Cybersecurity in the Power Electronics

T. Martins, and S. Oliveira

***Abstract*—Confidentiality, integrity and availability are essential features for devices connected to the Industrial Internet of Things. However, cybersecurity was never a main concern for power electronics because most of the devices were designed to operate in an isolation mode, without connectivity and data transfer with other devices. With the digital transformation and the industry 4.0, there was a disruptive change in this scenario. Companies, governments and universities have been studying and developing mechanisms to mitigate vulnerabilities in these devices. This article is a literary review on cybersecurity in power electronics with an introduction on digital transformation, industry 4.0 concepts and cybersecurity in the Industrial Internet of Things, presenting some real cyberincidents, tools adopted by companies and researches.**

***Index Terms*—cybersecurity, IoT, IIoT, Industry 4.0, Automation, Power electronics.**

I. Introdução

A Internet Industrial das Coisas (IIoT, *Industrial Internet of Things*) possibilitará o desenvolvimento de fábricas, redes elétricas e muitos outros sistemas inteligentes, criando oportunidades de mercado para fabricantes de equipamentos, provedores de internet e desenvolvedores de *software* (Programa de Computador). Estima-se que até 2022 mais de um trilhão de sensores, máquinas, objetos e dispositivos de Internet das Coisas (IoT, *Internet of Things*) estarão conectados, gerando 45% de todo o tráfego da Internet, sendo que deste tráfego, 37% será gerado por aplicações das áreas de manufatura e 7% por aplicações de geração, transmissão e distribuição de eletricidade [1], [2].

Sistemas IIoT conectam e integram sistemas de controle industriais com sistemas analíticos, corporativos e autônomos, deste modo otimiza-se a operação, possibilita o controle, a colaboração e a tomada de decisão muitas vezes autônoma de equipamentos e processos de negócio, evoluindo a manufatura para a nova era industrial, a Indústria 4.0 [3].

A IoT possibilita a criação de sistemas cibernéticos físicos (CPS, *Cyber-physical systems*) mais eficientes e consequentemente mais inteligentes, como conversores de frequência e motores conectados à rede de computadores, controlando processos industriais, ou como a recente regulamentação da União Europeia que permitirá que clientes de serviços públicos, se tornem fornecedores de energia com a criação das redes locais de energia (E-LANs, *Energy local area networks*), formadas por equipamentos inteligentes integrados, que cooperam entre si, para garantir o funcionamento do sistema [1]. Esta capacidade de controle remoto com fluxo bidirecional de informações tem muitas vantagens, mas torna os sistemas vulneráveis a *cyberattacks* (Ataques Cibernéticos).

Tradicionais sistema de tecnologia da informação (TI), diferem de sistemas de tecnologia operacional (TO), pois empregam sensores e atuadores em ambientes industriais e estes interagem com o mundo real onde alterações descontroladas podem gerar perigosas situações em campo. Esse risco potencial eleva a importância da segurança, acima dos níveis esperados em muitos ambientes tradicionais de TI [3]. Algoritmos de controle, ferramentas de aplicação e metodologias de análise abrangendo a *cybersecurity* (Segurança Cibernética), devem ser projetadas e consideradas para que estes equipamentos inteligentes se tornem escaláveis e confiáveis, garantindo a disponibilidade, integridade e confidencialidade do sistema [3].

Nesse contexto, este trabalho apresenta o estado da arte e visa, contribuir com a área eletrônica potência no que diz respeito à segurança cibernética. Através de uma revisão bibiográfica, busca-se realizar introdução sobre o movimento da transformação digital e da indústria 4.0, conceitualizar fundamentos de *cybersecurity* na IIoT, apresentar alguns casos reais de incidentes industriais, bem como, as iniciativas globais, industriais e acadêmicas na aplicação de *cybersecurity* na área de eletrônica de potência.

II. Transformação Digital e Indústria 4.0

De acordo com o mercado as indústrias de manufatura exigirão uma transformação digital nos próximos anos para continuarem competitivas e se diferenciarem de seus concorrentes [4]. Atualmente poucos fabricantes estão respondendo às oportunidades e ameaças apresentadas pela revolução digital de maneira abrangente e coordenada. Sabe-se que a manufatura gera mais dados do que qualquer outro setor da economia, no entanto a maioria das empresas descarta grande parte dos seus dados, antes que os tomadores de decisão tenham a chance de usá-los, eliminar essa lacuna gerará lucros e crescimento [4].

Com o surgimento da indústria 4.0 [5], ou a quarta revolução industrial, produtos mais sofisticados auxiliarão no desenvolvimento de fábricas, redes elétricas e muitos outros sistemas e redes inteligentes. Consumidores poderão participar ativamente do mercado de eletricidade, gerando sua própria eletricidade, consumindo ou vendendo-a de volta ao mercado, levando em conta os custos e benefícios ofertados, naquele determinado momento, pelo sistema [1].

Na Figura 1 estão ilustradas, as tecnologias posicionadas como pilares para o avanço da indústria 4.0, [5]. A coleta e a análise de dados de equipamentos e sistemas operacionais, sistemas corporativos e de clientes, apoiarão as decisões em tempo real. Com base no armazenamento destes dados reais, será possível simular o modelo de forma muito próxima

T. Martins, Universidade do Estado de Santa Catarina (UDESC), Joinville, Santa Catarina, Brasil, tiagomts@gmail.com

S. V. G. Oliveira, Universidade do Estado de Santa Catarina (UDESC), Joinville, Santa Catarina, Brasil e Universidade Regional de Blumenau (FURB), Blumenau,Santa Catarina, Brasil, sergio_vidal@ieee.org.

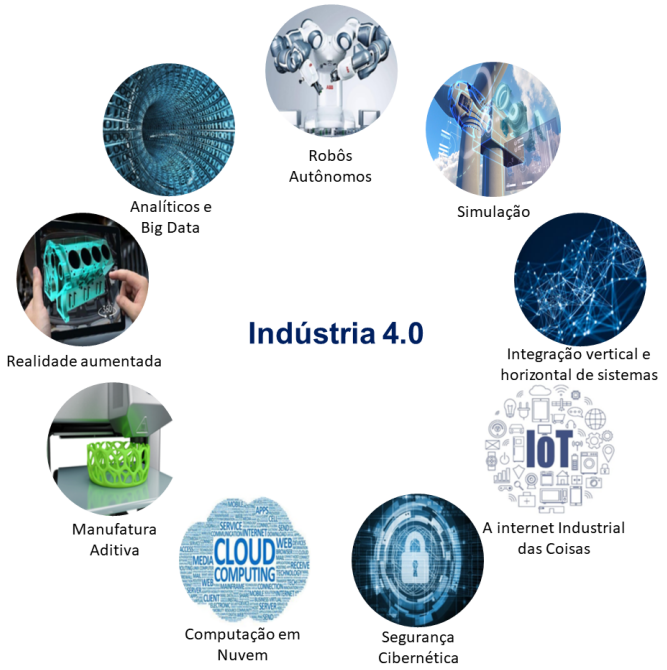

Fig. 1. Pilares da indústria 4.0 [5].

do mundo real. Robôs estão se tornando mais autônomos, flexíveis e cooperativos, no futuro eles vão interagir entre si e de modo seguro trabalhar lado a lado com os seres humanos. O compartilhamento de dados, permitirá a criação cadeias de valor verdadeiramente automatizadas e a IIoT possibilitará que até mesmo dispositivos menos sofisticados, possam usar computação embarcada para se conectar à internet.

Nos próximos anos o desempenho das tecnologias evoluirá e consequentemente a *cloud* (nuvem) melhorará, atingindo tempos de resposta de apenas alguns milissegundos. Pensando nisto, empresas devem desenvolver suas ofertas digitais preparadas para operação em nuvem, buscando diminuir dependências, entregar, disponibilidade e desempenho dos seus serviços, para quaisquer clientes no mundo.

Empresas começaram a adotar a manufatura aditiva, como a impressão 3D, para desenvolver protótipos ou para produzir peças unitárias de um determinado produto. No futuro, elas devem usar a realidade aumentada para fornecer informações em tempo real, melhorar a tomada de decisões e os procedimentos operacionais de seus funcionários.

Como estar conectado será essencial na Indústria 4.0, com a comunicação bidirecional destes sistemas, faz-se necessário proteger linhas de fabricação e sistemas industriais críticos de ameaças de *cybersecurity*. Desde modo comunicações seguras e confiáveis, bem como controle de acesso, serão essenciais para equipamentos compatíveis com a indústria 4.0 [5].

III. Fundamentos de Cybersecurity na Internet Industrial das Coisas

Antes da indústria 4.0, o termo proteção de equipamentos, era diretamente relacionado ao seu grau de proteção para aplicação em áreas classificadas, por exemplo, IP67 [6]. Hoje o cenário é outro e o tema *cybersecurity* é recente para muitos pesquisadores da eletrônica de potência. Este tópico visa apresentar e conceitualizar os principais fundamentos de *cybersecurity*: seus atores, ferramentas, ataques mais disseminados, bem como, metodologias para gestão e mitigação de riscos, vulnerabilidades e incidentes.

A. Atores

Quem são os atores de *cyberattacks*, o que eles querem e como planejam obtê-lo? Embora exista uma variedade de agentes e ameaças por aí, a maioria deles se enquadra nas seguintes categorias [7]:

1) Criminosos Profissionais: Geralmente o objetivo dos criminosos profissionais é o ganho financeiro, através de ataques digitais, realizam ameaças ou extorquem as suas vítimas com dados roubados durante ataques digitais [7].

2) Governos: Governos estão se organizando e investindo em capacidades cibernéticas ofensivas. O uso militar de capacidades digitais, ataques digitais com o objetivo de adulteração e manipulação de dados, é cada vez mais utilizado para complementar ferramentas convencionais [7].

3) Terroristas: Até agora não conseguiram utilizar *cyberattacks* para realizar um atentado de grandes proporções contra a humanidade. No entanto, causam alerta social com ataques digitais em pequena escala [7].

4) Vândalos cibernéticos: Realizam ataques digitais como passatempo, ou seja, uma forma de desafio para demonstrar suas próprias capacidades. O nível de conhecimento para estes ataques geralmente é baixo, se aproveitam de sistemas menos seguros, geralmente equipamentos residenciais [7].

5) Interno: Ameaças internas podem vir de ações não intencionais, descuidos ou de funcionários mal-intencionados, que por motivos financeiros, políticos ou pessoais, manipulam deliberadamente sistemas ou vazam informações sigilosas [7].

6) Organizações privadas: Organizações privadas podem realizar ameaças com o intuito de afetar a confidencialidade dos sistemas para ganhos financeiros, melhorar sua posição competitiva, ou para espionagem industrial [7].

B. Ferramentas e Tipos de Ataques

Malwares (*software* mal-intencionados são as principais ferramentas usadas para obter acesso não autorizado a computadores, roubar informações e interromper ou desabilitar redes e serviços [7]:

1) Vírus e Vermes (Worms): São tipos de *malwares* que se propagam multiplicando-se, tornando-se parte de outro programa. Vírus e vermes podem variar de gravidade, causando efeitos levemente irritantes a danos extremamente críticos. Vermes se diferem na sua disseminação, pois de forma independentes, se propagam através de vulnerabilidades no equipamento infectado [9].

2) Cavalos de Tróia (Trojans): São programas que fingem ser legítimos, mas fornecem aos agentes mal-intencionados uma *backdoor* (acesso pela porta dos fundos) no sistema operacional [9].

3) Software Espiões (Spyware): Um termo geral para programas que monitoram e coletam informações de um sistema [9].

4) Robôs (Bots): Um robô mal-intencionado é um *malware* projetado para infectar e possibilitar o controle remoto de um equipamento. Uma vez infectado ele pode ser recrutado de forma invisível para formar grupos de robôs *botnets* (redes de robôs). Com uma *botnet* invasores podem lançar ataques de grande proporção, contra os seus alvos, ou usar o poder computacional da *botnet* para atividades como a mineração de *criptocurrency* (moedas digitais) [7], [9].

5) Kits de exploração (Exploit kit): Existem desenvolvedores de *software* que oferecem kits de exploração prontos para uso e com interfaces amigáveis para infectar usuários com *malware* [10].

6) Ataques de negação de serviço: Atores continuam descobrindo novos métodos para viabilizar ataques de negação de serviço (DDoS, *Distributed Denial-of-Service*). O nível de conhecimento necessário para um ator realizar um ataque DDoS não é alto, devido ao número de sites disponíveis que oferecem DDoS como serviço [7], [9].

7) Ataques de phishing: Para conduzir um ataque de *phishing*, um ator mal-intencionado tenta se passar por uma determinada pessoa ou corporação para pescar seu alvo. Os agentes mal-intencionados que usam ataques de *phishing* geralmente tentam falsificar o logotipo ou o site de uma corporação ou indivíduo [7].

8) Man-in-the-Midle (MITM): É um tipo de ataque onde o invasor toma o controle do canal de comunicação entre dois ou mais dispositivos. [11]. De um modo geral, o ataque MITM visa comprometer:

1) Confidencialidade, interceptando a comunicação;
2) Integridade, interceptando a comunicação e modificando mensagens;
3) Disponibilidade, interceptando e destruindo mensagens ou modificando mensagens para fazer com que uma das partes encerre a comunicação [12], [13];

C. Gestão de Vulnerabilidades

Uma vulnerabilidade é uma fraqueza em um produto ou componente de terceiros que pode gerar um incidente de segurança [14].

Vulnerabilidades são divulgadas e publicadas por órgãos ligados ao *Computer Emergency Response Team* (CERT) [15]. No Brasil, o CERT.br [16] é responsável por tratar incidentes de segurança em computadores conectados à Internet.

D. Gestão e Mitigação de Riscos

A gestão de riscos de segurança da informação é o conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para mitigar ou eliminar os riscos [14].

O processo de gerenciamento de risco inicia com a definição dos critérios, do escopo, e dos limites que serão considerados na avaliação dos riscos. Identificar os riscos a partir das vulnerabilidade existentes; levantar e estimar a probabilidade de um incidente ocorrer, a partir daquele determinado risco e priorizá-los, de modo que, os investimentos em mecanismos de proteção, estejam de acordo com o grau de importância para o negócio, são passos essenciais para o êxito do processo.

O tratamento deve sempre iniciar do risco mais prioritário para o menos prioritário, quando possível, deve-se focar em: eliminar riscos considerados demasiadamente elevados para o negócio; mitigar, reduzindo a probabilidade de um incidente ocorrer para limites aceitáveis; transferi-los ou compartilhá-los com outra entidade; contratação de seguro por exemplo, também é valido quando não for viável eliminá-los. Quando o investimento em contramedidas se mostra inviável, aceitá-los e monitorá-los pode ser a única opção para a organização. [14], [17].

E. Gestão de Incidentes

Um incidente é uma vulnerabilidade explorada ou um problema de segurança emergente, como uma tentativa de invasão. Ao ocorrer um incidente muitas vezes é necessário realizar contramedidas imediatas, como recuperar, reinicializar ou até mesmo desconectar os sistemas afetados [7].

É importante que organizações destinem uma equipe de profissionais capacitados para atuar e manter um processo de gestão de incidentes, visando coordenar ações a serem realizadas no tratamento e resposta durante incidentes.

IV. Incidentes de cybersecurity em Tecnologia Operacionais

A. Stuxnet

O *worm* Stuxnet, foi o primeiro *malware* que obteve êxito em atacar um sistema de controle industrial (ICS - *Industrial Control System*) em 2010, foi utilizado para interromper o processo de enriquecimento de urânio nas instalações nucleares iranianas em Natanz.

Acredita-se que estas instalações eram seu único objetivo, pois o STUXNET foi desenvolvido por alguém que tinha o entendimento detalhado do processo industrial da planta iraniana. Geralmente é difícil encontrar *worms* que contenham vulnerabilidades desconhecidas (*zero-day vulnerabilities*), no entanto o Stuxnet foi muito bem elaborado, seu código com 500 kilobytes, era 50 vezes maior que a média dos *worms* da época e continha 4 destas vulnerabilidades.

O *worm* procurava por conversores de frequência fabricados pela FararoPaya e alterava a frequência de operação das centrifugas para faixas fora dos limites de operação do equipamento, como consequência obteve êxito na interrupção do processo de operação da usina [7] [18].

B. Dragonfly/Havex

A campanha Dragonfly (Libélula), foi uma campanha de espionagem que visou vários sistemas de controle industriais (ICS) empresarias, com ênfase nas indústrias de energia elétrica e petroquímicas, estima-se que no geral mais de 2.000 empresas tiveram suas instalações espionadas pelo *malware* Havex através do padrão Classico do OPC [20], que não possui recursos de segurança [21].

C. Vulnerabilidade Jeep Cherokee

Em 2015, pesquisadores invadiram e modificaram o sistema de controle do Jeep Cherokee. A existência de uma *backdoor* possibilitou através da rede celular, acesso ao *software* Uconnect que conecta o Jeep à internet. Com o uso de um *Fentocell* (Pequena Estação Radio Base) conseguiram controlar o veículo a uma distância de até 70 milhas, desativar o sistema de frenagem e desligar o motor do veículo, enquanto o mesmo trafegava pela rodovia [22].

O exercício foi realizado para demostrar que carros conectados também podem ser vulneráveis e sofrer ataques. Após descoberta a vulnerabilidade a Fiat Chrysler, precisou realizar o *recall* (chamada para reparo de defeitos de fabricação pelo fabricante), de aproximadamente um milhão e meio de veículos [23].

D. Crashoverride

Em dezembro de 2016 o *malware* Crashoverride, foi utilizado para um *cyberattack* em uma subestação de transmissão de energia em Kiev na Ucrânia. O ataque resultou em um blecaute onde mais de 80 mil residências ficaram sem eletricidade [10]. O Crashoverride foi o primeiro *malware* projetado e implantado para atacar redes elétricas, mesmo tendo causado um dano notório nas instalações de Kiev, especialistas acreditam que o ataque pode ter sido uma prova de conceito para entender o potencial do *malware*. O *malware* adotou uma abordagem semelhante ao Stuxnet com conhecimento do processo industrial, utilizou o protocolo OPC e as bibliotecas das Interfaces Homem-Máquina (HMI, *Human Machine Interface*), no entanto ele fez todas essas coisas com sofisticação adicional, criando uma plataforma para conduzir ataques em vários ambientes e não confinados apenas a plataformas e fornecedores específicos [7].

V. Cybersecurity aplicada na Eletrônica de Potência

A. Pesquisas e Iniciativas Mundiais

Operadores e companhias de geração, fornecimento e distribuição de energia reconhecem que existem vulnerabilidades em redes inteligentes (Smart Grids) e que ataques bem-sucedidos como o de Kiev, podem voltar a ocorrer em outras infraestruturas [24].

Com o intuito de mitigar ameaças digitais, empresas e órgãos governamentais veem se unindo para criar novas linhas de defesa contra esses *cyberattacks*. Nos EUA, a Casa Branca aprovou o Plano Nacional de Ação de Segurança e Resiliência da Rede Elétrica, um esforço colaborativo entre os governos federais dos EUA e Canadá. O plano tem como objetivo proteger a rede elétrica atual e melhorar a preparação, gerenciar contingências e aprimorar os esforços de resposta e recuperação para construir, no futuro uma rede elétrica mais segura e resiliente. [24]

Na mesma linha, o Departamento de Energia (*DoE*) e o Departamento de Segurança Interna (*DHS*), investem em projetos com a visão de que até 2020, os sistemas de fornecimento de energia resilientes serão projetados, instalados, operados e mantidos para sobreviver a incidentes cibernéticos. Dentre eles destacam-se o projeto Sistemas de Entrega de Energia Evolutiva e Sustentável (*SEEDS*) da Universidade de Arkansas que recebeu a quantia de 12,2 milhões de dólares, conduzido pelo professor Alan Mantooth, presidente da IEEE Power Electronics Society, tem como objetivo conduzir pesquisas e desenvolver tecnologias inovadoras de *cybersecurity*, ferramentas e metodologias que promovam a capacidade do setor de energia de sobreviver a ataques e incidentes cibernéticos sem afetar funções críticas do sistema [1], [24]. O outro projeto em andamento é a mitigação de ataques de falsificação de dados no controle automático de geração (AGC), conduzido pelo professor Qinghua Li, também da Universidade de Arkansas, recebeu 22,2 milhões de dólares em recursos. O AGC é um sistema para ajustar a potência de vários geradores em diferentes usinas, em resposta a mudanças na carga. Como uma rede elétrica exige que a geração e a carga sejam equilibradas, ajustes frequentes na saída dos geradores são necessários para manter o equilíbrio do sistema. Contudo, invasores podem falsificar a frequência ou as medições de troca de potência da linha para causar um erro e criar instabilidade na rede elétrica, a equipe de Li desenvolveu uma tecnologia, que utiliza rede neurais para aprender padrões normais, detectar a falsificação de dados e anomalias no AGC com intuito de aumentar a resiliência da rede elétrica [24].

Na Europa, a fim de aumentar a conscientização dos Estados-Membros sobre os incidentes cibernéticos, a Comissão Europeia em 2016, assinou um acordo de *cybersecurity* com a indústria europeia, intensificando os esforços para combater ameaças digitais. Acredita-se que nesta parceria público-privada sejam mobilizado 1,8 bilhões de euros para investimentos em *cybersecurity* até 2020. A parceria contará com a participação de membros das administrações públicas nacionais, regionais e locais, centros de investigação e universidades da união europeia, e tem como objetivo promover a cooperação no processo de investigação e inovação e criar soluções de *cybersecurity* para vários setores como, energia, saúde, transportes e finanças [25].

Em conjunto com esta parceria o parlamento europeu aprovou e adotou, a Diretiva Segurança das Redes e da Informação, com o objetivo de criar uma série de medidas jurídicas para aumentar o nível global de *cybersecurity* na União Europeia, garantindo a conscientização e preparação dos estados-membros, exigindo que eles estejam adequadamente equipados, em termos de capacidade técnica e organizacional, para evitar, detectar e mitigar incidentes e riscos ligados às redes e aos sistemas de informação. A diretiva também determina a necessidade de se criar grupos de cooperação, a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os estados-membros, disseminando a cultura de segurança em todos os setores da sociedade. Principalmente, para as áreas de tecnologia da informação e comunicação, de empresas e órgãos responsáveis por recursos essenciais como: energia, transportes, água, infraestruturas, mercado financeiro, saúde, etc. Determinando, que empresas desses setores, identificadas pelos Estados-Membros como, operadoras de serviços essenciais, adotem medidas de segurança apropriadas e notifiquem incidentes

graves à autoridade nacional pertinente [26].

No Brasil, o tema da segurança das redes no setor de energia foi levado à Associação Brasileira das Empresas de Transmissão de Energia Elétrica (Abrate), para discutir como as empresas podem se proteger de *cyberattacks*. Empresas como a Eletrosul, já realizaram algumas iniciativas com o intuito de se proteger, porém defendem a padronização de contramedidas para *cybersecurity* no setor evitando que cada companhia se projeta do seu jeito. O plano da Abrate era ter até o fim de 2018, um documento com propostas para unificar os procedimentos de proteção no setor elétrico [27].

A UTC América Latina (*UTCAL, Utilities Telecom & Tecnnology Council Latin America*), associação das empresas e profissionais de telecomunicações nas áreas de energia, gás e água, segue na mesma linha da Abrate e também vem defendendo há dois anos que a Agência Nacional de Energia Elétrica (Aneel) e o Ministério de Minas e Energia criem direcionamentos para minimizar os riscos de *cyberattacks* no Brasil. A entidade encomendou um estudo junto ao CPqD, onde mostra que o impacto de um *cyberattack* que afetasse por cinco horas o abastecimento de energia das empresas CEB-DIS, Cemig-D, Eletropaulo e Light, geraria um prejuízo de 642 milhões de reais. Portanto além de um programa de segurança para o setor elétrico, a UTCAL defende que a Aneel autorize que parte do valor aplicado pelas empresas de geração, transmissão e distribuição de energia para pesquisa e desenvolvimento (P&D) seja também usado para *cybersecurity*, pois muitas empresas vêm enfrentando dificuldades de caixa e poderiam ter nessa flexibilização do uso dos recursos destinados a P&D, investimento em *cybersecurity* e consequentemente uma forma de se protegerem e, ao mesmo tempo, atender a Lei.

De acordo com a Aneel, por enquanto a discussão sobre essa flexibilização do uso dos recursos dos projetos de P&D para evitar *cyberattacks* ainda não está entre as prioridades da instituição. No entanto, algumas iniciativas já foram realizadas como o Workshop Internacional de Segurança Cibernética, realizado em outubro de 2016, em parceria com a UTCAL, tendo como objetivo, discutir à *cybersecurity* no setor de energia elétrica. Evento que teve a participação do Operador Nacional do Sistema (ONS), da Agência Brasileira de Inteligência (ABIN), do Centro de Defesa Cibernética do Exército Brasileiro (CDCIBER), do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br/NIC.br), do Centro de Pesquisa e Desenvolvimento em Telecomunicação (CPqD), das concessionarias: AES Eletropaulo, Cemig, Elektro, e empresas de *cybersecurity* como Siemens, Cisco, Nokia e TISafe. Portanto, neste momento, uma alternativa para as empresas, seria desenvolver projetos de P&D ligados a *cybersecurity*, assim, poderiam aproveitar os recursos obrigatórios para P&D na proteção de suas redes [27], [28].

Outras iniciativas mundiais, como a do grupo de trabalho de segurança do Consórcio da Internet Industrial (IIC, *Industrial Internet Consortium*) [35], foram criadas com o intuito de desenvolver, acelerar, criar um consenso, e promover práticas para a indústria no que diz respeito à segurança em sistemas industriais conectados a internet (Indústria 4.0). O guia de referência para a segurança na internet industrial (IISF, *Industrial Internet Security Framework*), publicado em setembro de 2016, é um documento abrangente, resultado de um trabalho colaborativo realizado pelos membros do IIC na construção de uma internet industrial segura e confiável. Compreende as melhores práticas de visão, experiência e segurança da IIoT, explicando como a segurança se encaixa nos negócios e operações industriais, definindo blocos de construção funcionais e fornecendo orientações técnicas e práticas para a implementação de segurança na internet industrial [3].

B. Protegendo Sistemas de Potência

Aplicações e sistemas eletrônicos de potência, como um acionamento motorizado em um processo industrial, fontes de alimentação, componentes de uma *E-LAN*, transformadores eletrônicos, agora estão acessíveis pela porta Ethernet e em muitas vezes conectado à internet, portanto vulneráveis a *cyberattacks*.

A CUI [29], fabricante de fontes de alimentações cuja solução de potência definida por software (SDP, *Software Defined Power*), desenvolvida em conjunto com a Virtual Power Systems [30], está sendo implantada rapidamente na indústria de TI e comunicações, para gerenciar e otimizar a entrega de energia, para *data centers* e sistemas de rede; vem tomando uma série de medidas para proteger sua solução que, a partir desta nova arquitetura, deixa de ser uma caixa isolada, para ser mais um dispositivo conectado a rede. *Handshake* (aperto de mão, ou seja, cumprimento entre dois dispositivos), para garantir a comunicação somente com dispositivos homologados e autenticação no acesso da porta JTAG, garantindo a programação segura do microntrolador são algumas das táticas aderidas pela empresa [24].

Além disso, de acordo com o fabricante, o *firmware* (*software* que gerencia e controla o componentes físicos de um equipamentos), será desenvolvido para validar se o *software* instalado foi adulterado, executando verificações automáticas na inicialização, além da validação ainda pode-se optar por soluções baseadas em *hardware* (parte física de um equipamentos eletrônico), elevando a confiabilidade da solução pois os *hackers* terão dificuldades de acessar a camada física para obter sucesso em seus *cyberattacks* [1], [3], [24]. Isto exigirá que a empresa pense em segurança em todos os seus processos industriais, desde a linha de fabricação, rastreando *software*, etiquetas, placas de circuito impresso, números de série, para garantir que seus testes automáticos verifiquem a versão correta do *firmware* instalado. Impedindo que seus dispositivos sejam alterados e configurados com *firmwares* customizados por terceiros [24].

A partir de agora, sistemas eletrônicos de potência para IoT necessitarão, a estreita colaboração entre especialistas em segurança e projetistas de eletrônica de potência para o desenvolvimento conjunto de um produto final sofisticado e robusto. O desafio reside em cada membro da equipe, aprender sobre os subsistemas da outra área para que o desenvolvimento conjunto resulte em um sistema otimizado [24]. Empresas, continuamente, devem buscar por soluções que impeçam *backdoors* em *softwares* e *firmware* que compõem seus produtos.

No entanto, esta abordagem não é simples, pois muitas vezes é necessário atravessar fronteiras, buscando garantir que não existam falhas ou *malwares* dentro de circuitos integrados, ou outros componentes fabricados por terceiros, para manter a integridade da cadeia de suprimentos e do dispositivo final [24]. Foi pensando nestes pontos que a PowerBox-Systems [31], fabricante europeia de fornecimento de energia, vem trabalhando em parceria com clientes e empresas especializadas em segurança, para adicionar camadas extras de segurança a suas fontes de alimentação digitais que, incorporam uma variedade de barramentos de comunicação e interfaces de usuário. Para desenvolver metodologias preditivas para análise de tráfego e eventos inesperados em seus produtos, buscou parcerias com universidades e pesquisadores que estão focados em encontrar, novas tecnologias de *cybersecurity* para a IoT que, não estejam focadas na atuais tecnologia de segurança e criptografia que oneram muito processamento do *CPS*, como por exemplo, o emprego de sensores, para monitorar e detectar *cyberattacks* em aplicações IoT [1], [24].

Proteger protocolos de comunicação, como o protocolo de gerenciamento de energia (PMBus, *Power Management Bus Protocol*) [32], também está no plano da Murata Power Solutions [33]. Embora o PMBus seja um barramento de comunicação interno em sistemas de fornecimento de energia, ele é vulnerável por meio do sistema operacional do equipamento. Portanto, o protocolo PMBus não foi desenvolvido contemplando segurança na comunicação, apesar de estar localizado em uma camada muito profunda, pode ser acessado externamente. Tendo acesso ao sistema operacional do dispositivo, neste caso, todos os benefícios do PMBus se tornam um problema em algum momento [24]. Robert V. White, que é considerado o pai da PMBus, disse que as especificações do PMBus permitem que fabricantes usem comandos específico para criar a sua própria camada de segurança no protocolo PMBus. Apesar disto, ele não sabe ao certo se isso foi, ou não, feito por um fabricante de dispositivo. No entanto, White afirmou que é importante ter em mente que, o PMBus está no nível mais baixo da hierarquia do sistema e não está conectado diretamente a dispositivos externos. Por ser baseado no protocolo I2C, o protocolo deve-se limitar a uma única placa de circuito. Portanto, para ter acesso no PMBus o criminoso precisa ter acesso físico à placa de circuito ou o controle do sistema operacional, sendo um problema muito mais grave para o sistema [24].

Preocupações semelhantes foram expressas pela empresa ELMG Digital Power [34]. A empresa tem como estratégia mitigar o risco evitando explorações conhecidas em algumas áreas consideradas frágeis à ameaças, como em barramentos para conexões de testes, de diagnóstico e de engenharia, barramentos I2C e SPI. Sempre que possível, fazem o particionamento do código da aplicação e do *driver* do conversor com uma separação física. Evitam atualizações em campo. Optam por soluções embarcadas em um único circuito impresso e, sempre onde possível, não fazem uso, de barramentos de comunicação sem camadas de segurança como o I2C, ou quando necessário, aplicam criptografia mínima, ofuscando os dados em uma camada superior ao barramento, para que os pacotes de dados fiquem um pouco ilegíveis. Controle de acesso do usuário com *logins* exclusivos, *logs* e regras para remover o acesso de um determinado usuário por determinado período são políticas também adotas e implementadas aos produtos da empresa [24].

C. Recomendações para cybersecurity de CPSs

Dispositivos terminais (*Endpoints*) são elementos de um sistema IoT que possui recursos de computação e comunicação e expõe seus recursos funcionais. Cada dispositivo possui diferentes requisitos e restrições de *hardware* que afetam o nível de proteção que pode ser alcançado. Mecanismos e técnicas de segurança devem ser aplicados aos dispositivos, dependendo de suas funções e seus requisitos de segurança. Proteger o dispositivo é assegurar a disponibilidade, confidencialidade e integridade da funcionalidade executada por ele. De acordo com o *IIC* os seguintes mecanismos e técnicas devem ser empregados a fim de mitigar vulnerabilidades e ameaças nos dispositivos:

- Segurança Física: Deve fornecer proteção física com mecanismos de prevenção contra adulteração e roubo para evitar alterações descontroladas ou remoção do dispositivo.
- Raiz de Confiança (RoT, *Roots of Trust*) [36]: Determina o nível de confiança na autenticidade das credenciais pertencentes a esse dispositivo específico. A raiz de confiança deve ser capaz de gerar, gerenciar e armazenar a identidade do dispositivo e não pode ser violada.
- Identidade: Distingui o dispositivo com base nas suas propriedades e certifica que o dispositivo é único e não foi clonado, adulterado.
- Controle de Acesso: Garante que a identificação, autenticação e autorização adequadas sejam realizadas antes da concessão de quaisquer recursos ou serviços do dispositivo.
- Proteção de Integridade: Validar a integridade do dispositivo. A identidade deve ser protegida adequadamente nas raízes de confiança para manter a integridade do dispositivo e evitar falsificação de identidade, e a integridade de dados deve ser monitorada e mantida para estabelecer confiança nos dados, validando que suas funções estão sendo executadas da forma prevista.
- Proteção de Dados: Proteger o acesso e impedir a falsificação de dados do dispositivo por meio de criptografia, técnicas de isolamento, realizando a decomposição do *software* em micro serviços (*containerization*) e controle de acesso.
- Análise e monitoração: Garantir a prevenção, detecção e recuperação de qualquer atividade desviante da política do dispositivo.
- Configuração e o gerenciamento: Garantir que todas as alterações feitas nos dispositivos sejam realizadas de maneira controlada e gerenciadas.
- Técnicas de Criptografia: Fazer uso de mecanismos de criptografia para a transformação de dados, a fim de ocultar seu conteúdo informativo, impedir sua modificação e seu uso não autorizado.

- Técnicas de Isolamento: Isolar camadas mais privilegiada do sistema de outras camadas menos privilegiadas, protegendo assim de atividades mal-intencionadas e das falhas que podem existir em uma das outras camadas existentes.

É importante que métodos de atualizações remotas sejam disponibilizados ao dispositivo, para controle de atualizações de políticas e configurações de segurança, possibilitando aplicação de *patches* para correção de vulnerabilidades conhecidas, de modo a garantir a disponibilidade do sistema pelos próximos 10 a 20 anos [3].

D. Normatizações

Quando a normatização dizer respeito à *cybersecurity*, estar em conformidade com determinadas normas, pode ser algo muito complexo. Pois idealmente, as implementações de segurança devem ser atualizadas periodicamente para se adaptar às novas ameaças e esta necessidade, possivelmente, desencadeará a re-certificação de certos produtos.

Um exemplo é o desafio apresentado pelas atualizações de segurança para dispositivos que precisam estar em conformidade com a Diretiva Européia de Máquinas 2006/42/EC2, apenas máquinas que cumpram a diretiva e recebem o selo CE podem ser vendidas dentro da União Europeia [37].

Atualmente a norma de segurança mais usada e disseminada no mundo é o ISO/IEC 27001: 2013 (ISO 27001), voltada principalmente para TI corporativa e utilizada em quase todas as grandes e médias empresas [3], [38].

Muitas normas não são obrigatórias como o caso da ISO/IEC 27002 e IEC 62443-2-3, que orientam os operadores sobre como implementar medidas adequadas para proteger o ambiente. No entanto, também existem normas obrigatórias como a NERC-CIP, norma norte-americana exigida pelo governo dos EUA e a BDEW, norma alemã/austríaca que também é exigida pelos seus respectivos governos [7].

Quando o assunto é segurança em automação industrial e sistemas de controle, a série de normas ISA/IEC 62443 deve ser considerada. Escrita por um trabalho conjunto entre o comitê ISA99 e o grupo de trabalho IEC TC65 WG10 da Comissão Eletrotécnica Internacional, a série engloba amplamente os conceitos de segurança eletrônica de sistemas de controle e manufatura, em diferentes tipos de sistemas, instalações e setores da indústria.

Os padrões 62443-4-1 e 62443-4-2 são amplamente esperados pelos proprietários e fornecedores de equipamentos. O primeiro define requisitos claros para o desenvolvimento de produtos, incluindo o uso de um ciclo de vida de desenvolvimento seguro. O segundo, detalha os requisitos técnicos de segurança para os componentes do sistema, construindo e complementando os requisitos de nível de sistema definidos na norma 62443-3-3. A conclusão e publicação destes documentos representa um avanço significativo de padrões e práticas para segurança de sistemas de controle industrial [3], [39].

O padrão IEEE 1686 rege *cybersecurity* de dispositivos eletrônicos inteligentes, o documento aborda acesso, operação, configuração, revisão de *firmware* e recuperação de dados destes dispositivos [3]. No que diz respeito a *cybersecurity* não se pode descartar normas para o desenvolvimento de *software*, como é o caso da norma IEC 62279, que define padrões para o desenvolvimento de aplicações de controle e proteção ferroviária; ISO 26262 para o setor automotivo; IEC 61511 controle de processos industriais e IEC 61513 instrumentação e controle de reatores nucleares.

Outro item que vem ganhando importância nos últimos tempos são as diretrizes, normas ou regulamentações desenvolvidas por determinados governos para proteger as Informações Pessoais e de Saúde de seus cidadãos. O GDPR da União Europeia e o HIPAA e PIPEDA da América do Norte. Como todas as empresas possuem dados pessoais relacionados, devem proteger informações como, contatos de clientes, fornecedores e dados pessoas do próprio departamento interno de RH, [3], [40].

VI. Conclusão

Com a transformação digital e a Indústria 4.0, equipamentos que antes operavam de forma isolada, vem sendo desenvolvidos para se conectarem a outros equipamentos criando sistemas totalmente integrados, gerando maior flexibilidade, velocidade, produtividade e qualidade no chão de fábrica.

Negligenciar a *cybersecurity* para atender custos e cronogramas no desenvolvimento de novos produtos conectados, pode ocasionar incidentes cibernéticos como nos casos do Stuxnet, Crassoverride e Jeep, gerando prejuízos consideráveis para a organização e clientes. Estes eventos foram suficientes para alertar blocos econômicos e países que se consideram alvos potenciais para estes criminosos. Muitos já iniciaram medidas, como normas e diretrizes, para mitigar a possibilidade de sofrerem com incidentes cibernéticos.

Soluções para a área de eletrônica de potência precisam ter cuidados extras pois, geralmente são empregadas em soluções e infraestrutura de serviços estratégicos como geração e distribuição de energia, sendo um dos alvos mais procurados por atores que desejam atacar aplicações e sistema industriais. Portanto estes equipamentos devem ser projetados e desenvolvidos para reduzir ao máximo suas vulnerabilidades. A análise deve iniciar na proteção física do equipamento, evitando acesso indevido a cartões de memória e em conexões de periféricos, como portas USB. Bem como, mecanismos que garantam a identidade e o controle de acesso do equipamento, com a autenticação, autorização e identificação do usuário. Sempre que possível deve ser empregada a proteção do barramento de comunicação, com o uso de técnicas de criptografia para ocultação dos dados, impedindo falsificação e garantindo a integridade da informação. Certificar a autenticidade do *firmware*, a partir de raiz de confiança baseada em *hardware*, e a implementação de ferramentas para atualizações de segurança, também são essências para garantir a disponibilidade e a vida útil da solução.

Apesar de muitas empresas já estarem fazendo o uso destes mecanismos para assegurar seus equipamentos, a aplicabilidade de alguns métodos da TI tradicional, como a criptografia pode ser inviabilizada financeiramente, pois consome considerável quantia de poder computacional para ser eficiente. Com o objetivo de criar novas tecnologias em *cybersecurity*, para endereçar soluções à estes dispositivos de baixo

custo e poder computacional, empresas do setor privado e órgãos públicos, veem constantemente investindo em projetos acadêmicos, que visam a aplicabilidade de Inteligencia Artificial e Aprendizado de Máquinas na área de *cybersecurity*.

Finalmente, este artigo buscou apresentar fundamentos, motivações, ferramentas e metodologias, que vem sendo empregadas no conceito de segurança cibernética, que possam ser embarcados em conversores e equipamentos no âmbito da eletrônica de potência.

AGRADECIMENTOS

À UDESC e à FURB pelos apoios institucionais, à WEG S.A. por incentivar seus profissionais na busca por conhecimento.

REFERÊNCIAS

[1] Balda, Juan Carlos et al. Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things. IEEE Power Electronics Magazine, v. 4, n. 4, p. 37-43, 2017.

[2] Al-Fuqaha, Ala et al. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, v. 17, n. 4, p. 2347-2376, 2015.

[3] Industrial Internet Consortium et al. Industrial Internet of Things Volume G4: Security Framework.
Ind. Internet Consort, p. 1-173, 2016.

[4] Hartmann, Brian; King, William P.; Narayanan, Subu. Digital manufacturing: The revolution will be virtualized. McKinsey Quarterly, Aug, 2015.

[5] Rubmann, Michael et al. Industry 4.0: The future of productivity and growth in manufacturing industries. Boston Consulting Group, v. 9, 2015.

[6] De Carvalho, Daniel Mendes. Sistema de Seguranca para Ambientes com Atmosfera Explosiva. Revista Brasileira de Mecatrônica, v. 1, n. 2, p. 14-25, 2018.

[7] Baars, Hans; Meulenbroek, Hans. Cyber security in energy automation. In: 2018 Petroleum and Chemical Industry Conference Europe (PCIC Europe) Paper No. EUR18_14.

[8] National Cyber Security Centre, Cyber Security Assessment Netherlands CSAN 2016. NCSC, 2016. Disponível em: ¡https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html¿. Acesso em: 20 set. 2018.

[9] CISCO. What Is the Difference: Viruses, Worms, Trojans, and Bots? Cisco 2018. Disponível em: ¡https://www.cisco.com/c/en/us/about/security-center/virus-differences.html¿ Acesso em: 19 set. 2018.

[10] Brocklehurst, Katherine. Crashoverride – First Malware Platform Designed to Take Down Electric Grids. Belden 2017. Disponível em: ¡https:lden.com/blog/ndustrial-security/crashoverride-first-malware-platform-designed-to-take-down-electric-grids¿ Acesso em: 20 ago. 2018.

[11] Conti, Mauro; Dragoni, Nicola; Lesyk, Viktor. A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, v. 18, n. 3, p. 2027-2051, 2016.

[12] Capec-94: Man in the Middle Attack. CAPEC 2014. Disponível em: ¡http://capec.mitre.org/data/definitions/94.html¿

[13] Green, Ian. DNS spoofing by the man in the middle. SANS Institute 2005. Disponível em: ¡https://www.sans.org/reading-room/whitepapers/dns/dns-spoofing-man-middle-1567¿ Acesso em: 5 set. 2018

[14] Santos, Valdeci Otacilio dos et al. Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001: 2006, 27002: 2005 e 27005: 2008. 2012.

[15] The CERT Division. Disponível em: ¡https://www.sei.cmu.edu/about/divisions/cert/index.cfm¿ Acesso em: 5 out. 2018

[16] CERT-BR, Sobre Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: ¡https://www.cert.br/sobre/¿ Acesso em: 5 out. 2018

[17] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005: Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação, 2008.

[18] Zetter, Kim. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books, 2014.

[19] Lee, Robert M.; Assante, Michael J.; Conway, Tim. ICS CP/PE (Cyber-to-physical or process effects) case study paper–media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline cyber attack. SANS Institute. 2014.

[20] Classic, OPC Foundation. Disponível em ¡https://opcfoundation.org/about/opc-technologies/opc-classic/¿ Acesso em: 25 out. 2018

[21] Samani, Raj. Operation Dragonfly Imperils Industrial Protocol, McAfee 2014 Disponível em ¡https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-dragonfly-imperils-industrial-protocol/¿ Acesso em: 25 out. 2018

[22] Miller, Charlie; Valasek, Chris. Remote exploitation of an unaltered passenger vehicle. Black Hat USA, v. 2015, p. 91, 2015.

[23] Seals, Tara; Chrysler Recalls 1.4m Vehicles for Remote Hacking Flaw, Infosecurity Magazine 2015 Disponível em: ¡https://www.infosecurity-magazine.com/news/chysler-recalls-14m-vehicles¿ Acesso em: 25 out. 2018.

[24] Bindra, Ashok. Securing the Power Grid: Protecting Smart Grids and Connected Power Systems from Cyberattacks. IEEE Power Electronics Magazine, v. 4, n. 3, p. 20-27, 2017.

[25] Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats, European Commission 2016 Disponivel em ¡http://europa.eu/rapid/press-release_IP-16-2321_en.htm¿ Acesso em: 25 out. 2018.

[26] Diretiva (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 European Commission. Disponível em ¡https://www.cncs.gov.pt/content/files/diretiva_2016_1148.pdf¿ Acesso em: 25 out. 2018.

[27] Pacheco, Paula. Sob ameaça de ciberataques, setor elétrico quer segurança, Estado de Minas Disponível em: ¡https://www.em.com.br/app/noticia/economia/2018/04/05/internas_-economia,949048/sob-ameaca-de-ciberataques-setor-eletrico-quer-seguranca.shtml¿ Acesso em: 30 out. 2018.

[28] Workshop Internacional de Segurança Cibernética, Agencia Nacional de Energia Elétrica, ANEEL 2016. Disponível em: ¡http://aneel.gov.br/workshop-internacional-de-seguranca-cibernetica¿ Acesso em: 30 out. 2018.

[29] CUI Inc. Disponível em ¡https://www.cui.com/company/about-us¿ Acesso em: 5 nov 2018.

[30] Virtual Power Systems. Disponível em ¡http://www.virtualpowersystems.com/company/¿ Acesso em: 5 nov 2018.

[31] Power Box Systems. Disponível em ¡https://www.powerbox-systems.com/powerbox-systems/mission-und-vision.html¿ Acesso em: 5 nov 2018.

[32] Power Management Bus. (PMBus) Disponível em ¡http://www.pmbus.org/About/AboutPMBus¿ Acesso em: 5 nov 2018.

[33] Murata. Disponível em ¡https://www.murata.com/en-us/about?intcid5c̄om_xxx_xxx_cmn_nv_xxx¿ Acesso em: 5 nov 2018.

[34] ELMG Digital Power. Disponível em ¡https://www.elmgdigitalpower.com/about-us/¿ Acesso em: 5 nov 2018.

[35] Industrial Internet Consortium. Disponível em ¡https://www.iiconsortium.org/about-us.htm¿ Acesso em: 5 nov 2018.

[36] Zimmer, Vincent; Krau, Michael. Establishing the root of trust. Intel 2016. Disponível em: ¡http://www.uefi.org/sites/default/files/resources/UEFI%20RoT%20white%20paper_Final%208%208%2016%20%28003%29.pdf¿ Acesso em: 25 nov 2018.

[37] DIRECTIVE, Machinery. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006. Official Journal of the European Union—09.06, p. L157, 2006.

[38] ISO/IEC, Information technology-Security techniques-Information security management systems-Requirements, ISO/IEC 27001:2013. International Organization for Standardization 2013.

[39] ISA-62443-4-1 (99.04.01) Security for industrial automation and control systems Draf 3, Edit 10 January 2016. Disponível em: ¡https://automatie-pma.com/wp-content/uploads/2016/09/ISA-62443-4-1-WD.pdf¿ Acesso em: 17 nov 2018.

[40] General Data Protection Regulation. Intersoft consulting. Disponível em: ¡https://gdpr-info.eu¿ Acesso em: 17 nov 2018.

Tiago Martins Nascido em Jaraguá do Sul/SC, em 1988. Bacharel em Engenharia de Telecomunicações pela Fundação Universidade Regional de Blumenau em 2010, é mestrando em Engenharia Elétrica pela Universidade do Estado de Santa Catarina. Atualmente é Analista de Infraestrutura de TI na empresa WEG Equipamentos Elétrico S.A., atua na execução de projetos de redes de computadores e telefonia da empresa.

Sérgio Vidal Garcia Oliveira nasceu em Lages, SC, Brasil, em 1974. Recebeu o B.S. em engenharia elétrica pela Universidade Regional de Blumenau (FURB) em 1999 e M.Sc. e doutor em engenharia elétrica pela Universidade Federal de Santa Catarina (UFSC), Florianópolis, Brasil, em 2001 e 2006, respectivamente. É professor de eletrônica de potência e acionamento elétrico na Universidade Regional de Blumenau (FURB) desde 2004 e, desde 2012, professor de eletrônica aplicada e projeto de conversor de eletrônica de potência na Universidade do Estado de Santa Catarina (UDESC). Seus tópicos de interesse de pesquisa são: acionamentos de motores integrados, transformadores de estado sólido, sistemas de geração distribuída e sistemas de tração elétrica. O Dr. Sérgio Vidal é membro da SOBRAEP - Sociedade Brasileira de Eletrônica de Potência. SBA - Sociedade Brasileira de Automação. IES - Sociedade de Eletrônica Industrial. PELS - Power Electronics Society e PES - Power & Energy Society.