DOI: 10.48011/sbse.v1i1.2475

Modelagem da segurança da informação em sistemas de automação e controle industriais: estudo de caso com a planta MecatrIME

Christiana Couto, Gustavo Claudio Karl Couto, Antônio Eduardo Carrilho da Cunha

Instituto Militar de Engenharia
Praça General Tibúrcio, 80, 22290-270, Praia Vermelha, Rio de Janeiro, RJ, Brasil.
(christianacouto,gustavokcouto,carrilho@ime.eb.br).

Abstract: In industrial environments, devices such as actuators and sensors are connected to the internet and the corporate network to optimize system management. This connection to external networks opens a path for malicious attacks that could harm the system. To study solutions for this scenario, a risk modeling was conducted on the MecatrIME computer integrated manufacturing platform of the Mechatronics Laboratory of the Military Institute of Engineering (IME). A security strategy was devised based on the station infected desconection, that was tested using a simulation tool. The results simulations under various attack scenarios were analyzed for evaluation of the proposed solution. The disconnected stations were protected from the attacks and, in addition, there was a decrease in the risk exposure rate and increased the time to compromise at stations that remained connected to the system. Besides that, some pre-configured security configurations were activated on the tool resulting in protection against the ARPPoisoning attack and mitigation of the other attacks effects.

Resumo: Em ambientes industriais, dispositivos, como atuadores e sensores, estão conectados à internet e à rede corporativa para otimizar a gestão do sistema. Essa conexão com redes externas abre um caminho para ataques mal intencionados que podem prejudicar o sistema. Para estudar soluções para esse cenário, foi implementada uma modelagem de riscos de ataques na plataforma de manufatura integrada por computadores MecatrIME, do Laboratório de Mecatrônica do Instituto Militar de Engenharia (IME). Uma estratégia de segurança foi elaborada, baseada na desconexão das estações atingidas. Foram realizadas simulações utilizando uma ferramenta e os resultados sob vários cenários de ataques foram analisados para a avaliação da solução proposta. As estações desconectadas foram protegidas dos ataques e, nas estações que se mantiveram conectadas ao sistema, houve diminuição na taxa de exposição ao risco e aumento do tempo médio de comprometimento. Além disso, ao ativar configurações de segurança predefinidas na ferramenta, houve proteção contra o ataque *ARPPoisoning* e mitigação dos efeitos dos outros ataques.

Keywords: Industrial automation and control systems; Modeling; Cyber-physical systems; Computer integrated manufacturing; Cybersecurity; Control plant; Electrical networks;

Palavras-chaves: Sistemas de controle e automação industriais; Modelagem; Sistemas ciber-físicos; Manufatura integrada por computadores; Segurança cibernética; Planta de controle; Redes elétricas;

1. INTRODUÇÃO

No século passado, em sistemas de controle e automação industriais (*Industrial Automation and Control Systems* - IACS), não havia um sistema de proteção de dados e dispositivos, como atuadores e sensores, não estavam conectados a uma rede integrada. Como esses sistemas estavam isolados, não houve uma especialização na elaboração dos protocolos de comunicação para proteger os equipamentos de possíveis ataques cibernéticos.

Mas com o tempo, esses dispositivos foram conectados à internet e à rede corporativa a fim de melhorar o gerenciamento do sistema. Essa conexão com redes externas abriu caminho para ataques mal intencionados, que podem prejudicar o sistema, porque agentes mal intencionados podem ter acesso à informação transmitida e causar problemas de segurança e privacidade.

O fato de serem sistemas ciber-físicos (*Cyber-Physical Systems*) (Refsdal and et al., 2015) difere os IACS dos

⋆ O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, utilizou infraestrutura computacional financiada com recursos do subprojeto Pesquisa cibernética do Projeto Estratégico do Exército Brasileiro e da Financiadora de Estudos e Projetos (FINEP).

sistemas tradicionais de tecnologia da informação porque, se os atacantes se apossarem da informação e adulterá-la, podem criar problemas físicos como acionamento ou desligamento indevido de equipamentos. Alguns exemplos de classes de ataques que podem ser explorados em IACS são negação de serviço (*Denial of Service* - (DoS)) e *Man-in-the-middle* (Zhu and Sastry, 2011).

Este trabalho apresenta uma modelagem e estratégias de segurança para a análise de risco de ataques cibernéticos em sistemas de automação e controle industriais. Foram realizadas simulações utilizando a ferramenta comercial SecuriCAD® da Foreseeti$_AB$ (2018) para comparar a disponibilidade do sistema modelado com e sem o uso de estratégias de defesa que são a desconexão das estações atingidas pelos ataques e o uso de diversos mecanismos de defesa predefinidos na ferramenta. A análise dos dados obtidos com as soluções propostas validou as estratégias.

Este trabalho está dividido em cinco seções, além desta introdução: na seção 2, são abordados os IACS; na seção 3, são apresentadas as particularidades da segurança da informação nesses sistemas; a seção 4 descreve a modelagem da plataforma MecatrIME e as simulações realizadas; na seção 5, são apresentados e discutidos os resultados e, por fim, na seção 6, são apresentadas as conclusões do trabalho.

2. SISTEMAS DE AUTOMAÇÃO E CONTROLE INDUSTRIAIS

Nesta seção, serão descritos alguns conceitos básicos sobre IACS, explicitando o *hardware*, o *software*, o funcionamento e a utilização de um modelo ideal. Uma configuração de um IACS típico, um sistema de gerenciamento de redes e os sistemas de supervisão e aquisição de dados (*Supervisory Control and Data Acquisition - SCADA*), se assemelha a Figura 1.

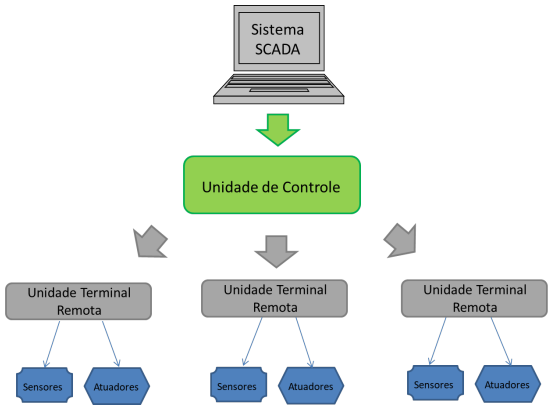

Figura 1. Modelo de um sistema de automação e controle industrial

Os sistemas SCADA são implementados em *software* para controlar e monitorar dispositivos dispersados espacialmente (**?**). A comunicação com o SCADA é feita através de uma interface gráfica que permite aos operadores monitorar e controlar o sistema em tempo real.

O comando dos dispositivos é feito por meio de uma unidade de controle, como ilustrado na Figura 1, que faz a conexão entre o SCADA e as unidades terminais remotas (*Remote terminal units* - RTUs). Uma RTU normalmente é um controlador lógico programável (*Programable logic controler* - PLC) que comanda dispositivos como atuadores ou sensores. Enquanto os PLCs devem estar próximos dos processos fabris que estão sendo gerenciados, outras RTUs podem ser gerenciadas a distância graças à conexão via Internet, Ethernet, rádio-frequência ou afins. Os protocolos de comunicação mais utilizados são o *Modbus*, o *Fieldbus*, o *Distributed network protocol* (DNP3) e o *Internet Protocol* (IP) (Gao and et al., 2010). Nenhum desses oferece assinaturas digitais e possuem diversas vulnerabilidades que podem ser exploradas (Kuzmanovic, 2003).

Um tipo de abordagem para sistemas industriais é a manufatura integrada por computadores (*Computer integrated manufacturing - CIM*) que consiste na automação completa de uma unidade de manufatura (Kalpakjian, 2006). Todas as operações são controladas por computadores, possuem estoque e distribuição comuns, utilizam sensores de tempo real e processos de controle em malha fechada o que aumenta a velocidade de processamento da manufatura.

A criticalidade temporal de um IACS implica na importância do respeito aos prazos por operar em tempo real. Uma interrupção inesperada não é aceitável (Krutz, 2015). A finalização de uma operação após o seu prazo é considerada inútil e pode causar um efeito cascata no mundo físico. Por isso, se houver algum ataque que provoque uma interrupção da operação, todo o processo seguinte será afetado.

Normas como a ISA 62443 (ISA, 2009) e a NIST SP 800-82 (Stouffer et al., 2015), tratam da segurança da informação nesses ambientes e detalham testes de segurança, monitoramento e detecção de intrusão.

3. SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE AUTOMAÇÃO E CONTROLE INDUSTRIAIS

A segurança da informação vem enfrentado desafios para se adaptar aos IACS. O fato de serem sistemas ciber-físicos os diferem dos sistemas tradicionais de tecnologia da informação porque se os atacantes se apossarem da informação e adulterá-la, podem criar problemas físicos como acionamento ou desligamento indevido de equipamentos. As alterações nos dados medidos pelos sensores podem levar a uma tomada de decisão errada pelos operadores da rede e prejuízos ao sistema.

O *worm* Stuxnet foi um caso de ataque ciber-físico famoso por causar danos a uma usina nuclear no Irã em 2010 (Langner, 2011). O *worm* tomou controle de um atuador em um SCADA e utilizou um ataque do tipo *replay* para fazer parecer aos operadores da usina que a operação estava normal.

A tendência à padronização dos *softwares* e *hardwares* utilizados em IACS facilita ataques, por isso, a comunicação precisa ser criptografada. Mas os mecanismos de segurança empregados em IACS não devem degradar a manutenibilidade, operabilidade e acessibilidade em caso de emergência (Stouffer et al., 2015). Devido a natureza física, tarefas realizadas pelo SCADA em IACs frequentemente precisam ser interrompidas e reiniciadas. Esse

aspecto temporal e as interrupções de tarefas dificultam os serviços dos mecanismos de segurança (Zhu and Sastry, 2011). Além disso, os recursos computacionais limitados dos dispositivos de campo dificultam a implementação de técnicas criptográficas comuns.

Em IACS, todos os dados corretos devem ser processados no seu tempo correto porque não é a duração temporal, mas sim o cumprimento do prazo que deve ser priorizado na análise da segurança. Por isso, garantir a disponibilidade da comunicação em IACS é considerado mais prioritário do que manter a sua confidencialidade. De forma contrária, a maior parte da pesquisa em segurança da informação foca em confidencialidade. Mas também deve-se considerar a integridade dos dados, já que um erro na transmissão pode acarretar em mau funcionamento dos equipamentos ou em uma análise errada das informações (ISA, 2009).

Devido à criticalidade dos sistemas operantes, é perigoso realizar testes no ambiente físico, então são utilizados gêmeos digitais (*Digital twin*) que consistem no uso de simulações holísticas para representar um sistema físico (Eckhart, 2018).

4. A MODELAGEM REALIZADA

Com o intuito de buscar novas estratégias para aumentar a segurança de IACS, foi criada uma modelagem e com base nela simulações seguindo a metodologia descrita por Terruggia and Ekstedt (2018), que oferece suporte ao usuário para realizar uma análise de risco. A metodologia utilizada neste trabalho faz uma estimativa da eficiência das medidas de mitigação aplicadas ao comparar os valores da ETR e do TMC nas diferentes configurações simuladas.

4.1 Descrição da planta

Neste trabalho, foi realizada uma modelagem da planta MecatrIME [1] ilustrada nas Figuras 2 e 3, do Laboratório de Mecatrônica do Instituto Militar de Engenharia (IME) para o estudo de IACS. Nenhum teste físico foi realizado para evitar danos à planta, por isso foram realizadas simulações para a análise de risco.

A planta é composta por uma estação de gerenciamento (P9), seis estações de produção (P2-P7), uma estação de controle do transporte de peças pela esteira (P8) e uma estação de armazenagem (P1) totalizando nove estações interligadas por uma esteira. As estações de produção ilustram alguns dos principais processos de fabricação industriais como torneamento (P2), fresamento (P3), soldagem (P4), metrologia (P5), montagem e inspeção visual (P6) e gravação a laser (P7). A estação de gerenciamento da planta representa a unidade de controle e as estações internas representam as RTUs.

A ligação entre elas é feita por cabos formando uma rede local (*Local Access Network* - LAN) Ethernet utilizando a pilha de protocolos de comunicação TCP/IP. A comunicação entre os computadores nas estações e a rede do IME é realizada por meio de um ponto de acesso para acesso à Internet. A LAN não está conectada à rede do IME. A

[1] `https://sites.google.com/ime.eb.br/mecatrime`

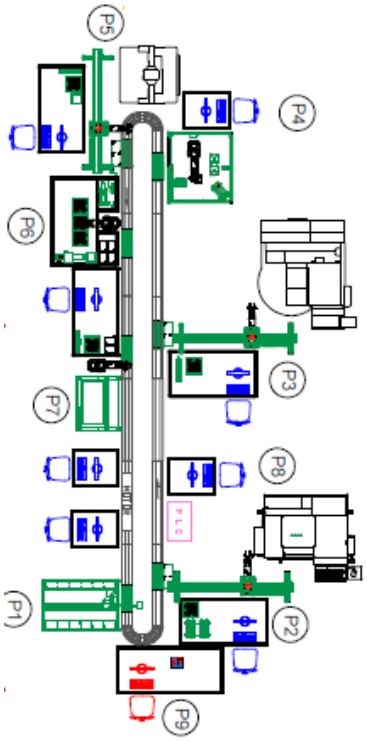

Figura 2. Mapa da MecatrIME

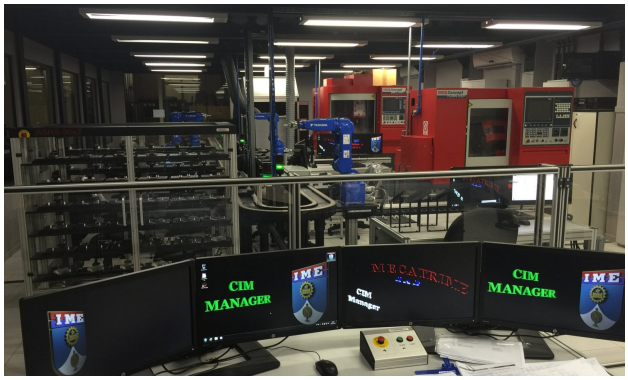

Figura 3. Planta MecatrIME utilizada

comunicação entre os dispositivos periféricos e os computadores nas estações é feita utilizando o protocolo RS232 como ilustra a Figura 4. Essa rede pode ser considerada como uma rede ponto-a-ponto (*peer-to-peer*) já que todas as estações podem enviar e receber mensagens entre si.

O *software* utilizado para o controle da planta é o OpenCIM que controla, monitora e opera a produção conforme a abordagem CIM IntelitekInc. (2019). O *software* é composto pelo módulo CIM *Manager* e os módulos *Station Manager*. O CIM *Manager* é o módulo instalado na estação de gerenciamento que coordena a funcionalidade de todos os dispositivos da planta através da LAN. O *Station Manager* é o módulo instalado em todas as estações, que as controla e se comunica com o CIM *Manager*.

As estações podem ser utilizadas de forma isolada, controladas somente pela estação de gerenciamento, ou de forma integrada. Esse processamento distribuído torna o sistema

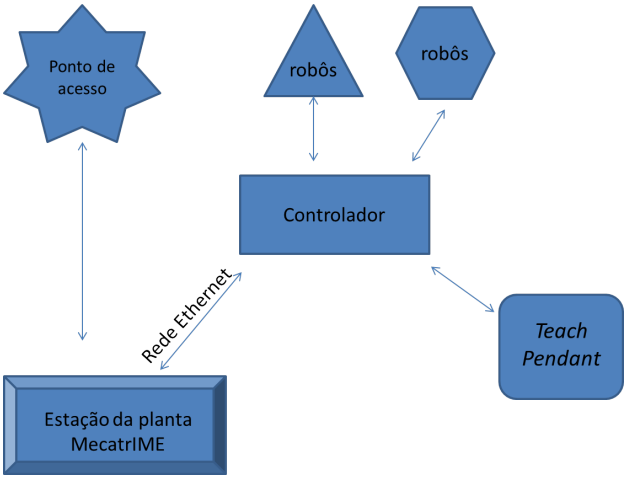

Figura 4. Rede de comunicação entre os dispositivos de uma estação da planta MecatrIME. Adaptado de IntelitekInc. (2019)

mais robusto porque, caso a estação de gerenciamento tenha algum problema, as máquinas ainda podem operar de modo individual.

Os computadores conectados à rede da MecatrIME não podem se conectar à rede sem fio do IME, ao mesmo tempo em que a linha de operação está em execução, por motivos de segurança, mas podem ser utilizados normalmente quando a planta não está em execução. As estações se conectam à Internet somente com as maquinas desligadas.

Para modelar a rede foi utilizado o *software* SecuriCAD® (Ekstedt and et al., 2015), uma ferramenta de modelagem de ameaças e gerenciamento de riscos, utilizado nos trabalhos de Terruggia and Ekstedt (2018) e Xiong and Robert (2019), que proporciona a simulação de diversos tipos de ataques e gera relatórios com os resultados. Com isso, pode-se compreender melhor a situação de segurança ciber-física da MecatrIME.

4.2 Descrição da simulação

A Figura 1 no apêndice apresenta o esquema criado para a simulação, no qual foram utilizados módulos diferentes para representar os elementos da MecatrIME como o ilustrado na Figura 5. O módulo da estação de armazenamento é um elemento *host* conectado a um sistema de detecção de intrusão (*Intrusion detection system - IDS*), um *software* Windows 7 que é o sistema operacional dos computadores da planta, um cliente e um controle de acesso.

Uma rede externa é associada à *intranet* do IME e uma rede interna representa a planta. A rede externa é composta por um módulo de servidor e um módulo de rede e foi modelada com o sistema operacional Linux. A comunicação com a rede interna é feita através de um roteador com um *firewall*. A rede interna é composta por um módulo representando a estação de gerenciamento (P9) e quatro estações internas representativas (P1,P2,P5 e P6). Cada módulo de estação é composto por um *host* representando um servidor e um cliente porque o OpenCIM é estruturado desse modo na realidade. Todos os fluxos de dados das estações possuem um IDS e, além disso, a estação de gerenciamento tem um sistema de prevenção de intrusão

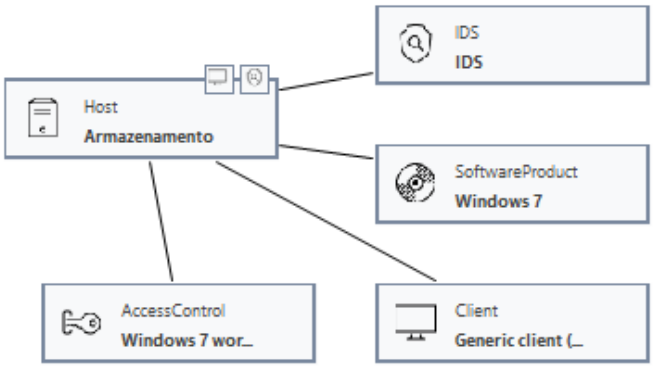

Figura 5. Módulo representando a estação de armazenamento no SecuriCAD®

(*Intrusion prevention system - IPS*). Esses sistemas de segurança ainda serão implementados na planta real.

É necessário definir no SecuriCAD® a consequência (*consequence*) que indica qual seria a severidade de um ataque bem sucedido ao sistema e por isso possui uma importância estratégica para os controladores da planta. Esse valor varia de 0 a 10, sendo que 10 representa a maior severidade.

A partir da simulação, o SecuriCAD® cria automaticamente o caminho de um ataque, que é o agregamento de grafos de ataques probabilísticos, para modelar a composição das vulnerabilidades encontradas pelo atacante para prejudicar o sistema. O SecuriCAD® faz uma análise de risco e gera relatórios com medidas como as exposições de confidencialidade, disponibilidade e integridade que compõem a Exposição total ao risco (ETR) e o Tempo médio de comprometimento (TMC) utilizados no trabalho de Johnson and et al. (2016). O TMC representa o tempo esperado que um atacante levaria para completar uma certa probabilidade de risco (Terruggia and Ekstedt, 2018).

4.3 Cenários Definidos

Os alvos selecionados para os ataques foram o servidor do IME, a estação de gerenciamento (P9), a estação de metrologia (P5) e uma estação do torno mecânico (P5). Eles foram definidos como ativos de alto valor no *software*. Dentre os tipos de ataques predefinidos disponíveis para cada um dos alvos selecionados, foram elaborados os seguintes cenários:

- Cenário 1: Atacante com acesso ao servidor do IME visa um ataque *ARPPoisoning* à estação de gerenciamento.
- Cenário 2: Atacante com acesso a estação de gerenciamento visa o comprometimento da estação de metrologia.
- Cenário 3: Atacante com acesso a estação de gerenciamento visa uma Negação de Serviço do servidor do IME.
- Cenário 4: Atacante com acesso ao roteador visa o comprometimento da estação do torno mecânico.
- Cenário 5: Atacante com acesso ao servidor do IME visa todos os outros cenários ao mesmo tempo.

Como exemplo, o grafo de ataque para o cenário 1 é ilustrado na Figura 2 do apêndice. O atacante é representado por um círculo vermelho e o alvo por um círculo azul. Pode-se observar que o atacante possui várias possibilidades de ataques que são indicados pelas setas.

4.4 A estratégia de defesa elaborada

A estratégia de defesa elaborada consiste em desconectar da rede a estação almejada pelo atacante para os cenários com somente um alvo (1-4).

No caso de um ataque a várias estações ao mesmo tempo (cenário 5), a estratégia de defesa consiste em desconectar da rede a estação considerada mais suscetível para o ataque segundo o grafo dos caminhos de ataques.

Para isso, seria necessário a inclusão de um IDS na planta. Esse estudo já está sendo realizado e uma nova análise, incluindo esse sistema e a criação de uma zona desmilitarizada para proteger a planta, será divulgada posteriormente.

5. RESULTADOS E DISCUSSÕES

Foram realizadas simulações com e sem a estratégia de defesa proposta. Além disso, foi realizada mais uma simulação na qual todas as opções de defesa predefinidos dos componentes foram ativadas para estudar essas medidas de proteção.

5.1 Resultados sem a estratégia de defesa proposta

Foram utilizadas como métricas para a análise de risco as exposições de confidencialidade, disponibilidade e integridade que compõem a Exposição total ao risco (ETR) e o Tempo médio de comprometimento (TMC).

Os resultados da simulação para os cenários definidos na subseção 4.3, estão mostrados nas tabelas 1 e 2.

Tabela 1. Resultados do experimento para os cenários definidos

Cenários	***Conseq.***	**TMC (dias)**	**ETR**(%)
Cenário 1	6	14	92
Cenário 2	10	5	100
Cenário 3	6	13	92
Cenário 4	10	8	99

5.2 Resultados com a estratégia de defesa proposta

Os resultados com a estratégia de defesa de desconectar as estações afetadas individualmente, estão apresentados nas Tabelas 3-5 respectivamente para as estações de controle de qualidade, de gerenciamento e de processamento. As exposições de confidencialidade, disponibilidade e integridade para esse cenário são apresentadas na Tabela 6.

Pode-se observar que os ataques apresentam uma Exposição total ao risco alta e resultados mais críticos ocorreram nos alvos que foram definidos como de maior consequência. O servidor do IME é atingido rapidamente devido ao contato direto do atacante, o que é representado pelo TMC igual a zero. O valor do TMC para os outros alvos é maior ou igual se comparado aos cenários nos quais são tratados como alvos isolados. Pode-se atribuir este resultado como um efeito de um custo maior de processamento das operações parciais do ataque.

O valor da ETR é próximo aos valores nos outros cenários, tendo uma diminuição de 2% para os cenários de comprometimentos das estações. Isso mostra que há uma

Tabela 2. Resultados do experimento para o cenários 5

Alvo	**Tipo de ataque**	***Conseq.***	**TMC (dias)**	**ETR**(%)
Servidor do IME	Negação de Serviço	10	14	92
Estação de gerenciamento	*ARPCache Poisoning*	10	5	100
Estação de controle de qualidade	Comprometimento	6	13	92
Estação do torno	Comprometimento	6	8	99

Tabela 3. Resultados para o cenário 5 após desconectar a estação de controle de qualidade

Alvo	**Tipo de ataque**	***Conseq.***	**TMC (dias)**	**ETR**(%)
Servidor do IME	Negação de Serviço	10	0	100
Estação de ger.	*ARPCache Poisoning*	10	5	100
Estação de controle de qualidade	Comprometimento	6	-	-
Estação do torno	Comprometimento	6	12	96

Tabela 4. Resultados para o cenário 5 após desconectar a estação de gerenciamento

Alvo	**Tipo de ataque**	***Conseq.***	**TMC (dias)**	**ETR**(%)
Servidor do IME	Negação de Serviço	6	0	100
Estação de ger.	*ARPCache Poisoning*	10	-	-
Estação de controle de qualidade	Comprometimento	6	11	95
Estação do torno	Comprometimento	10	11	96

Tabela 5. Resultados para o cenário 5 após desconectar a estação do torno

Alvo	**Tipo de ataque**	***Conseq.***	**TMC (dias)**	**ETR**(%)
Servidor do IME	Negação de Serviço	6	0	100
Estação de ger.	*ARPCache Poisoning*	10	5	100
Estação de controle de qualidade	Comprometimento	6	12	95
Estação do torno	Comprometimento	10	-	-

taxa menor de sucesso individualmente nos alvos quando vários alvos são almejados simultaneamente. A desconexão de cada estação individualmente também mitiga os efeitos do ataque nas outras estações o que é representado pelo aumento nos valores do TMC e diminuição dos valores da ETR.

O TMC da estação de gerenciamento aumentou de cinco para seis dias e o TMC da estação de metrologia de quinze para dezesseis dias após a desconexão da estação do torno. Somente no caso da estação de gerenciamento, houve um aumento no valor da ETR por essa ser o alvo de entrada para o atacante no cenário 5.

Tabela 6. Exposições de confidencialidade, disponibilidade, integridade e média

Cenários	**Exposição Média** (%)	**Exposição Confidencialidade** (%)	**Exposição Disponibilidade**(%)	**Exposição Integridade** (%)
Todo o sistema conectado	98	95	98	95
Estação de controle de qualidade desconectada	81	49	72	49
Estação de ger. desconectada	67	96	78	98
Estação do torno desconectada	81	48	72	48

Pode-se concluir a partir da tabela 6 que o tipo de exposição mais crítico é a de disponibilidade. Esse é o pior tipo de exposição para os sistemas industriais conforme explicado na seção 3. Além disso, a desconexão da estação de gerenciamento é a que mais aumenta a exposição média do sistema porque o IPS é implementado na ligação entre essa estação e o roteador.

Poderia-se criar um IPS de contingencia para esses casos. Assim, caso haja a necessidade de desconexão da estação ligada ao IPS, poderia-se ativar o outro. Se houvesse uma zona desmilitarizada entre a planta e o servidor do IME, poderia-se alocar o IPS nela. P

5.3 Resultados com as medidas de segurança ativadas

O SecuriCAD® disponibiliza várias medidas de proteção predefinidas como *antimalware* para o elemento *Host*, a versão segura do protocolo *Domain Name Server* (DNS) e o uso de tabelas estáticas de roteamento para o protocolo *address resolution* (ARP) para o elemento *Network* como ilustrado nas Figuras 6 e 7.

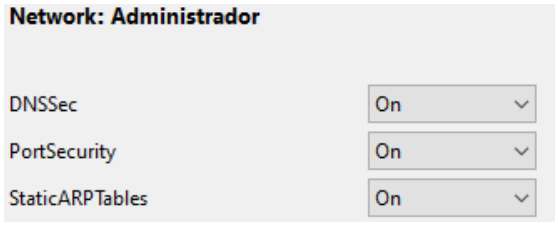

Figura 6. Medidas de defesa para um elemento do tipo Rede

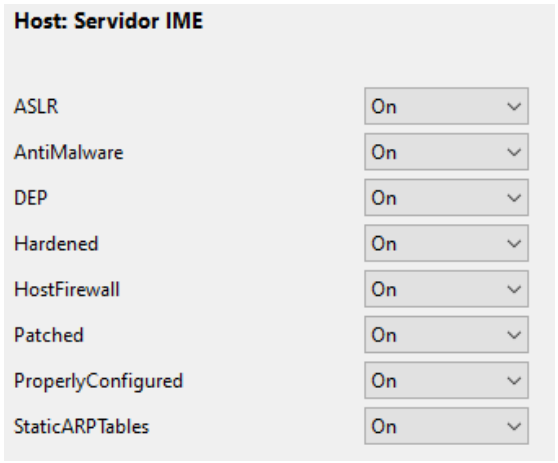

Figura 7. Medidas de defesa para um elemento do tipo *Host*

O cenário base com todas as medidas de proteção desativas foi comparado ao cenário com todas elas ativadas para avaliar a eficácia dessas medidas de proteção do sistema. Os resultados da simulação para o cenário 5 com as medidas de proteção ativas está ilustrado na Tabela 7.

A partir dos resultados, percebe-se que o atacante não consegue mais realizar o ataque de *ARPCachePoisoning* na estação de ger. porque a medida de Tabelas Estáticas de ARP está ativada. Comparando esses resultados com a tabela 2, observa-se que as medidas dos ataques nas outras estações foram mitigadas, ou seja, as medidas de proteção dificultaram o ataque de modo eficaz.

Não encontrou-se na literatura nenhum outro trabalho que tenha realizado uma experimentos de riscos de ataques cibernéticos a uma planta de manufatura integrada por computadores para que se pudesse comparar os resultados. Mas foi encontrado o trabalho de Wu et al. (2020) sobre uma plataforma de testes para esse caso que poderia ser utilizada.

Tabela 7. Resultados para o cenário 5 com as medidas de proteção ativadas

Alvo	**Tipo de ataque**	***Conseq.***	**TMC (dias)**	**ETR**(%)
Servidor do IME	Negação de Serviço	6	0	100
Estação de ger.	*ARPCache Poisoning*	10	-	-
Estação de controle de qualidade	Comprometimento	6	31	62
Estação do torno	Comprometimento	10	27	66

6. CONCLUSÃO

Neste estudo, foi avaliada uma estratégia de segurança para um IACS utilizando uma planta de testes em cinco cenários. A Exposição total ao risco (ETR) e o Tempo médio de comprometimento (TMC) foram medidos em cada caso através do *software* SecuriCAD® e os resultados foram analisados.

Foram consideradas as possibilidades de ataques nos quais o atacante busca comprometer uma estação, bloquear o tráfego de rede, mudar a comunicação dos protocolo e etc.

Após analisar os resultados, conclui-se que a solução proposta é eficaz ao proteger as estações que foram isoladas já que os valores de ETR e TMC são nulos o que representa que não foram infectadas. Além disso, houve uma diminuição dessas medidas nas estações que se mantiveram conectadas ao sistema. Como exemplo, o TMC da estação de gerenciamento aumentou de cinco para seis dias e o TMC da estação de metrologia de quinze para dezesseis dias após a desconexão da estação do torno. Somente no caso da estação gerenciamento, houve um aumento na ETR por ser essa o alvo de entrada para o atacante no cenário 5.

Este trabalho induz uma consideração sobre a segregação de redes em IACS. Pode-se evitar a propagação de um ataque para outros elementos da rede utilizando *firewalls*, por exemplo, para aumentar a segurança de cada separação entre os componentes.

A modelagem criada fornece uma referência de modelagem e análise de risco para pesquisas futuras sobre técnicas de segurança da informação em IACS. Trabalhos futuros poderiam estudar um ambiente mais complexo, outros cenários de ataque ou desenvolver outras estratégias de defesa.

REFERÊNCIAS

Eckhart, Matthias; Ekelhart, A. (2018). Towards security-aware virtual environments for digital twins. 61–72. doi:10.1145/3198458.3198464.

Ekstedt, M. and et al. (2015). Securicad by foreseeti: A cad tool for enterprise cyber security management. In B.H.S.M.W.G.A.K.G.G. Kolb Jens; Weber (ed.), *EDOC Workshops*, 152–155. IEEE 19th International Enterprise Distributed Object Computing Workshop (EDOCW). URL `http://dblp.uni-trier.de/db/conf/edoc/edoc2015w.htm`.

Foreseeti$_AB$(2018).*SecuriCAD; 1.4 User Manual*.5, 3*edition*.

Gao, W. and et al. (2010). On scada control system command and response injection and intrusion detection. In *eCrime*, 1–9. Proceedings of the eCrime Researchers Summit (eCrime), IEEE. URL `http://dblp.uni-trier.de/db/conf/ecrime/ecrime2010.html`.

IntelitekInc. (2019). *OpenCIM 5 User Manual*. Catalog No. 100094 Rev. J. URL `https://www.intelitekdownloads.com/Manuals/CIM-FMS/OpenCIM_User_guide_L.pdf`.

ISA (2009). *ISA. 2009. 62443: Industrial communication networks - Network and system security. International Standard*. 1st edition.

Johnson, P. and et al. (2016). Time between vulnerability disclosures: A measure of software product vulnerability. 278,295. Computers Security.

Kalpakjian, S.; Schmid, S. (2006). *Manufacturing engineering and technology*. Prentice Hall, 5ª edition.

Krutz, R.L. (2015). *Securing SCADA systems*. Wiley.

Kuzmanovic, Aleksandar; Knightly, E.W. (2003). Low-rate tcp-targeted denial of service attacks: the shrew vs. the mice and elephants. volume 14, 683–696. Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. URL `http://dblp.uni-trier.de/db/journals/ton/ton14.html`.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9, 49–51. doi:10.1109/MSP.2011.67.

Refsdal, A. and et al. (2015). *Cyber-systems*, 25–27. doi:10.1007/978-3-319-23570-7_3.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. NIST special publication 800, 82r2.

Terruggia, Roberta; Dondossola, G. and Ekstedt, M. (2018). Cyber security analysis of web-of-cells energy architectures. doi:10.14236/ewic/ICS2018.5.

Wu, M., Song, J., Sharma, S., Di, J., He, B., Wang, Z., Zhang, J., Lin, L.W.L., Greaney, E.A., and Moon, Y. (2020). Development of testbed for cyber-manufacturing security issues. *International Journal of Computer Integrated Manufacturing*, 33(3), 302–320. doi:10.1080/0951192X.2020.1736711.

Xiong, Wenjun; Fredrik, K. and Robert, L. (2019). Threat modeling and attack simulations of connected vehicles: A research outlook. doi:10.5220/0007412104790486.

Zhu, Bonnie; Joseph, A.D. and Sastry, S. (2011). A taxonomy of cyber attacks on scada systems. In *iThings/CPSCom*, 380–388. IEEE Computer Society. URL `http://dblp.uni-trier.de/db/conf/ithings/ithings2011.html`.

Apêndice

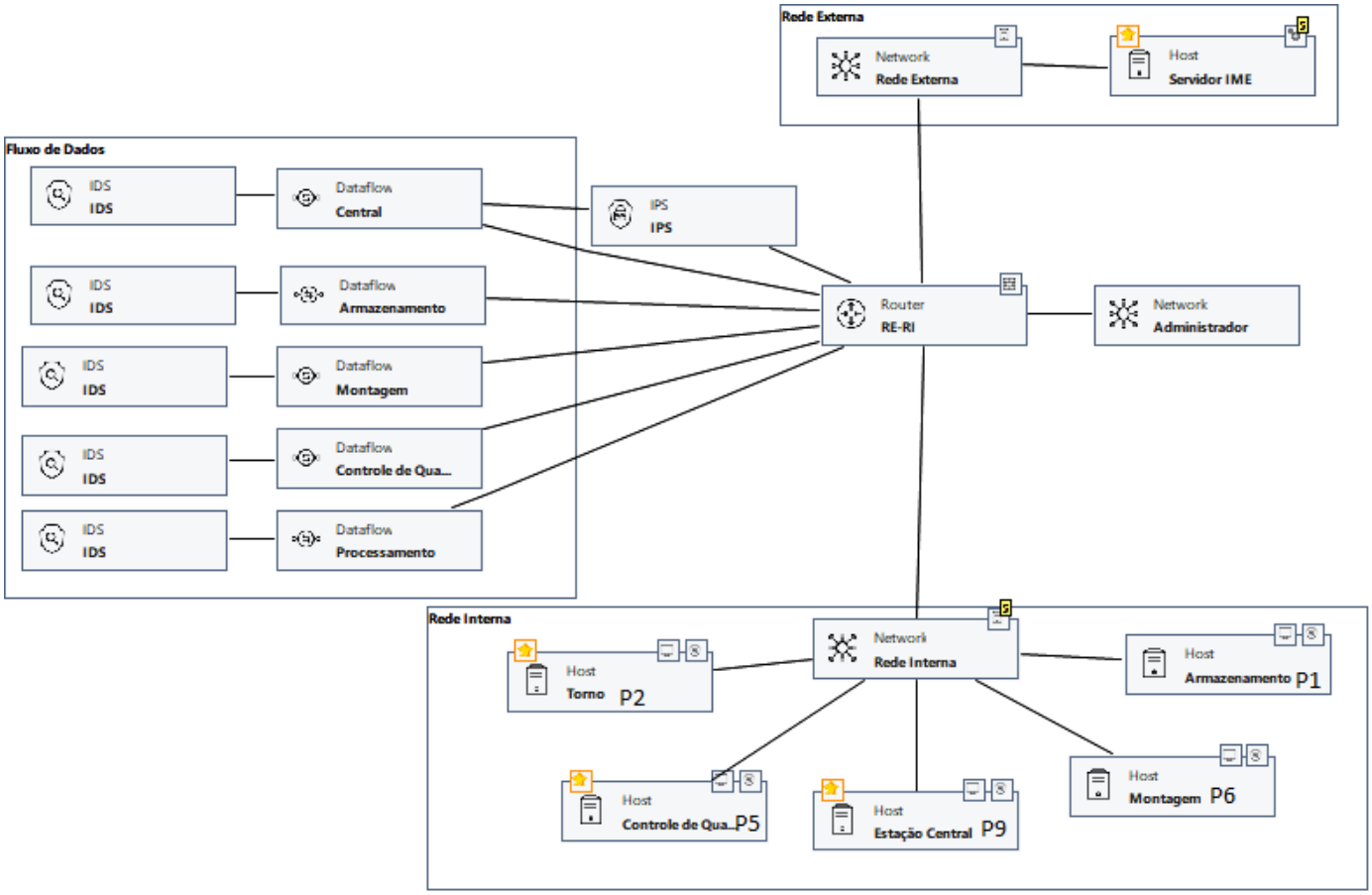

Figura .1. Simulação da planta

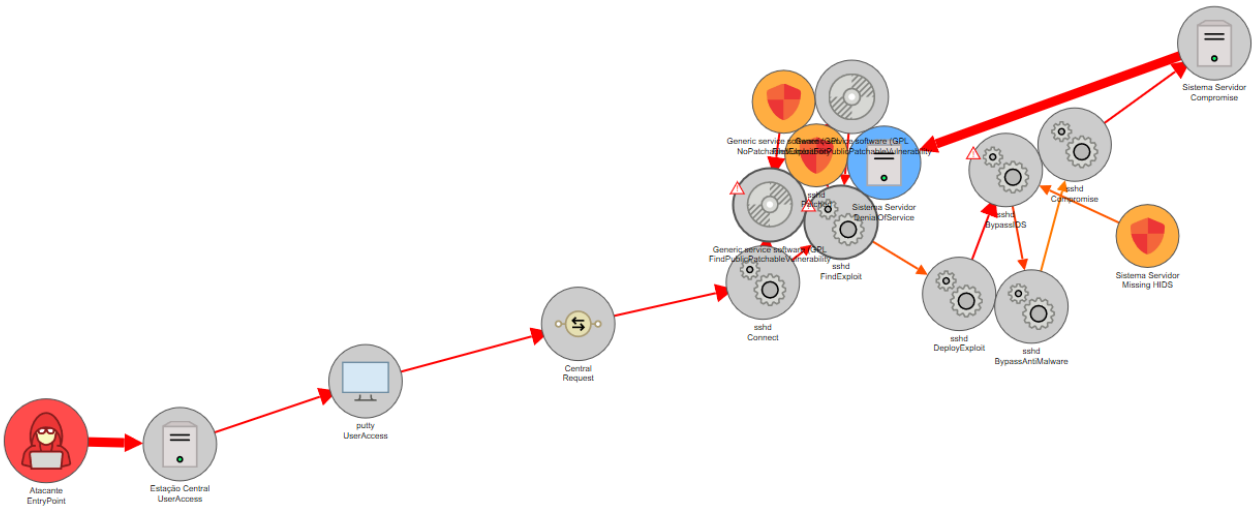

Figura .2. Grafo de ataques probabilístico do cenário 3