Grupo de Estudo de Sistemas de Informação e Telecomunicação para Sistemas Elétricos-GTL

SISTEMATIZAÇÃO DA VERIFICAÇÃO DO STATUS DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS PRINCIPALMENTE SUBESTAÇÕES DE ENERGIA EM CONFORMIDADE COM A ISA/ IEC-62443

FELIPE SABINO COSTA(1);
Moxa Brasil(1);

Rua Pereira Caldas, 59, Jardim da Gloria, CEP: 01546-100, São Paulo, Brasil
Tel: +55 11 96852-3781– Email: felipe.costa@moxa.com

RESUMO

A cibersegurança é um tema que vem ganhando notoriedade nos últimos tempos, apesar de ser um assunto discutido já há muitos anos, apenas recentemente tem se dado a devida atenção ao tema nos ambientes industriais, incluindo os sistemas de geração, transmissão e distribuição de energia, parte pelo avanço do desenvolvimento das ameaças para as aplicações industriais de uma forma geral e parte pelo aumento da automação de seus sistemas inerente ao aumento das demandas de produtividade e iniciativas de melhorias baseadas em conectividade, que por consequência aumentam as áreas de exposição a essas ameaças. Dentro desse contexto, uma série de normas têm sido discutidas, dentre elas a ISA/IEC-62443 que possui uma alta aplicabilidade em infraestruturas críticas, que é refletida nos ativos de rede em uma longa e complexa lista de configurações para auxiliar os sistemas industriais a possuírem uma proteção cibernética adequada aos seus riscos. Este trabalho irá apresentar uma abordagem sistemática e automática dessas configurações de segurança focada nos ativos de rede, que pretende diminuir a probabilidade de se implementar configurações incorretas ou incompletas concernentes as configurações manuais.

PALAVRAS-CHAVE

Cibersegurança Industrial, IACS, NERC CIP, sistema de verificação automático, Fator humano

1.0 - INTRODUÇÃO

Nos últimos anos tem crescido os ciberataques aos setores/infraestruturas industriais críticas, tais como: Energia, tratamento de água, hospitais, transporte, entre outros. Todos esses setores comumente necessitam do suprimento de energia elétrica para sua correta operação, fazendo com o que o setor elétrico seja o elo de ligação entre todos os setores críticos, tornando-o um setor vital para a soberania de qualquer país e por consequência um dos alvos prioritários dos ciberataques [1]. Considerando a sua natureza crítica, a implementação da cibersegurança passa a ser imprescindível para esse setor.

Entende-se que a implementação da cibersegurança deve ser considerada de forma holística, abrangendo os pilares que a IEC elenca como: “People”, “processes” and “technologies”, (em uma tradução livre: pessoas, processos e tecnologias) onde cada aspecto possui igual prioridade e relevância [2]. Este trabalho irá focar na perspectiva técnica das tecnologias da cibersegurança no que tange os ativos de infraestrutura de rede, apresentando uma forma de configuração sistemática e automática, para se evitar falhas humanas, verificando as funcionalidades existentes de cada dispositivo conectado à mesma rede, em conformidade à IEC-62443 secção 4 para o nível de segurança 2 “dois” (SL-2) (IEC 62443-4-2) [3], considerado nível de “hacker/cyber crime”, alertando caso os dispositivos não possuam os requisitos exigidos e/ou não estejam com eles habilitados.

2.0 - ABORDAGEM NORMATIVA

Estudos recentes demonstram que a melhor forma de proteger infraestruturas críticas na perspectiva normativa é utilizando uma abordagem híbrida de normas (verticais e horizontais), onde “normas horizontais” são conhecidas por serem de um espectro mais abrangente e flexível, como a ISA/IEC-62443 por exemplo, podendo ser aplicadas à uma grande variedade de infraestruturas críticas e as “normas verticais” são conhecidas por serem mais específicas de cada setor, como a NERC CIP para o setor elétrico por exemplo [2]. Esta recomendação recorre ao fato de que ao se aplicar ambos tipos de normas traz-se uma robustez processual maior à empresa no que tange a abrangência dos diferentes pilares da ciberseguraça, pois por natureza, cada sistema normativo foca em partes mais especificas dos pilares, uma vez que se use diferentes normas, suas abordagens tendem mais a se complementar do que à se opor, trazendo para a empresa uma abordagem altamente multifocal.

Diferentes empresas possuem diferentes níveis de maturidade com relação à implementação da cibersegurança [4] mas entende-se que como uma boa prática é se iniciar à estrutura processual com as normas horizontais e posteriormente ir se complementando com as normas verticais, tendo em vista que nessa ordem, uma estabelece base para a outra. Nenhum dos tipos de norma é necessariamente mais eficiente do que o outro, mas pelo contrário, ambas são igualmente necessárias e complementares [2].

Com base nessa abordagem, pretendemos apresentar o conjunto de normas ISA/IEC-62443 [3,5,6,7,8,9,10,11] doravante denominada apenas “norma” como aplicável a qualquer processo industrial crítico, na secção 4 da norma, ela elenca boas práticas e requisitos os quais os componentes devem possuir, ativos de redes incluídos, em ordem de se estabelecer uma resiliência e um impeditivo maior sob tentativas de ciberataques proporcionais aos níveis de complexidade denominadas “Security Levels” (níveis de segurança em uma tradução livre).

Cada nível de segurança possui uma clara definição quanto as habilidades, motivações, intenções e recursos que o nível está apto a proteger. Partindo do pressuposto de que a norma já apresenta as melhores práticas para níveis

predeterminados, o sistema de verificação de segurança automático apresentado neste trabalho, toma como base os parâmetros por ela elaborados, onde o nível 2 “dois” (SL-2) de segurança foi definido como o nível mínimo admissível para infraestrutura críticas, sendo apta a lidar com as tentativas mais simples e comuns de invasão, tais como: Ataque de força bruta, escâner de rede e autenticação fraca, entre outros, associando essas funcionalidades à uma interface gráfica simples e intuitiva.

Adicionalmente, entende-se que ataques mais sofisticados elaborados pelos níveis superiores, níveis 3 e 4 de “terrorismo” e “ataques de nações” respectivamente, exigiriam uma combinação muito maior de recursos (software, hardware) e um tempo muito maior de desenvolvimento postergando ainda mais o início da implementação desses, nos atuais equipamentos, além de, estatisticamente, não corresponderem à maior parte dos ciberataques [1] e o nível de segurança 1 para “empregados descuidados” é insuficiente.

3.0 - IMPORTÂNCIA DA SISTEMATIZAÇÃO

A utilização de uma forma sistemática e principalmente automática na implementação das configurações é imprescindível para se garantir uma uniformidade e, mais importante, uma repetibilidade consistência e confiável das configurações. Essa iniciativa tem por objetivo diminuir a interferência humana no processo, pois é sabido que o fator humano é tido como uma das principais causas de incidentes cibernéticos independentemente se são atos intencionais ou não [1].

O automatismo do processo se torna ainda mais necessário em atividades repetitivas, pois geralmente seres humanos tendem a cometer mais erros nesse tipo de processo, aumentando a sua quantidade conforme a complexidade da tarefa [12]. Sendo assim, garantir a mínima interferência humana nesse processo de configuração, diminui a possibilidade da falha, que indiretamente resolve além da problemática em si da cibersegurança, ou seja, de se assegurar as configurações adequadas para cada nível de segurança, também elimina a possibilidade de se haver falhas na aplicação destas nas rotinas de configuração por uma inadequada programação humana.

Este tipo de vulnerabilidade causada por uma incorreta implementação das funcionalidades necessárias por falha humana, é extremamente complexa de ser detectada, pois dependendo do processo de auditoria que a empresa possui, esse pode ser guiado a acreditar em uma falsa conformidade, visto que quem realiza as configurações pode de fato acreditar que fez as devidas implementações, mas efetivamente elas não foram instaladas. Esse tipo de problema tende a ser exponencialmente maior se esses processos de auditoria forem manuais [12], sem considerar atos deliberados de alterações incorretas ou danosas, ambos cenários sendo denominados de ameaças internas do termo em inglês “insiders” [13] que o sistema de cibersegurança deve também identificar e evitar que essas ameaças internas prejudiquem a correta operação sistêmica.

Deve ser dada a devida atenção não apenas às metodologias em si, ou seja, “o que implementar”, mas também à forma na qual elas são implementadas, “o como”. Realizando a implementação de uma forma sistemática e automática é possível dirimir consideravelmente esses riscos, aumentando a confiabilidade e garantia da segurança das infraestruturas segundo os níveis preestabelecidos pela norma.

3.1 Sistema de referência

A norma na sua secção 1 (IEC-62443-1-1) [11] introduz sete “7” requisitos fundamentais que os equipamentos de comunicação devem possuir, que traduzidos livremente seriam: controle de acesso, controle de operação, integridade de dados, confidencialidade dos dados, controle de fluxo de dados, tempo de resposta em eventos e disponibilidade sob ataques.

Adicionalmente, a norma também determina alguns requisitos de sistemas e de adequação aos respectivos níveis de segurança. Isto se deve ao fato de que niveis maiores de segurança irão exigir mais recursos e complexidade de configurações e também é verdade que níveis inferiores, menos dos mesmos. Sendo assim, os níveis de segurança (SLs) estabelecidos pela norma, devem implementar diferentemente os requisitos fundamentais para atingir seus objetivos. O anexo B da IEC-62443-3-3 [7] possui uma clara relação dos requisitos com os níveis de segurança, permitindo criar uma lista totalmente auditável de cada equipamento para cada respectivo nível de segurança.

4.0 - PROBLEMÁTICAS

Este sistema de verificação de segurança visa defender os sistemas de automação contra os tipos de ameaças definidos pela norma, porém sua utilização traz uma robustez maior também em outros aspectos que serão apresentados a seguir

4.1 Componente Humano

Como explanado anteriormente, uma problemática extremamente importante dentro do contexto discutido, é justamente como o ser humano pode trazer algumas vulnerabilidades adicionais ao sistema de automação. As principais vulnerabilidades levantadas neste estudo irão ser denominados para efeitos didáticos de: Processo de configuração, processo de tomada de decisão e processo híbrido, que partem da hipótese que diferentes processos decisórios são necessários para uma implementação da cibersegurança, ainda que mesmo a própria neurociência não tenha claro como efetivamente os processo e interações de tomada de decisão ocorram dentro cérebro humano, entende-se de forma geral que processos mais ou menos complexos produzem diferentes intensidades de esforço dentro dele [14], logo, todo desenvolvimento deve levar em consideração também as dinâmicas do cérebro humano na tomada de decisão.

4.2 Processo de tomada de decisão

Para este trabalho, “tomada de decisão” seriam todas as decisões de natureza especifica que exigem que o usuário defina algo que a norma deixa à ele a escolha, como por exemplo, se deve ou não aplicar as configurações de segurança em um processo existente, pois somente ele pode avaliar à sua aplicabilidade e impacto. Dentro dessas decisões, a definição do nível de segurança (SL) é de extrema importância.

Outro conceito importante trazido pela norma [11] que exige a tomada de decisão, são as zonas de segurança, onde os equipamentos de uma mesma zona devem estar protegidos por um mesmo nível de segurança efetivo (SL-A), mas não necessariamente todas zonas devem possuir os mesmos níveis de segurança. Por essa razão é necessário deixar a possibilidade de se flexibilizar níveis menores ou mesmo customizáveis de segurança, vide figura 1.

É imprescindível destacar que a implementação dessas funcionalidades caso seja um sistema já em operação, mesmo sendo recomendadas pela norma, deve ser avaliada através de uma adequada análise de risco quanto ao impacto na atual operação do sistema, por essa razão, nenhuma implementação é realizada de forma automática sem o consentimento do usuário.

O sistema de verificação de segurança deve apenas auxiliar o usuário a implementar facilmente as suas decisões, porém sem comprometer ou influenciar seu processo de decisão. Nesse sentido, alguns recursos foram implementados, baseados na dinâmica do cérebro humano.

Um primeiro fator relevante é a utilização de representação gráfica para apresentar os equipamentos ao invés de listas, já há muito tempo é discutido, que o cérebro humano processa diferentemente imagens de palavras [15] e que apesar de terem muitos processos cognitivos semelhantes imagens e palavras acabam por terem tempos de processamento diferentes, levando à predição de que imagens são processadas mais rapidamente do que palavras, havendo diferentes explicações e teorias para isso, envolvendo como esses acessam o sistema semântico, ou mesmo, se acessam os mesmos sistemas [16]. Independente desta disussão, justamente por imagens serem mais rapidamente processadas e reconhecidas pelo cérebro humano, foi definido a utilização de representações gráficas para faciliar a identificação muito mais rapidamente do status das configurações de segurança de cada dispositivo, como demonstrado na figura 3.

Um segundo e último ponto levado em consideração no desenvolvimento do processo decisório, foi a diferenciação de cores para destacar diferentes níveis de segurança, pois o cérebro humano reconhece, através da retina, diferentemente as tonalidades de cores, excitando mais ou menos as classes de cones dos quais as retinas são constituídas [17] sendo assim, cores com espectros diferentes corroboram para uma rápida identificação dos status de segurança de cada dispositivo, bem como, uma tomada de decisão.

4.3 Processo de Configuração

Comparado com os processos de tomada de decisão o processo de configuração tende aparentar ser mais simples, porém como já apresentado neste trabalho, este processo possui outras dificuldades, como a repetitividade e complexidade de configurações que podem levar a erros de configuração.

A lista proveniente do anexo B da IEC-62443-3-3 [7], anteriormente mencionada, é justamente a base para que o sistema de verificação de segurança possa comparar sem subjetividade se os equipamentos auditados estão corretamente configurados ou não.

Ao se realizar uma varredura da rede e se comparar as configurações atuais com as desejadas, se resolve atos deliberados ou não de comprometimento das configurações de cibersegurança, garantindo uma uniformidade da segurança dentro da zona, pois a segurança da zona é definida pelo seu elo mais fraco, sendo portanto de extrema

importância que todos os equipamentos pertencentes a uma mesma zona tenham as mesmas proteções, seja através de recursos próprios ou por contramedidas.

Adicionalmente este recurso também auxilia em uma auditoria automática do sistema, onde ainda que o usuário tenha feito alguma alteração indevida, uma nova auditoria pode ser feita rapidamente e essa vulnerabilidade encontrada. Nesse aspecto, o “pilar do processo” é fundamental, pois será ele que irá garantir a periodicidade que os sistemas e auditorias devem ser realizados.

4.4 Processo hibrido

O processo híbrido irá trabalhar com ambos conceitos discutidos, onde o usuário está no processo de configuração e também dever participar de um processo decisório.

Quando o sistema de verificação de segurança faz a varredura e encontra uma disparidade de configurações entre as recomendadas pela norma e as atuais implementadas, existirão dois principais cenários prováveis como resultado.

No primeiro cenário o usuário identifica quais sugestões podem ser implementadas, autorizando o sistema a realizar a atualização, partindo do pressuposto que o equipamento possui recursos tecnológicos necessários disponíveis, representado pela figura 2.

No segundo cenário apenas diferiria que ao serem levantadas as disparidades o equipamento não possuiria essas funcionalidades e recursos, neste caso, provavelmente seria necessária uma análise de riscos para avaliar se o sistema pode ou não permanecer com essas vulnerabilidades ou se existem contramedidas cabíveis para contorná-las. Independente dos cenários, é importante que o usuário implemente as funcionalidades de segurança mínimas necessárias discutidas pela norma para que a zona à qual ele pertence esteja uniformemente segura.

Todos os processos decisórios aqui apresentados são passíveis de comprometerem a segurança do sistema de automação, entende-se que nem todos devem ser realizados sem o auxilio do ser humano, porém é altamente recomendável que todas as etapas repetitivas e processuais intermediárias que são processos que não envolvem tomada de decisão, apenas implementação, possam ser realizadas de forma consistente e confiável, onde processos automáticos são extremamente adequados.

5.0 - IMAGENS DO SISTEMA

A figura 1 demonstra a possibilidade de se configurar diferentes níveis de segurança no sistema de verificação de segurança e em seguida alguns itens que fazem parte das funcionalidades auditadas.
.

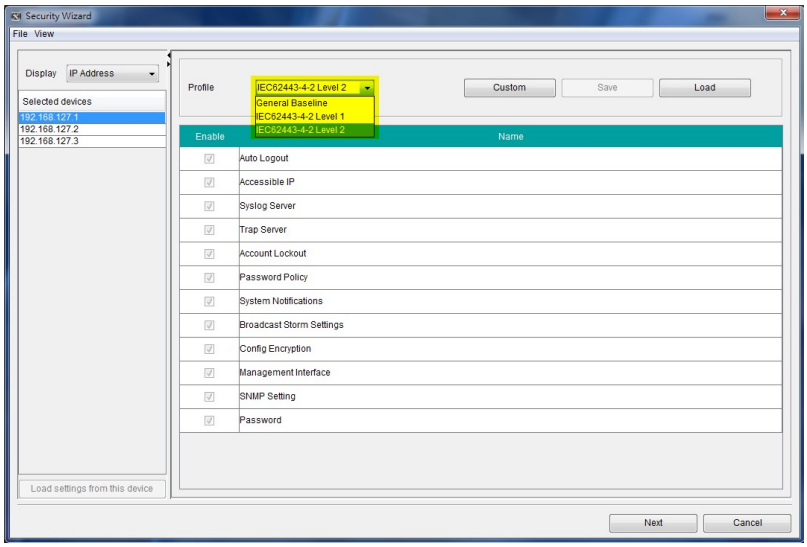

FIGURA 1 – Lista das funcionalidades objetivas a serem auditadas [18]

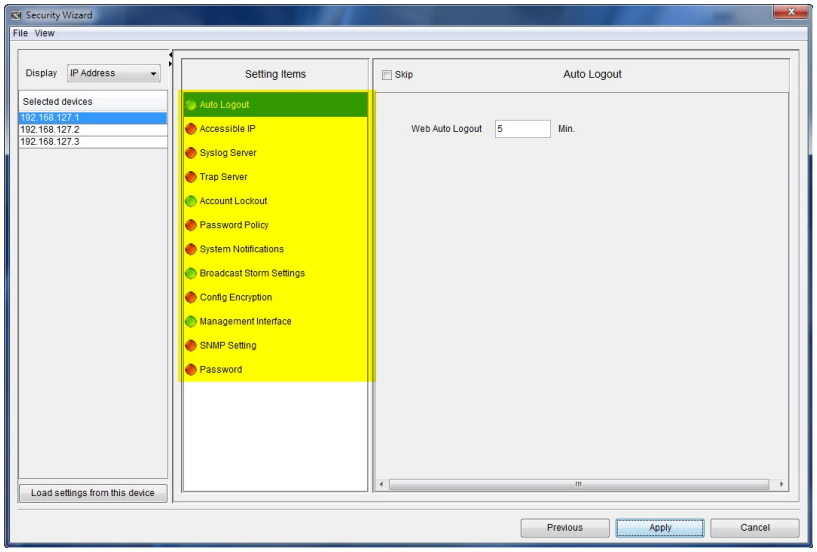

FIGURA 2 – Em vermelho funcionalidades não habilitadas, porém existentes [18]

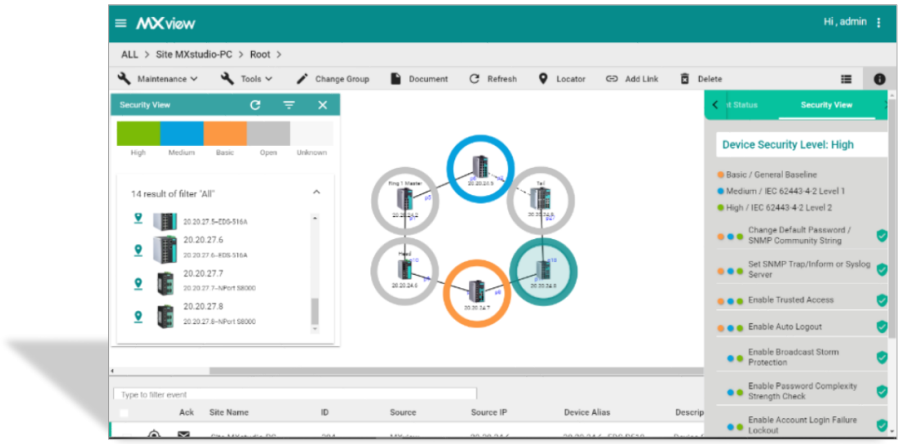

FIGURA 3 – Arquitetura gráfica com status de segurança com sistema de cores [18]

6.0 - CONCLUSÃO

Comprovadamente, métodos sistemáticos e automáticos são mais confiáveis principalmente se comparados aos processos repetitivos e manuais. Desta forma, por se tratar de um tema tão sensível e importante para indústria é fundamental que todas as funcionalidades de segurança cibernética existentes, e principalmente adequadas a cada sistema, sejam implementadas corretamente.

De forma alguma pretende-se indicar que esse sistema de verificação de segurança deve ser visto como único recurso para assegurar uma implementação de cibersegurança, pois entende-se que cibersegurança é complexa e exige uma abordagem multifocal conforme já discutido. Porém, é notável que esse tipo de ferramenta pode auxiliar os responsáveis pela implementação da segurança cibernética, em uma abordagem sem viés através de uma implementação objetiva dos requisitos recomendados pela norma, tendo em vista que, o fator humano na implementação manual dessas configurações pode levar o sistema a permanecer com vulnerabilidades às ameaças cibernéticas, devido a aplicações incorretas dessas, ainda que os ativos de rede possuam contramedidas embarcadas disponíveis.

Nesse âmbito, um sistema de verificação de segurança automático é um recurso importante nas iniciativas de proteção cibernética de qualquer processo de automação industrial crítico, principalmente se associada a outras contramedidas discutidas na norma, bem como, à aplicação dos demais pilares igualmente importantes como pessoas e processos.

7.0 - REFERÊNCIAS BIBLIOGRÁFICAS

1. NCCIC. **ICS-CERT Annual Assessment Report,** [2017]. Disponível em: < https://ics-cert.us-cert.gov/Other-Reports>. Acesso em: 31 mar. 2019.

2. IEC Cyber security Brochure overview. [2018] Disponível em: < https://www.iec.ch/cybersecurity/?ref=extfooter >. Acesso em: 31 mar. 2019.

3. IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

4. ARC Advisory Group. **Cybersecurity Maturity Model**, [2019]. Disponível em: < https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model >. Acesso em: 31 mar. 2019.

5. IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

6. IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

7. IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

8. IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

9. IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment

10. IEC TR 62443-3-1:2009 industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems

11. IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

12. Dekker, Sidney. **The Field Guide to Understanding 'Human Error',** [2017]. Disponível em: < http://leonardo-in-flight.nl/PDF/FieldGuide%20to%20Human%20Error.PDF > Acesso em: 31 mar. 2019.

13. M Adams, M Makramalla. **Cybersecurity Skills Training: An Attacker-Centric Gamified Approach,** [2015]. Disponível em: < https://timreview.ca/article/861>. Acesso em: 31 mar. 2019.

14. H. R. Heekeren et al. **A general mechanism for perceptual decision-making in the human brain,** [2004]. Disponível em: <https://www.nature.com/articles/nature02966>. Acesso em: 31 mar. 2019.

15. Potter, Potter, M. C.. **Short-term conceptual memory for pictures. Journal of Experimental Psychology: Human Learning and Memory, 2(5), 509-522**, (1976) Disponível em: < https://psycnet.apa.org/record/1976-29232-001>. Acesso em: 31 mar. 2019.

16. Giorgio Ganis, Marta Kutas and Martin I. Sereno. **The Search for "Common Sense"**: **An Electrophysiological Study of the Comprehension of Words and Pictures in Reading,** [1996]. Disponível em: < http://www-cogsci.ucsd.edu/~coulson/cogs179/ganis96.pdf>. Acesso em: 31 mar. 2019.

17. Stephen Engel et al. **Colour tuning in human visual cortex measured with functional magnetic resonance imaging,** [1997]. Disponível em: <http://invibe.net/biblio_database_dyva/woda/data/att/f903.file.pdf>. Acesso em: 31 mar. 2019.

18. Moxa Inc. **MXview 3.0 User's Manual,** [2019]. Disponível em: <https://www.moxa.com/Moxa/media/PDIM/S100000150/moxa-mxview-series-manual-v1.1.pdf >. Acesso em: 31 mar. 2019.

8.0 - DADOS BIOGRÁFICOS

Engenheiro e instrutor certificado em Cibersegurança (ISA/IEC-62443) na sede da ISA (International Society of Automation) nos EUA, com especiliação em cibersegurança pelo MIT (Massachusetts Institute of Technology) e em Cibersegurança Industrial pelo Departamento de Segurança Interna do Estados Unidos (United States Department of Homeland Security (CISA)), Inovação e Estratégia pela Univerdade de Harvard (Harvard University) e gestão de projetos pela USP (Universidade de São Paulo), além de certificado em redes pela Moxa e pela CISCO e em gestão de projetos pelo PMI (Project Management Institute). Com mais de 14 anos de experiência no mercado de automação, dos quais, os últimos 5 anos dedicados no desenvolvimento de soluções de comunicação e cibersegurança de missão critica no mercado Brasileiro e atualmente o especialista Nacional de Cibersegurança Industrial (IACS) da Moxa no Brasil.