são cada vez mais utilizados em meios operativos, bem como 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,

2 Orbit VSAT Antennas. Em: http://www.marinesatellitesystems.com/index.php?page_id=811#511. Acesso em: 30/7/2016.

por isso, sua segurança deve ser planejada e executada permanentemente. A motivação deste estudo decorre da alta dependência entre um SCF e um meio operativo, da crescente vulnerabilidade ao longo do tempo que ocorre nesse tipo de sistema e da falta de um procedimento sistemático no âmbito da MB para a sua segurança.

O objetivo deste artigo é apresentar os riscos de uma falta de segurança em SCF e propor atividades e uma abordagem de implantação dessas atividades para aprimorar a segurança de SCF existentes na MB, em especial naqueles sistemas utilizados nos meios operativos de superfície atualmente incorporados e em uso.

Nesse sentido, o restante deste trabalho está organizado da seguinte forma. No título 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 título 3 são tratados a fundamentação de segurança para SCF e os respectivos trabalhos que visam promover a segurança destes sistemas. No título 4 é apresentada a proposta de atividades. Finalmente, nas conclusões são discutidas a implantação dessas atividades e trabalhos futuros.

VALIDAÇÃO EM CASOS REAIS

A tecnologia de SCF tem sido empregada por um amplo espectro de setores e foram projetados para ter 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, não houve melhora na segurança.

Nesta seção serão descritos alguns desses casos em que uma ou mais vulnerabilidades foram exploradas, causando efeitos nos respectivos processos físicos. Esses casos foram validados em ambiente de laboratório, por meio de experimentação, e também no ambiente real, com ações por agentes maliciosos.

Projeto Aurora (*MESERVE, 2007)* – O Department of Homeland Security (DHS), órgão governamental dos Estados Unidos da América (EUA), 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 com capacidade de geração aproximada de 2 MW. No experimento, os pesquisadores, por meio de uma ação cibernética, abriram e fecharam os disjuntores do gerador fora de sincronia, variando rapidamente a carga e, consequentemente, maximizando o estresse mecânico. Esse estresse gerou vibrações mecânicas tão intensas que o gerador foi perdendo uma série de partes e, em três minutos, ocorreu um dano catastrófico.

Carro Comercial (*SCHNEIDER, 2015***) – Em julho de 2015, dois pesquisadores de segurança conduziram um experimento em que foram capazes de controlar, por meio de uma conexão sem fio, um carro do modelo Jeep Cherokee em movimento. Essa conexão sem fio era provida por meio da rede de dados de telefonia celular, disponibilizada pela central multimídia do carro.

Inicialmente os pesquisadores assumiram o controle do sistema de entretenimento provido pela central multimídia e do limpador de para-brisas. Em seguida, eles

conseguiram controlar o ar-condicionado, desativar o acelerador – inibindo os comandos do motorista via pedal – e acionar os freios do carro.

Após esses dois exemplos experimentais, serão descritas ações maliciosas promovidas com o intuito de causar algum prejuízo ou dano de forma deliberada, a partir dos efeitos cinéticos decorrentes dessas 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, num dia de manutenção, eles perceberam que, após reprogramarem os sistemas de bombeamento, este era alterado. Após a contratação de uma firma de detetives e a comunicação do ocorrido à polícia, o ex-empregado foi capturado e ficou comprovada sua ação maliciosa.

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 serie 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 do tempo de sinal verde nas vias de menor fluxo. Como consequência, houve grandes congestionamentos na cidade, especialmente próximos ao aeroporto. Embora não tenham ocorrido acidentes entre veículos devido a este incidente, ele poderia facilmente resultar em efeitos cinéticos.

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 seu alto-forno. De acordo com esse relatório, o ataque usou engenharia social e técnicas de *spear-phishing*[3] para convencer o destinatário das mensagens a abrir um anexo ou visitar um *site* 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 pôde ser desligado corretamente.

Após esses exemplos, será descrito um dos mais famosos, se não o mais famoso, ataques cibernéticos de efeitos cinéticos de que se tem conhecimento.

Usina de Enriquecimento de Urânio, em Natanz, Irã (*FALCO, 2012)* – Em 2010, começaram a surgir na mídia histórias de um novo *worm*, denominado Stuxnet, que ainda não havia sido descrito. Um *worm* é um programa malicioso que tenta penetrar redes e sistemas de computadores. Quando um *worm* consegue entrar, ele se replica, a

3 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, fazendo-se 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 fazer parte de um mesmo departamento numa empresa (CONKLIN; WHITE, 2014).

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[4], e foi descoberto em 17 de junho de 2010 por uma firma de segurança da Bielorussia.

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 à destruição das centrífugas de enriquecimento. Ele alterava a frequência dos conversores entre 1.410 Hz, depois 2 Hz e 1.064 Hz, 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.

O Stuxnet foi cuidadosamente desenvolvido e é um *malware* especificamente orientado. Para se chegar a esse resultado, o projeto de desenvolvimento do Stuxnet deve ter envolvido muitos especialistas, tanto no domínio cibernético, para sobrepujar os mecanismos de segurança, quanto no domínio nuclear, para atuar nos mecanismos de controle do processo de enriquecimento.

O ataque à usina de enriquecimento de urânio no Irã serve como exemplo operacional do uso de armas cibernéticas cinéticas, e seu sucesso pode ter dado início a uma nova corrida armamentista, ou melhor, ciberarmamentista, entre os programas de desenvolvimento de guerra cibernética dos Estados.

Esses ataques revisados ilustram que os efeitos cinéticos são uma ameaça válida e crível. O Projeto Aurora mostra que equipamentos de geração de energia precisam ter o seu risco avaliado do 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, nas turbinas de propulsão, nos geradores de energia e nos respectivos mecanismos de controle.

As lições decorrentes do experimento com o carro, que permitiu um controle elevado do mesmo, e do controle de tráfego em Los Angeles mostram que o aumento da interconectividade de sistemas, assim como a sua integração com demais componentes internos, deve ser acompanhada de uma avaliação de riscos sistemática e 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, ambos podem ser explorados a distância, e a integração sem a devida proteção traz novas vulnerabilidades, como, no caso do automóvel, o controle de pontos críticos.

Como ilustrado no caso do Sistema de Águas e Esgoto na Austrália, um aspecto a ser observado é o acesso de pessoas aos SCF, o que incrementa a necessidade de uma política de pessoal voltada para a segurança desses sistemas[5], em especial para terceiros envolvidos na manutenção desses sistemas.

4 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.

5 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.

O exemplo do alto-forno na Alemanha mostra que as redes de controle precisam de proteção intra-rede e inter-rede. As ligações da rede de um SCF com a rede administrativa, se forem necessárias, devem ter seu risco avaliado, e devem ser tomadas as devidas ações para se mitigar os riscos identificados.

O ataque à usina de enriquecimento executado por meio do *malware* Stuxnet, apesar de acarretar num efeito considerável, não significa que seja fácil desenvolver tal tipo de *malware*, haja vista as dificuldades para o seu desenvolvimento e emprego. Entretanto, esse evento acarretou na revisão de normas de segurança, como as normas da serie ISA/IEC- 62443, aperfeiçoando suas recomendações e os processos a serem adotados com o intuito de elevar a segurança de SCF.

Considerando os SCF hoje empregados na MB, a possibilidade que vulnerabilidades similares existam e que ameaças façam uso delas só aumenta com o tempo. Nesse sentido, pode-se identificar alguns possíveis pontos a serem tratados na MB. Ao longo do ciclo de vida, novos componentes são atualizados ou adicionados a SCF 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. Como exemplo, pode ser citado um sistema de armas que, ao ser atualizado, passe a utilizar um sistema operacional de tempo real comercial e de uso mais amplo, empregue processadores comerciais de uso comum na indústria e faça uso de um barramento para troca de dados com tecnologia e padrões de mercado. Este mesmo sistema de armas pode vir a receber um novo componente em seu barramento, para coletar dados relacionados a sua manutenção, e esse componente ser baseado num computador pessoal executando uma distribuição Linux como sistema operacional.

Num futuro breve, os submarinos 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[6].

Num futuro breve, os submarinos e os novos navios disporão de sistemas de gestão da plataforma com alta integração entre os diversos subsistemas componentes do meio

FUNDAMENTOS DE SEGURANÇA PARA SISTEMAS CIBERFÍSICOS

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

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

Nos dias atuais há uma ampla disponibilidade de dispositivos de baixo custo empregando o Protocolo de Internet (IP) e que agora estão substituindo as soluções proprietárias antes utilizadas em 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 o 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 aos sistemas de TI, mas leva a um decréscimo significativo no isolamento de um SCF do mundo exterior, criando 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 a alguma distância, sem ter acesso físico direto ao equipamento.

Os processos de segurança para SCF devem considerar os aspectos de TI, de processos físicos e da interseção entre eles

Como visto na validação em casos reais, tanto o meio cibernético quanto o processo físico possuem vulnerabilidades que podem ser exploradas e, consequentemente, acarretar em efeitos cinéticos. Essa combinação do meio físico com o cibernético leva a processos de segurança que contemplam os dois meios, mas cada um possui as suas singularidades. Os processos de segurança para SCF devem considerar os aspectos de TI, de processos físicos e da interseção entre eles.

Para sistemas de TI, a segurança é entendida como a união de três macroatividades, que são: prevenção, detecção e resposta (CONKLIN; WHITE, 2014). Cada técnica de segurança ou tecnologia aplicada à segurança pode ser vista em uma ou mais destas atividades, e os objetivos da segurança são a confidencialidade, a integridade e a disponibilidade dos dados nos sistemas. 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, ou seja, a detecção, de modo a permitir que os meios para se resolver o problema possam ser adequadamente empregados, isto é, que a resposta seja executada.

Empregando um conceito de segurança mais genérico, 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 sobre como sistemas que controlam processos físicos são projetados e operados. No caso de SCF em meios operativos, pode-se acrescentar o risco no emprego e desempenho dos meios.

Ao longo do tempo, algumas normas sobre a segurança de SCF já foram publicadas. Mais especificamente, dentro dessa categoria de sistemas, essas normas visam aos Sistemas de Controle Industrial

(ICS[7]), ao Sistema de Supervisão e Aquisição de Dados (SCADA[8]), aos Sistemas de Controle Distribuído (DCS[9]) e a outras configurações de sistemas de controle, tais como as que incorporam CLP. Segundo a norma IEC 61131[10], um CLP é uma solução proprietária de *hardware* e *software* para aquisição de dados e controle de processos. Um 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, os componentes empregados na sua implementação e programação – o *software* – têm forte similaridade com os SCF utilizados em meios operativos de superfície, como o controle da propulsão executado pelo SCMPA. 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 os títulos traduzidos, 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- 62.443[12].

A norma NIST 800-82 é editada pelo National Institute of Standards and Technology (NIST) do Departamento de Comércio dos EUA. Já a norma ISA/IEC 62.443 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. Ao longo dessas normas, outras são citadas para referenciar conceitos já empregados em áreas como o gerenciamento de riscos e segurança de sistemas de TI.

Considerando uma organização como a MB, e aderente a sua estrutura organizacional hoje vigente, este trabalho tratará de aspectos relacionados ao processo de gerenciamento da segurança de sistemas ciberfísicos, a partir de uma visão de mais alto nível. Desse ponto de vista, este processo poderá ser instanciado e especializado nos meios operativos, quando deverão ser empregados detalhes mais técnicos também previstos nessas normas e em outras mais especializadas.

Antes de abordar o processo para a segurança de SCF, será feita uma breve comparação entre SCF e sistemas de TI para se destacar as particularidades entre ambos.

Comparação entre SCF e Sistemas de TI

Um SCF controla o mundo físico, enquanto sistemas de TI gerenciam dados. As características que os diferem incluem os riscos e prioridades, e, a partir da norma NIST-800-82, pode-se destacar uma série de aspectos comparativos entre SCF e sistemas de TI que serão descritos a seguir.

Em geral, SCF possuem requisitos de desempenho e são sistemas de tempo real críticos, isto é, quando o prazo para exe-

7 Do inglês *Industrial Control System – ICS*.
8 Do inglês *Supervisory Control and Data Acquisition – SCADA*.
9 Do inglês *Distributed Control System – DCS*.
10 Esta norma é um padrão para Controlador Lógico Programável (CLP).
11 Do inglês *Guide for Industrial Control Systems Security*.
12 Do inglês *Security for Industrial Automation and Control System*s.

cução de uma tarefa não pode ser violado. Em geral esses 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.

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 sua 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, a integridade e a disponibilidade. Para os SCF, as preocupações são a segurança da vida humana, a perda de equipamento, perda de produtos e da produção, a tolerância à falha para prevenir danos e a aderência às 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, e o entendimento dos efeitos sobre esses processos 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. A característica de trabalhar em tempo real e com dispositivos de capacidade de processamento variável torna os SCF um tipo de sistema com recursos restritos, sem que se possam incorporar algumas capacidades de segurança existentes em sistemas de TI, como, por exemplo, incitação e registro de erros (*logging*).

A gerência de mudanças é importante para manter a integridade de um sistema, seja ele de TI ou um SCF, pois um *software* desatualizado representa uma das maiores vulnerabilidades. 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, e um agendamento de uma atualização pode precisar ser feito com antecedência a fim de não comprometer o processo físico devido a uma parada. Uma outra particularidade é que alguns produtos podem utilizar um *software* sem manutenção do fabricante, por ter sido descontinuado, ficando, por isso, sem possibilidade de atualização.

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, e soluções de segurança de terceiros podem não ser permitidas devido à licença de uso, ou por causa da perda da assistência devido à utilização de um produto de terceiro.

O tempo de vida de um componente de TI típico é da ordem de três a cinco anos, podendo ser menor devido à rápida evolução tecnológica. Para SCF em que a tecnologia é desenvolvida para atender a requisitos bem específicos de uso e implementação, o tempo de vida dos itens pode ser de dez a 15 anos.

Gerenciamento de Riscos

A maneira de tratar a segurança dos SCF é por meio de um processo de 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 como um processo de tomada de decisão, em que: é determinado o que pode ocorrer ao negócio, avaliado o impacto caso isso 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 na norma ISO/IEC 15408, que trata da Avaliação de Segurança de Tecnologia da Informação. Um risco é a possibilidade de sofrer uma perda ou prejuízo. O gerenciamento de risco é o processo completo de tomada de decisão para identificar ameaças, 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 a qual alguém, ou uma 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 prevenir, detectar ou mitigar o risco associado a uma ameaça.

Esses conceitos podem ser vistos e relacionados entre si 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 essas 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 desses riscos. Como surgem continuamente novas ameaças ao longo do tempo, a avaliação de riscos deve ser uma atividade periódica.

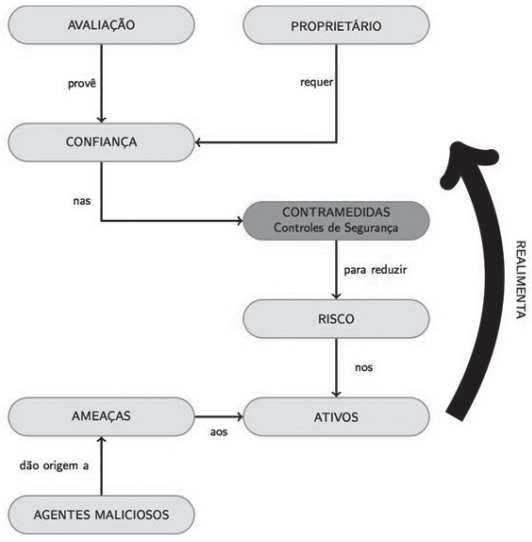

Figura 1: Conceitos de alto nível e relações entre si (adaptado da norma ISO/IEC 15408)

Gerenciar risco é uma atividade que requer o envolvimento de toda uma organização desde o mais alto nível, com a visão e os objetivos estratégicos, passando pelos profissionais no nível médio, planejando e gerenciando projetos, até os indivíduos na linha de frente, que operam os sistemas.

De acordo com a norma NIST-800-82, esse gerenciamento é um macroprocesso, distribuído por toda uma organização, e com os seguintes componentes:

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 constante.

O componente de Concepção consiste no desenvolvimento de um arcabouço para a tomada de decisões no gerenciamento de risco, bem como no 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.

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, com o risco identificado. 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 à 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, afetando os demais componentes desse processo.

Esses diferentes componentes servem para facilitar a visão do macroprocesso de gerenciamento de riscos da organização, agrupando uma série de atividades ao longo dela. A norma NIST-800-39 (Gerenciamento do Risco de Segurança da Informação[13]) propõe empregar uma abordagem em camadas para visualizar esse processo. 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 missão e processo de negócio; e

3) nível sistema de informação.

O processo é conduzido e visto pelas três camadas, atendendo aos seus objetivos e contribuindo para um 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, cujos objetivos devem contribuir e estar alinhados com o nível organização. Esse nível provê, ainda, a priorização de missões

13 Do inglês *Managing Information Security Risk*.

e funções, o que, por sua vez, leva às estratégias de recuperação de sistemas críticos.

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

Por fim, no nível sistema de informação os riscos são guiados pelo contexto e pelas decisões das camadas superiores. Na norma NIST-800-37 (Guia para a Aplicação do Arcabouço de Gerenciamento de Riscos em Sistemas de Informações Federais: uma abordagem de Ciclo de Vida para Segurança[14]), é proposto um arcabouço de gerenciamento de riscos para o nível sistema de informação.

Na Figura 2 está ilustrada a sequência das atividades do arcabouço de gerenciamento de riscos no nível de sistema de informação. Esse arcabouço é um processo que prevê uma sequência de atividades e que se realimenta. Ele começa na atividade 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[15] para os sistemas, fundamentado na categorização anterior. Uma revisão e um refinamento desse conjunto base podem ser necessários, baseando-se na avaliação de riscos da organização e das condições locais. Escolhidos os controles de segurança, eles serão implementados e também deverá ser descrito o emprego destes com os sistemas de informação e o ambiente de operação. Os controles de segurança são avaliados usando-se procedimentos 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. A operação dos sistemas é autorizada, baseada na determinação dos riscos ao funcionamento da organização, aos indivíduos e aos ativos e na decisão de quais riscos são aceitáveis. Finalmente os controles de segurança dos sistemas são monitorados de modo contínuo; as mudanças no sistema, inclusive no ambiente de operação, são documentadas; são conduzidas análises de impacto de segurança das mudanças e é relatado aos responsáveis o estado de segurança do sistema.

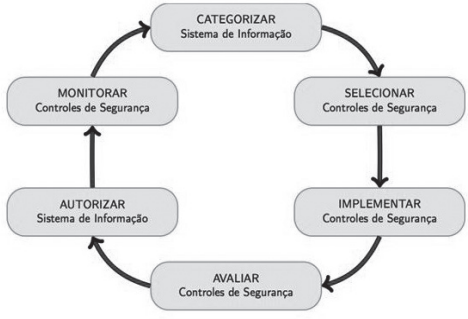

Figura 2: O gerenciamento de riscos no nível informacional (adaptado de NIST-800-37)

Um controle de segurança, ou contramedida, é uma medida tomada para prevenir, detectar ou mitigar o risco.

Devido à característica de um SCF atuar no meio físico, os efeitos decorrentes de uma falha neste tipo de sistema podem acarretar em danos no meio físico. Desse modo, juntamente

14 Do inglês *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

15 Um controle de segurança, ou contramedida, é uma medida tomada para prevenir, detectar ou mitigar o risco.

com os controles, que foram gerados para sistemas de TI, a norma ISA/IEC 62.443, já citada anteriormente e voltada para SCF, é utilizada em conjunto para atender a especificidades de segurança de SCF. Assim, será feita uma revisão das metodologias aplicáveis à identificação do impacto de riscos para SCF.

Aspectos específicos para SCF

Como visto anteriormente, segurança é a ausência de condições que possam causar morte, lesões, danos ou perda de equipamentos ou propriedade, ou danos ao meio ambiente. Esse conceito de segurança é o principal fator que afeta as decisões de como os sistemas que controlam processos físicos são projetados e operados. Desta forma, no componente avaliação 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 num risco no meio físico. Seguindo a norma NIST 800-82, a avaliação do potencial 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.

Entre as abordagens propostas na literatura para auxiliar na avaliação potencial de incidente destacam-se a Análise do Modo e Efeito de Falha (FMEA)[16], a Análise de Árvore de Falhas (FTA)[17] e a Sneak Path Analysis (SPA) (BAYBUTT, 2004). Esses tipos de análise empregam dados de projeto dos sistemas em questão.

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

FMEA – contém cinco elementos básicos:

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 for o método de análise, todos fornecem diferentes resultados na identificação do impacto no meio físico e demandam uma série de informações sobre

16 Do inglês Failure Mode and Effect Analysis – FMEA.
17 Do inglês Fault Tree Analysis – FTA.

os sistemas analisados, incluindo dados de projeto e especificações, bem como profissionais qualificados e com conhecimento do domínio em que o SCF é empregado.

Considerações

Um produto de segurança ou uma tecnologia não pode proteger adequadamente um SCF. A proteção deste tipo de sistema é calcada na combinação de políticas de segurança nas respectivas implementações, nas quais estarão incluídos os produtos e tecnologias.

Como visto até agora, as normas revisadas anteriormente procuram tratar da segurança de SCF olhando para a organização como um todo e 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 ininterrupta e contendo um mecanismo de realimentação capaz de contribuir para a melhoria contínua do próprio gerenciamento de riscos para os SCF e, com isso, aperfeiçoar o gerenciamento de riscos de toda a organização. A partir do "o que" deve ser feito, obtido da revisão das normas enumeradas, cabe questionar como fazê-lo.

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?

– Quais 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, será apresentada a proposta de atividades a ser empregada na proteção de SCF embarcados em meios operativos, considerando os conceitos e aspectos revisados anteriormente.

PROPOSTA DE ATIVIDADES PARA A SEGURANCA DE SCF 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. Anteriormente 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 suas diferenças em relação a sistemas de TI e às singularidades em relação a sua segurança.

Considerando o problema definido neste trabalho e a revisão dos conceitos para a proteção de SCF, nesta parte serão propostas as atividades a serem desenvolvidas para estabelecer a proteção de SCF em meios operativos da MB e uma abordagem para a implantação dessas atividades, sem tratar da estrutura organizacional, na MB, que se responsabilizará por essas atividades. Esta proposta leva em conta os seguintes condicionantes, decorrentes do estado atual:

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 desses sistemas, bem como de visão, em qualquer nível organizacional, dos riscos ao cumprimento dos objetivos e missões atribuídos aos meios.

O processo de gerenciamento de riscos anteriormente descrito prevê que este

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. Com este alinhamento ficará mais claro como subsistemas interagem para entregar um resultado de maior valor e os respectivos riscos à execução de tarefas e ao desempenho nas tarefas poderão ser melhor visualizados pelo comando do navio.

O nível mais alto, o organizacional, 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 deste nível e espera-se que o mesmo aconteça num momento posterior, após os níveis de missão e informacional terem sido estabelecidos.

Assim, considera-se que, num primeiro momento, as atividades propostas cubram os níveis informacional e de missão para, num momento posterior e após a consolidação desses dois níveis, elas possam vir a evoluir e cobrir a visão no nível da organização.

Para instanciar a visão no nível de missão, este trabalho sugere que se empregue a Sistemática para Avaliação Operacional (AO) na MB, descrita na publicação EMA-333 (BRASIL, 2004).

O emprego da Sistemática para AO no gerenciamento de riscos é a visão num nível mais elevado que o informacional e considera requisitos de desempenho. Outro aspecto que também corrobora o emprego da Sistemática de AO no gerenciamento de riscos é a composição de sistemas e os riscos derivados da ligação entre esses sistemas, que não poderiam ser vistos olhando-se para cada sistema individualmente. Num sistema de armas, uma série de subsistemas pode ser empregada 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 voo.

Sistemática para Avaliação Operacional

A Sistemática para AO na MB 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 em que 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 é considerada para se entender o problema e formular um plano de avaliação. Esses documentos são compostos pelos Requisitos de Estado-Maior (REM), pelos Requisitos de Alto Nível dos Sistemas (RANS), pelas Especificações de Alto Nível dos Sistemas (EANS) e pelos 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 de tarefa(s), ameaça(s), cenário(s) e função(ões), previsto(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 dos SCF no nível da missão dos meios.

Gerenciamento de riscos

Os componentes indicados para o gerenciamento de riscos descritos anteriormente ficariam instanciados da forma a seguir. A Concepção irá estabelecer uma base para a gestão de risco, definindo o escopo dentro da organização. Devido à ausência de um gerenciamento de riscos anterior, num primeiro momento se considera a tolerância ao risco a condição mínima de funcionamento de um meio. As premissas quanto ao risco, que inclui as suposições sobre as ameaças e vulnerabilidades, podem ser simples e pouco numerosas no início do gerenciamento e guiadas pela Sistemática de AO. Esta também ajudará na definição das prioridades e dos compromissos, como a importância relativa da tarefa e, as compensações entre diferentes riscos e prazos que a organização tenha para tratar os riscos. Essas premissas também farão 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. Como as possibilidades de identificação de riscos são grandes no nível informacional, a visão no nível de missão, proporcionada pelo emprego da sistemática de AO, e uma priorização de quais tarefas são as mais importantes a um meio ajudarão a reduzir o espaço de possibilidades na identificação desses riscos e a dar prioridade àqueles que possuem um maior impacto no desempenho dos meios. Nesse componente podem ser empregadas as técnicas descritas para a avaliação potencial de incidentes, como a FMEA e FTA.

A Avaliação também estabelecerá a frequência e a sistemática de coleta de informações para a avaliação de risco, o seu processamento e sua 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 realizadas neste componente, para permitir avaliar o intervalo de tempo para se identificar um risco e propor uma ação correspondente. Isso irá determinar, no futuro, o tamanho das equipes de avaliação, bem como ajudará a 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, definidos e implantados os controles de segurança, bem como são implementadas as respostas a partir destas linhas de ação. Aqui a tarefa é mais técnica e precisará de uma equipe especializada e multidisciplinar. Um aspecto importante a relembrar é a situação dos meios, que já estão em operação, e por isso nem todo tipo de controle pode ser implantado. Também 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 será 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 identificados, esta rastreabilidade devera 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 processo de realimentação. Como ilustrado na Figura 1, ao longo do tempo novas vulnerabilidades e ameaças surgirão, bem como novos casos ocorrerão em outras Marinhas e SCF similares. A realimentação é fundamental para que o grau de risco, seja qual for o nível da organização, possa ser gerido de maneira adequada. Esta realimentação também pode ser vista do lado de fora da organização. Por exemplo, num segundo momento do processo de gerenciamento de riscos pode-se iniciar a troca de informações com outros organismos que também cuidam de segurança cibernética de SCF, fundamentando-se essa troca numa relação de confiança, o que permitirá que se tome conhecimento de novas vulnerabilidades ou ameaças e que se antecipe na proteção dos SCF envolvidos.

O Programa de Implantação

Inicialmente, o programa sugere iniciar com a motivação por meio de um Caso de Negócio para Segurança. O foco do Caso de Negócio é estabelecer um senso de urgência, em vez de identificar vulnerabilidades, algo crucial para se obter a cooperação necessária para 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 em casos reais num SCF 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, os sistemas envolvidos e o domínio cibernético.

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 sugerida a criação de uma nova organização responsável por desempenhar as atividades aqui propostas na estrutura da MB, e como ainda não existe um órgão com esta responsabilidade, sugere-se a formação de um núcleo no nível do Comando em Chefe da Esquadra, pois as experiências obtidas neste núcleo poderão, no futuro, ser disseminadas a outros meios operativos subordinados. Quanto ao pessoal que irá compor este núcleo, atualmente os profissionais na MB com capacidade técnica estão distribuídos por diversas organizações, e caberia decidir colocá-los com dedicação exclusiva para produzir os artefatos necessários ao programa. Também poderá ser preciso capacitar esse pessoal, bem como visitar outros órgãos governamentais que já possuam programas similares.

Entre os artefatos deste programa, destacam-se o seu escopo do programa, seus objetivos e as partes afetadas por ele. Apesar da necessidade deste progra-

ma cobrir a organização e se integrar a outros, para diminuir seu próprio risco 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 irá gerar aprendizado para os demais da classe, permitindo formar uma base de conhecimento mais madura ao final.

A integração do programa deverá considerar, principalmente, as normas já existentes sobre segurança de sistemas de informação, sendo a principal delas o EMA-416 – Doutrina de Tecnologia da Informação da Marinha (BRASIL, 2007).

Considerações

Nesta parte, foi destacado como os componentes do processo de gerenciamento de riscos devem ser instanciados para serem implantados. Este processo foi descrito em alto nível e demandará a participação de diversos atores pertencentes a setores distintos da MB. O processo deverá ser cíclico e, ao longo do tempo, aumentará 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.

CONCLUSÕES

Os sistemas ciberfísicos 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 a execução das tarefas a eles atribuídas. Para se contrapor às vulnerabilidades, a segurança desses sistemas deve ser planejada e executada permanentemente, integrada a outras políticas ora em vigor na MB.

Atualmente, no âmbito da MB esses sistemas não possuem uma política dedicada à sua segurança e 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 ciberfísicos e, em algumas dessas normas, há participação de órgãos normativos brasileiros.

As normas internacionais revisadas aqui 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 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 a execução 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 e, consequentemente, dos riscos ao cumprimento de alguma missão.

A 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. Isso permitirá que se empregue um maior número de soluções voltadas para a segurança, bem como integrar futuros meios na arquitetura de gerenciamento de riscos já utilizada, que aumentará o seu escopo e incluirá outros meios, como submarinos, aeronavais e de fuzileiros navais.

🗁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<GUERRAS>; Guerra cibernética; Sistema de comando; Tecnologia da Informação; Informática;

REFERÊNCIAS

APPLEGATE, Scott D., The Dawn of Kinetic Cyber (CyCon), 5th International Conference on Cyber Conflict, Tallinn, Estonia, 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/metrafficlights9>. 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.

CLEMENTS, Paul; NORTHROP, Linda. Software Product Lines: Practices and Patterns, 3ª-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-internetof-things/>. Acesso em: 29 Jul. 2016.

CONKLIN, Arthur; WHITE, Greg. CompTIA Security+, 4ª 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, Estonia, 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, 18ª 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, Cabl e News Ne twor k (CNN) , 26 Se t . 2007. [Onl ine] . 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-800-82 Rev. 2. Guide for Industrial Control Systems Security, Departamento de Comercio 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.