UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TÉCNOLÓGICA – CTT
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM ENGENHARIA ELÉTRICA

TIAGO MARTINS

ESTUDO E APLICAÇÃO DE SEGURANÇA CIBERNÉTICA PARA CONVERSORES ESTÁTICOS CONECTADOS À IIOT

JOINVILLE
2021

TIAGO MARTINS

ESTUDO E APLICAÇÃO DE SEGURANÇA CIBERNÉTICA PARA CONVERSORES ESTÁTICOS CONECTADOS À IIOT

Dissertação submetida ao Programa de Pós-Graduação Profissional em Engenharia Elétrica, do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para obtenção do grau de Mestre em Engenharia Elétrica.
Orientador: Prof. Dr. Sérgio Vidal Garcia Oliveira

JOINVILLE

2021

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Setorial do CCT/UDESC,

com os dados fornecidos pelo(a) autor(a)

Martins, Tiago
Estudo e aplicação de segurança cibernética para conversores estáticos conectados à IIoT / Tiago Martins. -- 2021.
154 p.

Orientador: Sérgio Vidal Garcia Oliveira
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação , Joinville, 2021.

1. Segurança cibernética. 2. Conversor. 3. IIoT. 4. Indústria 4.0. 5. IEC 62443. I. Oliveira, Sérgio Vidal Garcia. II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação . III. Título.

TIAGO MARTINS

ESTUDO E APLICAÇÃO DE SEGURANÇA CIBERNÉTICA PARA CONVERSORES ESTÁTICOS CONECTADOS À IIOT

Dissertação submetida ao Programa de Pós-Graduação Profissional em Engenharia Elétrica, do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para obtenção do grau de Mestre em Engenharia Elétrica.
Orientador: Prof. Dr. Sérgio Vidal Garcia Oliveira

BANCA EXAMINADORA

Prof. Dr. Sérgio Vidal Garcia Oliveira
UDESC (Orientador/Presidente)

Membros:

Dr. Gleisson Jardim Franca
WEG Drives & Controls Automação LTDA

Prof. Dr. Charles Christian Miers
UDESC

Prof. Dr. Joselito Anastácio Heerdt
UDESC (Suplente)

Joinville, 28 de maio de 2021.

Dedico à minha esposa, aos meus filhos e aos meus familiares, que me incentivaram e me deram todo o suporte para que eu pudesse obter mais esta conquista.

AGRADECIMENTOS

Agradeço aos meus filhos pela paciência e compreensão.

À minha esposa pelo amor e por ter dado todo o suporte necessário, para que eu pudesse me dedicar e nunca desistir.

Aos meus pais que sempre estiveram ao meu lado, me apoiando e me incentivando na busca pelo conhecimento.

Ao meu amigo Richard, por ter me incentivado a buscar novos desafios e me acompanhado no início desta jornada.

Aos meus gestores e a WEG S.A. pelos recursos, pelo tempo e pela flexibilidade.

Aos meus familiares, amigos e colegas pelo apoio durante toda esta jornada.

Ao meu orientador, deixo um agradecimento especial, por compreender o meu esforço, em compartilhar o tempo entre a minha vida pessoal, profissional e acadêmica, me orientando de forma excepcional, sempre que se fez necessário.

RESUMO

Conversores estáticos e demais equipamentos da área de eletrônica de potência, estão cada vez mais conectados à Internet e integrados ao domínio da tecnologia da informação. Fabricantes de conversores, já ofertam soluções digitais para assistência remota e monitoramento em tempo real de seus produtos. Tais capacidades, necessitam de um fluxo bidirecional de informação e consequentemente tornam os sistemas vulneráveis a ataques cibernéticos. Neste trabalho, com o objetivo de se elevar a maturidade da segurança e do controle de acesso de conversores estáticos aplicados em acionamentos elétricos, propõe-se o desenvolvimento de um subsistema de segurança cibernética para ser incorporado ao sistema de comando de um conversor estático indireto CA/CA. Primeiramente, realiza-se uma revisão de literatura sobre transformação digital, Indústria 4.0 e segurança cibernética na área de eletrônica de potência e no domínio da tecnologia operacional, na qual apresentam-se seus fundamentos, os conceitos de disponibilidade, integridade e confidencialidade, atores, tipos de ataques, incidentes ocorridos e iniciativas adotadas pelo setor elétrico e pela indústria de manufatura. Após, com base nas especificações da norma IEC 62443-4-2, e em recomendações dos *frameworks* de segurança cibernética desenvolvidos pelo National Institute of Standards and Technology (NIST) e pelo Internet Industrial Consortium (IIC), aplicam-se mecanismos como assinatura digital e chaves criptográficas, para a construção de uma raiz de confiança (RoT) e de um canal de comunicação seguro, através do protocolo Modbus/TLS, para o desenvolvimento de um controle de acesso baseado em funções (RBAC), com o intuito de possibilitar a segregação dos direitos de uso de usuários humanos e demais dispositivos. Finalmente, estes mecanismos são submetidos a ensaios e seus resultados são comparados aos requisitos especificados na IEC 62443-4-2, com o intuito de quantificar a aderência do subsistema de segurança cibernética a norma.

Palavras-chave: Segurança cibernética. Conversor. IIoT. Indústria 4.0. IEC 62443.

ABSTRACT

Static converters and other equipment in power electronics are increasingly connected to the Internet and integrated into the information technology domain. Converter manufacturers already offer digital solutions for remote assistance and real-time monitoring of their products. Such capabilities require a two-way flow of information and consequently make systems vulnerable to cyberattacks. In this work, to increase the maturity of the cybersecurity and access control of static converters applied to electrical drives, it is proposed the development of a cybersecurity subsystem be incorporated into the control system of an AC-AC indirect converter. A literature review on digital transformation, Industry 4.0 and cybersecurity is carried out in the area of power electronics and in the operational technology domain, where its foundations are presented, the concepts of availability, integrity and confidentiality, actors, types attacks, incidents and initiatives adopted by the electricity sector and the manufacturing industry. Based on the specifications of the IEC 62443-4-2 standard and recommendations of cybersecurity frameworks developed by the National Institute of Standards and Technology (NIST) and the Internet Industrial Consortium (IIC), mechanisms such as digital signature apply, cryptography and public keys are used, for the construction of a Root of Trust (RoT) and a secure communication channel, through the Modbus/TLS protocol, for the development of an access control based on roles (RBAC), to enable the segregation and use control of human users and other devices. These mechanisms are subjected to tests. Their results are compared to the requirements specified in the IEC 62443-4-2, in order to quantify the adherence of the cybersecurity subsystem to the standard.

Keywords: Cybersecurity. Converter. IIoT. Industry 4.0. IEC 62443. Drives