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 DE FREQUÊNCIA CONECTADOS À IIOT

JOINVILLE
2021

TIAGO MARTINS

ESTUDO E APLICAÇÃO DE SEGURANÇA CIBERNÉTICA PARA CONVERSORES DE FREQUÊNCIA 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 de frequência 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 Profissional em Engenharia Elétrica, 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 Profissional em Engenharia Elétrica. III. Título.

TIAGO MARTINS

ESTUDO E APLICAÇÃO DE SEGURANÇA CIBERNÉTICA PARA CONVERSORES DE FREQUÊNCIA 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

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3D	Three Dimensions – Três dimensões
3G	Third generation – Terceira geração de telecomunicações móveis sem fio
4G	Fourth generation – Quarta geração de telecomunicações móveis sem fio
5G	Fifth generation – Quinta geração de telecomunicações móveis sem fio
ABIN	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
ACL	Access control list – Lista Controle de Acesso
AGC	Automatic Generation Control – Controle automático de geração
AIC	Availability, Integrity and Confidentiality – Disponibilidade, integridade e confidencialidade
ANEEL	Agência Nacional de Energia Elétrica
ATP	Advanced Persistent Threat – Ameaça avançada persistente
BDEW	Bundesverband der Energie- und Wasserwirtschaft – Associação Alemã de Indústrias de Energia e Água
CDCiber	Centro de Defesa Cibernética do Brasil
CI	Circuito Impresso
CIA	Confidentiality, Integrity and Availability – Confidencialidade, integridade e disponibilidade
CIP	Critical infrastructure protection – Proteção de infraestrutura crítica
Nuvem	Cloud Computing – Computação em nuvem
CNPE	Conselho Nacional de Política Energética
CoT	Chain of Trust – Cadeia de confiança
CPqD	Centro de Pesquisa e Desenvolvimento em Telecomunicação
CPS	Cyber-Physical System – Sistema Físico Cibernético
CRC	Cyclic Redundancy Check – Verificação de redundância Cíclica
CRL	Certificate Revocation List – Lista para revogação de certificados digitais
CS	Cybersecurity – Segurança Cibernética
CSR	Certificate Signing Request – Arquivo para requisitar um certificado digital
CVE	Common Vulnerabilities and Exposures – Vulnerabilidades e exposições comuns
DAR	Data-at-Rest – Dados em repouso

DDoS	Distributed Denial-of-Service – Negação de serviço distribuida
DHS	Department of Homeland Security – Departamento de Segurança Interna
DIM	Data-in-Motion – Dados em movimento
DIU	Data-in-Use – Dados em uso
DoE	Department of Energy – Departamento de Energia
DoS	Denial-of-Service – Negação de Serviço
E-LAN	Energy -Local Area Network – Rede local – Energia
ERP	Enterprise Resource Planning – Planejamento dos Recursos da Empresa
EUA	Estados Unidos da América
FPGA	Field Programmable Gate Arrays
GDPR	General Data Protection Regulation – Regulamento Geral de Proteção de Dados
HIPAA	Health Insurance Portability and Accountability Act – Lei de portabilidade e responsabilidade de seguro saúde
HMI	Human Machin Interface – Interface Homem Máquina
HRoT	Hardware Root of Trust – Raiz de Confiança em Hardware
I2C	Inter-integrated Circuit Protocol – Protocolo circuito inter-integrado
IaaS	Infrastructure as a Service – Infraestrutura como Serviço
IACS	Industrial Automation and Control System – Sistema de automação e controle industrial
IEC	International Electrotechnical Commission – Comissão Eletrotécnica Internacional
IEEE	Institute of Electrical and Electronics Engineers – Instituto de Engenheiros Eletricistas e Eletrônicos
IGBT	Insulated-Gate Bipolar Transistor
IIC	Internet Industrial Consortium – Consórcio da Internet Industrial
IIoT	Industrial Internet of Things – Internet Industrial das Coisas
IISF	Industrial Internet Security Framework – Estrutura Segurança na Internet industrial
IoT	Internet of Things – Internet das Coisas
IP	Internet Protocol – Protocolo Internet
ISA	International Society of Automation – Sociedade Internacional de Automação
ISO	International Organization for Standardization – Organização Internacional para Padronização

JTAG	International Organization for Standardization – Organização Internacional para Padronização
LAN	Local Area Network – Rede local
LGPD	Lei Geral de Proteção de Dados Pessoais
LTE	Long Term Evolution – Padrão de comunicação 4G Evolução de Longo Prazo
M2M	Machine-to-Machine – Máquina para Máquina
MAC	Media Access Control – Controle de acesso de mídia
MD5	Message-digest 5
MES	Manufacturing Execution System – Sistema de Execução da Manufatura
MITM	Man-in-The-Middle – Ataque de interceptação do canal de comunicação
MME	Ministério de Minas e Energia
MMU	Memory Management Unit – Unidade de gerenciamento de memória
NERC	North American Electric Reliability Corporation – Corporação norte-americana de confiabilidade elétrica
NESA	Near East South Asia Center
NIST	National Institute of Standards and Technology - Instituto Nacional de Padrões e Tecnologia (EUA)
OCSP	Online Certificate Status Protocol - Protocolo de status de certificado online
OLE	Object Linking and Embedding – Vinculação e incorporação de objetos
ONS	Operador Nacional do Sistema
OPC	OLE for Process Control – OLE para controle de processos
OS	Operational System – Sistema Operacional
P&D	Pesquisa e Desenvolvimento
PaaS	Platform as a Service – Plataforma como Serviço
PIN	Personal Identification Number – Número de Identificação Pessoal
PIPEDA	Personal Information Protection and Electronic Documents Act – Lei de Proteção de Informações Pessoais e Documentos Eletrônicos
PLC	Program Logic Controller – Controlador Lógico Programado
PMBus	Power Management Bus Protocol – Protocolo de gerenciamento do barramento de energia
RAM	Memória RAM
REE	Rich Execution Environment – Ambiente de execução rico.
RoT	Roots of Trust – Raiz de Confiança
RTOS	Real Time Operational System – Sistema Operacional de tempo real

RTU	Remote Terminal Unit – Unidade terminal remota
SaaS	System as a Service – Sistema como Serviço
SCADA	Supervisory Control and Data Acquisition – Sistemas de supervisão e aquisição de dados
SD	Secure Digital –Digitalmente seguros (Cartões SD)
SDP	Software Defined Power – Potência Definida por Software
SEEDS	Secure Evolvable Energy Delivery Systems – Sistemas de Entrega de Energia Evolutiva e Sustentável
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface Protocol – Protocolo Interface Periférica Serial
SSL	Secure Sockets Layer – Protocolo camada de soquetes seguros
SVM	Security vulnerability management – gerenciamento de vulnerabilidade de segurança
TCP	Transmission Control Protocol – Protocolo de controle de transmissão
TEE	Trusted Execution Environment – Ambiente de execução confiável
TI	Tecnologia da Informação
TLS	Transport Layer Security – Protocolo de segurança da camada de transporte
TO	Tecnologia Operacional
TPM	Trusted Platform Modules – Módulos de plataformas confiáveis
UE	União Européia
UMTS	Universal Mobile Telecommunication System – Padrão de comunicação 3G Sistema de telecomunicação móvel universal

SUMÁRIO

1 INTRODUÇÃO

A Internet Industrial das Coisas (IIoT, *Industrial Internet of Things*) possibilitará o desenvolvimento de fábricas, redes elétricas e outros sistemas inteligentes, criando oportunidades de mercado para fabricantes de equipamentos, provedores de Internet e desenvolvedores de *software*. Estima-se que ao final desta década, mais de um trilhão de sensores, máquinas, objetos e dispositivos de IIoT estarão conectados, gerando 45% de todo o tráfego da Internet. Sendo que destes, 37% será gerado por coisas da área de manufatura e 7% por coisas relacionadas a eletricidade. [1]-[2]

Um sistema IIoT conecta e integra sistemas de controle industriais com sistemas analíticos, corporativos e autônomos. Otimizando a operação, possibilitando o controle, a colaboração e a tomada de decisão muitas vezes autônoma de equipamentos e processos de negócio, evoluindo a manufatura para uma nova era industrial, conhecida como Indústria 4.0. [3]

Sistemas de tecnologia operacional (TO) diferem dos tradicionais sistemas de tecnologia da informação (TI), porque usam sensores e atuadores em ambientes industriais. Estes interagem com o mundo real na qual, alterações descontroladas podem gerar perigosas situações em campo. Esse risco potencial eleva a importância da segurança, confiabilidade, privacidade e resiliência destes sistemas, acima dos níveis esperados em muitos ambientes tradicionais de TI. [3]

A Internet das Coisas (IoT, *Internet of Things*) possibilita a criação de Sistemas Físicos Cibernéticos (CPSs, *Cyber-Physical Systems*) mais eficientes e consequentemente mais inteligentes, como conversores estáticos conectados à rede de computadores, controlando processos industriais, sendo controlado e monitorado remotamente [2]. Esta capacidade de controle remoto com fluxo bidirecional de informações tem muitas vantagens, mas torna os sistemas vulneráveis a ataques cibernéticos.

1.1 OBJETIVO PRINCIPAL

O presente trabalho tem como principal objetivo: estudar, projetar, desenvolver e aplicar segurança cibernética (CS, *Cyber Security*), em dispositivos da área de eletrônica de potência na era da Indústria 4.0. Ao final do projeto, pretende-se apresentar ferramentas embarcadas no dispositivo que permitem assegurar sua disponibilidade, integridade e confidencialidade.

1.2 OBJETIVOS ESPECÍFICOS

Realizar revisão de literatura sobre segurança cibernética, suas motivações devido a transformação digital e Indústria 4.0, fundamentos, incidentes e pesquisas em tecnologias operacionais e sua aplicação na eletrônica de potência, mais especificamente em conversores estáticos aplicados em acionamentos elétricos.

Desenvolver e aplicar ferramentas de segurança cibernética para conversores estáticos de potência, realizando:

a) proteção da integridade, com o armazenamento seguro da identidade e a validação do *firmware* durante o processo de inicialização;
b) confidencialidade das credenciais e dos dados trafegados na comunicação com o *software* de parametrização;
c) controle e segmentação do acesso ao equipamento, com autenticação, autorização e auditoria de usuários.

Apresentar os resultados alcançados, com o objetivo de validar se as ferramentas desenvolvidas e aplicadas, irão mitigar as vulnerabilidades de segurança cibernética, existentes nos conversores atuais, elevando a sua maturidade na era da indústria 4.0.

1.3 JUSTIFICATIVA E RELEVÂNCIA

Este trabalho visa contribuir para evolução da área de eletrônica de potência nacional no que diz respeito à segurança cibernética. Acredita-se que existam poucos trabalhos em língua portuguesa, que abordam o tema. Motivados pelo recente interesse da comunidade da eletrônica de potência internacional, no qual pode-se destacar os artigos [2] e [4] publicados pela IEEE Power Electronics Magazine em 2017.

Na área de eletrônica de potência, conversores de energia possuem tensões de saída CA ou CC e dispositivos semicondutores tem como característica o chaveamento em altas frequências de comutação (acima de 20 kHz). A tarefa de detectar um ataque cibernético em tempo hábil nestes conversores se torna muito difícil, algoritmos de controle, ferramentas e metodologias para análise e aplicação da 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. [2]

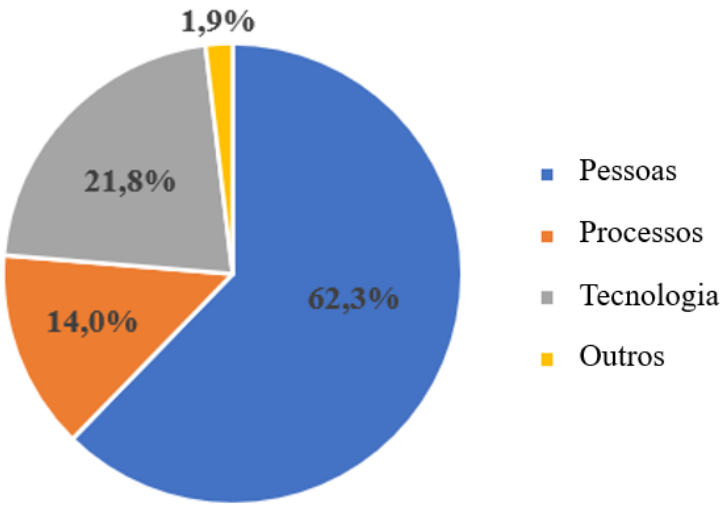
Uma pesquisa sobre segurança cibernética no domínio da tecnologia operacional (TO) realizada pelo instituto SANS em 2019 [5]. Entrevistou de forma global, mais de trezentos

profissionais que trabalham ou atuam com sistemas de controle operacionais. A pesquisa revela (Figura 1) que 62,3% dos entrevistados consideram, pessoas como o principal risco de comprometimento a segurança cibernética de um sistema de automação e controle industrial (IACS, *Industrial Automation and Control System*), definida na IEC 62443 como:

"coleção de pessoas, hardware, software e políticas envolvidas na operação do processo industrial e que podem afetar ou influenciar sua operação segura, protegida e confiável." [6]

O que não surpreende, porque o elemento humano está no cerne dos incidentes e violações de segurança cibernética. Elemento este, que é seguido de forma distante pela tecnologia (21,8%) e por processos (14%). [7]

Figura 1 – Maior risco de comprometer seus sistemas de TO



Fonte: Adaptado de SANS Institute. [7]

Pessoas é uma categoria de risco ampla, abrangendo atores externos e internos, de ações intencionais (mal-intencionadas) a não intencionais (acidentais, involuntárias, etc.). No entanto, de acordo com o relatório de investigações de violação de dados de 2020 da empresa de tecnologia Verizon, aproximadamente 30% das violações de segurança são ocasionadas devido a atores internos. [8]

Isto porque, ameaças internas são particularmente difíceis de se proteger, especialmente em TO, onde o conhecimento da situação e do processo são essenciais para reconhecer potenciais vulnerabilidades de segurança. Além disso, não é incomum no domínio de TO, pessoas terem mais privilégios de acesso do que o necessário para o seu trabalho, uma vez que

os mecanismos de acesso nestes dispositivos geralmente são limitados e privilégios de acesso mais elevados são concedidos, a pessoas com perfil de uso menos privilegiado, como operadores, durante imprevistos ou intervenções [7]. Pois erroneamente, considera-se que ambientes de TO, estão seguros contra ameaças de segurança cibernéticas.

1.4 ABRANGÊNCIA E DELIMITAÇÃO DO ESCOPO

Equipamentos da área de eletrônica de potência, estão sujeitos a vários tipos de ataques cibernéticos. Os mais comuns, são os ataques realizados na camada de *software*, porém também existem ataques de *hardware* de baixa complexidade, no qual utilizam-se ferramentas acessíveis para depurar interfaces JTAG e ataques de alta complexidade, no qual utiliza-se de laboratórios e equipamentos sofisticados, como microscópios eletrônicos, para realizar ataques a propriedade intelectual dos equipamentos, visando a realização da engenharia reversa.

Este trabalho delimita-se em mitigar ataques de *software* de baixa complexidade, desconsiderando ataques sofisticados aos componentes eletrônicos do dispositivo. Investigações e visões gerais sobre engenharia reversa de hardware são apresentadas nos trabalhos [9] e [10].

O escopo do projeto do controle de acesso proposto, visa proteger a disponibilidade do conversor, sua integridade e a confidencialidade dos seus dados contra ataques casuais, coincidentes ou intencionais por usuários não autorizados, sejam eles humanos, malwares ou dispositivos, que utilizem meios simples, poucos recursos, baixa motivação e habilidades em sistemas de automação e controle industrial.

As ferramentas desenvolvidas e aplicadas para a validação do conhecimento adquirido, limitam-se a um controle de acesso local, no qual, credenciais e regras de acesso são gerenciadas nativamente pelo subsistema de segurança cibernética do conversor. Desde modo, a sua aplicabilidade em ambientes com múltiplos conversores, pode trazer complexidade ao gerenciamento seguro destas credencias, pois não faz parte do escopo deste trabalho, o controle de acesso centralizado. No qual realiza-se, o gerenciamento das regras e credenciais de forma simultânea para todos os conversores.

A apresentação dos resultados em comparação com a norma IEC 62443-4-2, delimita-se unicamente na intenção de aproveitar a estrutura da norma, como forma de quantificar e qualificar os resultados obtidos. Pois sua publicação ocorreu durante o desenvolvimento deste trabalho e alguns de seus requisitos fundamentais, estão alinhados ao escopo previamente definido.

1.5 PUBLICAÇÕES

Em agosto de 2019 o artigo *Cybersecurity in the Power Electronics*, fruto deste trabalho, foi publicado na IEEE Latin America Transactions. [11]

Confidencialidade, integridade e disponibilidade são recursos essenciais para dispositivos conectados à IIoT. No entanto, a segurança cibernética nunca foi uma preocupação primordial para a eletrônica de potência, porque a maioria dos dispositivos foram projetados para operar de modo isolado, sem conectividade e transferência de dados com outros dispositivos. Com a transformação digital e a Indústria 4.0, houve uma mudança disruptiva neste cenário. Empresas, governos e universidades vêm estudando e desenvolvendo mecanismos para mitigar vulnerabilidades nesses dispositivos. O artigo publicado, apresenta uma revisão literária sobre segurança cibernética na eletrônica de potência, com uma introdução sobre transformação digital, conceitos da Indústria 4.0 e segurança cibernética na IIoT. Apresentando incidentes, pesquisas e ferramentas adotadas.

2 MANUFATURA DIGITAL

De acordo com o mercado, as indústrias de manufatura exigirão uma transformação digital nos próximos anos para continuarem competitivas e até mesmo se diferenciarem de seus concorrentes [12]. Tecnologias de manufatura digital e a Indústria 4.0, transformarão a manufatura influenciando áreas de pesquisa e desenvolvimento, suprimento, operações, *marketing*, vendas e serviços. No entanto, estas indústrias não somente irão consumir produtos e serviços inteligentes, como precisarão, preparar seus produtos e serviços para possibilitar a transformação digital dos seus próprios clientes.

2.1 TRANSFORMAÇÃO DIGITAL

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 poucas empresas estão aproveitando esses dados para conseguir capturar informações que possam gerar algum diferencial. A maioria das empresas descarta grande parte dos seus dados, antes de transformá-los em informações, para que os tomadores de decisão tenham a chance de usá-los. Empresas que conseguirem eliminar essa lacuna e gerar informações valiosas com esses dados, irão gerar lucros e crescimento. [12]

Tecnologias de manufatura digital e a IoT, permitirão que empresas conectem seus ativos a um segmento digital, construindo um fluxo contínuo de dados em toda a cadeia de valor, que ligará todas as fases do ciclo de vida do produto, do projeto à operação [12].

Alguns fabricantes já ofertam soluções digitais para diagnóstico e monitoração de seus produtos. A WEG em 2020 lançou o *Drive Scan*, disponibilizando informações dos seus conversores estáticos através da solução WEG *Motor Fleet Management* [13]. A ABB, oferta o *Ability Condition Monitoring for Drives* [14] e a Siemens oferta monitoração através da sua plataforma digital Mindsphere. [15]

Produtos mais sofisticados auxiliarão no desenvolvimento de fábricas, redes elétricas e muitos outros sistemas 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. [2]

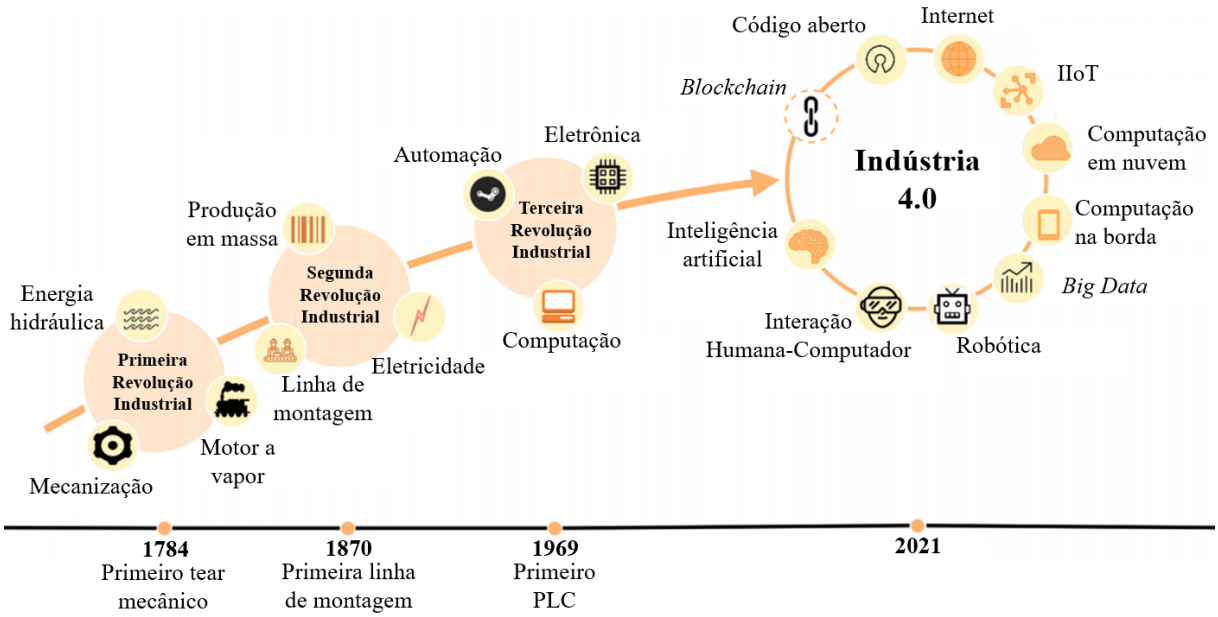
2.2 INDÚSTRIA 4.0

Nesta seção o conteúdo apresentado baseia-se nos trabalhos [16] e [17].

A Indústria 4.0, considerada por muitos como a quarta revolução industrial, é a digitalização e transformação de células automatizadas em instalações totalmente integradas, que se comunicam entre si e oferecem maior flexibilidade, velocidade, produtividade e qualidade no chão de fábrica [18]. Ou seja, um novo patamar de automação baseada na combinação de múltiplas tecnologias e soluções inovadoras, com o objetivo de alcançar um alto nível de eficiência operacional e produtividade na manufatura. [19]-[20]

Desde o século XVIII, o mundo passou por três revoluções que marcaram períodos de sua industrialização mundial (Figura 2). O primeiro, do final do século XVIII ao início do século XIX, usava como fonte de energia o vapor d'água e foi caracterizado pela invenção do tear mecânico em 1784 [16]. O segundo, do final do século XIX ao início de 1970, baseado na produção em massa e da divisão de trabalho, caracterizado pela implementação da linha de montagem em 1870, usava como fonte de energia a eletricidade [16]. O terceiro e atual período, iniciou nos anos setenta, representado pela automação após a invenção do controlador lógico programado (PLC, *Programmable Logic Controller*) em 1969. [16]

Figura 2 – Linha de tempo da revolução industrial



Fonte: Adaptado de Aceto et al. [17]

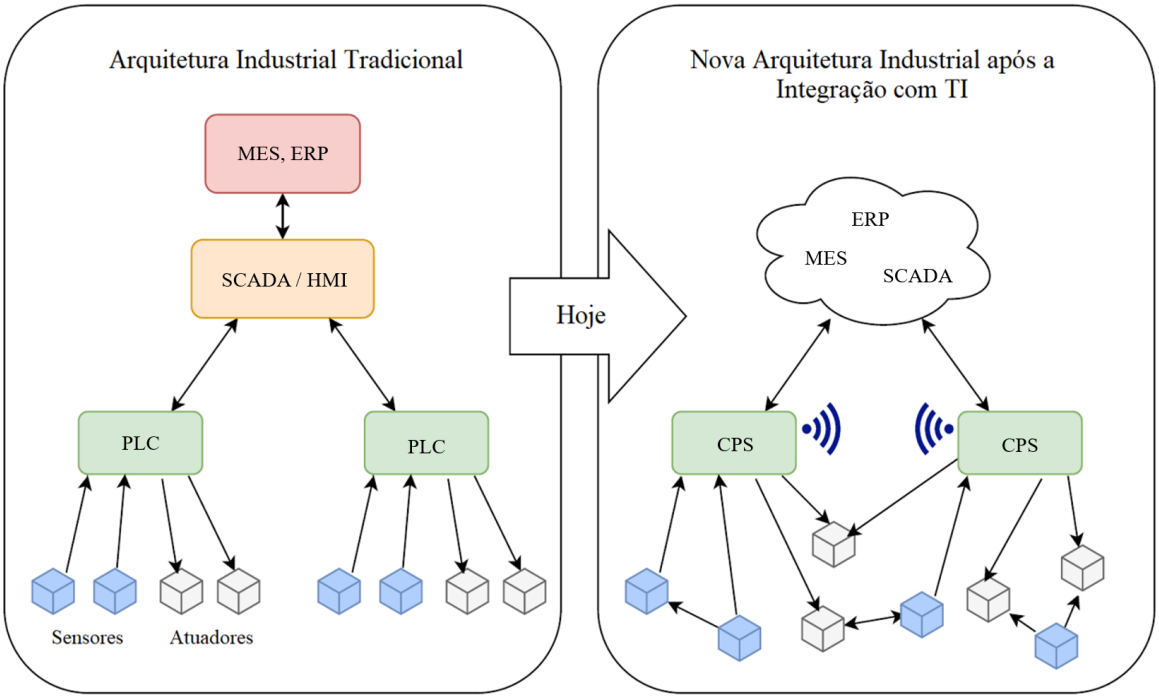
Após a introdução da mecanização, através da máquina a vapor, da eletricidade em conjunto com as linhas de montagem e da automação, a industrialização vai em direção a

transformação digital, com uma indústria cada vez mais automatizada e interconectada, apelidada como Indústria 4.0, a potencial quarta revolução industrial é baseada principalmente em CPSs, técnicas para extração e análise de uma grande quantidade de dados, como o *Big Data* e da IoT, caracterizada pela presença generalizada de uma variedade de objetos interconectados, como telefones celulares, sensores, atuadores e demais tecnologias. [17]

Um CPS refere-se a um mecanismo mecânico (físico) controlado por sistemas computacionais que trabalham de forma colaborativa, com sensores e atuadores capturando dados do processo e regulando seus parâmetros de acordo com um conjunto de regras definidas, obtendo assim uma interação entre os componentes físicos e computacionais [21]. Por exemplo, um conversor acionando um motor, conectado a uma rede de computadores que controla o processo industrial. [2]

Nessa transformação, sensores, máquinas, estações de trabalho e sistemas de TI serão integradas ao longo da cadeia de valor. A Figura 3 apresenta a evolução de um PLC para um CPS, agora CPSs podem interagir uns com os outros, usando protocolos de comunicação padrões, realizar análise de dados para prever falhas, configurar-se e adaptar-se a mudanças que podem surgir durante o processo de fabricação. [18],[20]

Figura 3 – Evolução da arquitetura industrial



Fonte: Adaptado de Lopez e Rubio. [22]

Um dos conceitos chaves que colocam a Indústria 4.0 possivelmente como a quarta-revolução industrial é a integração dos três eixos [23]:

a) integração horizontal, que diz respeito à cooperação entre empresas ao longo de uma cadeia de valor;
b) integração vertical, que se refere à ampla automação dentro de uma única empresa;
c) integração de ponta a ponta, que prevê conexões, máquina para máquina (M2M), homem para máquina, homem para homem, entre as cadeias de valor de todos os participantes.

Alguns estudos também apontam que são cinco, as principais características que definem a Indústria 4.0: [24]-[25]

a) a digitalização, otimização e customização da produção;
b) automação e adaptação;
c) interação homem para máquina;
d) serviços e negócios de valor agregado;
e) troca automática de dados e comunicação.

Além disto, a Figura 4 apresenta as nove tecnologias que são posicionadas como pilares para o avanço da Indústria 4.0 pois possibilitam alcançar as características apresentadas.

Figura 4 – Os nove pilares da Indústria 4.0

Fonte: Adaptado de Rübmann.[18]

A coleta e a análise de dados de equipamentos e sistemas operacionais, sistemas corporativos e de clientes, apoiarão as decisões em tempo real [17]. Com base no armazenamento destes dados reais, será possível simular o modelo de forma muito próxima do mundo real 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. [18]

Nos próximos anos o desempenho das tecnologias evoluirá e consequentemente a nuvem (cloud) melhorará, atingindo tempos de resposta de apenas alguns milissegundos [18]. Permitindo a alocação sob demanda de infraestrutura, plataforma e *software* como serviço (IaaS, PaaS e SaaS), faturamento por consumo a curto prazo, sem compromisso prévio do usuário [17]. Pensando nisto, empresas devem desenvolver suas ofertas digitais visando a escalabilidade e preparando-as para operação em nuvem, buscando diminuir dependências e garantir a disponibilidade e o desempenho das suas soluções, para quaisquer clientes no mundo.

Empresas adotam a manufatura aditiva, como a impressão 3D, para desenvolver protótipos ou para produzir peças unitárias de um determinado produto [18]. No futuro, devem usar a realidade aumentada para fornecer informações em tempo real, melhorar a tomada de decisões e os procedimentos operacionais de seus funcionários. [18]

A IoT, provavelmente um dos principais pilares da Indústria 4.0, é um conceito intimamente relacionado a "*ubiquitous computing"* do final dos anos oitenta, embora o primeiro uso do termo foi relatado por Kevin Ashton em 1999, relacionados com a utilização de etiquetas de identificação por radiofrequência (RFID) na logística. [26]

Definida pela ITU (International Telecommunication Union) como:

"Uma infraestrutura global para a sociedade da informação, possibilitando serviços avançados interconectando coisas (físicas e virtuais) com base nas tecnologias de informação e comunicação interoperáveis existentes e em evolução." [27]

Sua aplicação específica na indústria, também é conhecida como IIoT, e é definida pelo Industrial Internet Consortium como:

"Máquinas, computadores e pessoas que permitem operações industriais inteligentes, usando análises avançadas de dados para resultados transformacionais dos negócios" [28]

Em um nível básico, a IIoT pode ser resumida como máquinas industriais equipadas com sensores, conectadas através de tecnologias da Internet a outras máquinas para, por exemplo, monitoramento, análise e gerenciamento. [17]

Com a IIoT até mesmo em dispositivos menos sofisticados, pode-se usar computação embarcada para conectá-los à Internet. Isso permitirá que estes dispositivos monitorem, analisem, interajam uns com os outros e enviem informações a controladores centralizados. Deste modo descentraliza-se a análise e a tomada de decisões permitindo respostas em tempo real, possibilita operação assistida e manutenção remota destes equipamentos. [18]

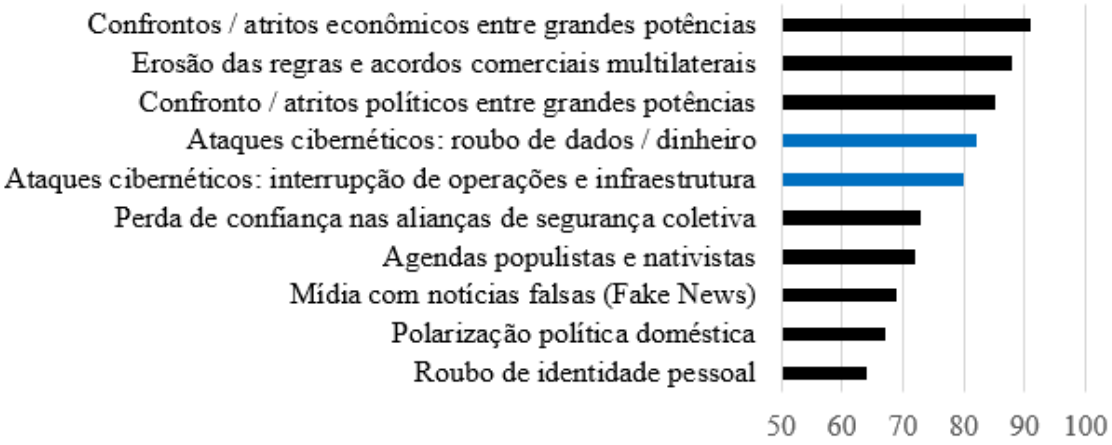
Como estar conectado será essencial na Indústria 4.0, com a comunicação bidirecional destes sistemas, faz-se necessário proteger linhas de fabricação e sistemas industriais críticos de ameaças de segurança cibernética. Deste modo, comunicações seguras e confiáveis, bem como, controle de acesso, serão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

3 SEGURANÇA CIBERNÉTICA

Na eletrônica de potência o termo proteção de equipamentos, era diretamente relacionado ao seu grau de proteção para aplicação em áreas classificadas, por exemplo, IP67 [29]. Com a Indústria 4.0 o cenário é outro, e o tema segurança cibernética é recente para muitos pesquisadores da área.

Ao longo dos últimos anos a segurança cibernética tem se tornado uma preocupação global, com a evolução das tecnologias e produtos cada vez mais conectados. Conforme apresenta-se na Figura 5, pesquisas realizadas anualmente pelo Fórum Econômico Mundial, vem posicionando ataques cibernéticos contra instituições financeiras e infraestruturas, no topo da lista de riscos globais na perspectiva de risco de curto prazo [30]. Não imaginavam os entrevistados, que em 2020, se iniciaria a pandemia do COVID-19 levando a humanidade a uma crise sanitária global sem precedentes.

Figura 5 – Perspectiva de risco de curto prazo, porcentagem de entrevistados que espera que os riscos aumentem em 2019



Fonte: Adaptado de Fórum Econômico Mundial. [30]

Este capítulo visa apresentar e conceituar os principais fundamentos de segurança cibernética: seus atores, ferramentas, ataques mais disseminados, bem como, metodologias para gestão e mitigação de riscos, vulnerabilidades e incidentes.

O Internet Industrial Consortium (IIC) define segurança cibernética como:

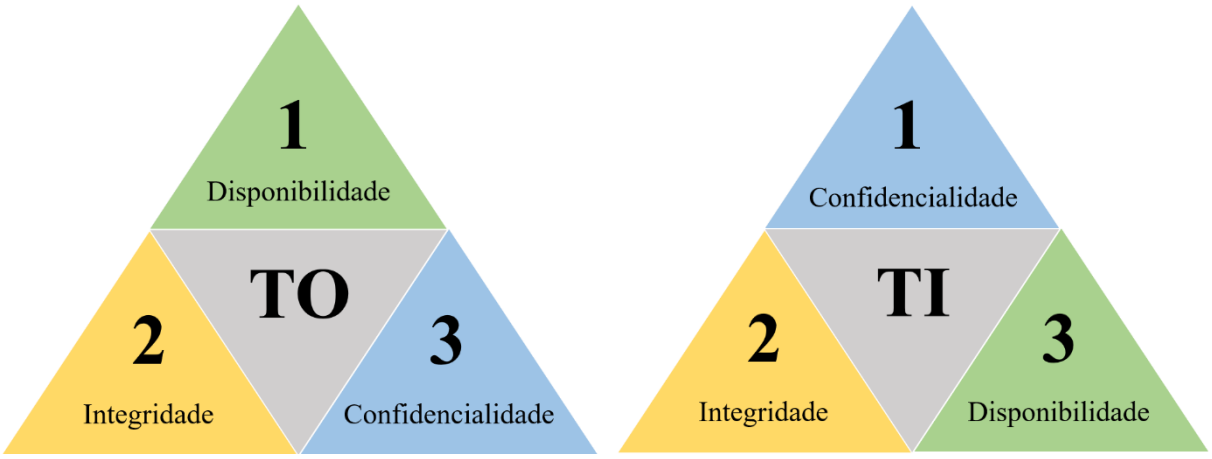
"A condição de um sistema estar sendo protegido contra alteração, destruição, acesso não intencional ou não autorizado." [3]

A segurança cibernética de um sistema é contínua e não um estado binário. Nunca, um sistema estará totalmente protegido contra ameaças cibernéticas, sua segurança deve frequentemente ser reavaliada em termos de risco. Os elementos de risco à segurança incluem, o ator (alguém que está tentando causar danos ao sistema), a ameaça (algo que está tentando causar danos ao sistema), o alvo (ativo de valor), vulnerabilidades que possam ser exploradas e contramedidas [3]. Os elementos que precisam ser mantidos para garantir a segurança cibernética do sistema são: a confidencialidade; a integridade; e a disponibilidade.

3.1 FUNDAMENTOS DE SEGURANÇA CIBERNÉTICA

Na tecnologia operacional (TO), ao contrário da tecnologia da informação (TI), a disponibilidade é considerada primordial, seguida pela integridade, sendo a confidencialidade geralmente a última consideração, levando ao acrônimo DIC (Disponibilidade, Integridade e Confidencialidade, do Inglês AIC - *Availability, Integrity and Confidentiality*), ilustrado pela Figura 6, também conhecido como tríade da segurança cibernética. [3]

Figura 6 – Tríades da segurança cibernética TO versus TI



a) Tríade DIC segurança cibernética na TO b) Tríade CID segurança cibernética na TI

Fonte: Elaborado pelo autor.

3.1.1 Disponibilidade

A disponibilidade geralmente compreende dois aspectos: negação de serviço (DoS, *Denial-of-Service*) e perda da capacidade de processamento de dados [31]. Os controles de disponibilidade geralmente envolvem redundância e controle de alterações de engenharia [3].

A disponibilidade garante que o sistema e suas informações sejam acessíveis aos usuários autorizados sempre que necessário.

3.1.2 Integridade

O desafio da segurança cibernética nessa área, é assegurar que quaisquer alterações no sistema sejam autorizadas e aplicadas corretamente, garantindo que os estados e as respostas do sistema estejam integras, ou seja, sempre conforme pretendido [31]. Os controles de integridade incluem ***Hash***, função somas de verificação (***Checksums***), antivírus, lista de permissões, assinatura digitais, bem como demais ferramentas para controle dos processos físicos do sistema [3]. A integridade protege as informações do sistema contra destruição e alterações não autorizadas, intencionais ou acidentais.

3.1.3 Confidencialidade

Controles de confidencialidade incluem tecnologias de controle de acesso e criptografia [31]. Geralmente é comprometida quando, o ator de um ataque descobre, como ignorar mecanismos de controle de acesso ou a existência de fragilidades no perímetro do sistema. Redes de comunicação e áreas de armazenamento são assuntos críticos com relação a confidencialidade de um sistema [3]. A confidencialidade protege as informações de um sistema, para que indivíduos ou programas não autorizados não possam acessar determinadas informações.

3.1.4 Atores

Quem são os atores de ataques cibernéticos, o que eles querem e como planejam obtê-lo? Embora existam uma variedade de atores, a maioria deles se se enquadram nas categorias apresentadas por [11]. Criminosos profissionais, ganham dinheiro através de ataques digitais, quando contratados para campanhas de espionagem industrial, ou quando extorquem vítimas que tiveram seus dados roubados ou criptografados. Vândalos cibernéticos geralmente realizam ataques como passatempo e ameaças internas podem vir de ações não intencionais ou de funcionários mal-intencionados, que por motivos financeiros, políticos ou pessoais.

3.1.5 Ameaças e tipos de ataque

Malwares (programas de computador mal-intencionados) são as principais ferramentas usadas para obter acesso não autorizado a computadores, roubar informações e interromper ou desabilitar redes e serviços [32].

Vírus de computador e vermes (*Worms*), se replicam com o intuito de causar dano aos equipamentos infectados. Cavalos de Tróia (Trojans) fingem ser programas legítimos para abrir uma porta dos fundos (*backdoor*), Angler, Black Energy, Grey Energy [33]-[35] são kits de exploração (*Exploit kit*), *malwares* que oferecem interfaces amigáveis para a realização de ataques cibernéticos. Geralmente são usados em ataques do tipo, ameaça persistente avançada (ATP, *Advanced Persistent Threat*) [36]. O trabalho [11] resume e apresenta a maioria deles.

3.1.6 Gestão de vulnerabilidades, riscos e incidentes

Geralmente realizada por um grupo tomador de decisões, compostos por analistas e administradores sêniores, responsáveis por qualquer decisão de aceitar o risco residual, equilibrá-lo ou mitigá-lo com o investimento em tecnologia de segurança cibernética adicional [31]. Conforme apresentado em mais detalhes por [11], a gestão da segurança cibernética, se faz através da análise de vulnerabilidades, riscos e incidentes, e como qualquer outra atividade de mitigação e gerenciamento de risco, nunca cobre 100% dos riscos.

3.2 SEGURANÇA CIBERNÉTICA EM TECNOLOGIA OPERACIONAIS

Devido a conectividade das tecnologias operacionais com as tecnologias da informação, e estas consequentemente conectadas a Internet, os surtos de *malwares* vem se tornando cada vez mais comuns na área de TO.

Pesquisa realizada pela Kaspersky em 2018, indica que 64% das empresas, tiveram problemas com ataques cibernéticos em TO, nos últimos doze meses daquele determinado ano. [37]

Alguns ataques cibernéticos bem-sucedidos, chamaram atenção de muitos setores industriais, por ser um dos principais alvos dos ataques em TO o setor elétrico já iniciou investimentos em pesquisas para o desenvolvimento de novas tecnologias com o intuito de se proteger. [4]

Muitas empresas temem ataques de espionagem industrial, pois presam por sua propriedade intelectual. A segurança cibernética, definida como um dos pilares da Indústria 4.0, acelerou a busca e o desenvolvimento de tecnologias de segurança na indústria de eletroeletrônica e de eletrônica de potência, devido aos seus componentes estarem cada vez mais conectados e expostos.

3.2.1 Principais incidentes

Ao longo da última década, devido a evolução da manufatura com a automação industrial, em conjunto com as novas tecnologias de TI, uma série de incidentes cibernéticos de considerável importância aconteceram na indústria.

A Figura 7 apresenta alguns deles. Em [11] resume-se alguns, entretanto mais detalhes podem ser encontrados nos trabalhos [32], [34]-[35], [38]-[45].

3.2.2 Pesquisas e iniciativas para proteção do setor elétrico e sistemas de potência.

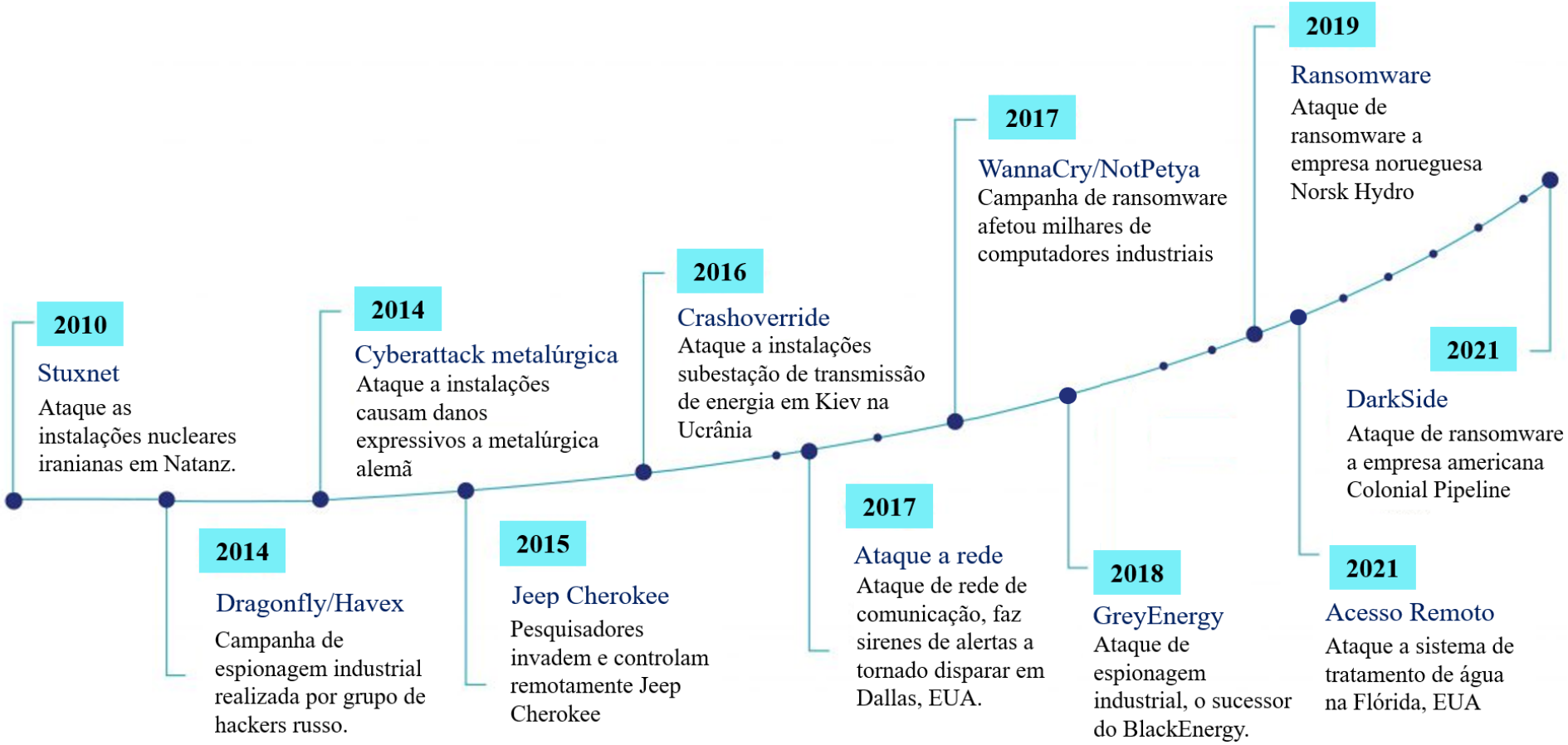
Operadores e companhias de geração, fornecimento e distribuição de energia reconhecem que existem vulnerabilidades em redes inteligentes (*Smart Grids*) e que ataques bem-sucedidos como o de Kiev [34], podem voltar a ocorrer em outras infraestruturas. [4]

Com o intuito de mitigar ameaças digitais, empresas e órgãos governamentais vem se unindo para criar linhas de defesa contra esses ataques cibernéticos. Pesquisas e iniciativas mundiais para proteção do setor elétrico e de sistemas de potência são apresentadas em [11].

No Brasil o tema é discutido pelo menos desde 2016 [11]. Apesar de não apresentar grandes avanços nestes últimos anos, em 2021 o Conselho Nacional de Política Energética (CNPE), presidido pelo Ministro de Minas e Energia (MME) aprovou a criação de um grupo de trabalho para abordar o tema. Formado por agentes públicos, instituições do setor e especialistas da sociedade civil, com o objeto de se estabelecer diretrizes para implementação da segurança cibernética no setor de energia elétrica do Brasil. A criação deste grupo, apresenta ser um passo significativo, para elevar a maturidade da segurança do setor. [46]

Para a indústria, o grupo de trabalho de segurança cibernética criado pelo Consórcio da Internet Industrial (IIC, *Industrial Internet Consortium*) [47], tem como objetivo, desenvolver, acelerar, criar um consenso, e promover práticas no que diz respeito à segurança cibernética em sistemas de automação e controle indústrias conectados a IIoT.

Figura 7 – Linha de tempo, ataques cibernéticos a tecnologias operacionais



Fonte: Elaborado pelo autor.

O guia de referência para a segurança na IIoT (IISF, *Industrial Internet of Things Security Framework*), desenvolvido pelo grupo de trabalho, publicado em setembro de 2016. É um documento abrangente, que 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]

3.2.3 Normatizações

O anexo A do IISF [3], apresenta um resumo sobre normas de segurança cibernética para dispositivos a serem conectados a IIoT. E [32], dispõe de um capítulo com normas e legislações relacionadas a soluções e tecnologias para automação da energia.

Atualmente a norma de segurança da informação mais usada e disseminada no mundo é a ISO/IEC 27001:2013 [48], considerada como referência internacional para a gestão da segurança da informação, assim como a ISO 9001 é a referência internacional para a gestão da qualidade.

Porém, quando o assunto é segurança cibernética para sistema de automação e controle industrial (IACS), a série de normas IEC 62443 deve ser considerada (Figura 8). Esta é o resultado de 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 para o IACS, em diferentes tipos de sistemas, instalações e setores da indústria. [3]

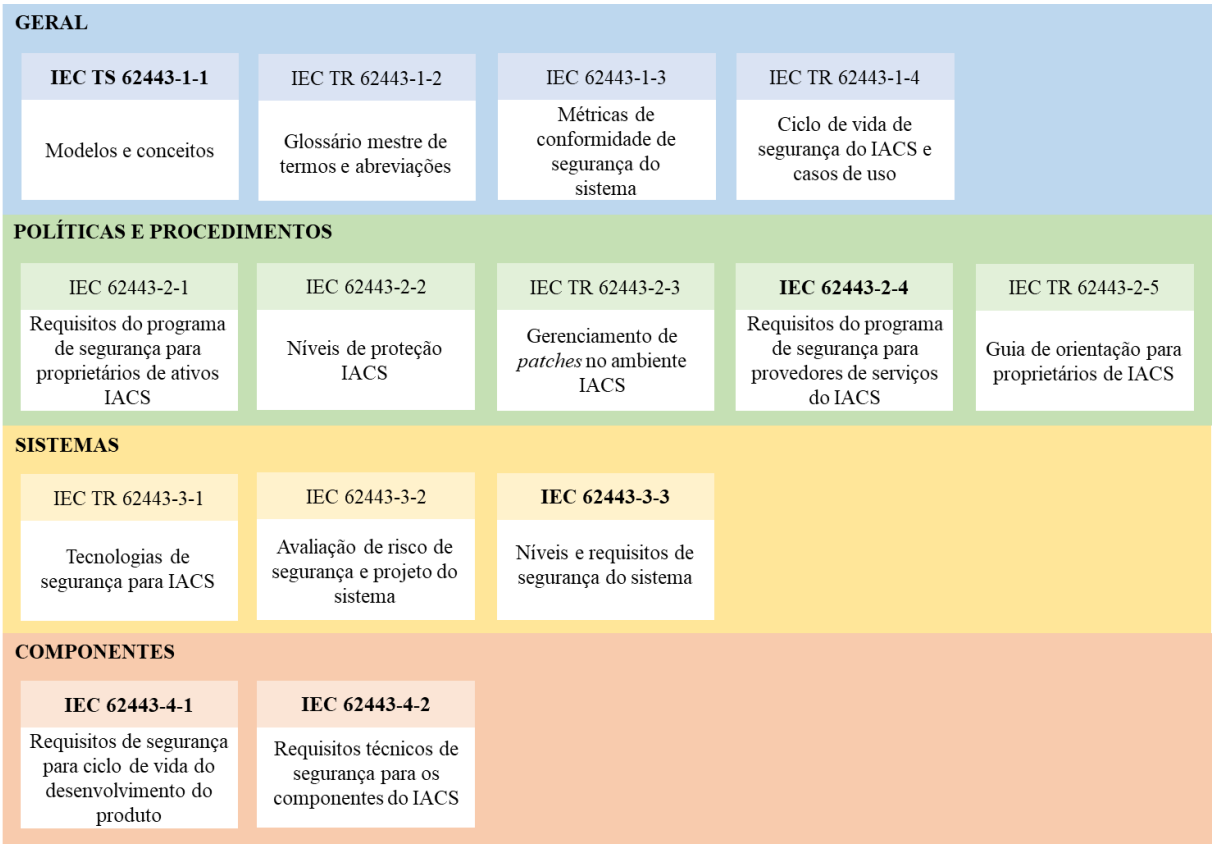
A parte IEC 62443-2-4 [49] especifica requisitos de segurança que provedores de serviços podem oferecer à proprietários de IACS, durante atividades de integração e manutenção de uma solução de automação. A IEC 62443-4-1 [50] define um ciclo de vida de desenvolvimento seguro (SDL, *Development Life-Cycle*) com o propósito de certificar que fabricantes considerem segurança, desde a concepção de seus produtos.

A IEC TS 62443-1-1 [51], específica modelos e conceitos, bem como, os sete requisitos fundamentais (FR, *Foundational requirement*) para a segurança cibernética do IACS. Os detalhes técnicos com requisitos de sistema (SR, *System Requirement*) são especificados na IEC 62443-3-3 [52] e a IEC 62443-4-2 [6], especifica os requisitos técnicos de segurança cibernética para o componente, definido pela própria norma como:

"Entidade pertencente a um IACS que exibe as características de um ou mais de um, dispositivo host, dispositivo de rede, aplicação de software ou dispositivo embarcado." [6]

A Figura 9 apresenta os sete requisitos fundamentais e os seus respectivos requisitos do componente (CR, *Componente Requirement*) especificados na IEC 62443-4-2. Para alguns casos, a norma também proporciona requisitos de aprimoramento (RE, *Requirement Enhancement*) que combinados e associados aos sete requisitos fundamentais, determinam os requisitos, para se alcançar os quatro níveis de segurança das capacidades do IACS e de seus componentes (SL-C, *Capability Security Level*). Um exemplo para melhor compreensão de como a norma estrutura cada CR, se faz presente no ANEXO A.

Figura 8 – Normas que compõe a série IEC 62443



Fonte: Adaptado de IEC. [6]

Outra área da segurança cibernética que vem ganhando importância nos últimos tempos, é a proteção das informações pessoais. Governos vêm determinado diretrizes e regulamentações para proteger as informações pessoais de seus cidadãos. O GDPR da União Europeia, HIPAA e PIPEDA da América do Norte e a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais para o Brasil (LGPD) [53]-[55]. Empresas que ofertam serviços digitais são questionadas quanto à conformidade com a auditoria SOC2 ou superior (*Service and Organization Controls 2*) [56], e o mesmo é valido para empresas de manufatura que ofertam soluções digitais.

Figura 9 – IEC-62443-4-2, sete requisitos fundamentais e seus respectivos requisitos de componente

IEC 62443-4-2

FR 1 - CONTROLE DE IDENTIFICAÇÃO E AUTENTICAÇÃO

CR 1.1 - Identificação e autenticação de usuário humanos
CR 1.2 - Identificação e autenticação de dispositivos e processos
CR 1.3 - Gerenciamento de contas
CR 1.4 - Gerenciamento do identificador
CR 1.5 - Gerenciamento do autenticador
NDR 1.6 - Gerenciamento de acesso sem fio
CR 1.7 - Força da autenticação baseada em senha
CR 1.8 - Certificados PKI
CR1.9 - Força da autenticação baseada em chave publica
CR 1.10 - Feedback do autenticador
CR 1.11 - Tentativa de autenticação sem sucesso
CR 1.12 - Notificação de uso do sistema
NDR 1.13 - Acesso via redes não confiáveis
CR 1.14 - Força da autenticação baseada em chaves simétricas

FR 2 - CONTROLE DE USO

CR 2.1 - Aplicação de autorização
CR 2.2. - Controle de uso sem fio
CR 2.3 - Controle de uso para dispositivos móveis e portáveis
SAR/EDR/HDR/NDR 2.4 - Código Móvel
CR 2.5 - Bloqueio de sessão
CR 2.6 - Encerramento de sessão remota
CR 2.7 - Controle de sessões concorrentes
CR 2.8 - Eventos auditáveis
CR 2.9 - Capacidade de armazenamento para auditoria
CR 2.10 - Resposta a falhas de processamento de auditoria
CR 2.11 - Carimbo de tempo
CR 2.12 - Não repúdio
EDR/HDR/NDR 2.13 - Uso de interface de teste e diagnostico físico

FR 3 - INTEGRIDADE DO SISTEMA

CR 3.1 - Integridade da comunicação
EDR/HDR/NDR/SAR 3.2 - Proteção contra códigos maliciosos
CR 3.3 Verificação das funcionalidades de segurança
CR 3.4 - Integridade da informação e do programa
CR 3.5 - Validação da entrada
CR 3.6 - Saída determinística
CR 3.7 - Manipulação de erros
CR 3.8 - Integridade da sessão
CR 3.9 – Proteção da informação de auditoria
EDR/HDR/NDR 3.10 – Suporte para atualização
EDR/HDR/NDR 3.11 – Resistência e detecção de violação física
EDR/HDR/NDR 3.12 - Provisionamento da RoT do fornecedor de produtos
EDR/HDR/NDR 3.13 - Provisionamento da RoT do proprietário do ativo
EDR/HDR/NDR 3.14 - Integridade do processo de inicialização

FR 4 - CONFIDENCIALIDADE DOS DADOS

CR 4.1 – Confidencialidade da informação
CR 4.2 – Persistência da informação
CR 4.3 – Uso de criptografia

FR 5 - FLUXO DE DADOS RESTRITO

CR 5.1 – Segmentação de rede
NDR 5.2 - Proteção de limite de zona
NDR 5.3 - Restrições de comunicação de pessoa-a-pessoa, propósito geral

FR 6 - RESPOSTA A EVENTOS

CR 6.1 - Acessibilidade do registro de auditoria
CR 6.2 – Monitoramento continuo

FR 7 - DISPONIBLIDADE DE RECURSO

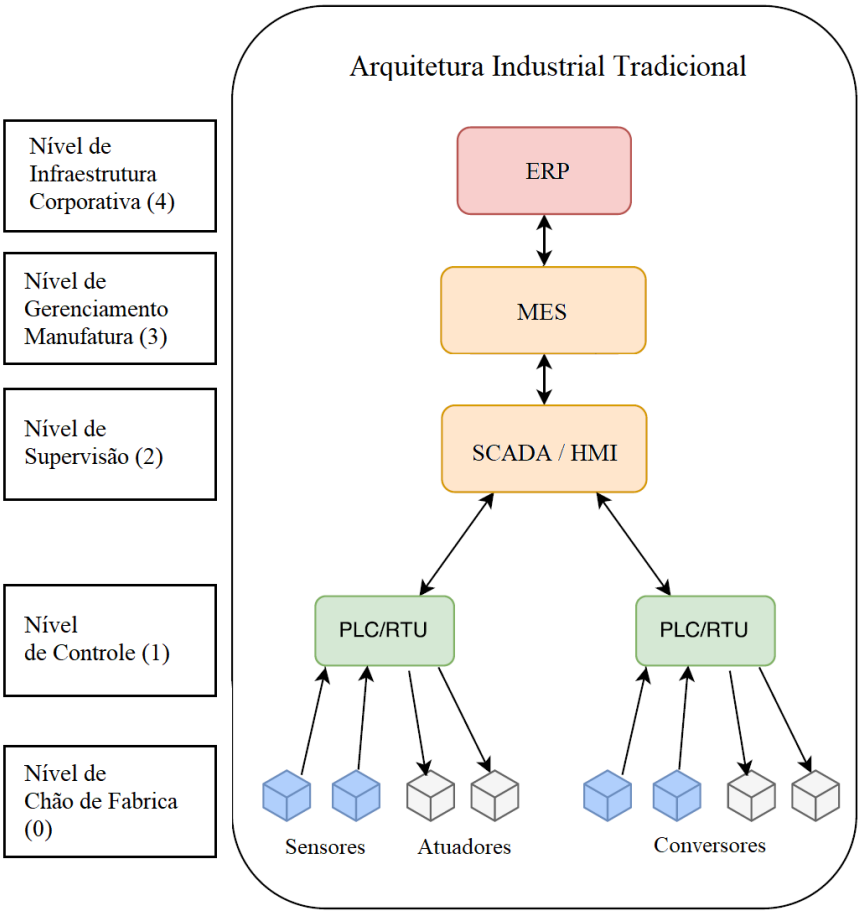
CR 7.1 – Proteção contra negação de serviço (DoS)
CR 7.2 – Gerenciamento de recursos
CR 7.3 - Backup do sistema de controle
CR 7.4 - Recuperação e reconstituição do sistema de controle.
CR 7.5 – Emergência alimentação de energia
CR 7.6 - Definições de configuração de rede e segurança
CR 7.7 - Menor funcionalidade
CR 7.8 – Inventário de componentes do sistema de controle

Fonte: Elaborado pelo autor

3.2.4 Segurança cibernética para a IIoT

Visando entender os requisitos para a segurança cibernética no ambiente da IIoT, primeiramente deve-se entender como as redes industriais são afetadas pela integração da TI, neste novo conceito de IIoT. Arquiteturas de redes industriais tradicionais, geralmente seguem o padrão ISA-95 apresentado pela Figura 10.

Figura 10 – Arquitetura da Automação Industrial, Padrão ISA-95



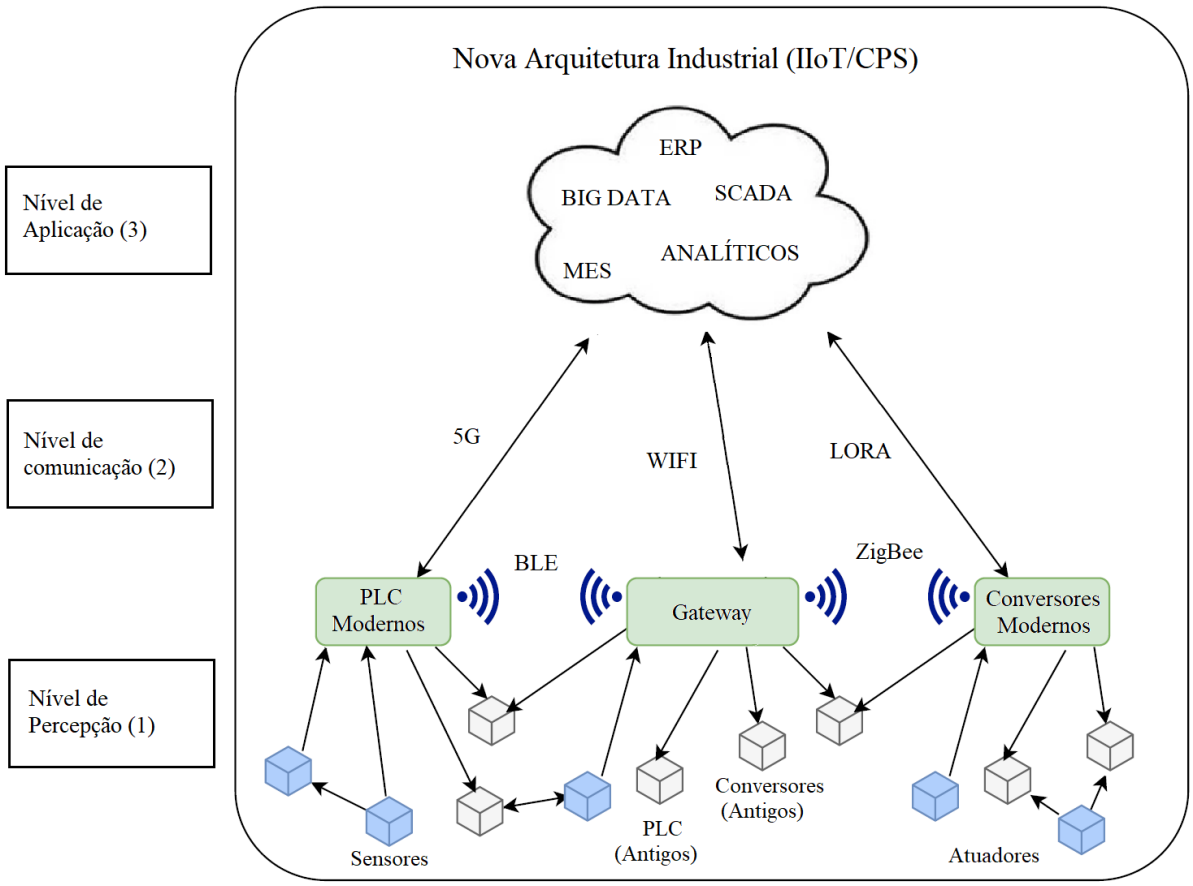
Fonte: Adaptado de Lopez e Rubio. [22]

Neste padrão os processos produtivos, compostos por sensores e atuadores, constituem a base da pirâmide (nível 0). No Nível 1 estão localizados os dispositivos de acionamentos, sejam eles, PLC, RTU, conversores etc. O Nível 2 representa os sistemas e dispositivos que controlam acionamentos e os processos de produção, *software* SCADA, HMI etc. No Nível 3 estão localizados os sistemas que controlam o fluxo de trabalho, ou seja, *software* MES etc. No topo (Nível 4), encontra-se os sistemas para planejamento dos recursos da empresa (ERP, *Enterprise Resource Planning*). [57]

A introdução de sistemas físicos cibernéticos (CPSs) nesse contexto, significa a introdução de tecnologias avançadas de conectividade e recursos computacionais para garantir uma aquisição de dados em tempo real e um processamento inteligente de dados. O objetivo é reunir informações de todas as máquinas que compõem o processo produtivo e executar análises específicas para extrair ***insights*** adicionais, fornecendo ***feedback*** do espaço cibernético ao espaço físico [22].

O novo modelo de arquitetura de acordo com [58] é constituído por três níveis, percepção, comunicação e aplicação (Figura 11).

Figura 11 – Arquitetura de Soluções IoT



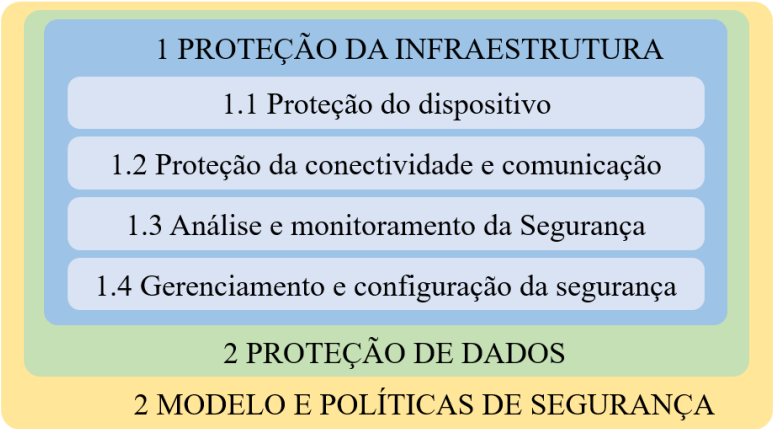
Fonte: Adaptado de Lopez e Rubio. [22]

Os dispositivos localizados nos níveis inferiores do padrão ISA-95, Nível 0 e Nível 1, agora interagem entre si a fim de coletar dados no nível de percepção. O nível de comunicação é responsável pela comunicação com a nuvem, e composto pelas tecnologias de comunicação: Bluetooth, IEEE 802.11, LoRA, 5G, etc. A nuvem localizada no nível de aplicação, é aproveitada para fornecer supervisão como serviço e interconectar todos os envolvidos no processo produtivo [59]. Dessa forma, um ambiente colaborativo pode ser criado por diversas

empresas cujas aplicações e restrições podem diferir, flexibilizando acordos globais e diminuindo a necessidade de adoção de especificação em comum. [22]

Em contrapartida, a modernização das tecnologias industriais e a interconexão dos CPSs com a Internet, possibilitam o surgimento de novas ameaças cibernéticas. Preocupado com a integridade, confidencialidade e disponibilidade da IIoT, o IIC desenvolveu o *framework* segurança cibernética para IIoT [3]. Conforme pode ser observado na Figura 12, o *framework* define e organiza a proteção destes sistemas em três camadas.

Figura 12 – Blocos para desenvolvimento de Segurança Cibernética em IIoT



Fonte: Adaptado de IIC. [3]

A primeira e principal camada é composta por quatro funções. A primeira, função de proteção do dispositivo, visa o desenvolvimento das seguintes capacidades defensivas:

a) fornecer proteção física com mecanismos de prevenção contra adulteração e roubo;
b) identidade e proteção de integridade para distinguir dispositivos com base nas suas propriedades, visando certificar que ele não foi adulterado ou clonado sendo único no sistema;
c) controle de acesso visando garantir que a identificação, autenticação e autorização sejam solicitadas antes da concessão de quaisquer recursos do dispositivo.

Capacidades estas que visam a proteção do dispositivo, no entanto, para aplicações IIoT nem sempre garantem a eficiência do sistema como um todo. Pois dispositivos se comunicam com outros componentes do sistema, fazendo com que as infraestruturas de telecomunicações também sejam fontes de vulnerabilidade.

Para mitigar tais vulnerabilidades, a função de proteção da conectividade e da comunicação, usa as capacidades de identidade, autenticação e criptografia disponibilizadas pela função de proteção do dispositivo, para implementar autenticação, autorização,

confidencialidade e integridade para o tráfego de comunicação [3]. Estando o dispositivo protegido, e a integridade da comunicação garantida, este estado seguro do sistema precisa ser preservado durante todo o ciclo de operação do dispositivo, isto é garantido pela função de análise e monitoração da segurança e pelo controle de alterações e configurações de todos os componentes deste sistema. [3]

A função de monitoramento e análise de segurança é responsável por capturar dados sobre o estado do dispositivo e da rede, gerando informações que possibilitem a detecção de certas violações de segurança do sistema. Um laço contínuo de três ações: monitorar, analisar e atuar. Monitorar para capturar dados das funções, obtendo informações sobre o desenvolvimento de controles de acordo com as políticas definidas para o sistema e registro remoto de eventos através de fontes de comunicação seguras. Analisar, a procura de eventos de violação do sistema, novas ameaças e vulnerabilidades. [3]

Nesta fase armazena-se informações para auditoria e análise futura, esta pode ser comportamental, no qual observa-se os padrões de uso no sistema e aprende qual é o comportamento apropriado para o sistema, ou baseada em regras, na qual monitora-se violações de regras de política predefinidas que definem eventos que nunca devem ocorrer no sistema. Depois de analisar eventos e tendências, é necessário atuar, de forma proativa ou preditiva, mitiga-se ameaças antes do ataque começar, de forma reativa para ataques em andamento, busca-se atenuar o impacto e recuperar o sistema. Ou até mesmo de forma subjacente, pela qual busca-se compreender a causa raiz da vulnerabilidade existente com a análise forense do ataque cibernético. [3]

Por fim a função de gerenciamento e configuração de segurança controla as atualizações de todos os componentes do sistema, controlando alterações na funcionalidade operacional dos dispositivos, garantindo que alterações sejam realizadas de modo seguro e controlado, assegurando a estabilidade do sistema. [3]

As próximas duas camadas de segurança definidas pelo *framework*, visam proteger e sustentar as quatro funções definidas pela camada principal.

A camada proteção de dados, se estende da proteção de dados internos do dispositivo, aos dados trafegados nas comunicações, ou gerados pelas funções de monitoramento e análise e de configuração e gerenciamento do sistema. Dados são difundidos em todo o sistema IIoT, cada conjunto de dados tem um ciclo de vida diferente, tempo de relevância e risco potencial associado ao seu comprometimento. A ameaça pode resultar de sua modificação, interceptação ou duplicação. [3]

Pode-se categorizar os dados de um sistema IIoT em três categorias. Dados em repouso (DAR, *Data-at-Rest*), são dados em armazenamento persistente como memória flash ou disco, Dados em uso (DIU, *Data-in-Use*), são dados colocados temporariamente em armazenamento não persistente como memórias de acesso aleatório (RAM) e dados em movimento (DIM, *Data-in-Motion*), dados que se deslocam entre dois ou mais pontos conectados. Estes dados devem ser protegidos contra acesso não autorizado e alterações não controladas, aplicando funções como controles de confidencialidade, controles de integridade, controle de acesso, controle de acesso, isolamento e replicação. O nível de proteção deve ser proporcional ao impacto da perda ou falsificação de dados, e um período de retenção deve ser definido. [3]

A terceira e última camada, define e desenvolve modelo e políticas de segurança, no qual governa-se como políticas são aplicadas ao sistema. Sempre em busca da confidencialidade, integridade e disponibilidade do sistema durante todo o seu ciclo de vida. Deve abranger todos os aspectos de segurança do sistema, ou seja, precisa definir como proteger dispositivos, comunicações e dados, o que deve ser monitorado, analisado e recuperado e quem e como as alterações podem ser feitas em todos os aspectos do sistema. A política de segurança inclui políticas para o sistema e subpolíticas para proteção de dispositivos, comunicações e proteção de conectividade, monitoramento e análise de segurança, configuração e gerenciamento de segurança e proteção de dados.

A análise de ameaças do sistema permite a criação dos objetivos de segurança do sistema, derivados de regulamentos e normas. A partir desses objetivos, as políticas de segurança aplicáveis são selecionadas com base no setor de manufatura, na base de clientes, na localização geográfica e em outras considerações [3]. A política de segurança descreve as considerações gerais sobre riscos de negócios e define as diretrizes para garantir o bom funcionamento diário do sistema.

3.3 SEGURANÇA CIBERNÉTICA EM CONVERSORES ESTÁTICOS

Conversores conectados à IIoT, podem ser instalados em uma variedade de ambientes, que diferem quanto aos requisitos de segurança necessários para proteger o sistema. De acordo com [60], ataques cibernéticos a dispositivos embarcados podem ser divididos em três classes:

a) *hack attack*, ataques realizados na camada de *software* através de *malwares*, análise de rede, etc;

b) *shack attack*, ataque de *hardware* de baixo custo, usando equipamentos que podem ser adquiridos com facilidade no mercado e tendo acesso físico ao equipamento onde pode-se depurar através de interface JTAG, escanear I/O, etc;
c) *lab attack*, o mais abrangente e invasivo, onde utiliza-se de um laboratório, com equipamentos especiais, por exemplo, microscópios eletrônicos, possibilitando a engenharia reversa do dispositivo.

Nesta seção realiza-se uma introdução sobre a arquitetura de conversores estáticos, apresenta-se vulnerabilidades na arquitetura atual, iniciativas realizadas por fabricantes de conversores estáticos e recomendações para o desenvolvimento de conversores mais seguros que pretendem ser conectados a IIoT.

Apesar de ataques de laboratórios serem uma ameaça a propriedade intelectual destes equipamentos, recomendações para mitigar esta classe de ataques não são contemplados neste trabalho.

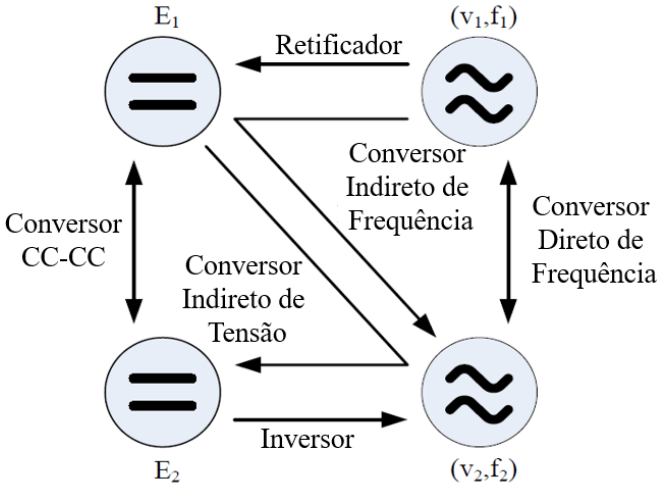
3.3.1 Arquitetura de conversores estáticos

Conversores realizam o tratamento eletrônico da energia elétrica, empregando elementos passivos (resistores, capacitores e indutores) e elementos ativos (semicondutores) tais como diodos, tiristores e transistores segundo critérios de projeto e funcionamento pré-estabelecidos. [61]

O diagrama da Figura 13 apresenta as principais funções que podem ser realizadas pelos conversores estáticos dependendo da arquitetura selecionada. Conversores podem ser diretos, quando realizam a conversão diretamente sem passar por um estágio intermediário, ou indiretos, quando se utiliza um estágio intermediário em corrente oposta a corrente de entrada e saída, ou seja, um conversor indireto CA/CA possui um estágio intermediário em CC, e um conversor indireto CC/CC possui um estágio intermediário em CA. [61]

Conversores estáticos tem sua arquitetura dividida entre potência e controle. Apesar de serem construídos, e possuírem características diferentes para atender diversas aplicações, como: sistemas fotovoltaicos, tração elétrica, acionamento de motores elétricos, conversão de tensão e corrente elétrica. Muitas características se assemelham, devido as funções de comunicação, entradas e saídas digitais e analógicas, exigidas pela indústria em equipamentos comerciais.

Figura 13 – Topologias conversores estáticos



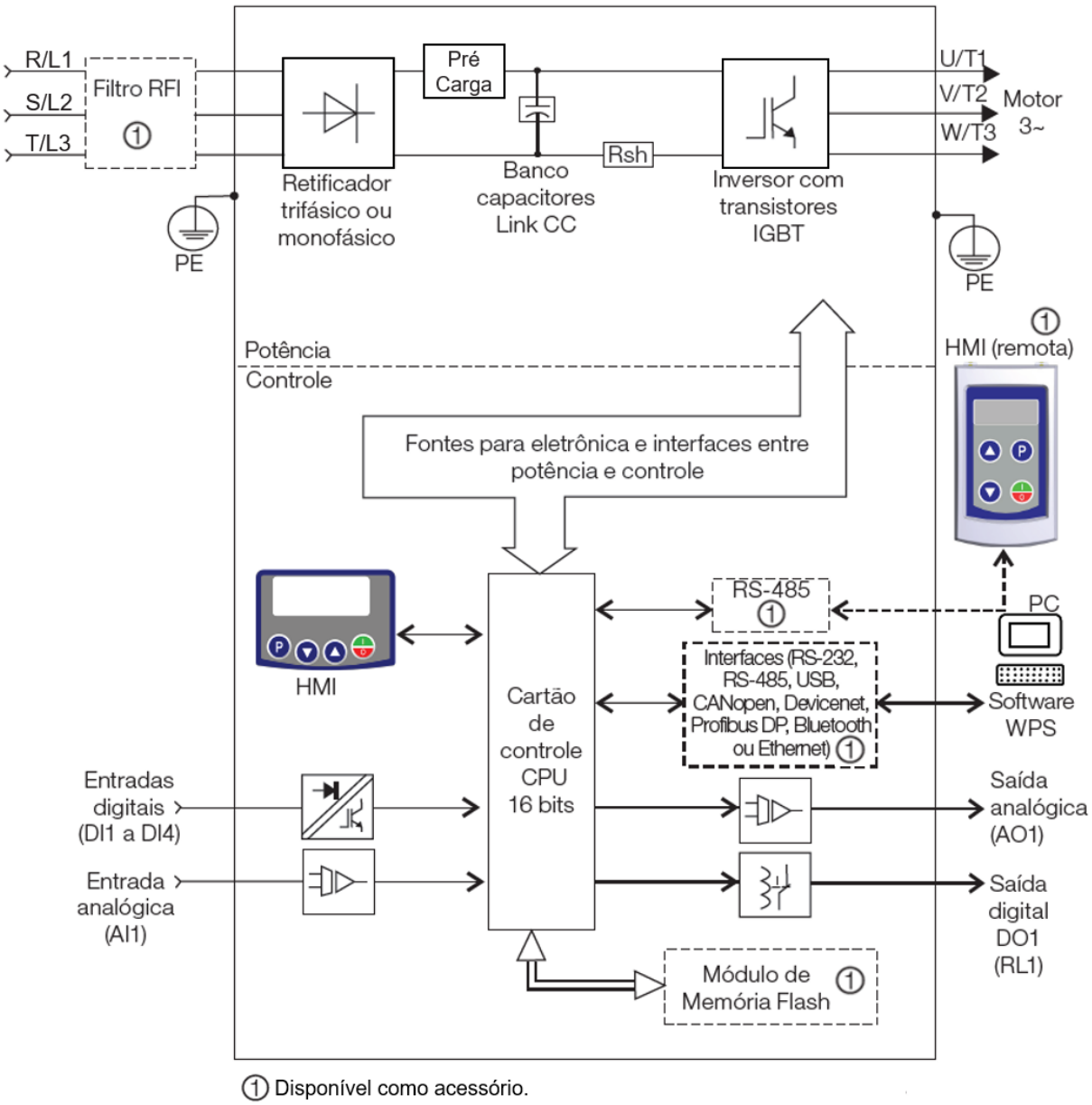
Fonte: Adaptado de Bottenberg. [61]

A Figura 14 apresenta o diagrama funcional de um conversor indireto de frequência CA/CA desenvolvido e comercializado pela WEG [62]. O circuito de potência é constituído por 3 blocos, retificador trifásico ou monofásico dependendo do modelo escolhido, sistema de pré-carga e banco de capacitores para barramento CC e inversor com transistores IGBT. Sendo que para o modelo em estudo o filtro RFI é comercializado como um acessório que pode ser acoplado ao circuito de potência do conversor. Fontes auxiliares e circuitos de disparo são funcionalidades que estão localizados na borda, ou seja, entre o circuito de potência e o circuito do controle pois atuam nas duas áreas do sistema. [63]

Além de realizar o controle do circuito de potência, o circuito de comando é responsável por todas as outras funcionalidades do inversor. Conforme observado no diagrama de blocos, todas as funcionalidades do CFW300 são desenvolvidas a partir de um microcontrolador de 16 bits. É comum entre inversores comerciais a disponibilização de entrada e saídas digitais e ou analógicas. O modelo em estudo, possuí quatro entradas digitais e uma saída digital a relê, uma entrada e uma saída analógica de 0 a 20mA.

O armazenamento do *firmware*, bem como, da configuração do dispositivo se faz através de memória flash. Interfaces de comunicação para uso de HMI remota e parametrização através do *software* de programação WPS, é possível realizar a parametrização do dispositivo através de conexão serial ou USB. E interfaces de comunicação são disponibilizadas através de acessórios que podem ser acoplados no equipamento, exemplo: Ethernet, RS232 e RS485, USB, CANopen, DeviceNet e Profibus-DP. [63]

Figura 14 – Representação da arquitetura do CFW300



Fonte: Adaptado de WEG [63]

3.3.2 Vulnerabilidade dos conversores atuais

A segurança física do dispositivo visa protegê-lo contra violação e vandalismo. Interfaces USB, Ethernet, seriais devem ser protegidas para evitar acesso indevido por terceiros. A maioria dos conversores possibilita alterar a sua configuração, através de HMI, com pouco esforço. A possibilidade de conectar uma HMI remota, geralmente instalada fora do painel do equipamento, eleva a possibilidade de controle remoto do conversor por indivíduos não autorizados. [3]

Protocolos de comunicação industriais também apresentam vulnerabilidades que podem ser exploradas, o protocolo Modbus/TCP por exemplo é um protocolo simples e sem criptografia que continua muito presente nas soluções industriais. [64]-[65]

Arquiteturas de conversores desenvolvidos para a Indústria 4.0 e IIoT, devem assegurar que a rede por onde trafegam pacotes de dados oriundos destes protocolos industriais tenham mecanismos de segurança adicional, como criptografia e segmentação, fornecida pela infraestrutura de rede, elevando a segurança destes equipamentos. Inclusive na comunicação com sistemas de supervisão e aquisição de dados (SCADA) ou de plataformas IoT. [3]

No dispositivo a interface Ethernet para conexão a redes TCP/IP, deve possuir ferramentas que evitem a conexão a redes não seguras, como suporte ao protocolo IEEE 802.1X e listas de controle de acesso (ACL, *Access List Control*) possibilitando a criação de regras de liberação e bloqueio de endereçamento IP e protocolos dos terminais remotos, sejam eles dispositivos ou aplicações.

A maioria dos conversores para acionamentos elétricos disponíveis no mercado, não possuem uma identidade e um controle de acesso robusto. A identidade de conversores, muitas vezes é realizada por um endereço MAC, IP ou em alguns casos cria-se algum mecanismo através do número de série destes equipamentos, isto porque na maioria destes conversores o controle de acesso não se faz a partir de uma identidade ou raiz de confiança. Geralmente realiza-se este controle através de uma simples alteração de parâmetro, ou nos melhores casos, através de uma senha padrão de quatro a oito dígitos[63],[66]-[68], ambos os casos permitem acesso total a configuração do equipamento. A mesma fragilidade é apresentada pelas interfaces de comunicação, que na maioria das vezes permiti acesso irrestrito ao equipamento, mesmo sem uma prévia autenticação no dispositivo, este é o caso do protocolo Modbus RTU.

O processo de inicialização, na maioria das arquiteturas comerciais atuais, não é validado, ou seja, o dispositivo poderia inicializar com *firmwares* não homologado armazenado no dispositivo. Em muitos casos, a validação do *firmware* é realizada somente durante a transferência do arquivo, através de cabeçalhos e CRC do arquivo binário.

O processo de transferência de *firmware* é algo crítico em conversores comerciais. Muitos fabricantes ainda evitam executá-los através de comunicação Ethernet, devido a criticidade na perda de pacotes de dados durante o processo. Como muitos dispositivos não são suficientemente inteligentes para analisar a integridade do novo *firmware*, ou se recuperar de um erro durante o processo de transferência de um arquivo, uma simples falha durante o processo poderia torná-lo indisponível [64].

Técnicas tradicionais de integridade de dados para conversores comerciais geralmente são realizadas através da validação de *hash*, por exemplo algoritmo MD5, SHA, etc. No entanto, com o poder computacional dos computadores atuais, estas técnicas já não são mais eficazes. Técnicas de criptografia devem ser utilizadas para proteger dados em repouso, armazenados em memórias flash [3]. A maioria das arquiteturas de conversores comerciais dispõem de memória não voláteis, para armazenamento de uma maior massa de dados. E em alguns casos, para armazená-los, opta-se pela utilização de cartões removíveis como cartões SD, Pendrive, etc. possibilitando a extração da informação, pois geralmente não são criptografados.

3.3.3 Iniciativas adotadas para conversores comerciais

Em 2017 durante a conferência de segurança cibernética SHA2017, realizada em Amsterdã, Holanda. A empresa ITSec em conjunto com o engenheiro de segurança cibernética Willem Westerhof, apresentaram o "*Horus Scenario*", um suposto cenário de apagão no continente Europeu, devido a um possível ataque cibernético em larga escala, aos inversores solares do continente.

Willian descobriu e registrou 17 vulnerabilidades (CVE, *Common Vulnerabilities and Exposures*), existentes nos inversores solares da fabricante alemã SMA, uma das principais fabricantes de inversores solares da Europa.

Os CVEs registrados, apresentam vulnerabilidades nos recursos de comunicação destes equipamentos, ataques DDoS podem ser realizados através de sessões Telnet, o protocolo proprietário SMAdata2+ é vulnerável a ataques de interceptação (MITM, *Man-in-The-Middle*), pois pode ser pode ser facilmente decriptado, senhas são trafegadas sem criptografia em alguns canais de comunicação e o produto não tem capacidade para uso de senhas fortes, possibilitando ataques de força bruta. Durante os testes Willian também conseguiu realizar a transferência de um *firmware* modificado e encontrou muitos equipamentos em produção conectados à Internet, que ainda estavam com a senha padrão "0000".

Em resposta a todas estas vulnerabilidades levantadas, a SMA se manifestou através de um documento (*whitepaper*) respondendo todos os CVEs registrados [64]. Justificou que arquitetura de comunicação para os seus conversores, prevê que eles tenham acesso à Internet através de *firewalls* e roteadores, o que diminui a necessidade de segurança nos protocolos de comunicação. Em nota, ela recomenda que seus clientes sigam as recomendações do documento, "Diretrizes para uma comunicação segura do sistema fotovoltaico" [69]. Este documento apresenta os riscos de se conectar inversores solares da SMA diretamente na

Internet, bem como, apresenta contramedidas que devem ser realizadas para diminuir a exposição destes equipamentos a ataques cibernéticos.

Em 2018 a Siemens, lançou um produto chamado Sinamics G120 Smart Access Module, ou seja, um modulo desenvolvido com o intuito de deixar seus produtos mais inteligentes, o modulo permite acesso a manutenção, monitoramento, comissionamento e parametrização de seus conversores G120 através de rede sem fio. Apesar de especificar uma senha padrão para conexão à rede sem fio disponibilizada pelo modulo, o sistema força o usuário a modificar a senha padrão durante a primeira conexão. Outra funcionalidade importante é o acesso através do protocolo seguro HTTPS, neste caso computador do usuário utiliza um certificado público para realiza o acesso ao modulo através de um canal criptografado elevando a segurança do sistema. [70]

Já a Huawei uma das maiores fabricantes de sistemas fotovoltaicos do mundo, proporciona inteligência e conexão aos seus inversores solares através de um *gateway*, denominado SmartLogger, além de ser o responsável pela interface entre protocolos e conexões, armazena histórico e proporciona conexão segura com o sistema de gerenciamento da Huawei. Isto porque, possibilita o uso de criptografia quando conectado ao sistema de gerenciamento do próprio fabricante, bem como, a aplicação de um segundo fator de autenticação, para elevar a robustez do controle de acesso do conversor [71].

Devido a questões de segurança, o SmartLogger é padronizado para desabilitar protocolos industriais, que não contemplam funcionalidades de segurança, como o Modbus-TCP. No entanto, muitas vezes estes protocolos são necessários, pois algumas aplicações necessitam comunicação com sistemas de gerenciamento de terceiros. Para criar uma camada adicional de segurança, quando exigido estes protocolos de comunicação, a Huawei desenvolveu uma espécie de ACL baseado no endereço IP do sistema de gerenciamento remoto. [71]

Em 2021 a Rockwell Automation anunciou a sua nova linha de conversores PowerFlex 755T. Seu diferencial quanto a segurança cibernética, são os novos *firmwares* que foram atualizados para elevar a segurança do IACS, com a disponibilidade do protocolo de comunicação CIP Security, que fornece confidencialidade e ajuda a evitar conexões não autorizadas e adulteração dos dados [72]. Protocolo desenvolvido pela ODVA para proteger comunicações industriais, é uma extensão do protocolo industrial comum (CIP, *Common Industrial Protocol*) e um dos primeiros protocolos de automação industrial a oferecer suporte à segurança da camada de transporte (TLS, *Transport Layer Security*). [73]

3.3.4 Recomendações para o desenvolvimento de segurança

Conforme apresentado nas seções anteriores, a maioria dos conversores estáticos disponíveis no mercado, não estão preparados para IoT, pois suas funcionalidades foram pensadas e desenvolvidas para operação em TO, na qual a segurança cibernética não é um pré-requisito.

Projetos de conversores desenvolvidos para TO, que foram adaptados para conexão com a Internet ainda continuam vulneráveis, pois como já mencionado, a segurança cibernética não é um estado binário e, portanto, o desenvolvimento de um conversor seguro, deve abordar assuntos relacionados à segurança cibernética desde a sua concepção.

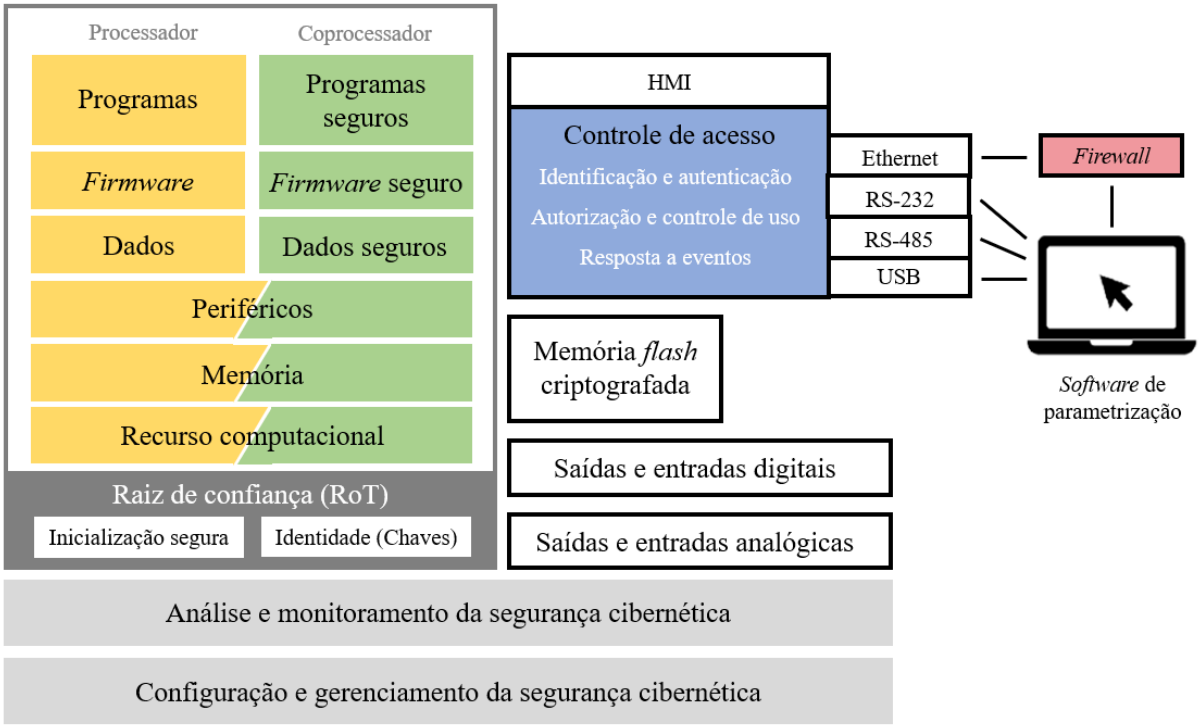
Portanto é de responsabilidade de cada desenvolvedor levantar as vulnerabilidades existentes em seu projeto e analisar quais os riscos de evoluírem para um incidente cibernético em sua respectiva aplicação. O tratamento de riscos deve sempre iniciar do mais prioritário para o menos prioritário, eliminando-os sempre que possível e analisando o custo-benefício de cada recurso de segurança a ser aplicado ou desenvolvido.

Nesta seção apresentam-se recomendações para o desenvolvimento de conversores seguros, para isto toma-se como base a norma IEC 62443-4-2[6] e os frameworks [3],[65]. A Figura 15 apresenta um resumo gráfico dos itens abordados nesta seção.

3.3.4.1 Segurança Física

A segurança física do conversor visa protegê-lo contra roubo, violação, vandalismo ou efeito adverso de condições ambientais. O acesso físico aos ativos deve ser gerenciado e protegido [65]. Interfaces para periféricos e acessórios como, serial e USB por exemplo, devem ser controladas, com o intuito de impedir a conexão não autorizada de periféricos. Recursos contra adulteração, como a validação da identidade através da assinatura digital destes acessórios, devem detectar e relatar qualquer alteração no *hardware* e bloquear a instalação de componentes não homologados para o determinado dispositivo. A construção mecânica do dispositivo, deve ser desenvolvida com o intuído de protegê-lo contra adulterações e violações, acessórios podem ser desenvolvidos com leiaute customizado, dificultando o acoplamento de acessórios desenvolvidos por terceiros. Além disso, todos os eventos detectados devem ser relatados, o estado da segurança física do dispositivo deve ser monitorado e controlado automaticamente por *softwares* especializados através de suas interfaces, como parte das funções de gerenciamento de configuração de segurança do dispositivo. [3]

Figura 15 – Representação resumo recomendações



Fonte: Elaborado pelo autor.

3.3.4.2 Identidade e Credencial

Credenciais são usadas para verificar a identidade do conversor. Um exemplo comum de uma credencial é um certificado digital, ou seja, uma estrutura criptográfica que liga chaves públicas a uma identidade. Existem várias normas que fornecem orientações sobre a escolha do nível de confiança e proteção para a identidade de dispositivos: ISO/IEC 29115, IEC 62443 e ISO/IEC 24760-1.1 são exemplos delas [3]. Identidades e credenciais devem ser emitidas, gerenciadas, verificadas, revogadas e auditadas. [65]

Criar uma identidade única para o conversor é algo simples, porém essencial, pois permite o desenvolvimento de uma ampla variedade de controles de segurança para o equipamento, como: autenticação, autorização e manutenção remota.

3.3.4.3 Identificação e autenticação

O controle de acesso ao conversor deve utilizar os conceitos de autenticação, autorização e segmentação de privilégios. Autenticação é a garantia de que uma característica reivindicada de uma entidade está correta. Autorização é a concessão de direitos, incluindo a concessão de acesso com base em direitos de acesso. A autorização depende da verificação da

identidade do conversor em comparação com os direitos e privilégios para acesso aos recursos do equipamento. [3]

De acordo com o requisito do componente 1.1 (CR) da norma IEC 62443-4-2, conversores devem fornecer a capacidade de identificar e autenticar todos os usuários humanos e em todas as interfaces capazes de fornecer acesso a eles. Identificar e obrigar a autenticação do usuário humano, possibilitando a segregação de funções e privilégio mínimo de acordo com as políticas e procedimentos de segurança aplicáveis. [6]

A autenticação da identidade desses usuários deve ser realizada por meio de métodos como senhas, *hashes*, biometria, etc, localmente pelo conversor ou através da integração com sistemas que possuam tal capacidade. O mesmo vale para o CR 1.2, identificação e autenticação de dispositivos e processo de sistemas, no qual deve-se mapear uma identidade conhecida, para um processo ou dispositivo de *software* desconhecido, de modo a torná-lo conhecido antes de permitir qualquer troca de dados com o conversor. [6]

Além de um identificador, um autenticador (CR 1.5) é necessário para provar a identidade do usuário. Os autenticadores do IACS incluem, mas não estão limitados a: *hashes*, chaves simétricas, chaves privadas, biometria, senhas, chaves físicas, etc. Deve-se garantir um ciclo de vida para os autenticadores, cuja conta seja criada automaticamente, exigindo que este autenticador seja atualizado, antes que proprietário da conta seja capaz de se autenticar. O gerenciamento de autenticadores deve ser especificado nas políticas e procedimentos de segurança, por exemplo, restrições para alterar autenticadores padrões, períodos de atualização, força do autenticador escolhido, etc. [6]

O CR 1.7 determina que componentes que utilizam autenticação baseada em senha, devem prover ou se integrar a sistemas que possuem a capacidade de forçar a configuração de senhas de acordo com as diretrizes reconhecidas internacionalmente. A habilidade de forçar a configuração de senhas fortes, baseadas em um tamanho mínimo, tempo de duração, variedade de caracteres minúsculos, maiúsculos, especiais, é necessário para ajudar a aumentar a segurança geral das senhas escolhidas pelo usuário. Já o CR 1.10, ***feedback*** do autenticador, especifica que componentes devem ofertar a capacidade de obscurecer as informações do autenticador, exibindo asteriscos ou outros caracteres aleatórios quando um usuário humano digita a senha durante o processo de autenticação. [6]

Sempre que possível deve-se optar pela autenticação mútua, na qual ambos, usuário humano e conversor comprovam sua identidade um para o outro, ao invés de autenticação unidirecional, isto impede a personificação de usuários não autenticados. A autenticação

multifator é recomendada sempre que possível para conversores em aplicações críticas, devido a sua complexidade e elevada segurança. [6],[65]

3.3.4.4 Autorização e controle do uso

O objetivo do controle de uso é proteger contra ações não autorizadas nos recursos do componente, verificando se os privilégios necessários foram concedidos antes de permitir que um usuário execute tais ações.

O CR 2.1, aplicação de autorização, especifica que conversores devem prover a aplicação de mecanismos de autorização para todos os usuários identificados e autenticados com base nas suas atribuições e responsabilidades. Após o sistema de controle verificar a identidade de um usuário (humano, processo de *software* ou dispositivo), ele também deve verificar se uma operação solicitada é realmente permitida de acordo com as políticas e procedimentos de segurança definidos. Políticas de controle podem ser baseadas em identidade, funções, regras, mecanismos associados a aplicação de a leitura e escrita, como listas e matrizes de controle de acesso. [6]

Bloqueio de sessão CR 2.5, especifica que se um conversor fornece uma interface para usuário humano, seja esta acessada localmente ou através de uma rede, o conversor deve fornecer a capacidade de protegê-la contra acesso futuro, realizando um bloqueio de sessão após um período configurável de inatividade. Que deve permanecer em vigor até que o usuário atual, ou um outro usuário autorizado, restabeleça a sessão através do procedimento de identificação e autenticação. [6]

O encerramento da sessão remota é especificado pela CR 2.6, que determinada que os componentes que ofereçam suporte a sessões remotas, devem fornecer também a capacidade de encerrar uma sessão remota automaticamente após um período configurável de inatividade ou manualmente por uma autoridade local. Refere-se a sessão remota, sempre que um componente é acessado além dos limites de uma zona pré-definida pelo seu proprietário. [6]

O CR 2.7, controle de sessões concorrentes, especifica que conversores devem prover capacidade para limitar o número de sessões concorrentes por interface, para qualquer tipo de usuário (humano, processo *software* ou dispositivos). Ataques DDoS podem causar incidentes por falta de recursos caso um limite não seja imposto. Existe uma diferença entre o bloqueio de um potencial usuário e o bloqueio de todos os usuários e serviços devido à falta de recursos. A orientação do fornecedor do produto ou do integrador do sistema é necessária, para um correto dimensionamento do número de sessões simultâneas a ser configurado. [6]

3.3.4.5 Resposta aos eventos

Mecanismos que coletem, relatem, preservem e correlacionem automaticamente evidências forenses, devem ser usados para monitorar a operação e garantir a ação corretiva de maneira oportuna ao conversor. A utilização de tais mecanismos é possível, pois uma vez identificadas, autenticadas e autorizadas, todas as requisições realizadas ao conversor devem ser registradas.

Eventos auditáveis, CR 2.8 da IEC 62443-4-2, especifica que conversores devem prover a capacidade de gerar eventos relevantes para auditoria, sobre a segurança das seguintes categorias:

a) controle de acesso;
b) erros;
c) eventos de operação componente;
d) eventos de *backup* e recuperação do sistema;
e) alterações de configurações;
f) eventos para auditoria.

Devem fornecer a capacidade de criar carimbos de tempo (CR 2.11), contemplando data e hora para uso nestes registros. Uma boa referência para o formato de carimbos de tempo é a norma ISO/IEC 8601:2019 [74]. Também devem garantir o não repúdio (CR 2.12), ou seja, o conversor deve fornecer a capacidade de provar que um determinado usuário humano executou uma ação específica. Ações específicas incluem a execução de ações do operador, alteração das configurações do sistema, criação de informações etc.

A capacidade de armazenamento para registros de auditoria, CR 2.9, também é um requisito importantíssimo, para o correto funcionamento do sistema. Conversores devem fornecer mecanismos de proteção, quando atingir ou ultrapassar a capacidade de armazenamento dimensionada, evitando falhas no dispositivo devido à falta de recursos para armazenamento de novos registros. [6]

Proteção esta, especificada pelo CR 2.10, resposta a falhas de processamento de auditoria, que determina que conversores forneçam mecanismos de proteção e resposta contra falhas, devido à falta de capacidade de armazenamento de novos eventos de auditoria. Por exemplo, sobrescrever os registros de auditoria mais antigos ou a interrupção da geração do log de auditoria. Ambas são respostas possíveis, porém implicariam na perda de essenciais informações para análises forenses futuras.

Os requisitos para a acessibilidade a estes registros de auditoria, são especificados pelo CR 6.1, este determina que os conversores devem possibilitar acesso aos registros de auditoria para ferramentas e ou humanos autorizados. O acesso a esses registros de auditoria, por um *software* especializado é necessário para aplicar filtros aos logs de auditoria, identificando e removendo informações redundantes e para geração de relatórios. O acesso manual aos registros de auditoria (como visualizações em tela ou impressões) é suficiente para atender ao requisito básico, mas é insuficiente para alcançar níveis superiores de proteção. [6]

3.3.4.6 Raiz de Confiança

Um certificado criptográfico é único e forte, dependendo do tipo selecionado. No entanto, se a chave privada associada ao certificado não for armazenada em memórias protegidas, o certificado ainda poderá ser comprometido. [3]

Raízes da confiança (RoT, *Root of Trust*), consiste em *hardware*, *software*, e processos que estabelecem a confiança do sistema. Em um dispositivo ela determina o nível de confiança na autenticidade das credenciais pertencentes a esse dispositivo específico. Deve ser capaz de gerar, gerenciar e armazenar pelo menos uma identidade, bem como, garantir a integridade do *firmware* [3]. O nível de segurança fornecido, depende de como ela é implementada. Preferencialmente deve ser implementada em *hardware* (HRoT, *Hardware Root of Trust*), pois proporciona um controle de segurança mais forte, que uma RoT baseada em *software* [59]. Tecnologias de *hardware* como Módulos de plataforma confiáveis (TPM, *Trusted Platform Module*), fornecem plataformas eficientes para a implementação do RoT [75]. Os autores [76], apoiam desenvolvedores na identificação das implicações do uso de TPMs na confiabilidade de seus sistemas. Destacando possíveis consequências no uso de TPMs em sistemas físicos cibernéticos.

3.3.4.7 Proteção de Integridade

A norma IEC 62443-4-2, a através do CR 3.4, Integridade do programa e da informação, especifica que métodos de verificação de integridade devem ser empregados para detectar, registrar, relatar e proteger adulterações de *firmware* e de informações no conversor. [6]

O processo de inicialização (*bootloader*), inicia os principais componentes de *hardware* e *firmware* principal do conversor. Realizar o controle deste processo, permite a validação da

integridade do *firmware* e ou sistema operacional e assegura que o conversor estará em um estado conhecido antes que qualquer outra função entre em execução. [65]

A inicialização segura pode ser verificada ou medida. A inicialização medida refere-se ao processo pelo qual cada entidade na sequência de inicialização, mede a próxima entidade na cadeia de execução antes de executá-la [3]. Cria-se uma cadeia de confiança durante a sequência de inicialização, na qual cada elemento do *firmware* principal é avaliado ao ser executado durante o processo de inicialização. [76]. O trabalho [77] apresenta um estudo de sua aplicabilidade a sistema da indústria de aviação, utilizando FPGA com recursos de segurança para construir uma RoT baseada em *hardware*.

O processo de inicialização verificado é realizado através da assinatura digital do *firmware*. A UEFI utiliza cadeia de confiança (CoT), para o processo de inicialização verificado [59]. Nesse tipo de proteção de inicialização, o sistema será interrompido se a validação da assinatura digital do *firmware* falhar.

Depois de atestada a integridade do processo de inicialização, o *firmware* ou sistema operacional entra em execução. Como em muitos casos, em ambientes industriais, conversores podem permanecer por muito tempo sem ser reinicializados, ferramentas que garantam a integridade estática e dinâmica durante a operação do conversor também devem ser utilizadas. [3]

Controles da lista negra procuram identificar arquivos que contenham elementos de código malicioso, comumente conhecidos como *malware*. Controles de lista branca, validam a integridade de programas e serviços confiáveis previamente assinados, antes de iniciar sua execução. Na prática, muitos fabricantes evitam essa técnica devido à complexidade em assinar todos os arquivos durante os ciclos de desenvolvimento e lançamento de *software*.

Como alternativa, pode-se utilizar o *hash*, se um executável específico não estiver no livro da lista de permissões, ou o *hash* do executável não corresponder ao *hash* do livro, sua execução será bloqueada. [3]

Conversores também devem prover a capacidade de proteger a integridade da comunicação (CR 3.1). Muitos ataques são baseados na manipulação de dados transmitidas em canais de comunicação. As redes comutadas ou roteadas fornecem uma oportunidade maior para os invasores manipularem os pacotes, pois o acesso não detectado a essas redes geralmente é mais fácil e os próprios mecanismos de comutação e roteamento também podem ser manipulados para obter mais acesso às informações transmitidas. A manipulação no contexto de um IACS pode incluir a alteração dos valores de medição de um sensor, alteração dos parâmetros de comando enviados de um programa para o conversor etc. [6]

Mecanismos de validação de entrada (CR 3.5) e Saídas determinísticas (CR 3.6), devem verificar sintaxe, comprimento, faixa de valores e conteúdo dos dados fornecidos ao conversor, antes de alterar os seus parâmetros e direcionar suas saídas para um estado predeterminado, quando sua operação normal não puder ser mantida. Elevando a proteção caso mecanismos de proteção como o controle de acesso tenham sido contornados. [6]

Ainda para dispositivos embarcados, através dos requisitos específicos EDR 3.12 e EDR 3.13 a norma IEC 62443-4-2 específica, que deve proteger a confidencialidade, integridade e autenticidade das chaves e dados do fornecedor e do proprietário do produto, a serem usados como uma ou mais raízes de confiança (RoT). [6]

3.3.4.8 Confidencialidade e Proteção dos Dados

A proteção de dados deve abranger dados em repouso, dados em uso, a para alguns casos, até mesmo dados em movimento [65]. Confidencialidade da informação CR 4.1 da norma IEC 62443-4-2, especifica que conversores devem fornecer capacidade de proteger a confidencialidade das informações em repouso, para as quais a autorização somente leitura é determinada.

A criptografia é uma das ferramentas utilizadas para a proteção destes dados, ela garante a confidencialidade, evitando acesso não autorizado por terceiros que não possuem a chave adequada para decriptar. A integridade dos dados visa garantir que qualquer alteração dos dados seja detectada. As técnicas tradicionais de integridade de dados para dispositivos de TO (por exemplo, verificação de CRC) aumentam a confiabilidade e a resiliência de um sistema, mas não são tão eficazes. Técnicas mais recentes, como assinaturas digitais, proporcionam maior confiança na integridade. [3]

Em caso de necessidade de criptografia (CR 4.3) para dados em movimento ou em repouso, como por exemplo *backups*, o conversor deve usar mecanismos de segurança criptográfica de acordo com práticas e recomendações de segurança internacionalmente reconhecidas. O mesmo é válido se certificados de infraestrutura de chave pública (PKI, *Public Key Infrastructure*) são utilizados (CR 1.8). A seleção da PKI apropriada, deve levar em consideração a política de certificados da organização, o risco associado à violação da confidencialidade das informações protegidas e a latência induzida pela sua utilização.

3.3.4.9 Disponibilidade dos recursos

Incidentes de segurança no conversor, não devem afetar as funções essenciais ou demais funções relacionadas à segurança cibernética. Portanto, deve-se garantir a disponibilidade do conversor contra a degradação ou negação de serviços essenciais, de modo a operar de forma confiável em condições normais de produção e previna situações de negação de serviço causadas por ações realizadas por outras entidades.

O requisito do componente 7.1, proteção contra negação de serviço, especifica que conversor devem fornecer a capacidade de manter as funções essenciais, mesmo se estiver operando em um modo degradado devido a um ataque de negação de serviço (DDoS). O CR 7.2, gerenciamento dos recursos, especifica que conversores devem ter a capacidade de limitar o uso de seus recursos, de modo a se proteger contra o esgotamento destes recursos, tarefas e processos de *software* de baixa prioridade, não devem afetar tarefas e processos de alta prioridade.

A disponibilidade de *backups* atualizados, fornece a capacidade de recuperar um sistema (CR 7.4) para um estado seguro e conhecido após interrupções ou falhas. Para que isto seja possível, o CR 7.3 especifica que conversores devem fornecer a capacidade de participar das operações de *backup* para salvaguardar o estado do conversor e as configurações realizadas pelos seus usuários.

3.3.4.10 Restrição do fluxo de dados

Fabricantes e fornecedores devem especificar a arquitetura do IACS provendo restrições de fluxo para seus conversores. Determinar e configurar mecanismos que variam desde a desconexão das redes do dispositivo, das redes comerciais ou públicas, ao uso de *gateways* unidirecionais, *firewalls*, configurações de zonas de desmilitarizada (DMZ, *Demilitarized Zone*) para gerenciar e segmentar os fluxos de informações.

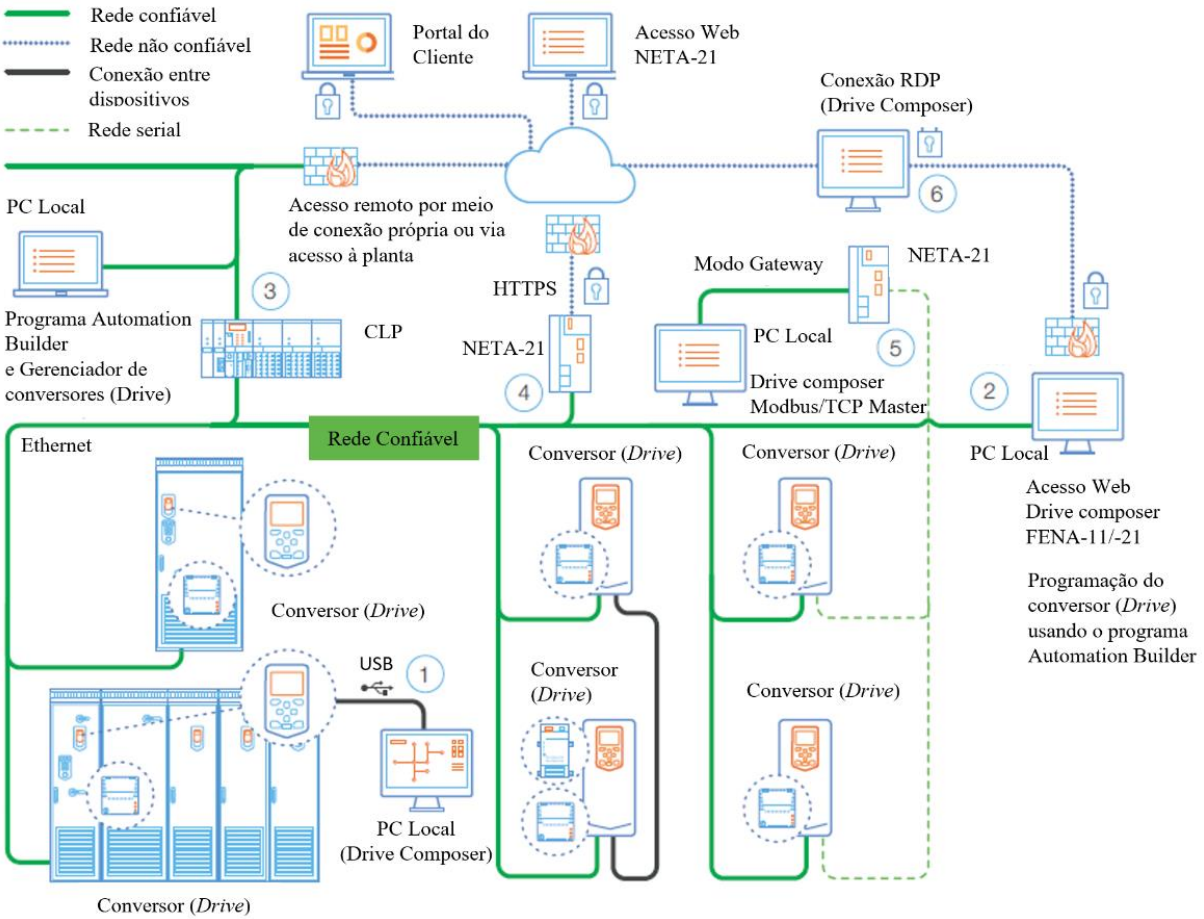
A segmentação da rede (CR 5.1), especifica que componentes devem oferecer suporte a uma rede segmentada, suportando arquiteturas de rede avançadas com base em segmentação lógica e criticidade de informações. Evitando a necessidade de segmentação física das redes, que também é valido pois fornece outros níveis de proteção, porém levará a um design de rede mais complexo e mais caro.

A Figura 16, representa uma rede industrial (planta fictícia) utilizando produtos e conversores da ABB. Normalmente este modelo de rede industrial, está conectada com

segurança às redes corporativas do cliente (não contempladas pela imagem) através de redes públicas ou privadas e a outras redes industriais dentro da planta.

O exemplo, apresenta como aplica-se, meios genéricos de proteção do ambiente de automação industrial contra acessos não autorizados, através da segmentação de redes. Para este caso, opta-se por criar proteção de defesa em profundidade (*defense-in-depth protection*), conceito no qual várias camadas de controles de segurança são posicionadas na rede através de firewalls.

Figura 16 – Planta de automação industrial, segmentação segura da rede



Fonte: Adaptado de ABB. [78]

O item 1, representa a conectividade direta ao conversor, através de comunicações seriais ponto a ponto, como é o caso das interfaces USBs. É importante que estas conexões sejam realizadas por computadores que estejam isolados de outras redes. Geralmente estes tipos de conexão, não utilizam mecanismos de confidencialidade dos dados em movimento, por considerar que esta é uma conexão local e muito bem controla, no entanto, o uso de computadores móveis conectados a redes móveis, pode fornecer um ponto de acesso direto ao equipamento. [78]

O item 2 apresenta, computadores que dispõem de sistemas supervisórios ou programas para a parametrização de conversores, geralmente estes computadores são acessados remotamente e *firewall* de próxima geração (NGFW, *Next-Generation Firewall*) [79] podem ser adicionados para o controle destes acessos. No item 5, acessos através dos protocolos seriais são realizados e protegidos pelo *gateway*. Mais exemplos e detalhes são apresentados em [78].

3.3.4.11 Arquitetura de Sistemas Distribuídos

Possibilita a segregação dos sistemas existentes no conversor, sistemas diferentes exigem diferentes níveis de segurança em uma mesma plataforma. Basicamente divide-se o sistema em vários blocos utilizando técnicas de isolamento, para evitar acesso direto entre eles, possibilitando acesso somente por uma interface de comunicação cuidadosamente controlada.

Técnicas de isolamento referem-se a técnicas usadas para proteger componentes e funções de um sistema, ou seja, assegurar que processos ou componentes comprometidos não afetem outros elementos do dispositivo, protegendo-o de falhas e atividades maliciosas. As técnicas de isolamento mais conhecidas são: isolamento de processos; isolamento virtual; isolamento por contêiner. [3]

O modelo de isolamento de processos, depende do sistema operacional para isolar componentes operacionais dos componentes de segurança. Os domínios de proteção hierárquica protegem funções e dados de falhas inadvertidas ou maliciosas, atuando como um portão para proteger camadas mais privilegiadas de camadas menos privilegiadas. O modelo de isolamento através de máquinas virtuais, usa um "*hypervisor*" para implementar o isolamento entre cada instância virtual em execução. Já o modelo de isolamento por contêiner, pode ser desenvolvido em *hardware* ou *software*. Os contêineres de *software* contam com o sistema operacional para impor os limites de isolamento de recursos. De *hardware*, separam a implementação de segurança, no mesmo chip ou na mesma placa de circuito impresso. Isso cria um coprocessador de segurança separado do processador principal. [3]

3.3.4.12 Ambiente de execução confiável

Projetistas de conversores podem desejar fornecer níveis de proteção adicionais, como permitir acesso a determinados componentes do sistema, somente por *softwares* confiáveis. Isso ajudaria a impedir que malwares acessem dados privados ou monopolizem recursos do sistema, prejudicando o desempenho do conversor. Por exemplo, o projetista poderia impedir acesso a

memória *flash* do conversor usada para armazenar dados sensíveis, como senhas, informações pessoais, sobre a aplicação, etc. [80]

Ambiente de execução confiável (TEE, *Trusted Execution Environment*) proporcionam integridade e confidencialidade para o sistema do conversor, provendo integridade para a inicialização da plataforma, armazenamento seguro, autenticação e identificação (RoT, *Rich Execution Environment*) e execução isolada, possibilitando um alto nível de segurança, separando as funcionalidades de segurança das demais rotinas operacionais do processador, ou seja, isola as funções de segurança do ambiente de processamento normal, também conhecido por (REE), no qual os sistema operacional ou *firmware* principal é executado. [81]

Um TEE baseado em *software*, pode ser um *gateway* virtual em execução dentro de uma máquina virtual ou de um contêiner [3]. Já um TEE baseado em *hardware*, utilizam arquiteturas de *hardware* como a M-Shield da Texas Instruments [82], ARM TrustZone [60] ou Intel SGX [83], que muitos consideram como híbrida, pois, é definida por *software* e suportada por *hardware* [59].

3.3.4.13 Firmware ou Sistema Operacional

Enquanto *software bare metal* (Sistema Monolítico) servem como uma implementação mínima das funções necessárias de gerenciamento do sistema computacional, um sistema operacional (OS, *Operational System*) ou um sistema operacional de tempo real (RTOS, *Real Time Operating System*) oferece suporte a multitarefa e gerencia o uso de recursos e processos do sistema. [3]

A maioria dos dispositivos embarcados industriais no mercado, dentre eles pode-se considerar os conversores, utilizam sistemas monolíticos projetados para trabalhar em microcontroladores, nos quais todos os processos (usuário e sistema) são executados em um único espaço de endereço sem restrições. Do ponto de vista da segurança cibernética, essa arquitetura é adequada apenas para simples aplicações, geralmente sem conexão direta com a Internet. Atualmente existem muitas bibliotecas para o desenvolvimento de ferramentas de segurança cibernética, disponibilizadas pelos próprios fabricantes de microcontroladores. No entanto, por serem desenvolvidas para aplicações e soluções especificas, geralmente não são testadas de uma maneira abrangente e suficiente. Estes são alguns motivos que elevam as vulnerabilidades destas arquiteturas monolíticas e tornam um risco o uso delas em CPSs. [84]

Microkernel é uma arquitetura de sistema que fornecem abstração mínima de "*hardware*" e funções elementares para o gerenciamento dos processos do sistema. A maior

parte do trabalho é realizada com a ajuda de processos de usuários dedicados que não são executados no *Kernel*. Isso ajuda a reduzir substancialmente a superfície de ataque dos serviços do *Kernel* [84]. Nos últimos anos resultados significativos do ponto de vista da segurança cibernética foram demostrados com a utilização destas arquiteturas, amplamente utilizadas por sistemas RTOS.

Sistemas monolíticos de *kernel* são outro tipo de arquitetura de sistema operacional. Esse talvez seja o tipo de arquitetura de sistema operacional mais difundido e popular para sistemas de uso geral (servidores, estações de trabalho, etc.). Diferentemente das soluções puramente monolíticas, os processos do usuário nos sistemas monolíticos do *kernel* são isolados do *kernel* e só têm acesso às suas funções através de um número limitado de chamadas do sistema [84]. Isso constitui uma vantagem do ponto de vista de segurança cibernética. Muitos serviços são executados no contexto do *kernel*, como implementações de protocolo, sistemas de arquivos, *drivers*, etc. Além disto, sistemas monolíticos de *Kernel*, como o Linux, gerenciam o acesso a regiões seguras e não seguras de memória através da Unidade de Gerenciamento de Memória (MMU, *Memory Management Unit*), enquanto um RTOS de *microkernel* não usa a MMU, portanto, não oferece a mesma proteção de memória.

3.3.4.14 Análise e monitoração

Os mecanismos de monitoramento também devem ser protegidos [65]. O monitoramento da segurança do conversor deve se preocupar com a detecção de possíveis violações ou comprometimento do equipamento, e ele pode ser executado internamente ou pode ser executado externamente ao conversor. [3]

3.3.4.15 Configuração e o gerenciamento

Os conversores devem garantir que alterações sejam realizadas de forma segura e controlada [65]. Todas as atualizações e alterações devem ser registradas, sempre que possível estes registros devem ser criptografados, isto para possibilitar posterior auditoria e recuperação do equipamento. [3]

Portanto, conversores devem fornecer a capacidade de serem continuamente monitorados (CR 6.2), usando práticas e recomendações da indústria de segurança comumente aceitas para detectar, caracterizar e relatar violações de segurança em tempo hábil. [6]

3.3.4.16 Software Parametrização

Normalmente, os fabricantes de conversores disponibilizam para seus clientes, *softwares* para parametrização e comissionamento dos seus equipamentos. A WEG por exemplo disponibiliza o WEG Programming Software (WPS) [85] e a Siemens possui o Sinamics Startdrive [86].

De certo modo, podemos considerar estes *softwares* como componentes da arquitetura de um conversor de mercado, pois são essenciais para parametrização, comissionamento e atualização de *firmware* destes equipamentos.

O modo como são integrados a arquitetura, bem como, tem a acesso as funcionalidades e parâmetros do conversor, são pontos importantes que devem ser avaliados no que diz respeito à segurança cibernética do sistema.

Sempre que possível deve-se realizar o uso de assinaturas digitais para garantir a integridade destes *softwares*, utilizar autenticação mútua para acesso privilegiado, criptografar o canal de comunicação entre *software* e conversor, implementar o princípio de menor funcionalidade para fornecer apenas recursos essenciais ao usuário do sistema, gerenciamento de vulnerabilidades, com possibilidade de atualização automática em conjunto com um ciclo de vida controlado e gerenciado para garantir a disponibilidade e qualidade do sistema. [3],[65]

4 PROJETO DO CONTROLE DE ACESSO

Conforme comentado no Capítulo 3, o CFW300 é um conversor indireto de frequência CA/CA desenvolvido e comercializado pela WEG, categorizado pela própria empresa como um mini inversor de frequência. Os conversores da linha CFW300 possuem as seguintes características:

a) corrente nominal de saída de 1,6 a 15,2 A (0,25 cv / 0,18 kW à 10 cv / 7,5 kW);
b) alimentação monofásica 100-127 Vca, 200-240 Vca monofásica ou trifásica, 380-415 e 440-480 trifásica ou em corrente contínua nas faixas de 280-340, Vcc 513-560 Vcc e 594-650 Vcc.

O conversor também conta com uma quantidade significativa de recursos, que não se limitam a: [87]

a) controle V/F, V/F quadrático ou vetorial VVW selecionáveis;
b) rampas de aceleração,desaceleração e rampa de desaceleração de emergência;
c) frenagem reostática;
d) proteção de sobrecarga e sobretemperatura no motor e nos IGBTs;
e) proteção de sobrecorrente;
f) função SoftPLC incorporada (funcionalidades básicas de um PLC);
g) função mestre Modbus.

Quanto à segurança cibernética, o conversor CFW300 possibilita somente a configuração de uma senha única de quatro dígitos numéricos, para proteção do acesso aos parâmetros de escrita através da HMI.

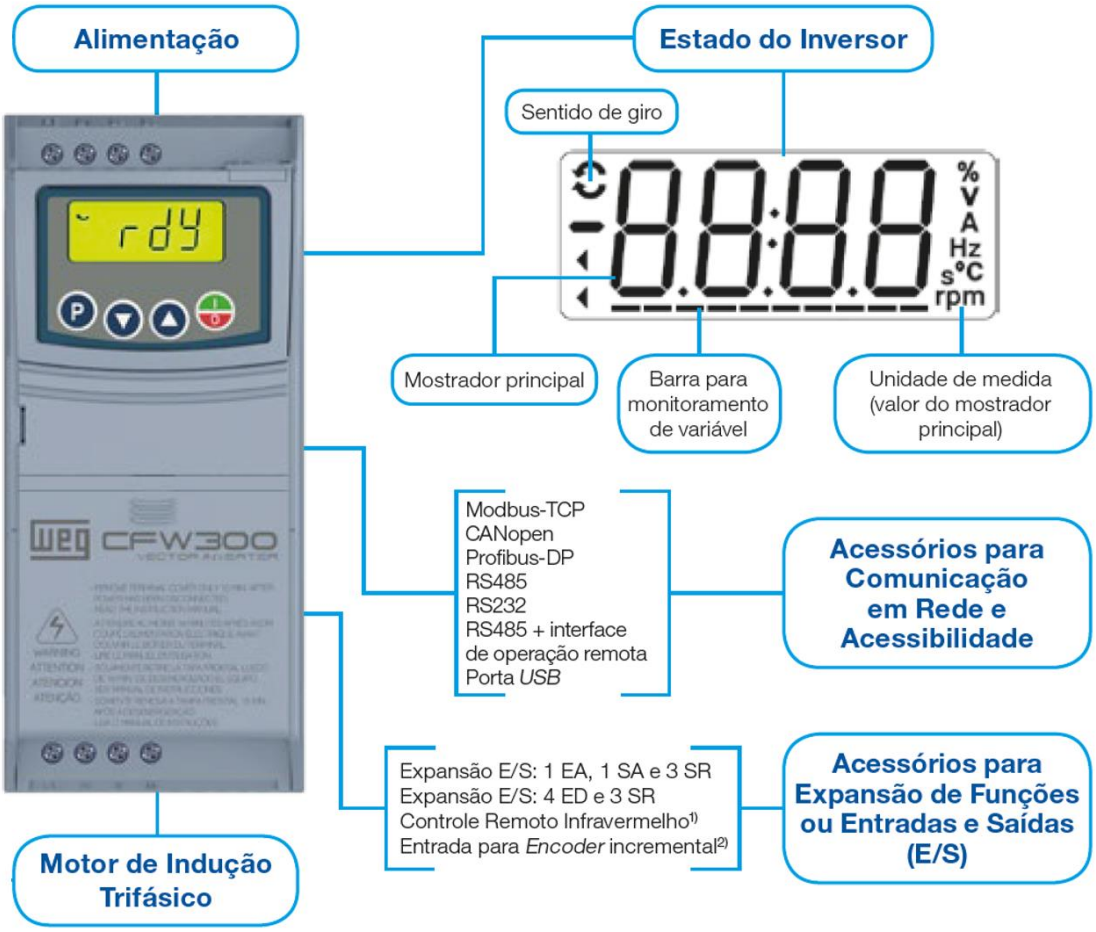
Entretanto, esta senha não é aplicável para monitoração e ou parametrização via o programa de computador WPS ou para acesso aos parâmetros através das redes de comunicação. Recursos viabilizados, somente com a adição dos módulos de comunicação. Estes módulos são acessórios comercializados separadamente pela WEG e agregam funcionalidades de comunicação por demanda para o conversor. A Figura 17 apresenta o CFW300, seus acessórios e algumas de suas características.

Com o objetivo futuro de elevar a maturidade da segurança cibernética nestes conversores, com base no *firmware* do sistema de controle do conversor CFW300 e na revisão de literatura apresentada nos capítulos anteriores. Este capítulo apresenta, o projeto do controle de acesso proposto por este trabalho, para assegurar a disponibilidade, integridade e a confidencialidade das informações do conversor, contra ataques casuais, coincidentes ou intencionais por usuários não autorizados, sejam eles humanos, *malwares* ou dispositivos, que

utilizem meios simples, poucos recursos, baixa motivação e habilidades moderadas em sistemas de automação e controle industrial, preparando-o para Indústria 4.0. Na qual, conversores são continuamente monitorados, interagem com sistema de tecnologia da informação e sistemas em nuvem e integram-se ao domínio de TI.

Deste modo apresenta-se nas próximas seções, detalhes sobre os projetos de *hardware* e *firmware*, bem como, os ensaios realizados para validar o funcionamento do controle de acesso elaborado.

Figura 17 – Apresentação do conversor CFW300, características e acessórios



Fonte: WEG. [87]

4.1 FERRAMENTAS UTILIZADAS

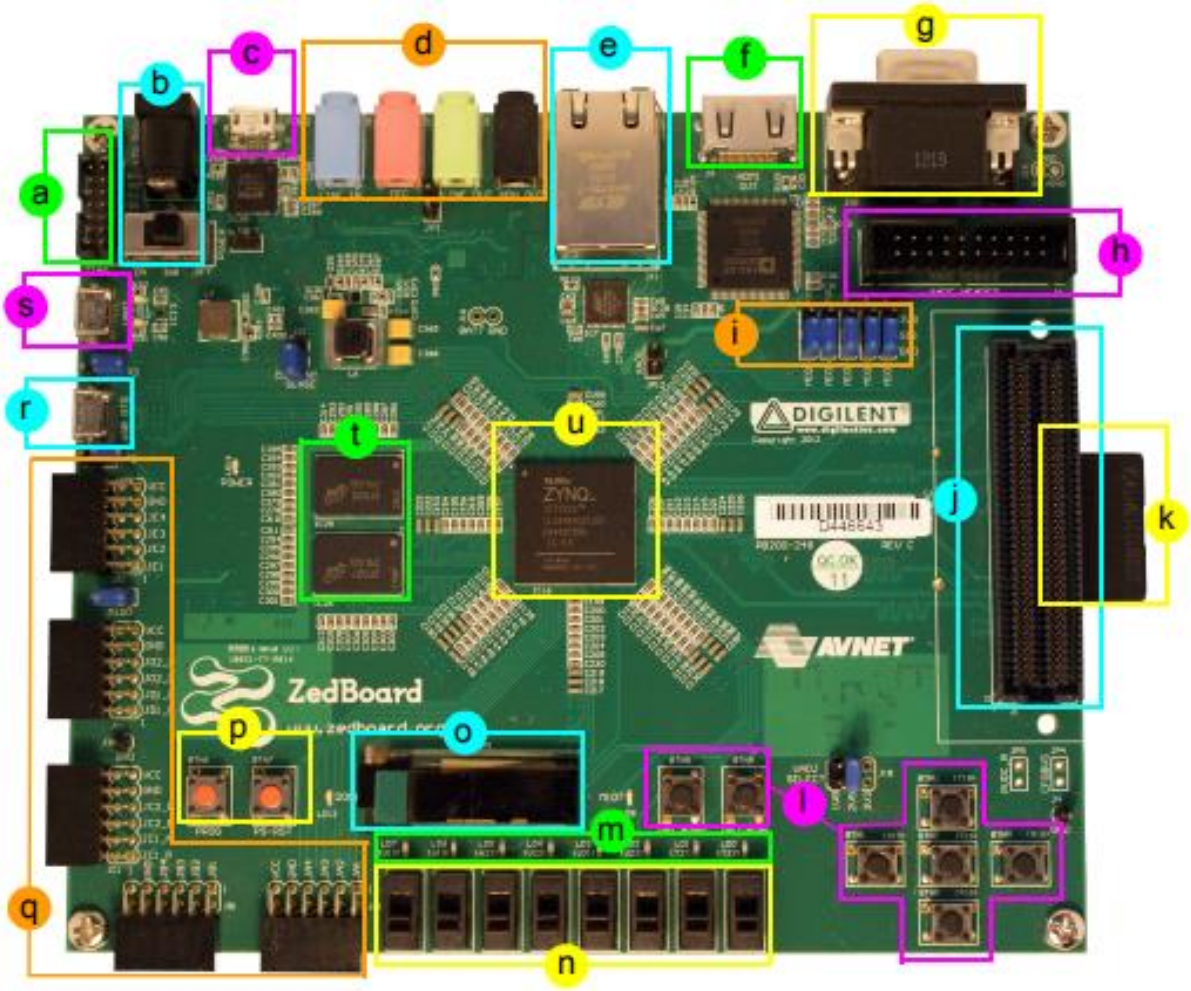
Apesar do trabalho se basear nas funcionalidades e arquitetura do CFW300 da WEG, opta-se por não utilizar o *hardware* do produto para o desenvolvimento e validação dos mecanismos de segurança cibernéticas e do protótipo, possibilitando que os mecanismos neste trabalho sejam aplicáveis a qualquer linha de conversores, independente de *hardwares*, microcontroladores e microprocessadores por eles utilizados.

No entanto, para garantir a compatibilidade dos mecanismos desenvolvidos, existe a premissa de desenvolvê-los utilizando linguagem de programação C e para melhor portabilidade, opta-se pelo uso de um sistema operacional de tempo real (RTOS), pois visa-se tirar proveito da camada de abstração de *hardware* que o sistema operacional concede, aos mecanismos para ele desenvolvidos.

4.1.1 Placa de desenvolvimento ZedBoard

Por disponibilidade opta-se pelo uso da placa de desenvolvimento ZedBoard Zynq-7000 ARM/FPGA SoC (Figura 18).

Figura 18 – Placa de desenvolvimento ZebBoard



Fonte: FPGAKey. [88]

A ZedBoard é uma placa de desenvolvimento de baixo custo para o SoC Xilinx Zynq-7000, esta placa possibilita o desenvolvimento de sistemas embarcados baseado em sistemas

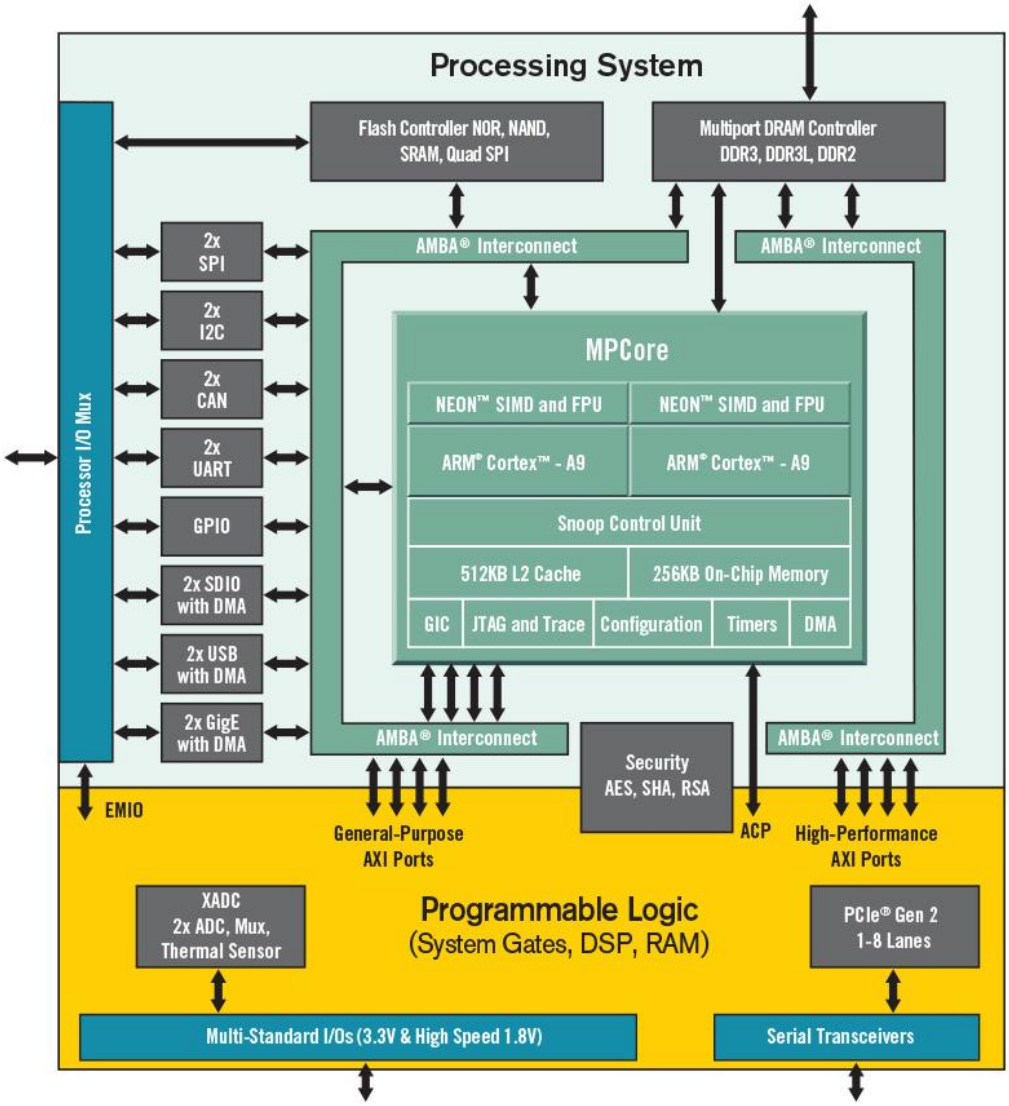
operacionais Linux, Android, MS-Windows ou RTOS. Além disso, dispõe de vários conectores para expansão [89], que fornecem acesso direto ao sistema de processamento ou a área de lógicas programáveis. As principais características desta placa de desenvolvimento são:

a) Conector interface Xilinx JTAG;
b) interruptor principal e entrada da fonte de alimentação;
c) conector interface programação USB-JTAG;
d) entrada e saída audio;
e) porta Ethenet;
f) porta HDMI;
g) porta VGA;
h) porta XADC;
i) jumpers para configuração inicial;
j) conector FMC;
k) conector para cartão SD;
l) botões do tipo *push bottons* para uso em aplicações do usuário;
m) leds para uso em aplicações do usuário;
n) interruptores para uso em aplicações do usuário;
o) display OLED;
p) botões de programação e *reset;*
q) conectores Pmod;
r) porta USB-OTG;
s) porta USB-UART;
t) 512 MB memória DDR3;
u) SoC Xilinx Zynq-7000 XC7Z020-CLG484, com processador ARM Cortex A9.

O sistema em um único chip (SoC, *System-on-a-chip*) embarcado na ZedBoard, é o modelo Zynq XC7Z020-CLG484 e pertence à família de SoCs Zynq 7000 fabricados pela empresa Xilinx. Estes dispositivos são equipados com processadores ARM Cortex-A9 de dois núcleos e com FPGAs da família Kintex-7 ou Artix-7.

Conforme pode ser observado na Figura 19, basicamente pode-se dividir o dispositivo em duas áreas. Uma é do sistema de processamento (PS, *Processing System*) e a outra a de lógica programável (PL, *Programmable Logic*) [90]. Além disto o SoC, disponibiliza várias interfaces de comunicação (SPI, I2C, CAN, UART etc.), controladores de memória *Flash* e DRAM, e um módulo de segurança em *hardware* que disponibiliza recursos de criptografia de dados, sem a necessidade de compartilhar processamento do ARM Cortex A9.

Figura 19 – Representação da arquitetura do SoC Xilinx Zynq 7000



Fonte: Xilinx. [90]

4.1.2 Módulo relógio de tempo real

A placa de desenvolvimento ZedBoard, por ser uma placa de baixo custo dentro da sua categoria [89], não disponibiliza recurso de relógio de tempo real (RTC, *Real Time Clock*). Para disponibilizar recursos de data e hora, utiliza-se então o módulo RTC DS3231 (Figura 20). Este módulo é composto por dois circuitos integrados, um o próprio DS3231, RTC com interface de comunicação I2C fabricado pela Maxim[91], o outro um 24C32, memória EEPROM de 32KB fabricada pela Microchip [92]. Optou-se por este módulo devido a comunicação I2C e pelo mesmo ser alimentado por barramento de 3,3Vcc o que o compatibiliza com as interfaces PMOD da placa ZebBoard.

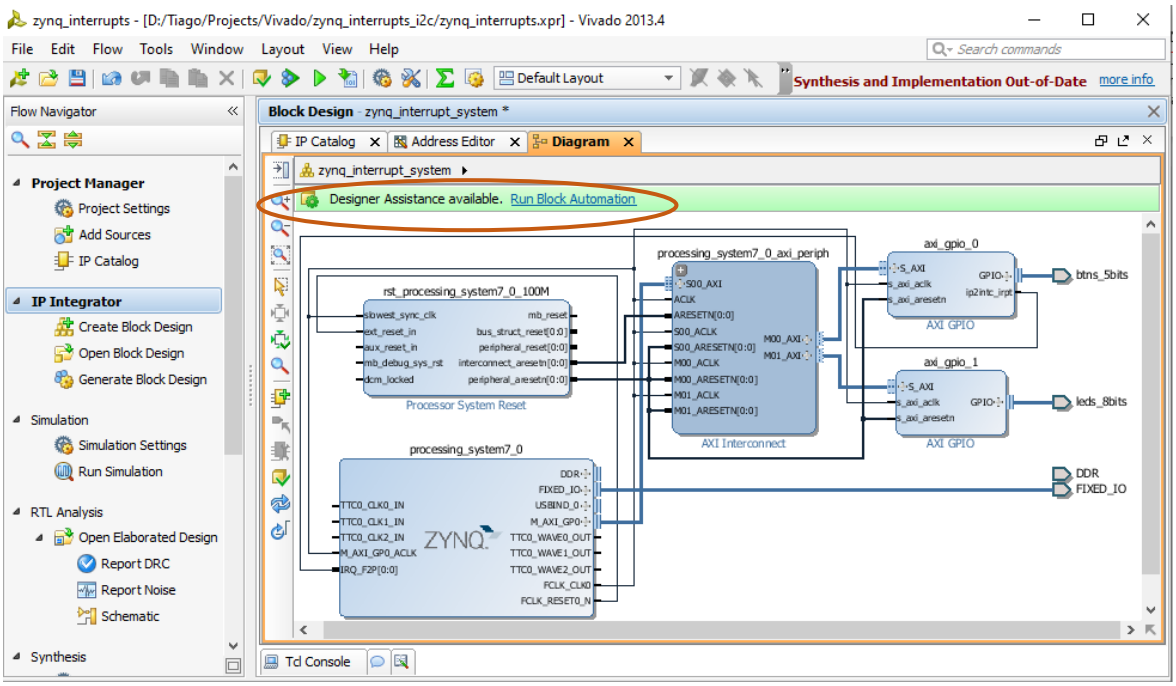
Figura 20 – Módulo RTC DS3231

Fonte: Ewald. [93]

4.1.3 Programa Vivado Design Suite

O Vivado Design Suite (Figura 21) é um ambiente de desenvolvimento (IDE, *Integrated Development Environment*) que oferece uma nova abordagem para o desenvolvimento de *hardware* embarcado em FPGA, com base em propriedade intelectual (IP, *Intellectual Property*) e utilizando linguagem C e C++.

Figura 21 – Interface IDE Vivado



Fonte: Vivado Design Suite 2013.4

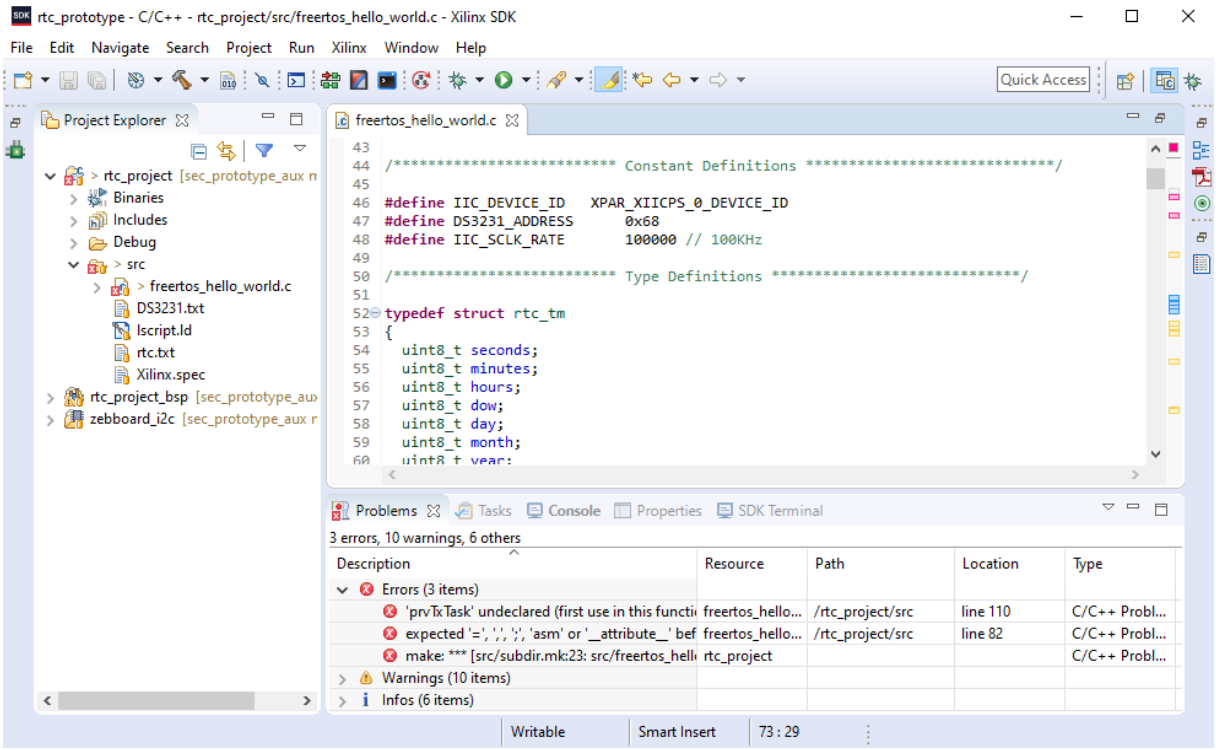
Ao contrário dos projetos tradicionais baseados em programação RTL, o design baseado em C e IP permite ciclos de desenvolvimento reduzidos na verificação, implementação e convergência de projeto [94]. A Xilinx e seus parceiros disponibilizam através desta IDE, uma rica biblioteca de IPs, amplamente testada e validada, gerando altos níveis de abstração para os

desenvolvedores. Como pode ser observado, o programa disponibiliza uma área de edição, aba Diagrama (*Diagram*), que possibilita a realização do projeto de *hardware* utilizando blocos IP, e quando possível disponibiliza a função Executar automação de bloco (*Run Block Automation*), que realiza de forma automática todas as interconexões necessárias entre os blocos inseridos no editor.

4.1.4 Programa Xilinx Software Development Kit

O Xilinx Software Development Kit (SDK) versão 2019.1 (Figura 22) é um ambiente de desenvolvimento em linguagem C e C++, para a criação de *firmwares* embarcados em quaisquer microprocessadores da Xilinx: Zynq, UltraScale + MPSoC, Zynq-7000 SoCs e os microprocessadores MicroBlaze.

Figura 22 – Interface IDE Xilinx Software Development Kit versão 2019.1



Fonte: Xilinx Software Development Kit 2019.1

Baseado no Eclipse 4.5.0, a IDE possibilita importar projetos de *hardware* embarcado realizados pelo Vivado Design Suite, configurando automaticamente: mapas de memória, registradores de periféricos, bibliotecas, opções do compilador, etc. Essa pré-configuração do projeto de *hardware* customizado, combinada com a geração automática de programa críticos do sistema, diminuem a curva de aprendizado e possibilitam ao desenvolvedor progredir

rapidamente, sem necessitar conhecimento avançado sobre a linha de produtos Xilinx [95]. Na janela da IDE, a esquerda em *Project Explorer*, disponibiliza-se uma lista em forma de arvore, contemplando todos os arquivos e pastas do projeto, a direita a IDE apresenta o código em C formatado para uma melhor compreensão do desenvolver, abaixo na aba *Problems*, são listados de forma categorizada todos os problemas existentes no projeto, contendo sua descrição, arquivo e a linha onde foi identificado pelo compilador.

4.1.5 WolfSSL

WolfSSL é uma biblioteca SSL/TLS leve baseada em linguagem C voltada para ambientes embarcados e RTOS, principalmente por causa de seu pequeno tamanho, velocidade, portabilidade e conjunto de recursos.

Suportando os novos padrões TLS 1.3 e DTLS 1.2, é até 20 vezes menor que a biblioteca OpenSSL amplamente difundida para ambientes Linux. Oferece uma API simples, uma camada de compatibilidade com o OpenSSL, suporte ao protocolo de status de certificado online (OCSP, *Online Certificate Status Protocol*), a lista de certificados digitais revogados (CRL, *Certificate Revocation List*), bem como, uma ampla lista de funcionalidades para criptografia e segurança de dados, que não se limitam a: [96]

a) SSL versão 3.0 e TLS versões 1.0, 1.1, 1.2, e 1.3 (cliente e servidor);
b) DTLS 1.0, 1.2 suporta (cliente e servidor);
c) funções *Hash*, MD2, MD4, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, BLAKE2b, RIPEMD-160, Poly1305
d) algoritmos de chave pública, RSA, DSS, DH, EDH, ECDH-ECDSA, ECDHE-ECDSA, ECDH-RSA, ECDHE-RSA, NTRU
e) geração de chaves ECC e RSA;
f) suporte a certificados do tipo PEM e DER;
g) suporte a autenticação mútua (cliente e servidor).

4.1.6 FreeRTOS

Desenvolvido em parceria com as principais empresas de circuitos integrados do mundo, o FreeRTOS é um sistema operacional em tempo real (RTOS), que existe a mais de 18 anos e é líder de mercado em aplicabilidade para microcontroladores e pequenos microprocessadores.

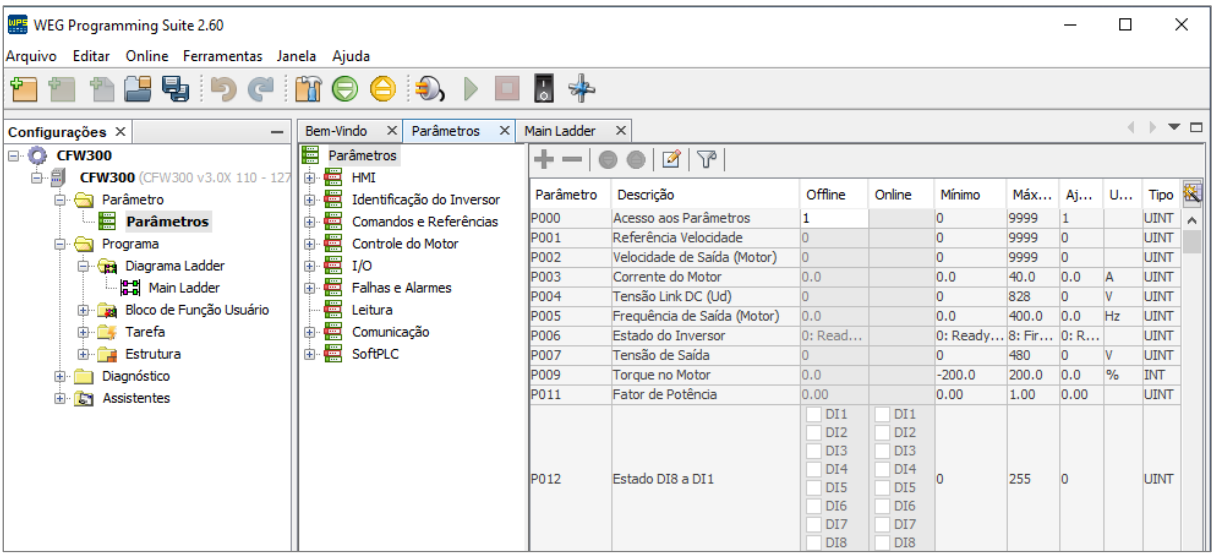
Distribuído gratuitamente sob a licença de código aberto do Instituto de Tecnologia de Massachusetts (MIT, *Massachusetts Institute of Technology*), o FreeRTOS inclui um *kernel* pequeno, geralmente seu tamanho varia de 6 a 12KB e de simples compreensão, núcleo composto por apenas 3 arquivos C, além disso fornece um conjunto crescente de bibliotecas, adequadas para uso em todos os setores da indústria. [97]

4.1.7 Programa WEG Programming Suite

Para realizar a monitoração e a parametrização de seus conversores, a WEG disponibiliza o programa de computador WEG Programming Suite (WPS). De acordo com [85], o WPS versão 2.60 é uma ferramenta integrada que auxilia na criação de aplicações na área de automação, permitindo a monitoração e alteração dos valores dos parâmetros, desenvolvimento e monitoramento de programas em linguagem Ladder (IEC 61131-3) para uso da funcionalidade de SoftPLC, disponível em conversores de diversas famílias de produtos WEG.

A Figura 23, apresenta a janela principal do programa WPS, a esquerda ficam as configurações, compostas dispositivos e seus recursos. Conforme pode ser observado, o recurso Parâmetros está selecionado, portanto a direita, podem ser visualizados todos os parâmetros do dispositivo, organizados através de um menu. A barra de ferramentas, disponibiliza botões para monitorar e realizar o *download* da configuração para o conversor.

Figura 23 – Interface do programa WPS



Fonte: WEG Programming Suite 2.60.

Para o desenvolver este trabalho fez-se necessário criar funcionalidades que até então não estavam disponíveis no programa WPS, estes recursos e janelas foram desenvolvidos em conjunto com os desenvolvedores do programa WPS. Alguns exemplos são: janela para autenticação dos usuários; janela para atualização das credenciais, janela para configuração dos mecanismos de segurança cibernética, comunicação segura entre o *software* e o *firmware* etc. Detalhes são apresentados individualmente nas próximas seções.

4.2 HARDWARE

O desenvolvimento do projeto de *hardware* (FPGA) do protótipo, baseou-se nos Capítulos 1 e 2 do livro The Zynq Book Tutorials for Zybo and Zedboard, que utiliza a IDE Vivado e linguagem de programação baseada em IP para programação do SoC embarcado na placa de desenvolvimento ZedBoard.

O Capítulo 1 demonstra, como programar a área PL do Zynq 7020 através de programação de blocos IPs, para acionar os *leds* disponíveis na placa de desenvolvimento. Para isto, utiliza-se o bloco AXI Interconnect, responsável por conectar um ou mais dispositivos mestre a um ou mais dispositivos escravos mapeados na memória AXI. [98]

Já o capítulo 2, demonstra como são criadas interrupções no sistema, através de um exemplo no qual é possível utilizar os interruptores disponíveis na placa de desenvolvimento para acionar os *leds* programados no capítulo 1. [99]

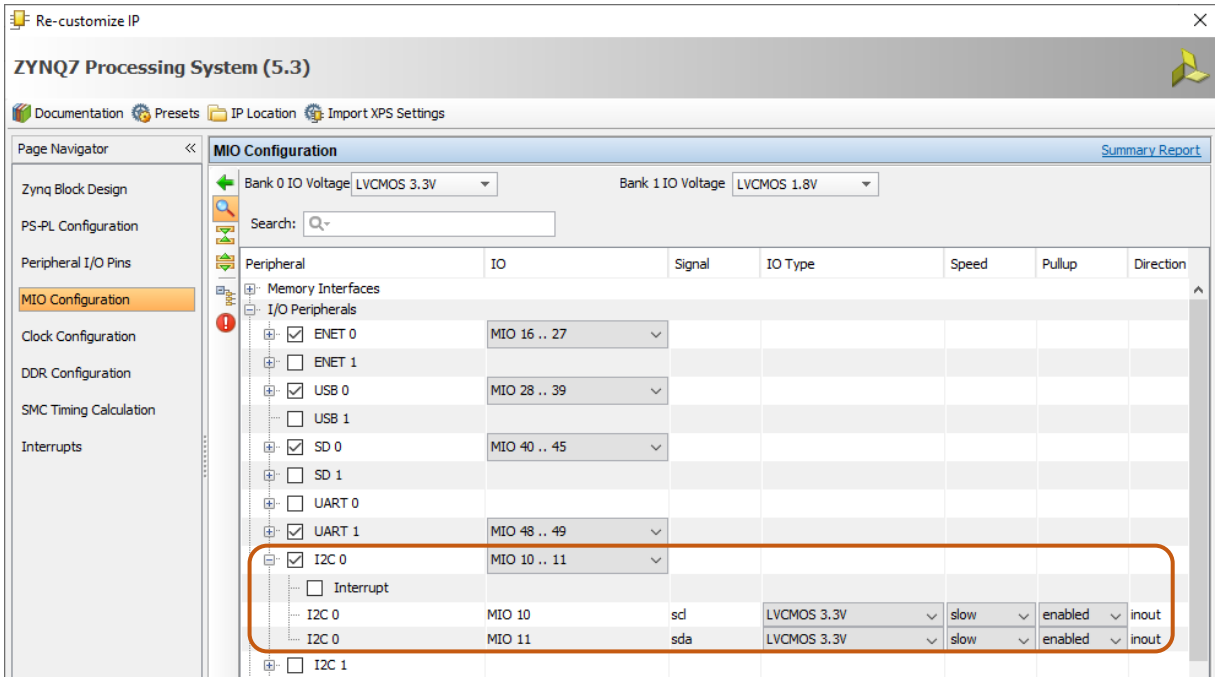
Conforme mencionado na sessão anterior, a ZedBoard não possui funcionalidade de RTC. Como o recurso de data e hora é essencial para o desenvolvimento dos mecanismos de segurança cibernética, seja para auditoria ou para validar a data de expiração de uma senha por exemplo, se fez necessário conectar um módulo RTC externo (DS3231), junto a placa de desenvolvimento, isto foi realizado através do barramento I2C e das interfaces de entrada e saída do tipo PMOD. Para isto segue-se o tutorial disponível em [100], elaborado com o propósito de instruir desenvolvedores na configuração de periféricos conectados aos conectores PMOD.

O Zynq 7020 disponibiliza conexões de entrada e saída multiplexadas (MIO, *Multiplexed I/O*) conectadas diretamente ao seu sistema de processamento, no entanto a ZedBoard utiliza estas conexões para conectar memórias DDR, memória *flash* QSPI, interface Ethernet, entre outros periféricos, limitando a disponibilidade de MIOs para os demais periféricos. Deste modo, obriga-se que a maioria dos conectores PMOD utilizem conexões de entrada e saída multiplexadas estendidas (EMIO, *Extended Multiplexed I/O*), estas conexões

são um pouco mais lentas pois não estão ligadas diretamente ao PS, havendo a necessidade de serem programadas na área PL. [101]

Para a conexão do Módulo RTC optou-se, por facilidade, pelo uso da interface PMOD JE1 da ZedBoard, porque ela é a única interface PMOD conectada através de MIO 10 e 11 diretamente ao PS, ou seja, foi configurado o uso de um barramento I2C para uso das conexões MIO 10 e 11 (Figura 24).

Figura 24 – Janela da IDE Vivado para configuração das conexões MIO

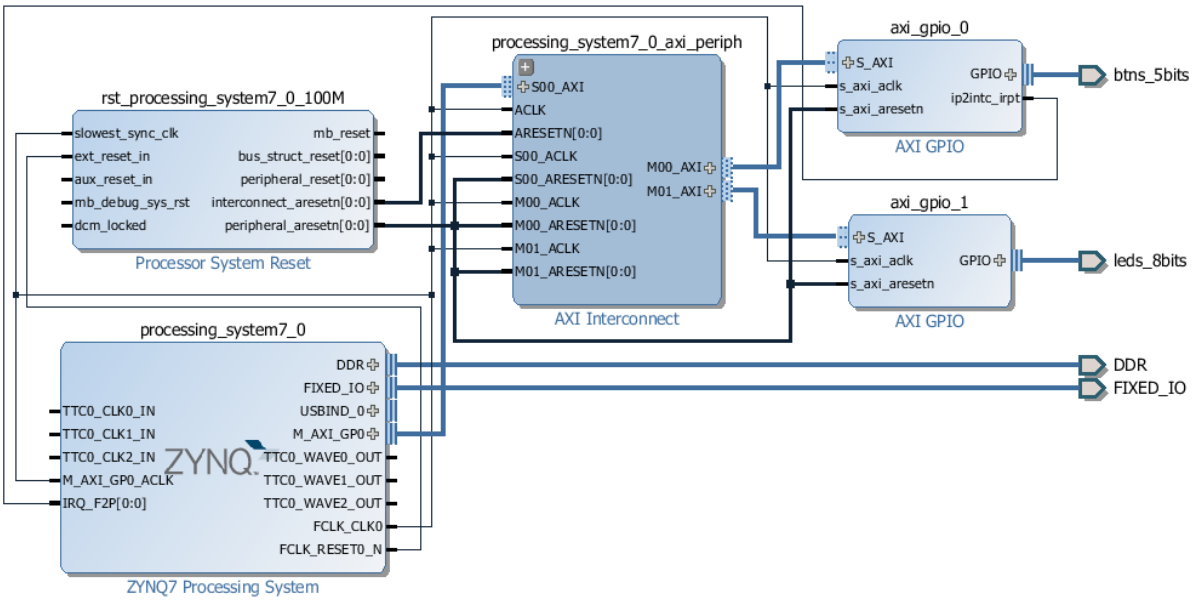


Fonte: Vivado Design Suite 2013.4

A Figura 25 apresenta o projeto de *hardware* a ser utilizado pelo protótipo para possibilitar a execução do *firmware* do sistema de controle do conversor e consequentemente a aplicação dos mecanismos de segurança cibernética para o desenvolvimento do controle de acesso.

O bloco principal ZYNQ7 Processing System, é o bloco para utilização de um dos dois núcleos (*cores*) ARM Cortex A disponíveis no SoC. Ele está interconectado a memória DDR, aos demais periféricos através da interface FIXED_IO e ao bloco AXI Interconnect (mestre), utilizado para possibilitar o acionamento dos *leds* e dos interruptores através do barramento de comunicação AXI e dos blocos escravos AXI GPIO. Além disto, existe o bloco auxiliar Processor System Reset que oferece a possibilidade de customização para reinicializações a serem realizadas no processador, na interconexão e nos periféricos.

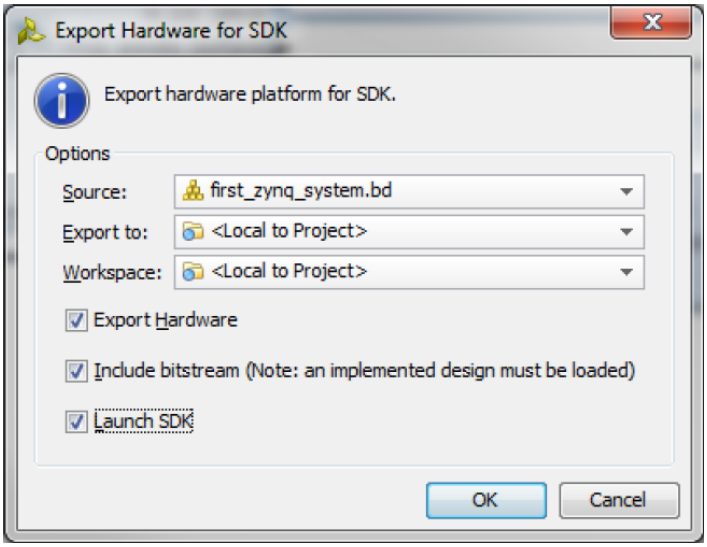
Figura 25 – Projeto de *hardware* realizado para o protótipo



Fonte: Vivado Design Suite 2013.4

Após conclusão do projeto de *hardware*, o programa Vivado possibilita exportar o projeto através da sua própria IDE (Figura 26).

Figura 26 – Programa Vivado, janela para exportação do projeto de *hardware*



Fonte: Vivado Design Suite 2013.4

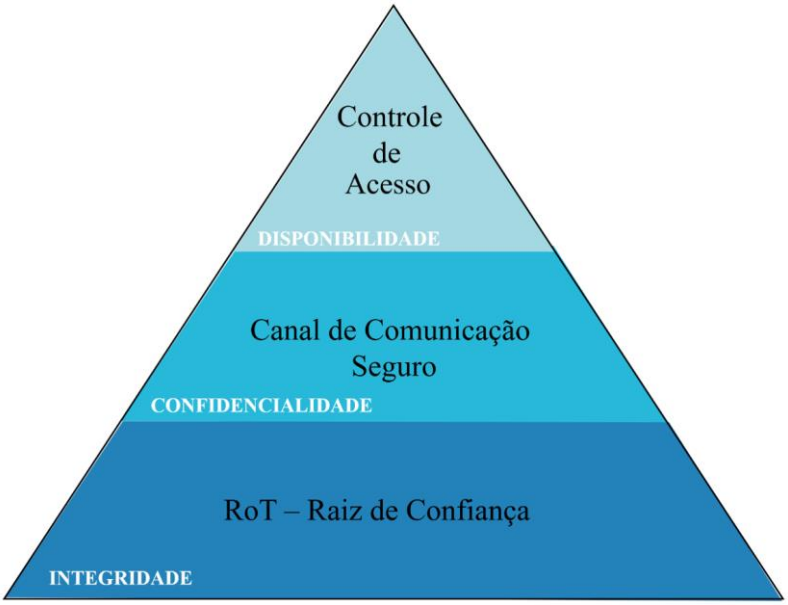
O projeto é exportado em conjunto com o “FPGA bitstream”, um arquivo que contém as informações de programação de um FPGA, a ser importado pelo SoC durante sua inicialização de modo que ele possa configurar o FPGA de acordo com o que foi previamente desenvolvido.

4.3 FIRMWARE

Conforme apresentado pelo Capítulo 3, para elevar a segurança cibernética do conversor deve-se garantir a disponibilidade, integridade e a confidencialidade, de modo a protegê-lo contra alteração, destruição, acesso não intencional ou não autorizado. Portanto, para garantir tais condições, o controle de acesso deve ser estruturado sob uma forte base, que garanta a integridade e a confidencialidade dos dados, por ele trafegados ou armazenados.

A Figura 27 busca apresentar esta estrutura em forma de pirâmide. A base garante a integridade, através da raiz de confiança do conversor, mais especificadamente com o armazenamento seguro da identidade, das chaves criptográficas e com a validação do *firmware* durante seu processo de inicialização. Na sequência, visa-se proporcionar um canal de comunicação seguro, para garantir a confidencialidade e a integridade dos dados por ele trafegados. Finalmente, no topo da pirâmide, o controle de acesso, baseado no conceito de Autenticação, Autorização e Auditoria (AAA, *Authentication, Authorization, and Accounting*)[102], para garantir a disponibilidade do conversor todos os seus usuários autênticos.

Figura 27 – Estrutura do controle de acesso



Fonte: Elaborado pelo autor.

O controle de acesso à conversores e demais equipamentos de automação industrial, visa restringir o que pessoas e entidades devem ser capazes de acessar e as conexões que podem

ser aceitas, tendo a capacidade de lidar com uma diversidade de dispositivos que compõem a infraestrutura industrial [58].

Para que isto seja possível, o administrador do dispositivo tem como desafio entender todo o processo industrial, concedendo a cada usuário ou entidade, os direitos de acessos que aquele determinado ator necessita, para cumprir seu papel dentro do IACS.

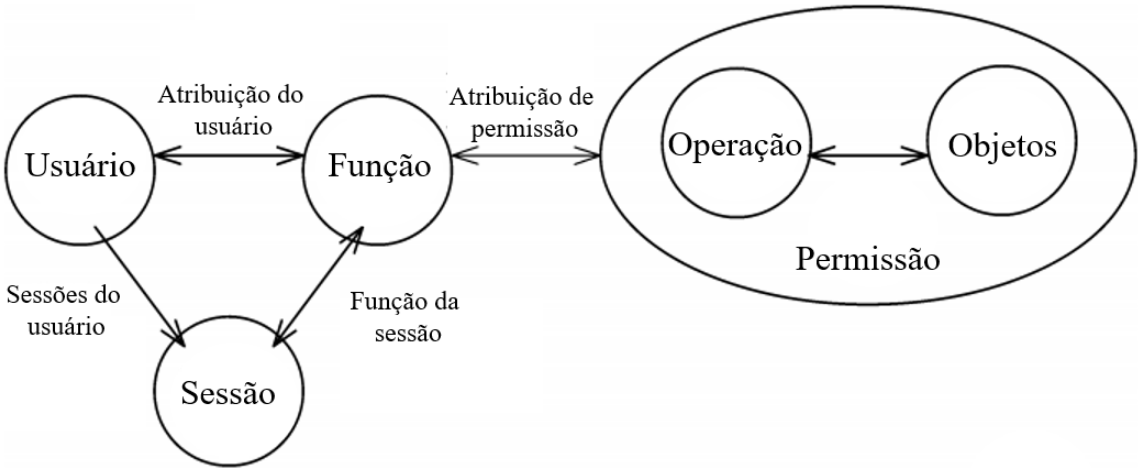
Ao longo dos anos muitos modelos de controle de acesso, foram pesquisados e desenvolvidos. Todos apresentam vantagens e desvantagens dependendo da sua aplicação, uma visam geral sobre modelos de controle de acesso podem ser encontrados nos trabalhos [22],[103]-[107].

O controle de acesso estudado, proposto e aplicado no desenvolvido deste trabalho, se baseia modelo de controle de acesso baseado em funções (RBAC, *Role-based access control*).

O RBAC tem como motivação que a responsabilidade de um sujeito (ator) é mais importante do que quem ele é. Neste modelo, usuários são autorizados a acessar os objetos do sistema, com base nas regras de acesso atribuídas as suas funções (*roles*). [103]

O modelo básico de controle de acesso baseado em funções, denominado Core RBAC por [107], é constituído por cinco elementos básicos: usuários, funções, objetos, operações e permissões. De um modo geral, o modelo é definido por: usuários individuais sendo atribuídos a funções e permissões sendo atribuídas a funções (Figura 28).

Figura 28 – Modelo básico do controle de acesso baseado em funções



Fonte: Adaptado de Ferraiolo. [107]

Uma função é um meio de atribuir relacionamento muitos para muitos, entre usuários e permissões individuais. Além disso, o modelo básico, inclui um conjunto de sessões, na qual cada sessão é um mapeamento entre um usuário e uma ou mais funções que são atribuídas a ele. Um usuário, pode ser um ser humano, uma máquina, redes, processos, etc. A função, é uma

função de trabalho dentro do contexto de uma organização. E a permissão, são os direitos para executar uma operação em um ou mais objetos protegidos pelo modelo RBAC. [107]

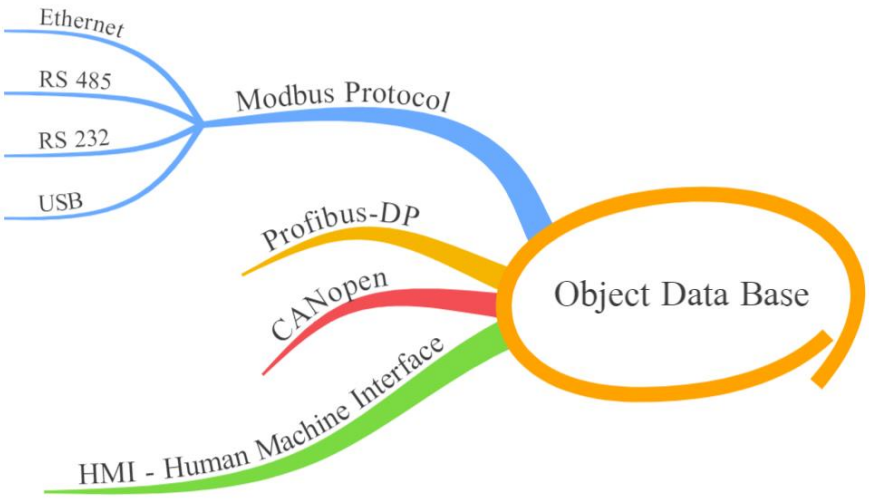
Deste modo, funções devem ser configuradas e atribuídas a usuários seguindo o princípio do privilégio mínimo, no qual usuários devem possuir apenas a permissão de acesso mínima que seja suficiente para cumprir as responsabilidades atribuídas a sua função dentro do IACS. [22]

Acredita-se que autorização de acesso RBAC, atenderá com excelência e sofisticação as necessidades do controle de acesso do conversor. Muitos conversores são limitados em recursos de *hardware* e possuem uma grande quantidade de parâmetros para serem controlados, este modelo permitirá, com uma dezena de funções, atender uma quantidade significativa usuários, redes e equipamentos.

Conforme anteriormente mencionado, o desenvolvimento do *firmware* do protótipo baseia-se no sistema de controle do CFW300. De modo simplificado o sistema de controle é representado pela Figura 29.

A base de dados de objetos (ODB, *Object Data Base*) armazena todos os parâmetros do conversor. Este subsistema gerencia de uma forma geral, o acesso a cada um destes parâmetros, conforme sua característica de escrita ou somente leitura.

Figura 29 – Representação da arquitetura do sistema de controle do CFW300



Fonte: Elaborado pelo autor.

Diretamente conectado ao ODB, estão a HMI e as camadas de aplicação dos protocolos de comunicação, e diretamente conectado a cada camada de aplicação estão as camadas inferiores do modelo OSI (Tabela 1) para cada um dos protocolos de comunicação. Na Figura 29 representado somente para o protocolo ModBus.

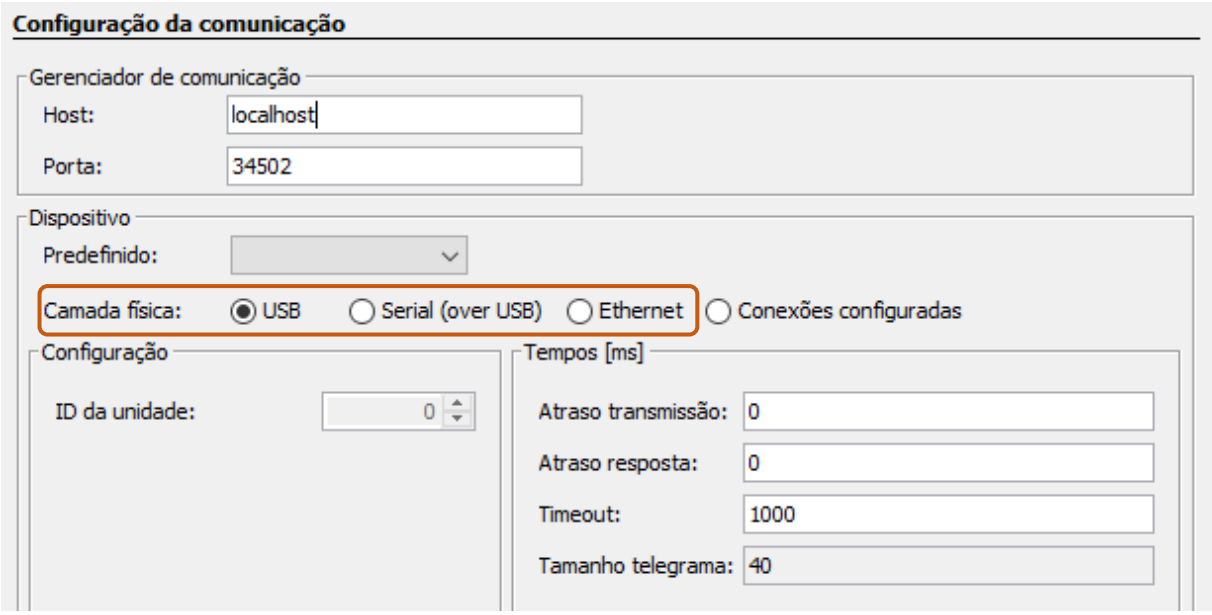
Tabela 1 – Modelo OSI para protocolos industriais

Camada	Modbus/TCP	Modbus/RTU	CANopen	DeviceNET	Profibus-DP
(7) Aplicação	Modbus	Modbus	CANopen	Família CIP	Profibus-DP
(6) Apresentação	N/A	N/A	CANopen	Família CIP	N/A
(5) Sessão	N/A	N/A	CANopen	Família CIP	N/A
(4) Transporte	TCP	N/A	N/A	DeviceNET	N/A
(3) Rede	IP	N/A	N/A	DeviceNET	N/A
(2) Ligação	Ethernet	Serial	CANBus	CSMA/NBA	FieldBus Data Link
(1) Física	Ethernet	RS-232/RS-485	CANBus	CANBus	RS-485/F.O.

Fonte: adaptado de [108].

Com o objetivo principal de identificar e autorizar o acesso de pessoas, o controle de acesso proposto, realizará o controle de uso com a identificação única, através do protocolo Modbus e via HMI. Pela interface homem máquina, pois como o próprio nome a descreve disponibiliza acesso local a operadores, mantenedores e administradores. Já o Modbus, por ser o protocolo utilizado pelo programa WPS, para monitoração e parametrização do conversor, seja por rede Ethernet ou serial RS-232, RS-485 e quando disponível USB (Figura 30).

Figura 30 – Janela WPS configuração da comunicação com o conversor



Fonte: Elaborado pelo autor.

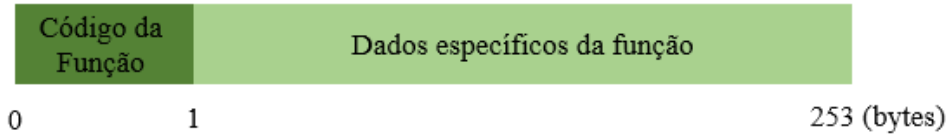
4.3.1.1 Protocolo Modbus

O Modbus é um protocolo industrial desenvolvido em 1979 com o propósito de possibilitar a comunicação entre dispositivos de automação. Originalmente implementado para transferir dados por uma camada de comunicação serial, evoluiu e atualmente também permite a transferência da dados através de uma camada TCP/IP. [109]

O protocolo opera no modo requisição resposta, através de um relacionamento mestre escravo, no qual a comunicação sempre ocorre em pares, um dispositivo mestre deve iniciar a requisição e então aguardar por uma resposta do dispositivo escravo. No protocolo Modbus as requisições são funções PDU (*Protocol Data Unit*) muito bem especificadas. [110]

Uma PDU é formada por um byte que define o código de função, seguido por até 252 bytes de dados (Figura 31). O código de função é o primeiro dado a ser validado pelo dispositivo escravo, que se não reconhecer o código de função, responderá com uma exceção. Se o código de função for aceito, o dispositivo escravo começará a decompor e analisar os próximos dados conforme definido pela determinada função.

Figura 31 – Pacote PDU do protocolo Modbus



Fonte: Adaptado de National Instruments. [109]

A Tabela 2 apresenta os códigos de função padrões fornecidos pela especificação. Os códigos de função de 1 a 64, 73 a 99 e de 111 a 127 são códigos públicos, reservados e com exclusividade garantida por norma, mas o padrão Modbus também permite a construção de funções proprietárias, possibilitando que os códigos de 65 a 72 e 100 a 110 sejam definidos pelo usuário.

Tabela 2 – Funções Modbus padrões e públicas

Código	Classe	Função
1	1	Read Coils
2	1	Read Discrete Inputs
3	0	Read Multiple Register
4	1	Read Input Register
5	1	Write Single Coil
6	1	Write Single Register
7	1	Read Exception Status (somente serial)
15	2	Write Multiple Coils
16	0	Write Multiples Registers
20	2	Read File Record
21	2	Write File Record
22	2	Mask Write Register
23	2	Read/Write Multiple Registers
24	2	Read FIFO

Fonte: Adaptado de National Instruments. [109]

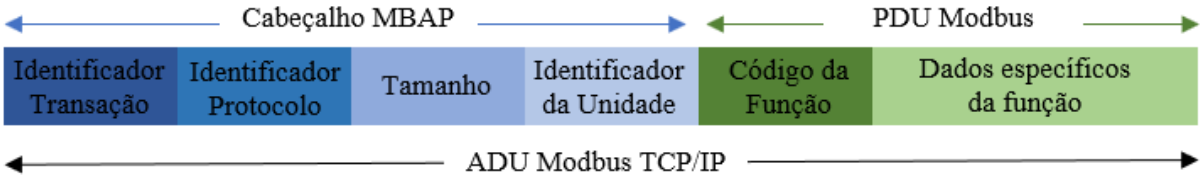
Os escravos usam exceções para indicar problemas no tratamento das PDU recebidas, exceções também são relatadas em um formato de pacote muito bem definido de dois bytes. O

primeiro byte de uma exceção deve conter o código de função recebida em hexadecimal, acrescentado do valor 0x80, por exemplo uma exceção para o código de função 0x03 (*Read Holding Register*) deverá retornar como exceção 0x83, isto limita em 127 (0x7F) a quantidade de funções que podem existir no protocolo Modbus. O segundo byte associado à resposta inclui código com o motivo da exceção. O padrão também especifica alguns destes, os mais comuns são:

a) função ilegal (*Illegal Function*, 0x01), o código de função não é suportado, para confirmar o código de função original, subtraia 0x80 do valor retornado;
b) endereço do dado ilegal (*Illegal Data Address*, 0x02), a requisição tentou acessar um endereço inválido.
c) valor do dado ilegal (*Illegal Data Value*, 0x03), a requisição tem dados incorretos.
d) falha no dispositivo escravo (*Slave Device Failure*, 0x04), ocorreu um erro durante o processamento da requisição. Geralmente indica que a requisição era válida, mas o escravo não conseguiu executá-la.

Ao longo dos anos surgiu a necessidade de atualizar o protocolo Modbus, para torná-lo compatível com novas tecnologias e novos protocolos de rede. Atualmente o Modbus é muito utilizado pela indústria junto ao protocolo Ethernet, denominado como Modbus/TCP. Esta nova versão do protocolo, utiliza funções ADU (*Application Data Unit*) para encapsular o PDU e torná-lo compatível com o protocolo Ethernet (Figura 32).

Figura 32 – Pacote ADU do protocolo Modbus TCP/IP

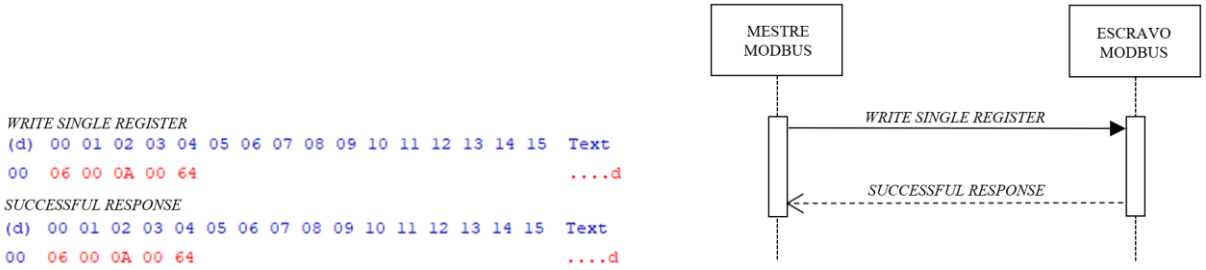


Fonte: Adaptado de National Instruments. [109]

As ADUs do tipo TCP são formadas pelo cabeçalho MBAP (*Modbus Application Protocol*) concatenado com a PDU. O MBAP é um cabeçalho de uso geral, que depende de uma camada de rede confiável, na qual, destaca-se o identificador de transações, um recurso valioso pois possibilita a realização de várias requisições simultaneamente. Por exemplo, um mestre pode enviar requisições 1, 2 e 3, e recebê-las as respostas na ordem 2, 1, 3. Nesse caso, o mestre pode combinar as requisições com suas determinadas respostas e interpretar os dados corretamente. [109]

No Modbus um registrador é definido como um dado de 16bits (2 bytes). A Figura 33 representa o uso do protocolo Modbus pelo programa WPS, para escrever o valor 100 (0x0064) no registrador 10 (0x000A) do conversor, através da requisição *Write Single Register Function* (código da função 0x06). Como resposta à requisição, o conversor responde a mesma PDU recebida confirmando que o valor foi escrito no registrador com sucesso.

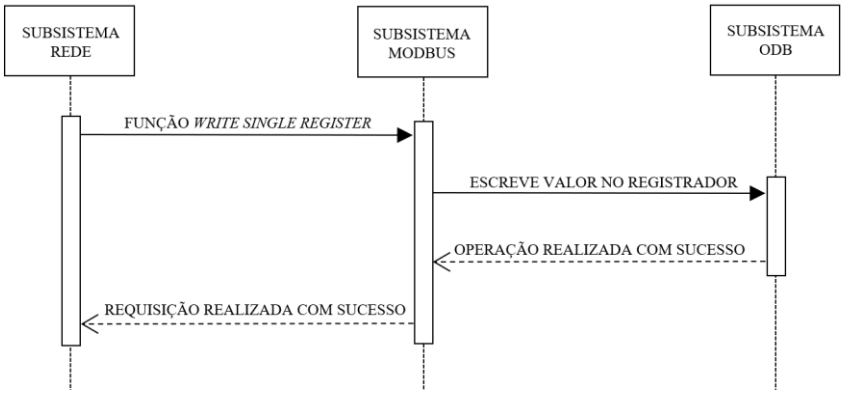
Figura 33 – Modbus PDU função Write Single Register



Fonte: Elaborado pelo autor.

Ao receber a requisição, o conversor através de seu subsistema de rede Ethernet (Figura 34), identifica que o protocolo utilizado para a comunicação é o Modbus e encaminha a requisição para ser analisada pelo subsistema Modbus. Este subsistema então reconhece e valida a requisição como uma tentativa de escrita no registrador e dispara uma ação de escrita para o registrador específico ao subsistema ODB. Uma vez escrito com sucesso o subsistema ODB, informa o subsistema Modbus que a ação foi realizada com sucesso, e este então prepara a resposta da requisição e a encaminha para o subsistema de rede que a retorna-a para o dispositivo mestre Modbus, neste caso o próprio programa WPS.

Figura 34 – Diagrama de sequência, requisição Modbus recebida pelo conversor

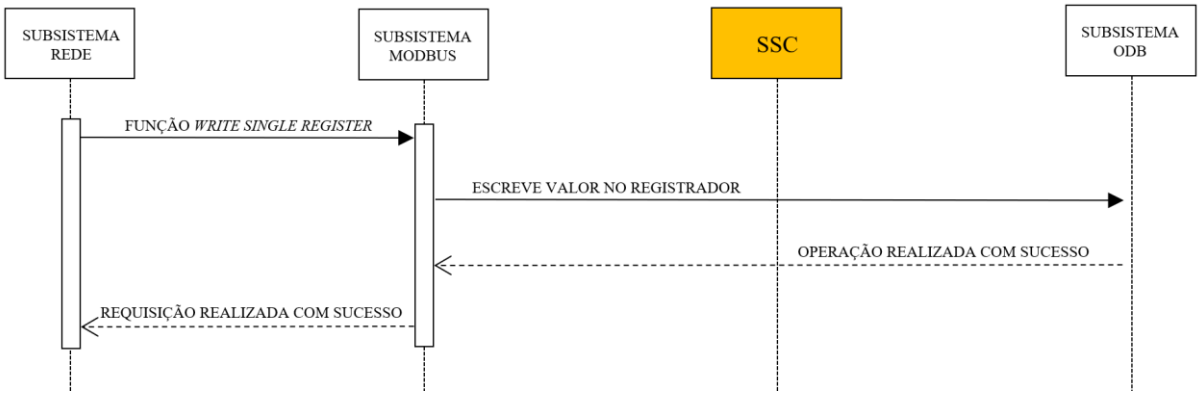


Fonte: Elaborado pelo autor.

Este trabalho, com base nas recomendações apresentadas no Capítulo 3 na Seção 3.3.4, propõe a criação do Subsistema de Segurança Cibernética (SSC), para ser integrado ao sistema

de controle do conversor. Este subsistema fará o controle de acesso ao conversor, contemplando os mecanismos de segurança cibernética necessários para autenticar, autorizar e auditar todas as requisições ao conversor (Figura 35).

Figura 35 – Representação sistema de controle com o SSC



Fonte: Elaborado pelo autor.

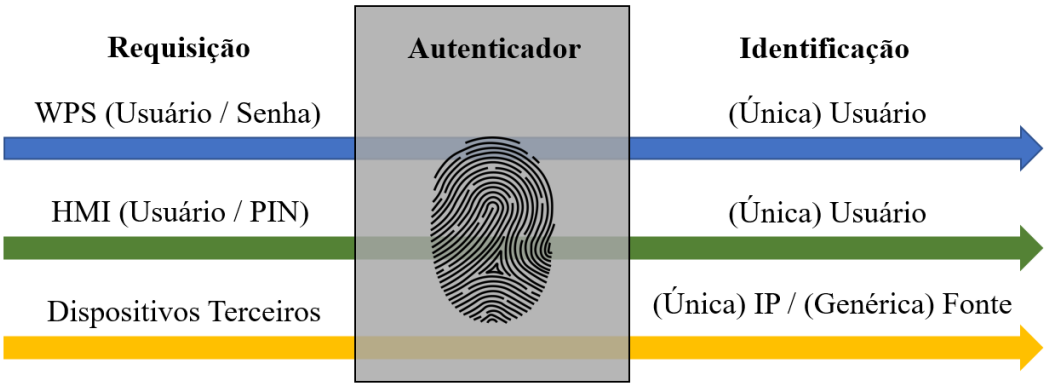
4.3.2 Controle de identificação e autenticação

A identificação de usuários através de mecanismos de autenticação é necessária para verificar a identidade dos usuários que requisitam acesso, evitando acesso por usuários não autorizados. Neste sentido a norma IEC 62443-4-2, especifica que se identifique e autentique todos os usuários (humanos, processos de *software* e dispositivos), antes de permitir que eles acessem o conversor.

Desde modo projeta-se o autenticador do SSC, para identificar de forma única a partir de um nome de usuário e se autenticar através de senha ou número de identificação pessoal (PIN, *Personal Identification Number*), requisições oriundas do programa WPS e da HMI. Bem como, este mesmo autenticador, visa possibilitar a identificação da instância ou pelo menos da tecnologia utilizada por esta instância, quando se realiza requisições através da rede de comunicação ao conversor. Possibilitando a segregação destes acessos conforme função do seu utilizador (Figura 36).

A Figura 37 representa de forma simplificada a identificação de dispositivos terceiros ou de protocolos industriais. Neste exemplo, um dispositivo requisita a escrita em um registrador do conversor através da função Modbus *Write Single Register*. Neste caso, o SSC, tem a capacidade de identificar a instância que está realizando tal ação, somente se o protocolo da comunicação dispor de um identificador.

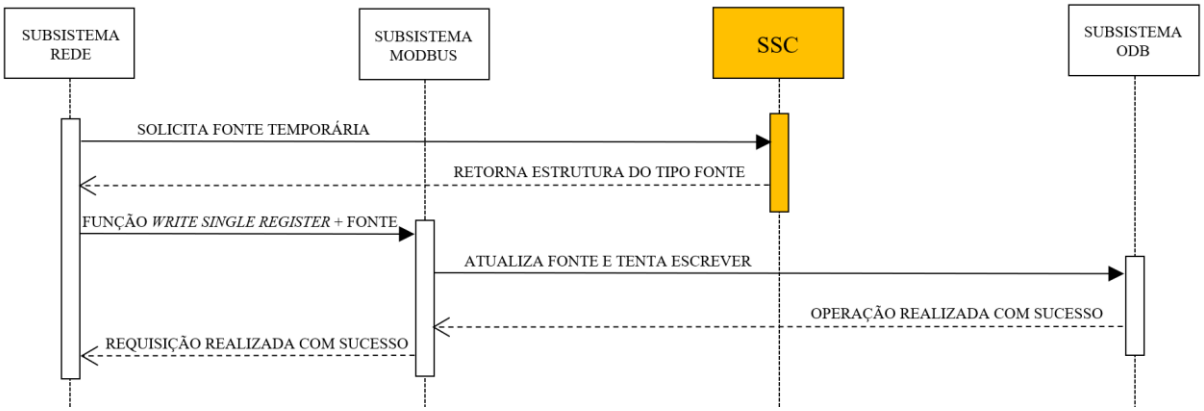
Figura 36 – Capacidade de identificação pelo autenticador



Fonte: Elaborado pelo autor.

Por exemplo, caso a requisição ilustrada pela Figura 37 utilize o protocolo de comunicação Modbus TCP/IP, será possível identificar a instância através do seu endereço IP e então após receber a estrutura do tipo fonte (Figura 38) o subsistema de rede, poderá atualizá-la com o endereço IP, que corresponde ao dispositivo daquela determinada requisição. Porém, se a requisição utiliza o protocolo Modbus RTU, ou seja, é realizada via comunicação serial, não dispõe de um identificador, podendo somente identificar o protocolo de comunicação utilizado para aquela determinada ação. Neste caso, a estrutura fonte, será somente atualizada com o protocolo de aplicação pelo subsistema Modbus.

Figura 37 – Diagrama de sequência da identificação de protocolos industriais



Fonte: Elaborado pelo autor.

Isto limita o autorizador, pois futuramente na estrutura fonte este terá somente a informação do protocolo de aplicação e poderá somente criar regras gerais a serem aplicadas para as requisições oriundas daquele determinado protocolo (no caso Modbus RTU), mas não segregará de maneira individual, como é possível no protocolo que dispõe de um identificador.

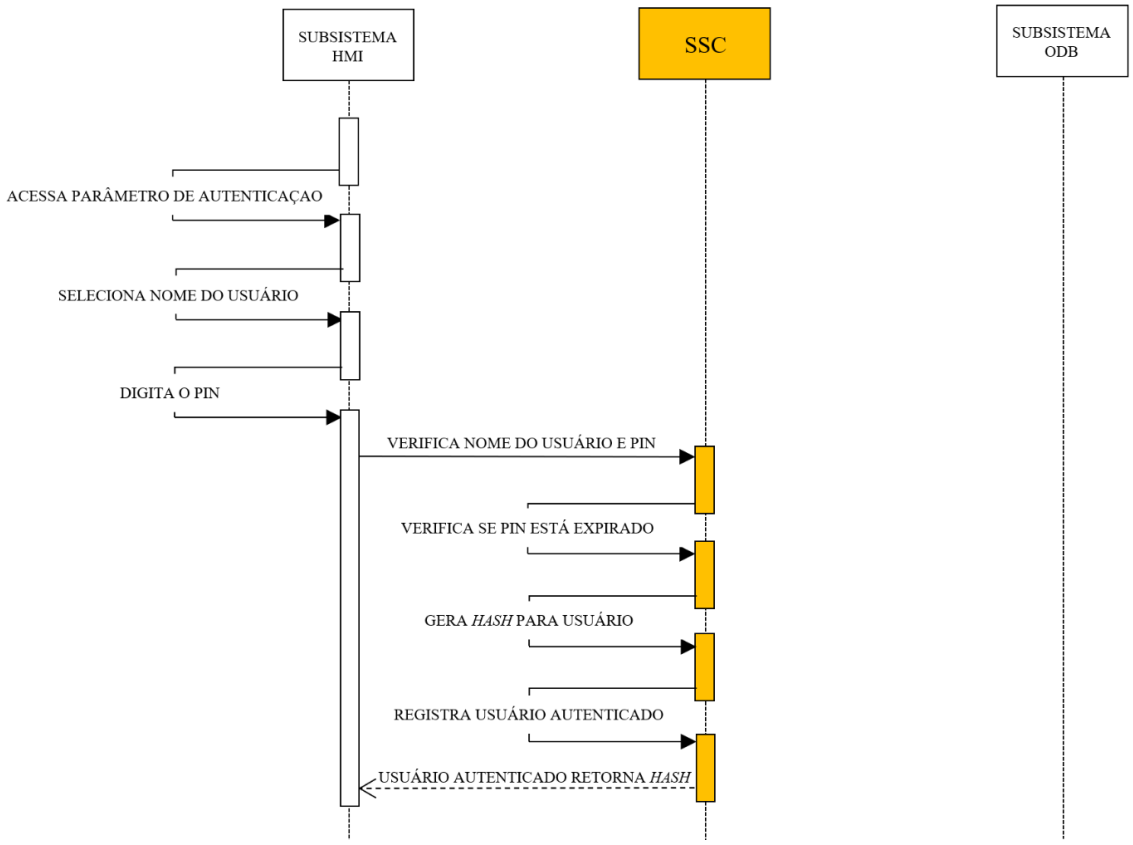
Figura 38 – Estrutura do tipo fonte, possuí informações sobre a requisição

```
34  typedef struct {
35      uint8_t source;                 //Source ex. NETWORK
36      uint8_t physicalInterface;      //P. Physical layer ex. ETHENERT
37      uint8_t protocol;               //P. Application layer ex.Modbus
38      uint8_t sessionType;            //If is authenticated
39      uint32_t sourceIpAddress;       //Identification ex. IP Address
40      char login[LOGIN_SIZE];         //User name
41      uint8_t role;                   //User role
42  } SOURCE;
```

Fonte: Elaborado pelo autor.

Requisições originadas pela HMI, conforme apresentando pela Figura 36, podem ser autenticadas e identificadas de forma única, pois o utilizador do sistema, necessitará se autenticar para acessar os parâmetros, antes de realizar ações no conversor. A Figura 39 representa de forma simplificada, o diagrama de sequência para o funcionamento desta autenticação.

Figura 39 – Diagrama de sequência da autenticação via HMI do conversor



Fonte: Elaborado pelo autor.

Antes de realizar qualquer ação ou ter acesso a informações do sistema, o usuário deverá se autenticar, através do parâmetro que corresponde a funcionalidade de autenticação. Ao

acessar o parâmetro, ele deverá procurar e selecionar o seu nome de usuário, que estará disponível na própria HMI, e entrar com o seu PIN, possibilitando que o sistema valide e identifique a sua identidade.

Uma vez autenticado, o SSC fornecerá um *hash* de 12 bytes, que permitirá identificá-lo durante todas as ações no sistema do conversor. Apesar deste ser considerado pequeno, pois corre risco de colisão, este trabalho levou em consideração para a sua definição as limitações do tamanho máximo do pacote Modbus.

Com o objetivo de autenticar pessoas que realizem requisições através do programa WPS, como a comunicação entre o WPS e o conversor utiliza o protocolo Modbus, que não dispõe de uma função de autenticação, se fez necessário projetar e desenvolver uma função proprietária para realizar tal processo.

Conforme mencionado na Seção 4.3.1.1 acima, o protocolo Modbus reserva alguns códigos de funções para serem utilizados na construção de funções proprietárias. Neste trabalho faz-se o uso deste recurso, para a construir um autenticador a ser aplicado na comunicação entre conversor e o programa WPS e ou demais dispositivos mestres que no futuro possam necessitar.

A Figura 40 representa a estrutura da nova função, denominada Credencial de segurança (*Security Credential)*. Recebe o código da função 105 (0x69) e possuí um byte subsequente, que é utilizado para determinar o tipo da função, que pode ser:

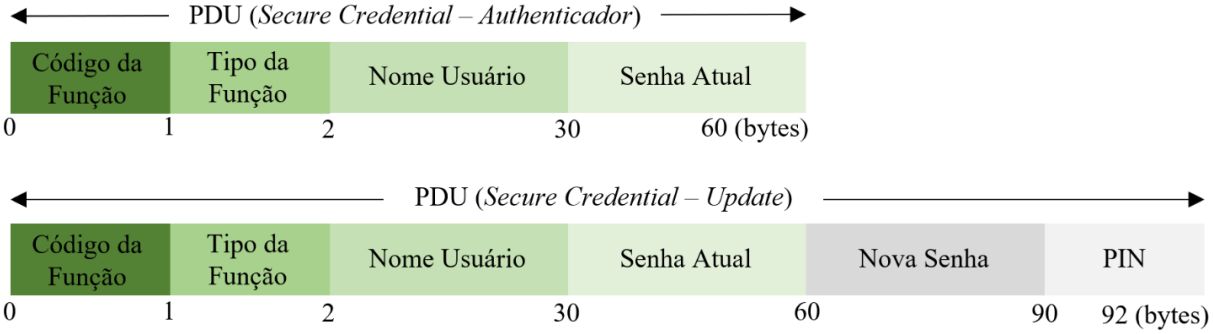
a) autenticação (*Authentication*) valor 1 (0x01), determina que a função será utilizada por uma requisição de autenticação comum, este byte é seguido pelo nome do usuário de até 28 caracteres e por uma senha de até 30 caracteres, na qual cada caractere (tabela de código ASCII) ocupa um byte de dados da função;
b) atualização (*Update*) valor 2 (0x02), determina que a função será do tipo atualização e autenticação, ou seja, além do usuário e senha a requisição irá informar uma nova senha de 30 caracteres e um PIN. Neste caso o SSC irá obrigatoriamente atualizar a senha e opcionalmente o PIN do determinado usuário, antes de realizar a autenticação. Opcionalmente, devido ao mesmo poder ser enviado com valor nulo, o que não alteraria o PIN atual que se limita ao uso local via HMI.

O processo de autenticação desenvolvido neste trabalho utiliza, a nova função Modbus em conjunto com o autenticador desenvolvido no SSC, para autenticar e identificar de forma única o usuário do programa WPS, possibilitando a segregação dos direitos de acesso, conforme a função da determinada pessoa dentro do IACS (Figura 41).

Ao receber qualquer requisição, o subsistema de rede solicita ao SSC um ponteiro da variável fonte temporária, ponteiro é uma variável que armazena o endereço de memória de

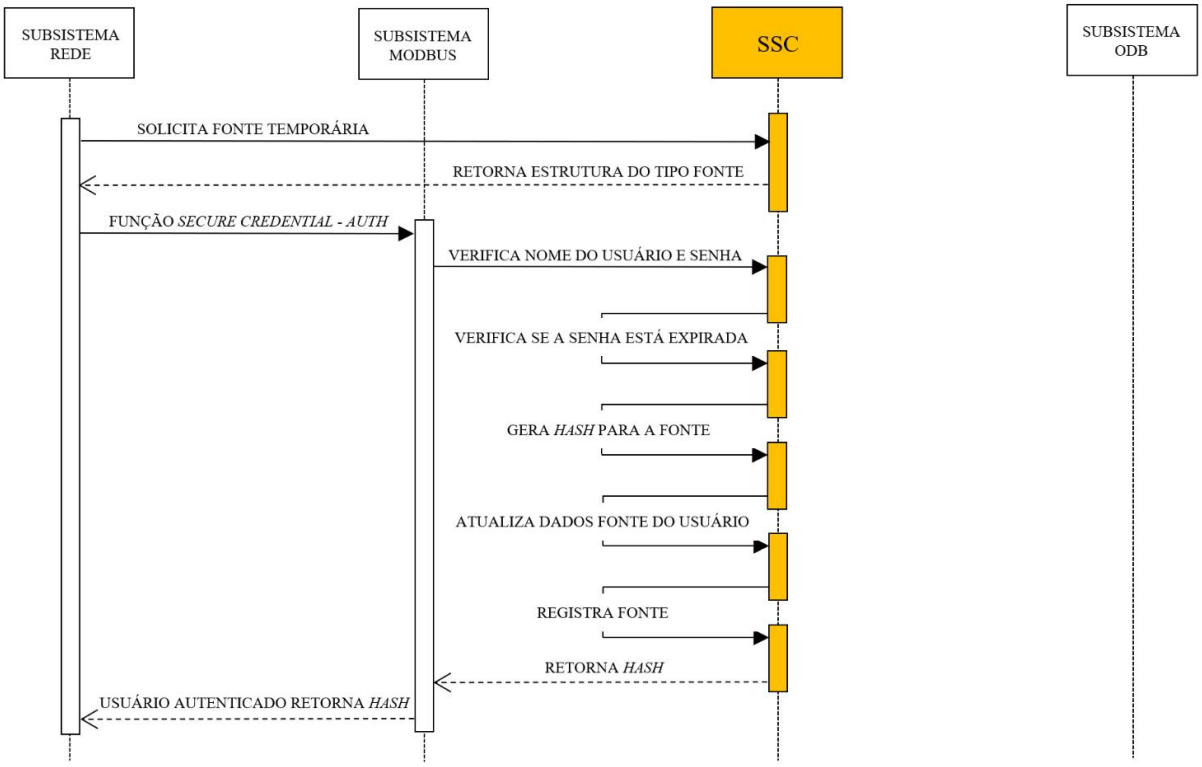
uma outra variável, conhecendo o endereço da variável fonte temporária, o subsistema de rede atualiza a fonte com as informações que ele tem disponível nesta etapa do processo, por exemplo endereço IP. Ao perceber que a requisição se trata de uma função Modbus, este encaminha a requisição para o subsistema Modbus, este ao identificar que a requisição se trata da nova função credencial de segurança do tipo autenticação, dispara uma solicitação de autenticação ao SSC, informando nome de usuário e senha para o autenticador.

Figura 40 – Estrutura da função Modbus para autenticação



Fonte: Elaborado pelo autor.

Figura 41 – Diagrama de sequência autenticação via WPS e Modbus



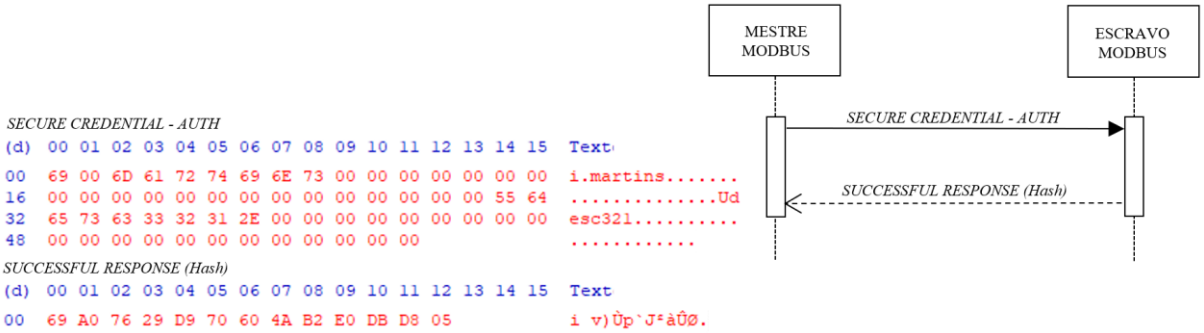
Fonte: Elaborado pelo autor.

Imediatamente ao receber a solicitação de autenticação, o SSC valida se o nome do usuário existe no gerenciador de contas do conversor e se senha informada está correta. Na

sequência, avalia se a senha não está expirada, atualiza a variável fonte, com as informações do usuário identificado, nome, função (*role*), carimbo de tempo e gera um novo *hash* de 12 bytes para identificação do usuário nas próximas requisições e finalmente registra o usuário na lista de identificadores autenticados, atrelando o *hash* gerado as informações daquela determinada fonte.

Uma vez autenticado, o SSC retorna o *hash* para o subsistema Modbus que o repassa como resposta a requisição de autenticação. A Figura 42, apresenta em detalhes a PDU da requisição e da resposta (código da função e *hash*), trocados entre WPS (mestre) e conversor (escravo) para uma autenticação realizada com sucesso.

Figura 42 – Modbus PDU função Security Credential – Authenticate



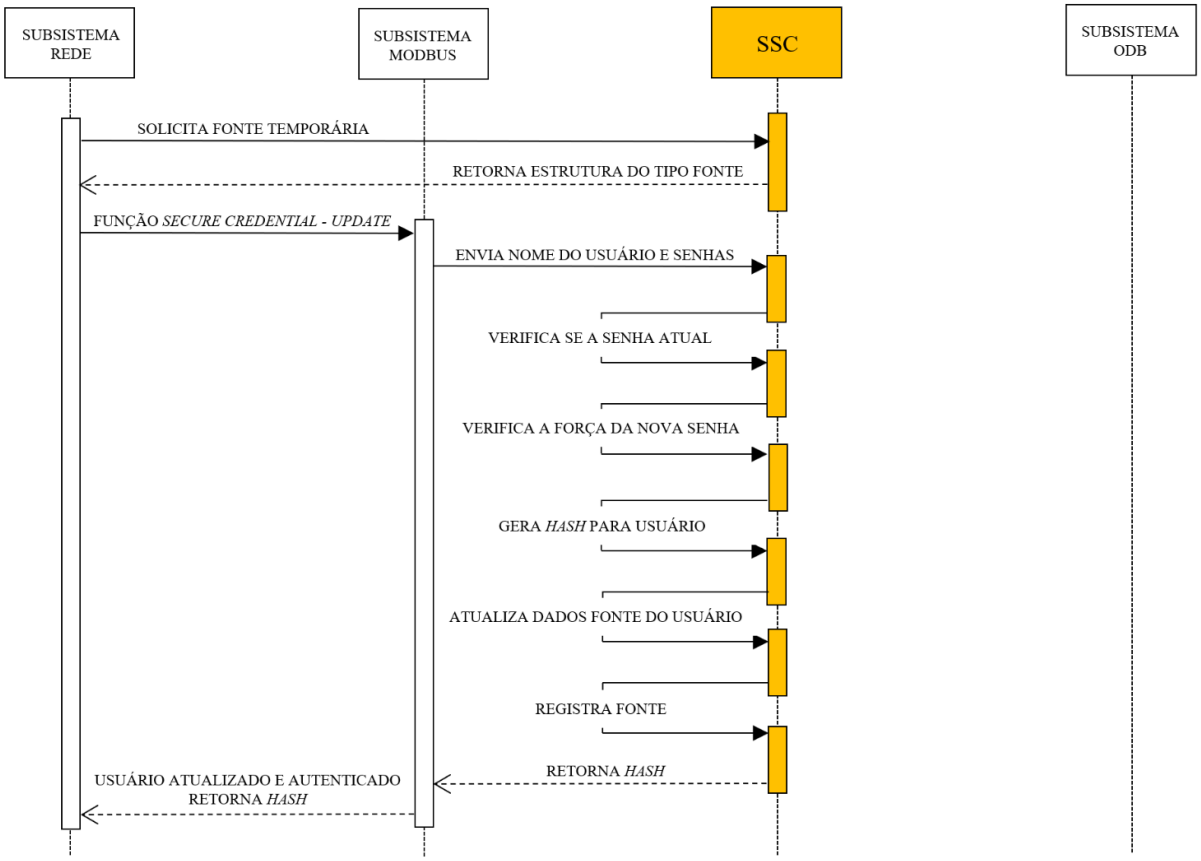
Fonte: Elaborado pelo autor.

O processo de atualização e autenticação (Figura 43) é muito semelhante ao processo de autenticação descrito acima, mas ao invés de requisitar diretamente a autenticação para o SSC, o subsistema Modbus requisita primeiro a atualização da senha do determinado usuário.

Ao receber a solicitação e após encontrar o nome do usuário, o SSC valida se a senha atual está correta, na sequencia valida se a força da nova senha está de acordo com a política de segurança selecionada para o conversor, caso a nova senha esteja de acordo com a política, a senha é atualizada e o usuário segue o mesmo fluxo de autenticação realizada pela requisição de autenticação, atualiza fonte, gera o *hash* e registra o usuário na lista de identificadores autenticados, finalmente retornando o novo *hash* como resposta para a requisição da função.

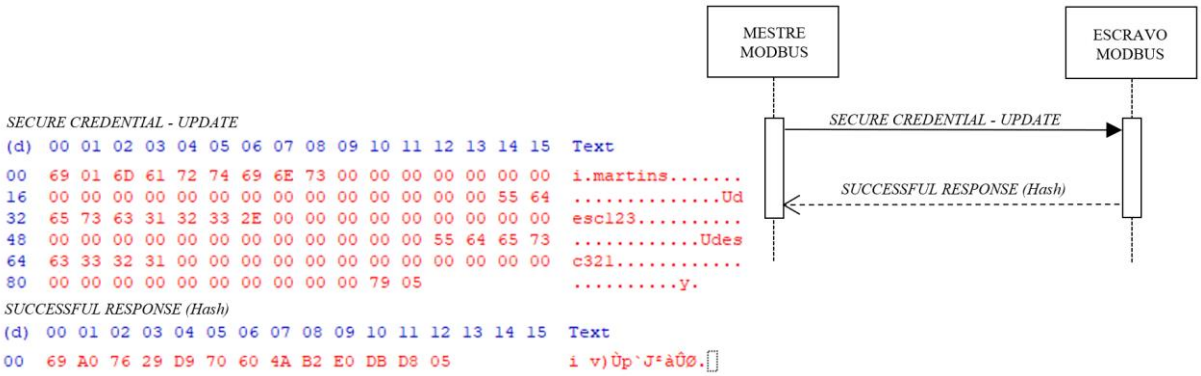
O PDU da requisição e da resposta, trocados entre WPS e conversor, durante o processo de atualização e autenticação é apresentado na Figura 44. Pode-se observar que a requisição contempla a senha atual, a nova senha e o novo PIN. A resposta é idêntica a recebida pelo exemplo da Figura 42, em ambos os casos o retorno de sucesso é o *hash* de 12 bytes.

Figura 43 – Diagrama de sequência da atualização e autenticação no conversor



Fonte: Elaborado pelo autor.

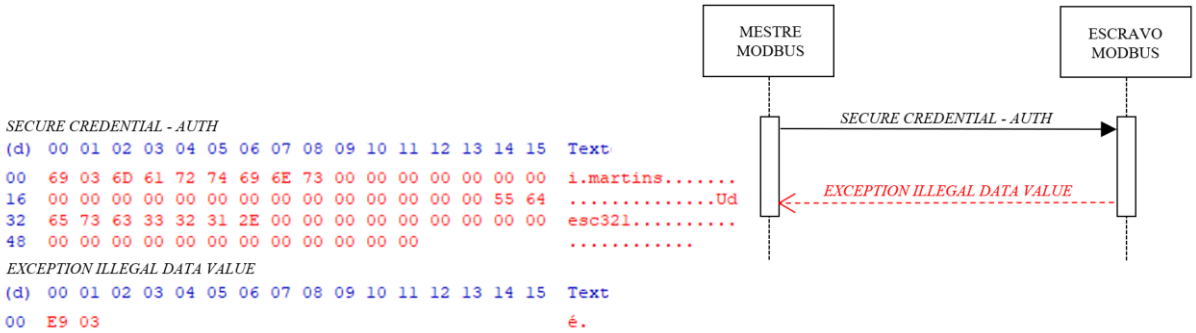
Figura 44 – Modbus PDU função Security Credential – Update



Fonte: Elaborado pelo autor.

Em caso de falha durante o processo de autenticação, o conversor irá responder a requisição realizada pelo mestre com uma mensagem de exceção. Caso o tipo da função seja diferente de autenticação (0x00) ou atualização (0x01), o conversor irá retornar uma exceção do tipo *Illegal Data Value*, informando que a requisição tem dados incorretos, conforme apresentado na Figura 45.

Figura 45 – Modbus PDU Security Credential – Illegal Data Value Exception

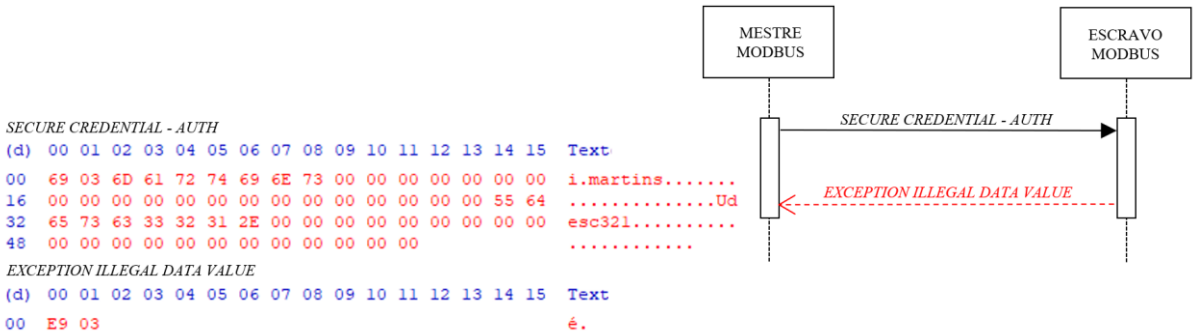


Fonte: Elaborado pelo autor.

A exceção de senha expirada apresentada pela Figura 46, é válida somente para a função do tipo autenticação, esta informa ao mestre que a senha do usuário está expirada e precisa ser obrigatoriamente atualizada por uma requisição do tipo atualização.

Sempre que um novo usuário for criado, ou uma conta seja resetada, por um usuário administrador no conversor, as senhas temporárias geradas para estas respectivas contas serão consideradas expiradas pelo SSC. Esta política forçará o dono da respectiva conta, atualizá-la, de modo que somente ele tenha acesso ao autenticador.

Figura 46 – Modbus PDU Security Credential – Expired Password Exception



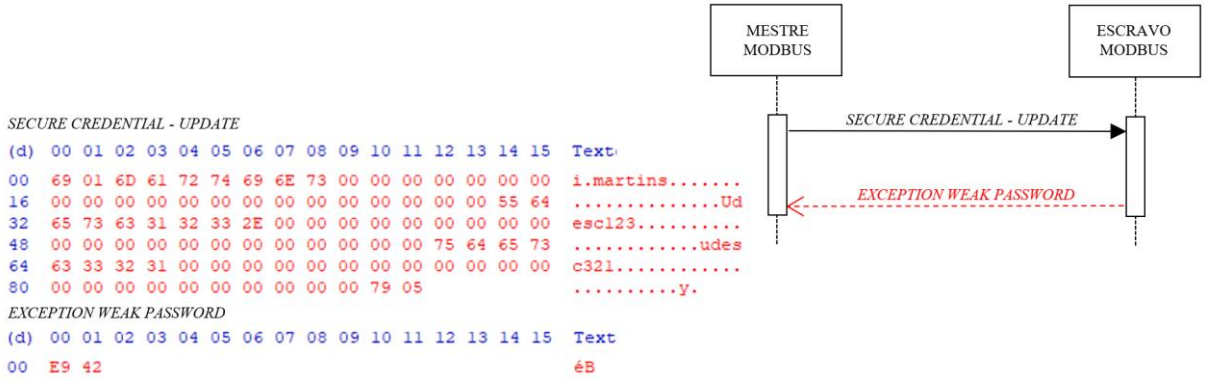
Fonte: Elaborado pelo autor.

A Figura 47 representa uma exceção do tipo senha fraca, ou seja, é válida somente para requisições do tipo atualização. Ela informa ao mestre, que a nova senha escolhida pelo usuário, não atende as políticas de força de senha determinadas pelo administrador do conversor, possibilitando ao mestre, neste caso mais especificamente ao WPS, apresentar uma mensagem bem específica ao usuário do programa.

Já a exceção de senha inválida, apresentada pela Figura 48 é válida para ambos os tipos de função, autenticação e atualização. Como o próprio nome a descreve, esta função informa ao mestre, que o nome do usuário ou a senha estão incorretos, possibilitando que o mesmo

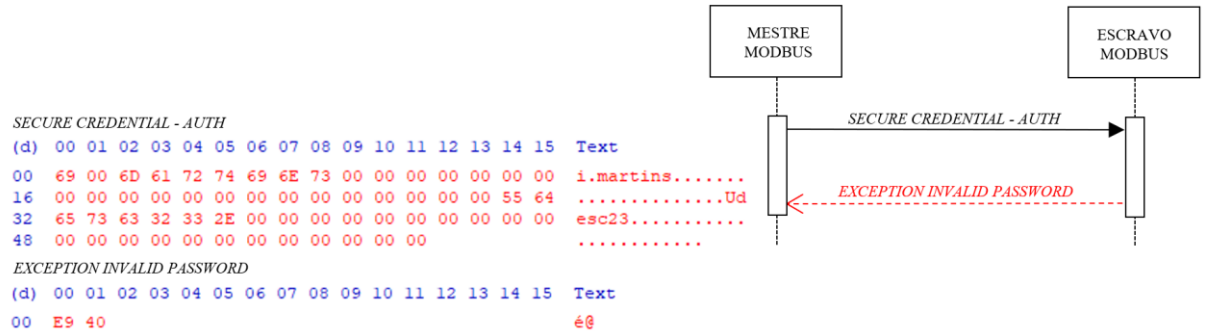
apresente uma mensagem específica para o utilizador, compreender que as credenciais informadas não são validas.

Figura 47 – Modbus PDU Security Credential – Weak Password Exception



Fonte: Elaborado pelo autor.

Figura 48 – Modbus PDU Security Credential – Invalid Password Exception



Fonte: Elaborado pelo autor.

Além de requisitos para o identificador e o autenticador, a norma IEC 62443-4-2 específica através do CR 1.3, gerenciamento de contas. Que o conversor deve prover a capacidade de suportar o gerenciamento de todas as contas nativamente de forma direta ou integrada a sistemas que realizem tal gerenciamento, ou seja, delega-se a avaliação da autenticação a um servidor de diretório (por exemplo, LDAP ou Active Directory). O CR 1.4, gerenciamento do identificador, determina que as contas gerenciadas pelo CR 1.3, requerem o uso de um ou mais identificadores únicos para identificar distintamente cada conta. Alguns exemplos são: nomes de conta; IDs de sistemas operacionais; certificados digitais do tipo X.509; etc.

O protótipo apresentado neste trabalho, gerencia nativamente todas as contas de usuário e conforme pode ser observado na Figura 49, cada usuário é estruturado com os seguintes dados:

a) nome do usuário (login) – nome de usuário único para diferenciar cada usuário do sistema;

b) ação (*action*) – usada somente pelo processo de atualização das credenciais, o processo valida a ação que deve ser realizada para a determinada conta de usuário, as ações podem ser: Adicionar, Modificar, Resetar e Deletar;
c) função (*role)* – função com as autorizações do determinado usuário;
d) número de identificação (*pin*) – Número de identificação de 4 dígitos utilizado para acesso via IHM;
e) extra – dado utilizado para serviços, um exemplo seria quando uma conta está bloqueada ou a senha precisa ser atualizado;
f) carimbo de tempo (*timestamp*) – informação sobre a última atualização realizada para a determinada conta, necessário para os processes de expiração de senha por exemplo.

Figura 49 – Estrutura de dados dos usuários

```
58  typedef struct user {
59      char login[LOGIN_SIZE];          //User name (login)
60      uint8_t action;                  //User action
61      uint8_t role;                    //User role
62      uint16_t pin;                    //Pin to HMI access
63      char pass[PASS_SIZE];            //Password to WPS access
64      uint16_t extra;                  //Extra services
65      uint32_t timestamp;              //Last updated timestamp
66  } SEC_USER;
```

Fonte: Elaborado pelo autor.

4.3.3 Controle de Uso

De acordo com a IEC 62443-4-2, uma vez o usuário identificado e autenticado, agora o autorizador do SSC, deverá controlar os direitos de acesso de cada usuário ao conversor. Possibilitando aos proprietários de ativos e integradores de sistema, definir os privilégios de cada função a ser atribuídas a cada usuário (humano, processo de *software* ou dispositivo) autorizado no conversor.

Neste trabalho, projeta-se o autorizador para receber do autenticador, um identificador único, *hash*, endereço IP, etc, ou quando não for possível, um identificador genérico do determinado canal de comunicação, exemplo Modbus RTU, e conceder a ele os seus respectivos direitos de uso (Figura 50).

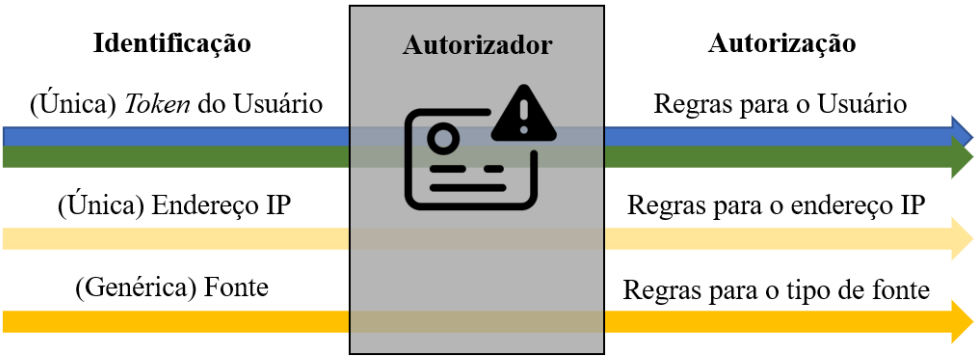
No modelo de controle de acesso baseado em funções (RBAC), todas os privilégios de acesso são atribuídos a uma função (*role*) e cada usuário é nomeado com a função que atende

a suas necessidades dentro do IACS. Por exemplo, um operador de máquina, ao se autenticar no conversor, seria identificado e receberia a função Operador, não teria acesso de escrita nos parâmetros de configuração, permitindo a realização de ações que se limitariam a sua função.

Como o protocolo Modbus utilizado na comunicação entre WPS e conversor, não prevê funcionalidade de controle de acesso. Conforme se fez necessário para o processo de autenticação, à autorização do acesso para usuários autenticados através do WPS no conversor, também é realizada através de uma nova função Modbus.

A função desenvolvida, encapsula o PDU da requisição Modbus original realizada pelo programa WPS e embarca em seu cabeçalho o *hash* recebido pelo processo de autenticação, possibilitando ao autorizador identificar qual é o usuário da respectiva requisição.

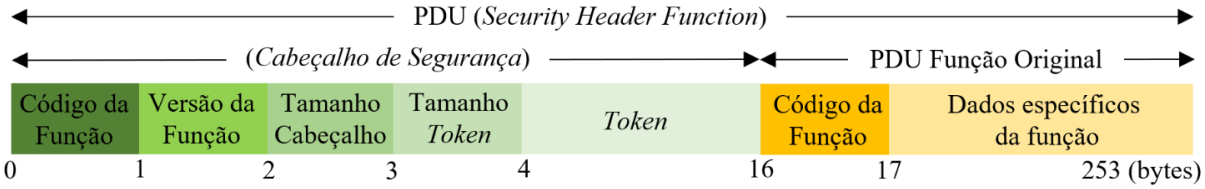
Figura 50 – Capacidade de autorização pelo autorizador



Fonte: Elaborado pelo autor.

A Figura 51 representa a estrutura da nova função, denominada Cabeçalho de segurança (*Security Header)*, por disponibilidade, recebe o código da função 107 (0x6B). Além do código da função, possuí um byte para informar a sua versão, para caso um dia necessite de alguma atualização, o tamanho do cabeçalho auxilia a identificar o início da função original, o tamanho do *hash* facilita o processo de extração do *hash* pelo SSC, na sequência vem o próprio *hash* do usuário de 12 bytes e finalmente finaliza com o PDU da requisição original.

Figura 51 – Estrutura da função Modbus *Security Header*

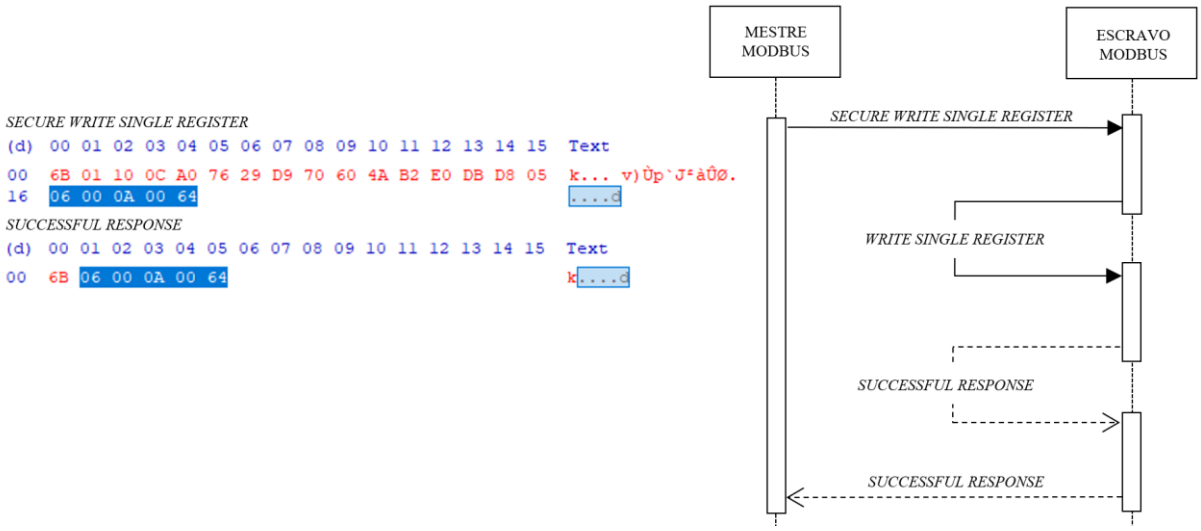


Fonte: Elaborado pelo autor.

A Figura 52 representa a mesma requisição ilustrada pela Figura 33, no entanto agora com o uso da nova função Modbus *Security Header* (0x6B). No exemplo o WPS escreve o valor 100 (0x0064) no registrador 10 (0x000A) do conversor, através da requisição *Write Single Register Function* (código da função 0x06). Como resposta a requisição, o conversor responde a mesma PDU recebida, só que agora como uma resposta a função (0x6B), confirmando que o usuário tem direito de acesso e o valor foi escrito com sucesso no registrador.

O processo de autorização (controle de uso) desenvolvido neste trabalho, para requisições Modbus realizadas pelo programa WPS (Figura 53), utiliza a nova função Modbus em conjunto com o autorizador desenvolvido no SSC, para negar ou autorizar o acesso aos parâmetros do conversor, possibilitando a segregação correta dos direitos de acesso, conforme a função do determinado utilizador dentro do IACS.

Figura 52 – Modbus PDU função Security Header – Write Single Register



Fonte: Elaborado pelo autor.

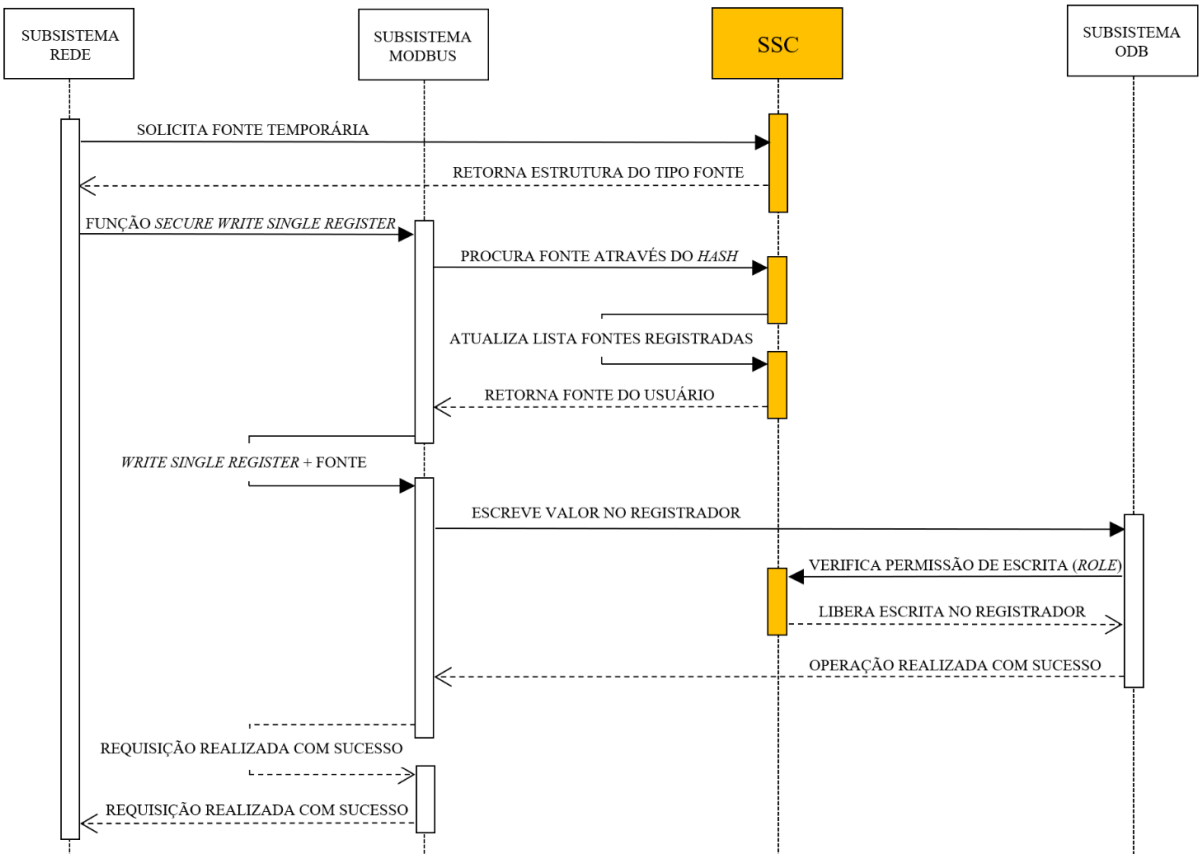
Ao receber uma requisição do tipo *Write Single Register* encapsulada pela função *Security Header*, o primeiro processo a ser realizado pelo subsistema de rede é solicitar o ponteiro da variável fonte temporária, o subsistema então atualiza a fonte com as informações que ele tem disponível nesta etapa do processo, identifica que a requisição é Modbus e a envia junto com a informação do ponteiro para o subsistema Modbus. Este subsistema identifica que se trata de uma função *Security Header*, extrai o *hash* do cabeçalho da função e busca por ele na lista de usuários autenticados, através de uma requisição ao SSC.

Encontrando-o na lista de usuário autenticados o SSC, após atualizar de identificadores registrados, eliminando todas as sessões expiradas, retorna o endereço da variável fonte autenticada, para ser utilizada pelo subsistema Modbus no lugar da fonte temporária.

Uma vez de posse da fonte autenticada, com todas as informações do determinando usuário, o próximo passo a ser realizado pela função *Security Header* é extrair o PDU da requisição original *Write Single Register* e enviá-la em conjunto com a fonte do usuário, para próprio subsistema Modbus, para ser tratada como uma simples função *Write Single Register*. Nesta etapa o subsistema Modbus inicia um processo de escrita junto ao subsistema ODB, no parâmetro (registrador) específico, informando ao subsistema ODB, qual é a função (*role*) daquele respectivo usuário.

O subsistema ODB valida junto ao SSC qual o direito de acesso da determinada função (*role*), naquele respectivo parâmetro, caso a permissão seja de escrita, o subsistema de segurança retorna para o subsistema ODB uma resposta positiva permitindo o acesso de escrita naquele parâmetro, o subsistema ODB escreve o novo valor no registrador do parâmetro e retorna uma resposta de operação realizada com sucesso para o subsistema Modbus, esta resposta é encapsulada pela função *Security Header*, retornando-a ao subsistema de rede e consecutivamente ao programa WPS, como sendo uma resposta de sucesso daquela própria função.

Figura 53 – Diagrama de sequência, autorização de escrita via Modbus e WPS



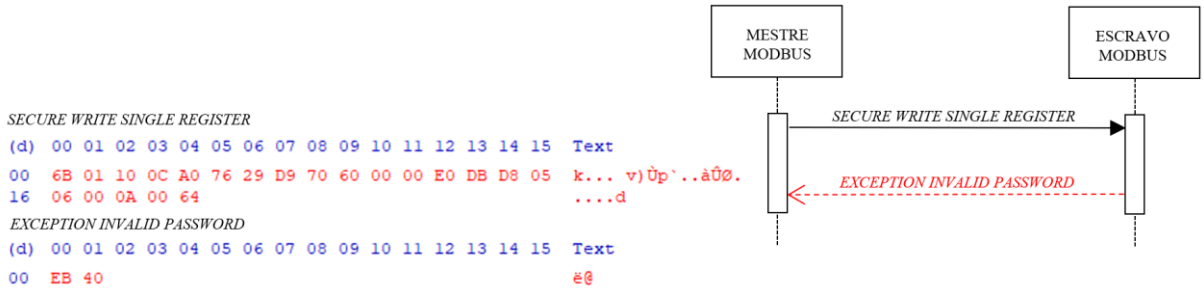
Fonte: Elaborado pelo autor.

Em caso de falha durante o processo de autorização com a nova função, o conversor irá responder a requisição realizada pelo mestre com uma mensagem de exceção.

A exceção de senha inválida (Figura 54), informa ao mestre que o *hash* não está autenticado, provavelmente neste caso o *hash* expirou e não está mais registrado, necessitando um novo processo de autenticação para aquele determinado usuário.

Como a função *Security Header* encapsula a função original, caso ocorra uma exceção para a função original ou o usuário não tenha permissão de acesso para o determinado parâmetro, a função irá retornar esta exceção encapsulada em uma resposta de requisição realizada com sucesso pela função *Security Header*

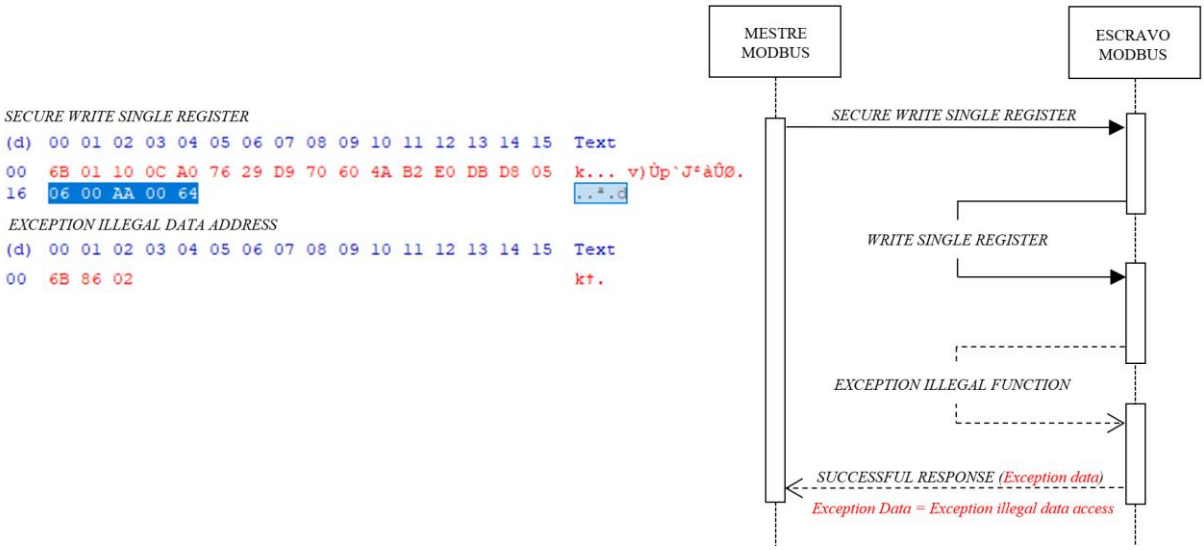
Figura 54 – Modbus PDU Security Header – Invalid Password Exception



Fonte: Elaborado pelo autor.

No exemplo, uma requisição de escrita a um registrador inexistente foi realizada, neste caso o *hash* foi encontrado, porém o subsistema ODB não encontrou o registrador, retornando uma exceção para a função *Write Single Register* (Figura 55)..

Figura 55 – Modbus PDU Security Header – Internal Function Exception

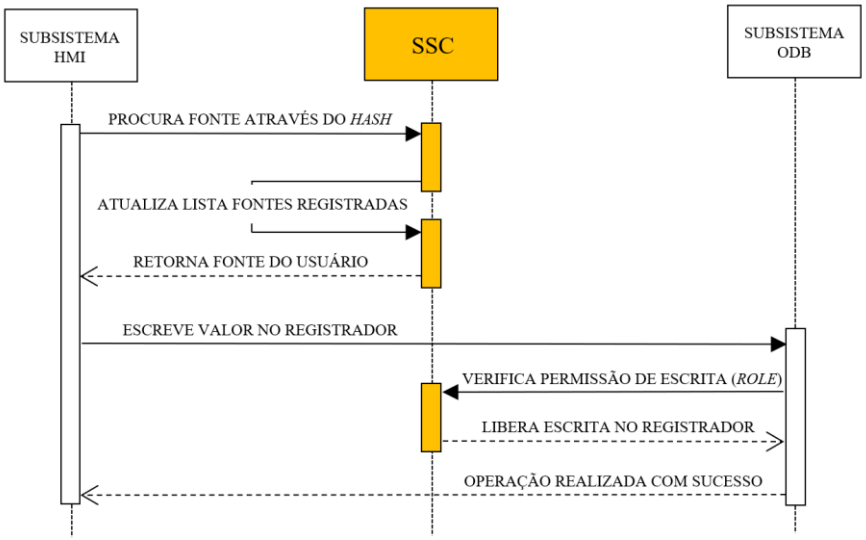


Fonte: Elaborado pelo autor.

Para autorizar requisições realizadas através da HMI, o autenticador também faz uso do *hash* gerado pelo processo de autenticação, para procurar a fonte autenticada no SSC. O processo é muito semelhante ao utilizado para requisições do WPS (Figura 53), porém não existe o uso do protocolo Modbus, pois a HMI requisita a fonte e a escrita do parâmetro (registrador) diretamente para o subsistema ODB (Figura 56).

Já para as demais requisições, oriundas de dispositivos de terceiros e demais tecnologias de comunicação como DeviceNET, Profibus-DP, Modbus RTU, Modbus TCP, etc. O processo de autorização realiza o controle de uso baseado no identificador, informado pelo processo de autenticação, que pode ser único (Endereço IP) ou genérico por exemplo para qualquer requisição de uma determinada tecnologia de comunicação.

Figura 56 – Diagrama de sequência, autorização escrita via HMI



Fonte: Elaborado pelo autor.

A Figura 57 apresenta o diagrama de sequência para conexões através do protocolo Modbus TCP, no qual utiliza-se como autenticador o endereço IP do mestre. Neste caso, a função (*role*) pode ser atribuída ao endereço IP, permitindo por exemplo criar uma função especifica para ser aplicada a um PLC e limitar o acesso de leitura e escrita a alguns parâmetros específicos do conversor.

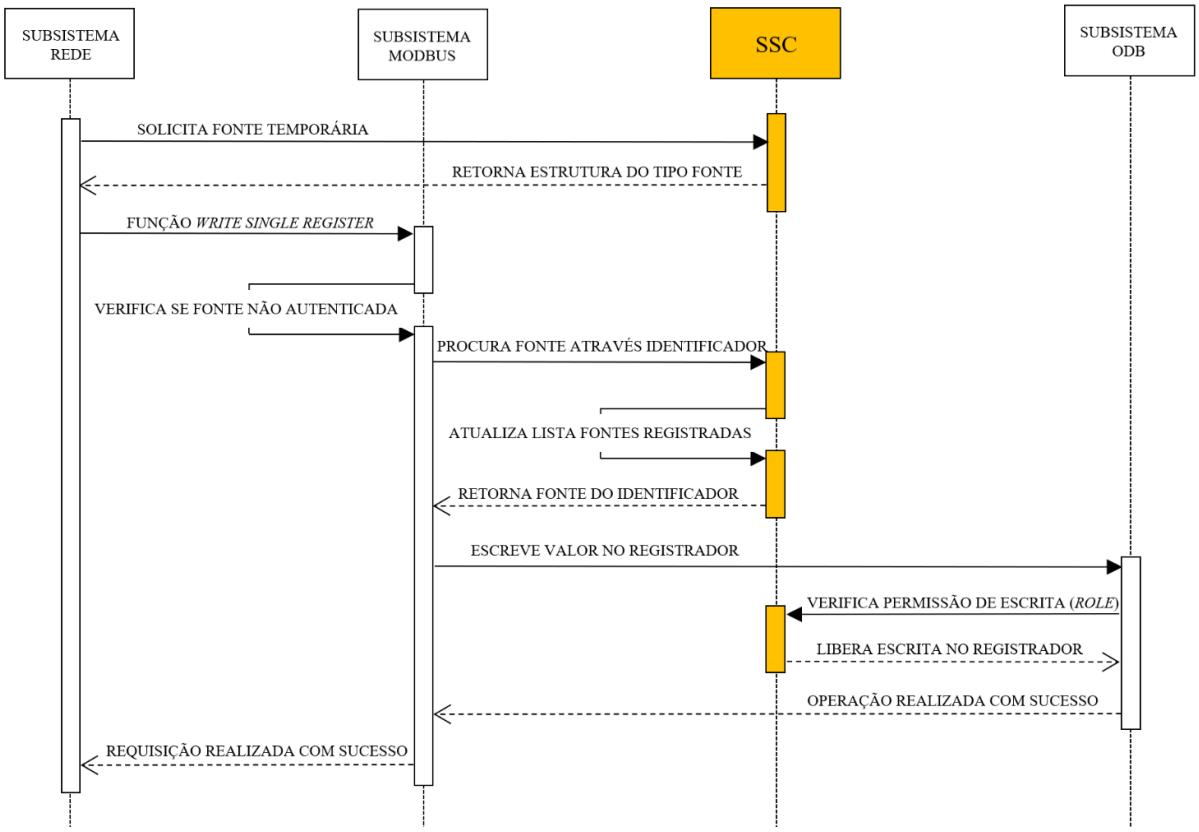
Ao receber uma requisição do tipo *Write Single Register*, o primeiro processo a ser realizado é solicitar o ponteiro da variável fonte temporária, o subsistema então atualiza a fonte com as informações disponíveis naquela etapa. Ao receber a requisição do subsistema de rede o subsistema Modbus verifica se a fonte não é do tipo autenticada e solicita ao SSC a fonte específica para o determinado identificador.

Encontrando-o na lista de identificadores registrados (conexões recentes não expiradas) o subsistema de segurança, após atualizar a lista de usuários e fontes autenticadas eliminando todas as sessões expiradas, retorna o endereço da variável fonte específica para o determinado identificador. Caso não encontre, primeiro ele precisa validar se o endereço IP foi configurado pelo sistema, posteriormente registrando-o na lista de identificadores registrados.

A lista de identificadores registrados, foi criada com o propósito de otimizar o processo de autorização, a partir da segunda requisição a ser realizada pelo mesmo identificador. Deixando aquele determinado identificador registrado, até que um tempo determinado pelo sistema seja excedido.

Uma vez em posse da fonte do identificador da determinada requisição, o subsistema Modbus inicia o processo de escrita junto ao subsistema ODB, mesmo processo apresentado pela Figura 53 e Figura 56.

Figura 57 – Diagrama de sequência, autorização de escrita via Modbus padrão



Fonte: Elaborado pelo autor.

4.3.4 Resposta aos eventos

Proprietários de ativos devem ter a capacidade de estabelecer políticas, controles e procedimentos de segurança para responder a incidentes de segurança cibernética. Neste trabalho projeta-se o SSC, para gerar e armazenar eventos às seguintes categorias:

a) autenticação:
   - senha do usuário está expirada;
   - usuário autenticado com sucesso;
   - identificador registrado (ex. endereço IP);
   - falha na autenticação senha inválida;
   - falha na autenticação usuário inválido.

b) autorização:
   - identificador não encontrado na lista de controle de acesso;
   - identificador validado com sucesso;
   - requisições de escrita em parâmetros (registradores) realizadas com sucesso.

c) conta de usuários:
   - senhas resetadas com sucesso;
   - função (role) alterada com sucesso;
   - senha fraca, não atende a política de segurança;
   - senha atualizada com sucesso;
   - deletada com sucesso;
   - criada com sucesso.

d) quaisquer alterações na configuração dos recursos de segurança cibernética.

Todos os eventos são armazenados em arquivos dentro da memória flash do conversor, visando obter retenção mínima de um ano. Os eventos são registrados em arquivos nomeados pelo mês e dia do evento, por exemplo "*March-30.log*". Portanto, todos os dias são criados arquivos de eventos, que serão sobrescritos anualmente. A Figura 58 apresenta um destes arquivos, pode-se observar que cada evento contempla:

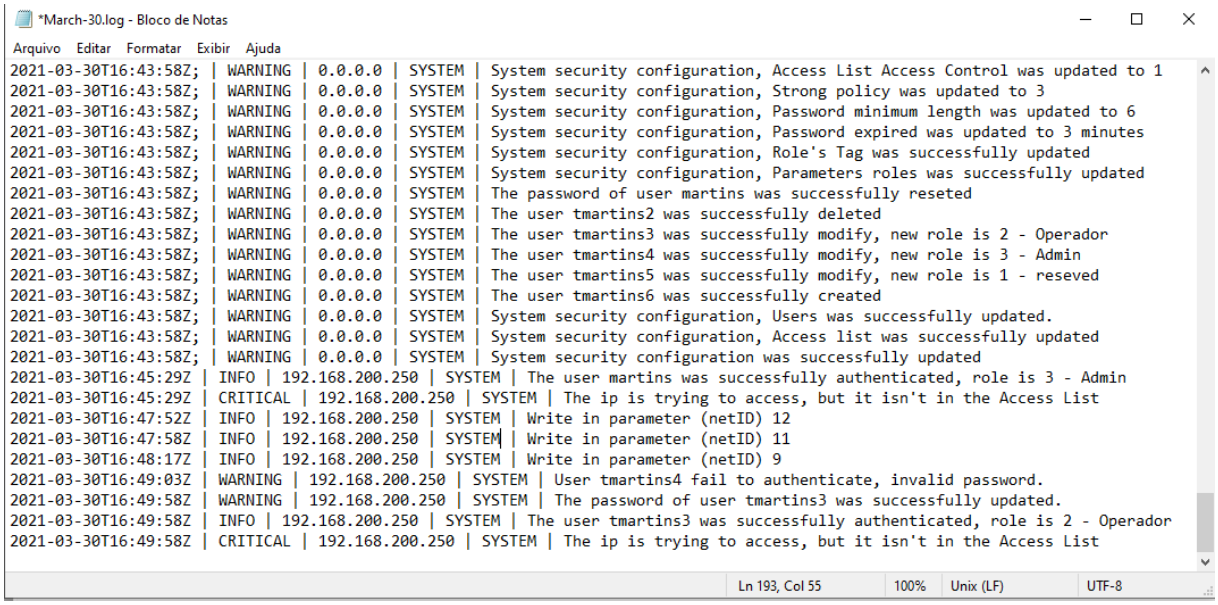
a) carimbo de tempo (*timestamp*);
b) categoria;
c) origem do acesso (dispositivo, processo do sistema, usuário);
d) identificado do evento;
e) resultado e descrição do evento.

4.3.5 Integridade do Sistema

Conversores geralmente passam por vários ciclos de teste durante sua inicialização (teste de unidade, teste de sistema etc.), para estabelecer se os seus componentes estão operando conforme planejado, antes mesmo de entrarem em produção.

Conforme descrito pelo Capítulo 3 Seção 3.3.4.6, aplicar módulos de plataforma confiáveis (TPM) em dispositivos embarcados, é uma forma eficiente para o desenvolver uma raiz de confiança baseada em *hardware*. Uma raiz de confiança de *hardware* contém as chaves usadas para funções criptográficas e permite um processo de inicialização seguro. É confiável e protegida por projeto, tornando-a imune a ataques de *malware* [111]. Comercialmente pode ser encontrada como um circuito impresso autônomo ex. SLB9670 [112], ou implementado como um módulo de segurança em um processador ou em um SoC.

Figura 58 – Arquivo diários com os eventos de auditoria


*March-30.log - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

```
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Access List Access Control was updated to 1
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Strong policy was updated to 3
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Password minimum length was updated to 6
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Password expired was updated to 3 minutes
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Role's Tag was successfully updated
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Parameters roles was successfully updated
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | The password of user martins was successfully reseted
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | The user tmartins2 was successfully deleted
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | The user tmartins3 was successfully modify, new role is 2 - Operador
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | The user tmartins4 was successfully modify, new role is 3 - Admin
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | The user tmartins5 was successfully modify, new role is 1 - reseved
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | The user tmartins6 was successfully created
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Users was successfully updated.
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Access list was successfully updated
2021-03-30T16:43:58Z; | WARNING | 0.0.0.0 | SYSTEM | System security configuration was successfully updated
2021-03-30T16:45:29Z | INFO | 192.168.200.250 | SYSTEM | The user martins was successfully authenticated, role is 3 - Admin
2021-03-30T16:45:29Z | CRITICAL | 192.168.200.250 | SYSTEM | The ip is trying to access, but it isn't in the Access List
2021-03-30T16:47:52Z | INFO | 192.168.200.250 | SYSTEM | Write in parameter (netID) 12
2021-03-30T16:47:58Z | INFO | 192.168.200.250 | SYSTEM | Write in parameter (netID) 11
2021-03-30T16:48:17Z | INFO | 192.168.200.250 | SYSTEM | Write in parameter (netID) 9
2021-03-30T16:49:03Z | WARNING | 192.168.200.250 | SYSTEM | User tmartins4 fail to authenticate, invalid password.
2021-03-30T16:49:58Z | WARNING | 192.168.200.250 | SYSTEM | The password of user tmartins3 was successfully updated.
2021-03-30T16:49:58Z | INFO | 192.168.200.250 | SYSTEM | The user tmartins3 was successfully authenticated, role is 2 - Operador
2021-03-30T16:49:58Z | CRITICAL | 192.168.200.250 | SYSTEM | The ip is trying to access, but it isn't in the Access List
```

Ln 193, Col 55 | 100% | Unix (LF) | UTF-8

Fonte: Elaborado pelo autor.

O SoC Zynq 7020 embarcado na placa de desenvolvimento ZedBoard, possibilita a construção de uma RoT baseada em *hardware*. Na qual, uma vez importada ao SoC, as chaves privadas são armazenadas em memória do tipo programável uma única vez (*OTP*, *One time programmable*).

Visando evitar complexidade para uso futuro da Zedboard, opta-se neste trabalho por desenvolver uma RoT baseada em *software* com o intuito de apenas validar o seu conceito. Desde modo, cria-se um processo de inicialização verificado do *firmware* principal e um par de chaves, que simplesmente são armazenados na memória *flash* disponibilizada pelo protótipo.

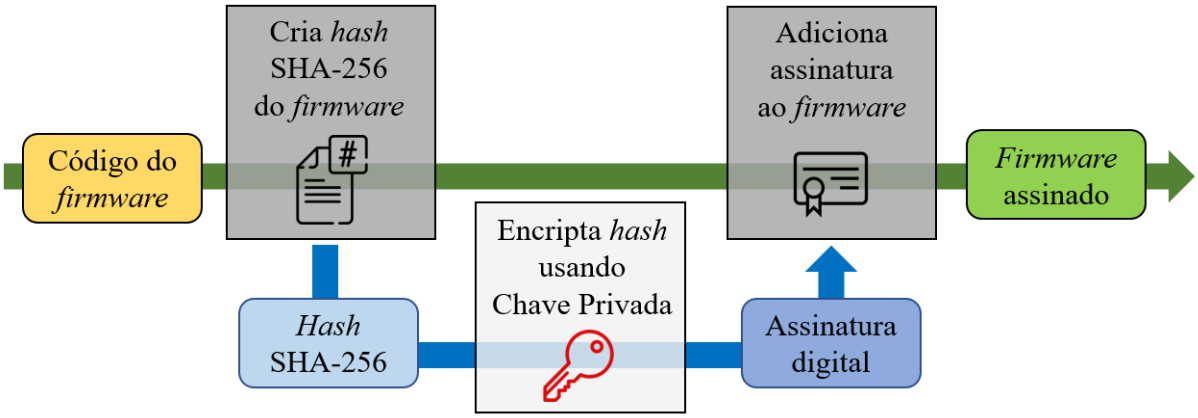
4.3.5.1 Processo de inicialização verificado

No processo de inicialização verificado, o código do *firmware* é assinado externamente e verificado pelo processo de inicialização (*bootloader*) com o uso de um par de chaves, uma pública e outra privada.

A Figura 59 apresenta o processo de assinatura do *firmware*. Após ser concluído e compilado, o *firmware* passa por um processo de assinatura digital, garantindo a sua integridade. A primeira etapa do processo é a geração de um *hash*, geralmente do tipo SHA-256, baseado no arquivo binário do *firmware* gerado pelo compilador. De posse deste código *hash*, o próximo passo do processo é a criação da sua assinatura digital, ou seja, este *hash* é criptografado pela chave privada (geralmente uma chave do tipo RSA-2048).

É crucial que a chave privada esteja segura e muito bem armazenada pelo fabricante, de modo a garantir que somente ele possa assinar os *firmwares* para o determinado produto. Uma vez gerada a assinatura digital, ela é adicionada ao *firmware*, geralmente opta-se por adicioná-la ao seu cabeçalho.

Figura 59 – Processo de assinatura do *firmware*



Fonte: Adaptado de Sectigo. [113]

O processo de inicialização verificado é executado pelo carregador de inicialização de primeiro estágio (*first stage bootloader*), comumente conhecido por *bootloader* (Figura 60).

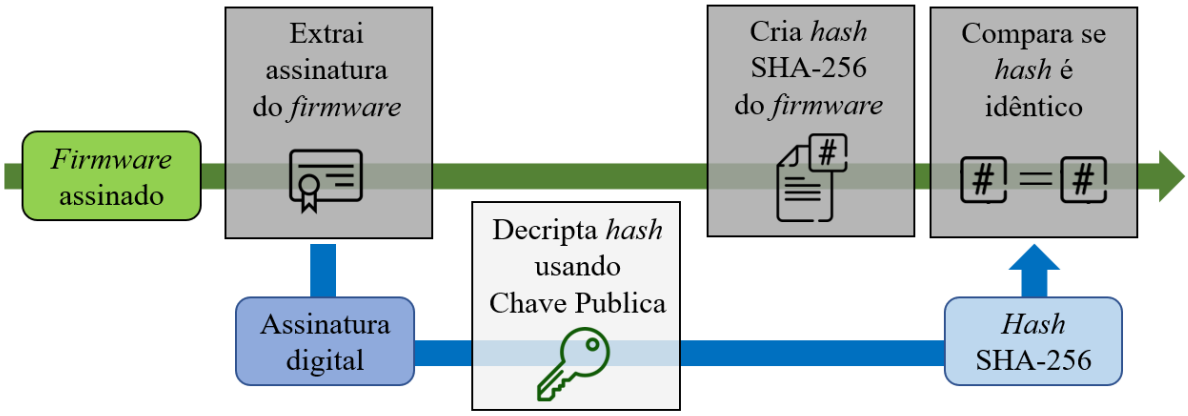
Antes de carregar o *firmware* principal do conversor, primeiro irá verificar a sua integridade. Para isto, extrai a assinatura digital embutida no arquivo do *firmware* e a decripta, utilizando agora a chave pública, que estará embarcada no produto e acessível ao *bootloader*.

Em posse do *hash* SHA-256 extraído da assinatura digital, o *bootloader* cria um novo *hash* com base no *firmware* disponível, mesmo processo realizado durante a assinatura do

firmware (Figura 59), e valida se os *hashes* são idênticos, deste modo confirma-se sua integridade, pois não houve alterações no arquivo binário do *firmware*.

Uma vez validado, o *firmware* principal do produto pode ser inicializado pelo *bootloader*, substituindo-o e assumindo o controle do produto.

Figura 60 – Processo de validação do *firmware*



Fonte: Adaptado de Sectigo. [113]

4.3.5.2 Processo de criação do par de chaves

Neste trabalho desenvolve-se um processo de criação de par de chaves, a ser executado durante a primeira inicialização do SSC. Uma vez habilitado o controle de acesso ao conversor, o SSC cria um par de chaves para o subsistema, este par de chaves visa garantir a integridade e confidencialidade do canal de comunicação e de alguns dados armazenados no conversor.

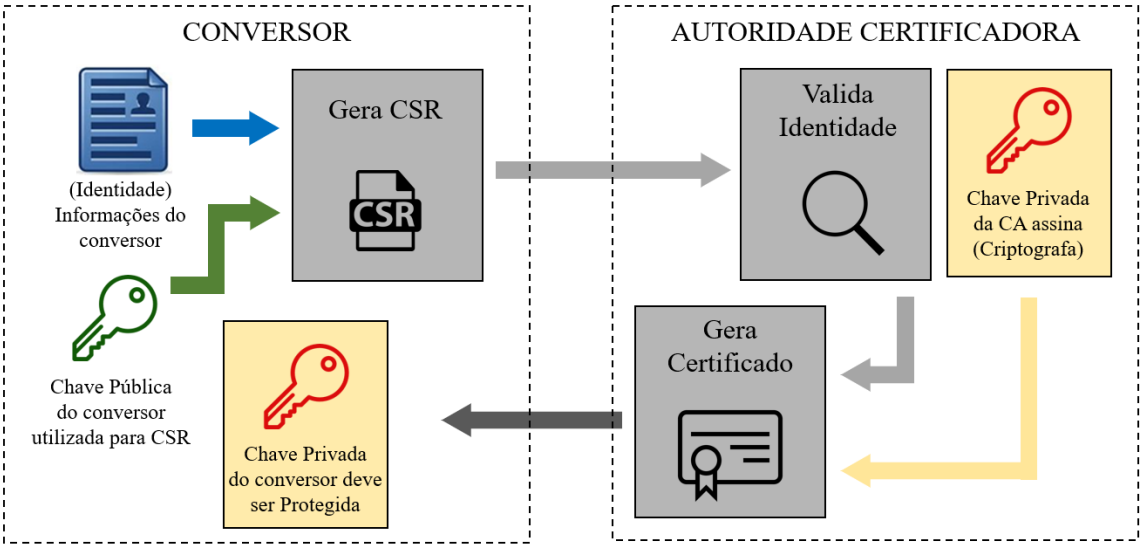
Uma vez criado o par de chaves, a chave pública fica disponível para ser exportada, através do arquivo de requisição de assinatura de certificado (CSR, *Certificate signing request*), que também contempla as informações do conversor. Este CSR pode ser submetido a uma autoridade certificadora (CA, *Certificate Authority*), que o assina através da sua chave privada, resultado em um certificado digital. Este certificado pode ser importado ao conversor, para possibilitar a construção de comunicações seguras (Figura 61).

Para desenvolver este processo, opta-se pelo uso da biblioteca WolfSSL e pelo uso de chave privada de 384 bits do tipo criptografia de curva elíptica (ECC, Elliptic curve cryptography) [114] e algoritmo de assinatura digital de curva elíptica (ECDSA, Elliptic Curve Digital Signature Algorithm) [115] para a geração da chave pública.

A segurança das chaves assinadas por ECDSA está diretamente relaciona a semente (*seed*) utilizada pelo seu gerador de números aleatórios (*random number generator*). Em 2011 a empresa Sony teve um incidente cibernético, com vazamento de dados de mais de 77 milhões

de usuários[116], devido à falta de randomização no processo de assinatura ECDSA, possibilitando à *hackers* extraírem a chave privada com base na chave pública [117]. Caso semelhante aconteceu a usuários Android e suas carteiras de Bitcoin [118].

Figura 61 – Requisição de assinatura de certificado



Fonte: Adaptado de Russell. [119]

Estudo sobre sementes geradas em *hardware* através de FPGA, pode ser encontrado em [120]. Para este trabalho utiliza-se como semente para o gerador de números aleatórios, a relação entre o carimbo de tempo e a temperatura, duas grandezas disponíveis através do módulo RTC DS3231.

4.3.6 Confidencialidade dos dados

Informações geradas pelo conversor, seja por dados em repouso, em uso ou em movimento, são de natureza confidencial ou sensível. Isso implica que alguns canais de comunicação e armazenamentos de dados, exigem proteção contra espionagem e acesso não autorizado. Garantir a confidencialidade das informações nos canais de comunicação e dos dados armazenados visa impedir o acesso não autorizado de informações.

Com o intuito de evitar ataques MITM e possibilitar a confidencialidade das credenciais, *hashes* e dados trafegados entre o programa WPS e o conversor, neste trabalho aplica-se um mecanismo de criptografia com base nas chaves criadas na Subseção 4.3.5.2 acima apresentada.

Para tal necessidade, visa-se aderência ao protocolo de segurança Modbus/TCP (*Modbus/TCP Security Protocol*), com um uso de criptografia simétrica e assimétrica através do protocolo de segurança TLS.

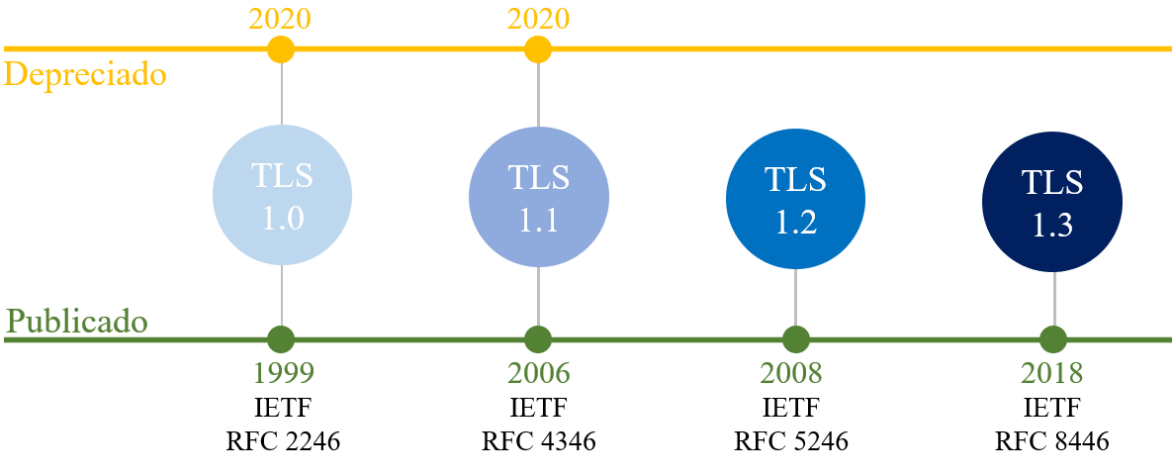
4.3.6.1 Protocolo de segurança da camada de transporte

O protocolo de segurança da camada de transporte (TLS, *Transport Layer Security*), como o próprio nome o descreve, atua na camada de transporte do modelo OSI, para fornecer segurança na comunicação TCP/IP entre dois dispositivos. Desenvolvido para substituir o protocolo de camada de soquete seguro (SSL, *Secure Sockets Layer*), atualmente o protocolo TLS está na sua quarta versão (Figura 62).

A primeira versão do protocolo de segurança da camada de transporte (TLS, *Transport Layer Security*), foi publicada em janeiro de 1999 [121], a segunda versão surgiu 7 anos depois [122], porém ambas já foram descontinuadas. A versão 1.2 do protocolo é amplamente utilizada [123], mas em 2018 foi publicada a versão 1.3 [124] sua mais recente versão, que além de ser mais segura, utiliza algoritmo de assinatura EdDSA[125], aperfeiçoou seu mecanismo de aperto de mão (*handshake*), deixando-o mais rápido.

O protocolo TLS utiliza criptografia simétrica e assimétrica. A criptografia assimétrica é utilizada durante o processo de *handshake*, neste processo garante a integridade e confidencialidade do canal de comunicação e consequentemente possibilita o compartilhamento seguro da chave a ser usada para a criptografia simétrica quando estabelecidas as sessões. [126]

Figura 62 – Versões do protocolo TLS



Fonte: Adaptado de Tech School. [126]

Ao longo dos anos o protocolo TLS vem sendo aplicado a muitos protocolos de aplicação, por exemplo: HTTPS (*Hyper Text Transfer Protocol over TLS*)[127]; SFTP (*File Transfer Protocol with TLS*) [128]; e SMTPS (*Simple Mail Transfer Protocol over TLS*) [129]; etc. Em 2018 a organização Modbus, publicou a especificação de segurança do protocolo

Modbus/TCP [130], visando elevar a maturidade de segurança cibernética do protocolo Modbus/TCP, que atualmente é amplamente aplicado a IACSs. Esta variante do protocolo Modbus/TCP também utiliza o TLS, como protocolo de transporte, possibilitando a criptografia das requisições e respostas por ele realizadas.

Neste trabalho aplica-se o protocolo TLS 1.2 através da biblioteca WolfSSL, com o objetivo principal de garantir a confidencialidade dos dados e um canal de comunicação seguro entre o programa WPS e o conversor.

Com a perspectiva de, no futuro, possibilitar a comunicação do conversor com dispositivos terceiro através do protocolo de segurança Modbus/TCP. Contempla-se neste trabalho, alguns itens especificados pelo protocolo. Desde modo, projeta-se o controle de acesso com a possiblidade de no futuro analisar funções (*roles*) atribuídas como extensões aos certificados, um exemplo pode ser observado pelo certificado do ANEXO B, bem como se utiliza a versão 1.2 do TLS e a porta 802 especificada pelo próprio protocolo, para realizar conexões seguras entre o conversor e o WPS.

A Figura 63 apresenta o processo de *handshake* realizado entre o programa WPS e o conversor. A comunicação inicia com uma conexão do programa WPS, na porta TCP 802 do conversor. Neste momento, inicia-se o processo de *handshake* do protocolo TCP (*Three-Way Handshake*), uma vez confirmado o acesso a porta pelo protocolo TCP, inicia-se o processo de *handshake* do protocolo TLS.

Figura 63 – Handshake do protocol TLS capturado pelo Wireshark

Source	Destination	Protocol	Length	Source Port	Destination Port	Info
192.168.200.250	192.168.200.10	TCP	66	55832	802	55832 → 502 [SYN] Seq=0 Win=
192.168.200.10	192.168.200.250	TCP	60	802	55832	502 → 55832 [SYN, ACK] Seq=0
192.168.200.250	192.168.200.10	TCP	54	55832	802	55832 → 502 [ACK] Seq=1 Ack=
192.168.200.250	192.168.200.10	TLSv1.2	198	55832	802	Client Hello
192.168.200.10	192.168.200.250	TLSv1.2	133	802	55832	Server Hello
192.168.200.10	192.168.200.250	TLSv1.2	818	802	55832	Certificate
192.168.200.10	192.168.200.250	TLSv1.2	239	802	55832	Server Key Exchange
192.168.200.10	192.168.200.250	TLSv1.2	63	802	55832	Server Hello Done
192.168.200.250	192.168.200.10	TLSv1.2	129	55832	802	Client Key Exchange
192.168.200.10	192.168.200.250	TLSv1.2	60	802	55832	Change Cipher Spec
192.168.200.10	192.168.200.250	TLSv1.2	139	802	55832	Encrypted Handshake Message
192.168.200.250	192.168.200.10	TLSv1.2	123	55832	802	Application Data
192.168.200.10	192.168.200.250	TLSv1.2	155	802	55832	Application Data
192.168.200.250	192.168.200.10	TLSv1.2	123	55832	802	Application Data
192.168.200.10	192.168.200.250	TLSv1.2	155	802	55832	Application Data

Fonte: Elaborado pelo autor.

O processo inicia com o cliente, neste caso o programa WPS, enviando um olá (*Client Hello*) contemplando todas os algoritmos de criptografia assimétrica por ele suportados, o

conversor então também diz olá (*Server Hello*) informando qual algoritmo de criptografia foi escolhido, dentre as opções a ele fornecidas.

Na sequência o próprio servidor envia três mensagens, a primeira contemplando o certificado do servidor (*Server Certificate*), a segunda com informações adicionais sobre a troca de chaves, esta é enviada apenas quando a mensagem de certificado do servidor não contém todos os dados suficientes [121], dependendo do algoritmo de criptografia escolhido e a teceria para avisar ao cliente que o servidor terminou de enviar as mensagens para a troca de chaves.

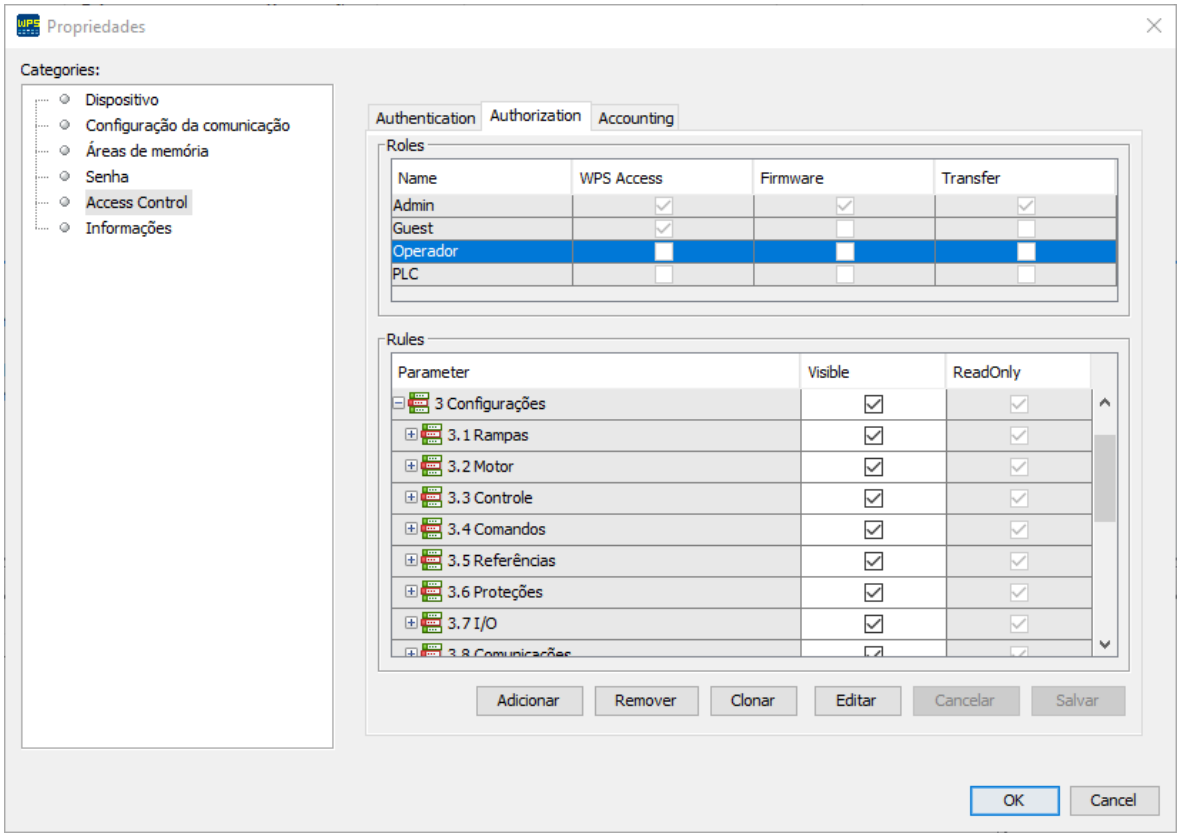
Após validar a autenticidade do certificado, e receber o *Server Hello Done*, o cliente gera um número aleatório, criptografa-o utilizando a chave pública do servidor, e envia a mensagem *Client Key Exchange*. O servidor recebe esta mensagem e tenta decriptá-la com base em sua chave privada. Em caso de sucesso, este avisa que a partir daquele momento (*Change Cipher Spec*), todas as mensagens serão enviadas com base nas chaves e algoritmo de criptografia simétrica negociadas e finalmente finaliza o processo de *handshake*, com o envio da mensagem (*Encrypted Handshake Message*). A partir deste momento, as sessões estabelecidas através do protocolo TLS, utilizam criptografia simétrica para garantir a confidencialidade dos dados trafegados entre o emissor e o receptor.

4.3.7 Disponibilidade dos recursos

A configuração e o *backup* das funcionalidades e mecanismos de segurança desenvolvidas neste trabalho, são projetadas para serem realizadas e gerenciadas através do programa WPS. A Figura 64, apresenta a janela do programa WPS que a configuração das funções (*roles*) a serem aplicadas a cada usuário. Pode-se observar, que foram criadas quatro funções, Admin, Guest, Operador e PLC. Cada função possibilita de forma individual escolher os direitos acesso aos parâmetros do conversor.

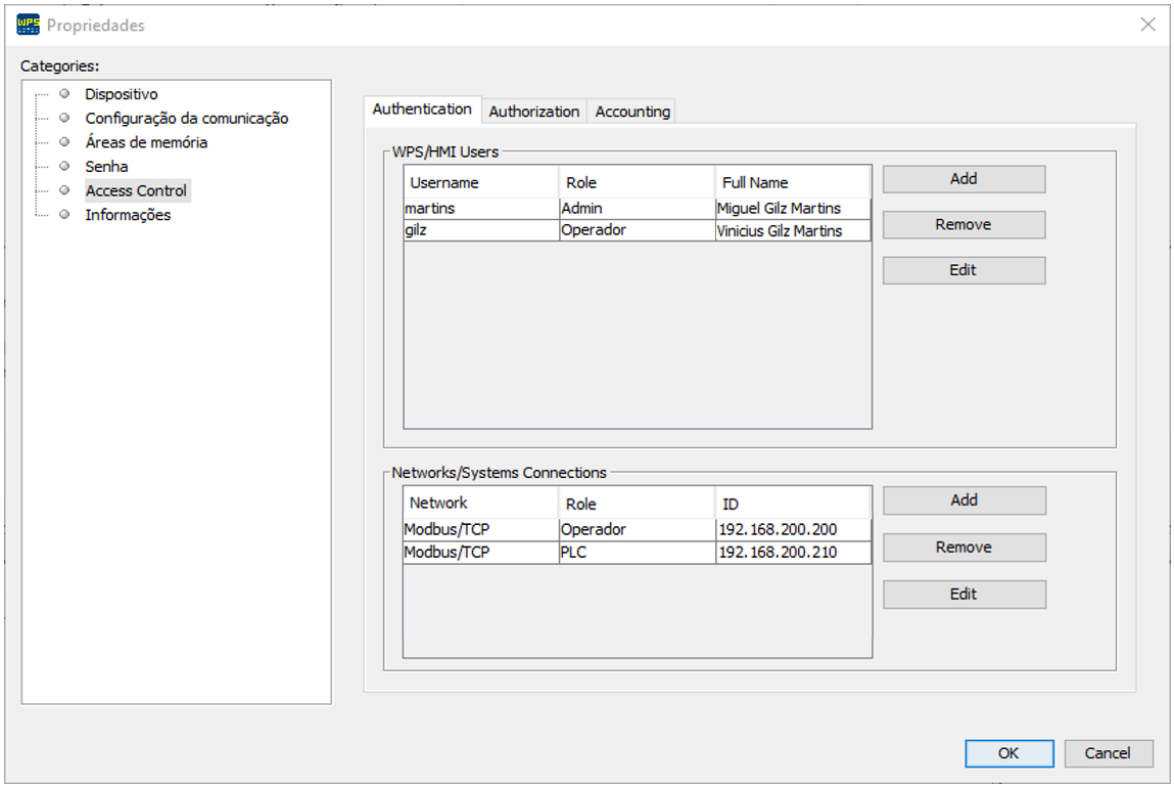
Após criadas e configuradas, as funções ficam disponíveis para atribuição aos usuários e aos identificadores para redes de comunicação. A Figura 65 apresenta a janela do programa WPS, disponibilizada para esta função. Duas contas de usuários foram criadas com suas respectivas funções, o usuário “martins” possui privilégios de administrador enquanto o usuário “gilz” tem acessos menos privilegiados, com a função “Operador”.

Figura 64 – Janela do WPS para configuração das funções (roles)



Fonte: Elaborado pelo autor.

Figura 65 – Janela do WPS para configuração dos autenticadores (usuários)



Fonte: Elaborado pelo autor.

O mesmo caso é válido, para os identificados de rede utilizados junto aos protocolos padrões. Sem acesso as funções proprietárias criadas para o Modbus, aplica-se funções distintas para os endereços IP, pois o Modbus/TCP permite a disponibilidade destes identificadores. Função “Operador” para o endereço 192.168.200.200 e função “PLC”, permitindo acesso a parâmetros específicos para o endereço 192.168.200.210.

Finalizadas as configurações a serem realizadas pelo usuário administrador do programa WPS. O próprio WPS compila as configurações realizadas pelo usuário, em conjunto com as configurações gerais para o SSC em um arquivo binário (Figura 66) a ser importado no conversor, através do recurso de download disponibilizado pelo próprio WPS.

Figura 66 – Estrutura configuração do usuário para o subsistema de segurança

```
{
SEC_CONFIG_FILE.fileVersion = 0x01;
SEC_CONFIG_FILE.fileHash = {0xDE,0x9F,0x2C,0x7F,0xD2,0x5E,0x1B,0x3A,0xFA,0xD3,
                            0xE8,0x5A,0x0B,0xD1,0x7D,0x9B,0x10,0x0D,0xB4,0xB3};
SEC_CONFIG_FILE.isSettingsUpdate = 0x01;
SEC_CONFIG_FILE.settings.secAuthIsEnabled = 1;
SEC_CONFIG_FILE.settings.secAclIsEnabled = 1;
SEC_CONFIG_FILE.settings.passStrongPolicy = 3;
SEC_CONFIG_FILE.settings.passMinumumLength = 6;
SEC_CONFIG_FILE.settings.passExpiredMinutes = 129600;
SEC_CONFIG_FILE.isParametersUpdate = 0x01;
SEC_CONFIG_FILE.isUsersUpdate = 0x01;
SEC_PARAMETER_ROLES parametersRoles[] = {
{ .parameterNetId = 1, .rolePermission = 228 },
{ .parameterNetId = 2, .rolePermission = 228 },
{ .parameterNetId = 3, .rolePermission = 228 },
{ .parameterNetId = 4, .rolePermission = 996 }
};
SEC_USER initUsers[] = {
{ .action = 0x00, .login = "martins", .role = 3, .pin = 1234,
  .pass = "Udesc123.", .extra = 0, .timestamp = 1618270633 },
{ .action = 0x00, .login = "gilz", .role = 2, .pin = 4321,
  .pass = "Udesc321.", , .extra = 1, .timestamp = 1618272623 },
};
SEC_CONFIG_FILE.isAclUpdate = 0x01;
SEC_ACL initAcl[] = {
{ .ipAddress = 0xd2c8a8c0, .role = 4 },
{ .ipAddress = 0xc8c8a8c0, .role = 2 }
};
SEC_CONFIG_FILE.isRolesUpdate = 0x01;
SEC_ROLES_TAG initRoles[] = { { .tag = "default" }, { .tag = "reseved" }, { .tag = "Operador" },
                              { .tag = "Admin" }, { .tag = "PLC" } };
SEC_CONFIG_FILE.crc = CRC16
}
```

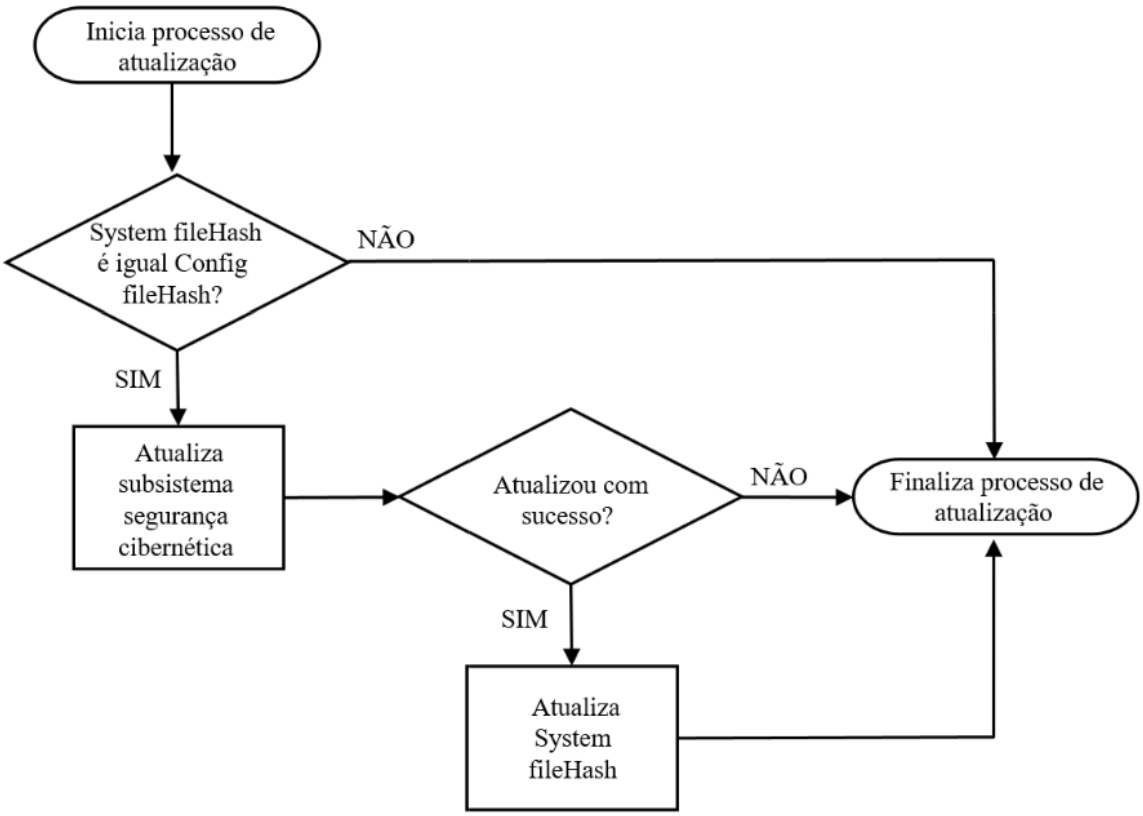
Fonte: Elaborado pelo autor.

O programa WPS, diferentemente do processo de monitoração e alteração online dos parâmetros do conversor, opera em um modo offline, no qual as configurações são realizadas no *software* e quando finalizadas, enviadas para o conversor. Com o propósito de se adequar a esta operação *offline*, o protótipo desenvolvido neste trabalho, opera com dois arquivos de

configuração na memória do conversor. Um arquivo com a configuração atual do sistema e um segundo arquivo com as novas configurações realizadas pelo usuário.

A Figura 67 apresenta o fluxograma do processo de atualização destas configurações. O processo de inicialização é disparado, durante a inicialização do conversor ou imediatamente após o conversor receber um novo arquivo de configuração.

Figura 67 – Fluxograma processo de atualização do SSC



Fonte: Elaborado pelo autor.

Ao iniciar o processo o SSC avalia se o *hash* do arquivo recebido é igual ao *hash* do sistema. Caso for igual, valida o arquivo de configuração e inicia a atualização, a partir das informações do novo arquivo. Ao concluir a atualização, o subsistema atualiza o seu *hash*, invalidando o arquivo de configuração, ou seja, na próxima inicialização os *hashes* não serão mais idênticos.

Deste modo para realizar alterações, no SSC, primeiro o usuário administrador precisará realizar o upload das atuais configurações de segurança do conversor, recebendo um arquivo atualizado com o *hash* válido, para quando finalizar as configurações poder realizar o *download* das configurações para o conversor.

4.4 ENSAIOS

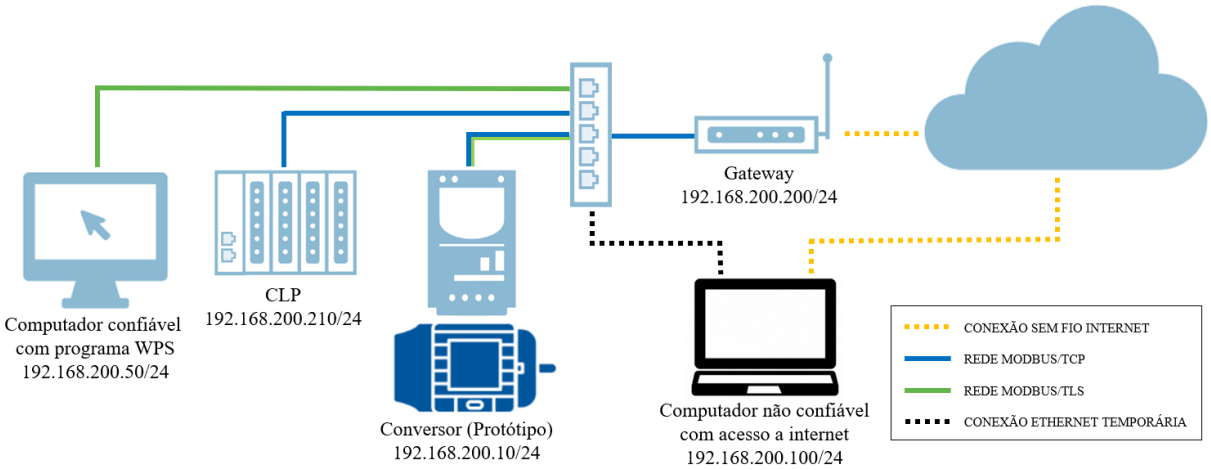
Nesta seção serão apresentados os ensaios realizados com o protótipo do conversor e com os mecanismos de controle de acesso e mitigação de vulnerabilidades desenvolvidos.

Conforme apresentado, neste trabalho projeta-se e desenvolve-se mecanismos de controle de acesso para atender todas as interfaces do conversor, HMI, Ethernet, comunicações seriais etc. Porém como abdicou-se do *hardware* do CFW300 e optou-se pela utilização da Zedboard, não foram desenvolvidas todas as suas interfaces no protótipo. Deste modo, os ensaios se limitam ao uso do protocolo Modbus/TCP, na interface de comunicação Ethernet e ao protocolo IPv4, pois o subsistema de rede do CFW300 não oferece suporte ao protocolo IPv6. Sendo assim, os ensaios contemplam três cenários:

a) acesso Modbus/TCP com o SSC desabilitado no protótipo;
b) acesso Modbus/TCP com o SSC habilitado no protótipo;
c) acesso autenticado através do programa WPS com o SSC habilitado no protótipo.

O diagrama proposto para a realização dos ensaios é apresentado na Figura 68. O cenário proposto para a realização dos testes, visa estar em conformidade com necessidades da indústria 4.0. Todos os componentes estão conectados via rede e se comunicam utilizando o protocolo Modbus/TCP.

Figura 68 – Diagrama de rede utilizado para o ensaio



Fonte: Elaborado pelo autor.

O PLC é o sistema de controle deste IACS, precisa enviar e receber requisições para o conversor (protótipo), um *gateway* realiza o monitoramento constante do conversor, enviando informações para a nuvem, dentro da rede industrial ele é o único que está conectado ao domínio de TI e a Internet, através da sua interface sem fio. O computador local, dispõe dos programas

de configuração do PLC e do conversor, neste caso mais especificadamente o programa WPS. Os direitos de acesso aos parâmetros do protótipo são apresentados pela Tabela 3.

Tabela 3 – Direitos de acesso dos dispositivos

Função (Role)	Direitos de acesso para leitura	Direitos de acesso para escrita
Administrador	Em todos os parâmetros	Em todos os parâmetros
PLC	Somente no parâmetro 21	Somente no parâmetro 21
Operador	Em todos os parâmetros	Nenhum

Fonte: Elaborado pelo autor.

Para a realização dos ensaios nos três cenários apresentados, simula-se que um computador não confiável foi conectado à rede. Este computador está comprometido e tentará alterar os parâmetros do conversor (Figura 69), ou seja, tentará acessar, ler e escrever em seus registradores.

Figura 69 – Parâmetros disponíveis no protótipo

Parâmetro	Descrição	Offline	Online	Mínimo	Máximo	Ajustes de Fábrica	Unidade
P0001	Output Speed (Motor)	0.1		0.0	400.0	0.1	Hz
P0002	Motor Current	0.0		0.0	40.0	0.0	A
P0003	Module Temperature	0.0		-200.0	200.0	0.0	ºC
P0004	DC Link Voltage	0		0	828	0	V
P0005	Output Frequency Motor	0.0		0.0	400.0	0.0	Hz
P0006	Output Voltage	0		0	480	0	V
P0007	Acceleration Time	50		1	9999	50	s
P0008	Deceleration Time	100		1	9999	100	s
P0009	Acceleration Time 2nd Ramp	50		1	9999	50	s
P0010	Deceleration Time 2nd Ramp	100		1	9999	100	s
P0011	1st / 2nd Ramp Selection	0: 1st Ramp		0: 1st Ramp	6: SoftPLC	0: 1st Ramp	
P0012	Minumum Frequency	3.0		0.0	400.0	3.0	Hz
P0013	Maximum Frequency	66.0		0.0	400.0	66.0	Hz
P0014	Maximum Output Current	1.6		0.0	40.0	1.6	A
P0015	Maximum Output Voltage	1000		0	1000	1000	V
P0016	Reference Selection	1: AI1		0: HMI	17: FI > 0	1: AI1	
P0017	FWD / REV Selection	4: DIx		0: Foward	12: SoftPLC	4: DIx	
P0018	RUN / STOP Selection	0: HMI Keys		0: HMI Keys	5: SoftPLC	0: HMI Keys	
P0019	MBTCP: Unit ID	255		0	255	255	
P0020	MBTCP: TCP Port	502		0	65535	502	
P0021	Speed Reference	30.0		1.0	400.0	30.0	Hz
P0022	IP Address	0.0.0.0		0.0.0.0	255.255.255.255	0.0.0.0	
P0023	Mask Address	0.0.0.0		0.0.0.0	255.255.255.255	0.0.0.0	
P0024	Gateway Address	0.0.0.0		0.0.0.0	255.255.255.255	0.0.0.0	

Fonte: Elaborado pelo autor.

4.4.1 Cenário 1 – Subsistema segurança cibernética desabilitado.

Este ensaio tem como objetivo, apresentar vulnerabilidades existentes nos conversores atuais, que não dispõem de um mecanismo de controle de acesso. Portanto, inicializa-se o protótipo com o SSC desabilitado, ou seja, não existem proteções para acesso via rede Modbus/TCP, a não ser o próprio tipo de acesso do parâmetro, somente leitura ou escrita e leitura.

Figura 70 – Inicialização do protótipo sem o SSC

```
COM5 - PuTTY

-----lwIP Socket Mode Echo server Demo Application ------
Board IP: 192.168.200.10
Netmask : 255.255.255.0
Gateway : 192.168.200.1
Start PHY autonegotiation
Waiting for PHY to complete autonegotiation.
autonegotiation complete
link speed for phy address 0: 1000

             Server   Port Connect With..
------------------- ------ -------------------
         echo server      7 $ telnet <board_ip> 7

Waiting for new connection
```

Fonte: Elaborado pelo autor.

O cenário supõe que um notebook comprometido, que pode ou não estar conectado à Internet via redes sem fio, é conectado à rede industrial. Para isto, utiliza-se um computador realizando requisições ao protótipo através do programa MultiCom2.

O MultiCom2, é um programa de computador desenvolvido pela WEG para uso interno, pelo departamento de pesquisa e desenvolvimento. O MultiCom2 realiza a função de mestre Modbus, possibilitando o uso em redes ethernet ou seriais (RS-232, USB, etc).

O suposto computador comprometido se conecta à rede industrial e recebe o endereço IP 192.168.200.100/24 (Figura 71).

Figura 71 – Endereço IP do computador não confiável

```
Prompt de Comando
C:\Users\tmartins>ipconfig

Configuração de IP do Windows


Adaptador desconhecido OpenVPN Wintun:

   Estado da mídia. . . . . . . . . . . . . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . . :

Adaptador Ethernet Ethernet 3:

   Sufixo DNS específico de conexão. . . . . . . :
   Endereço IPv4. . . . . . . . . . . . . . . . : 192.168.200.100
   Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . . :
```

Fonte: Elaborado pelo autor.

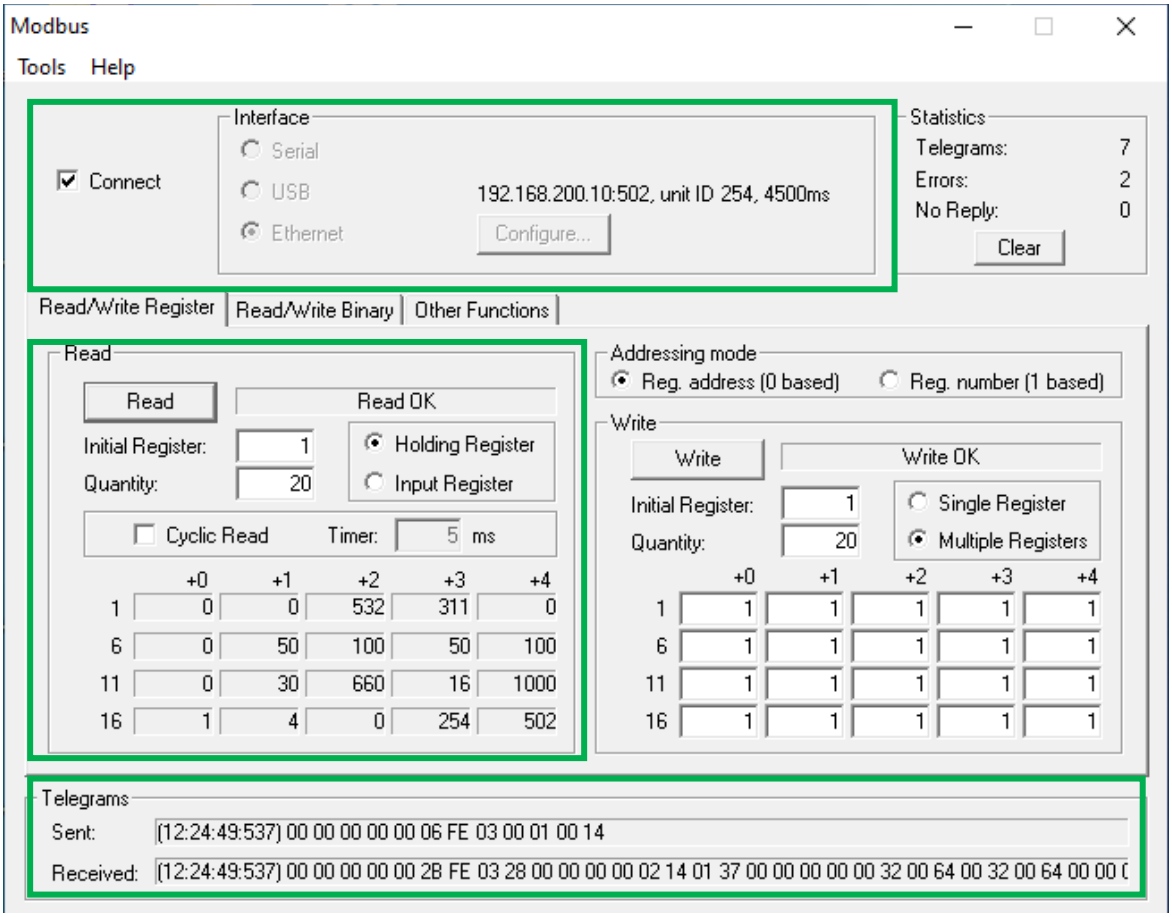
Ao ter acesso na rede industrial o computador não confiável, pode ser acessado remotamente caso também esteja conectado à Internet via sua interface sem fio, ou conter algum malware especializado em protocolos industriais.

O protótipo está disponível na rede no endereço IP 192.168.200.10:24 e seu Unit ID Modbus é o 254. Com o uso do programa MultiCom2, realiza-se uma requisição de leitura dos

primeiros 20 registradores do protótipo, através da função *Read Holding Register*. Como pode ser observado na Figura 72, o comando foi realizado com sucesso e o computador não confiável teve acesso de leitura a todos os 20 registradores solicitados.

Uma vez validado seu acesso de leitura aos registradores, o computador não confiável agora dispara uma requisição de escriva de um valor unitário para estes mesmos 20 registradores e como retorno, o computador recebe uma exceção, conforme apresentado em verde pela Figura 73.

Figura 72 – MultiCom2, Read Holding Register dos primeiros 20 registradores



Fonte: Elaborado pelo autor.

Porém, ao realizar uma nova requisição de leitura (Figura 73 em alaranjado) pode-se verificar que foi possível escrever em alguns registradores, ou seja, recebeu a exceção somente porque alguns daqueles registradores eram do tipo somente leitura e ocasionaram um erro durante a requisição.

Recebendo a informação dos valores 254 e 502 para os registradores 19 e 20, com um conhecimento básico sobre redes Modbus, o ator ou o *malware* considerará estes dois

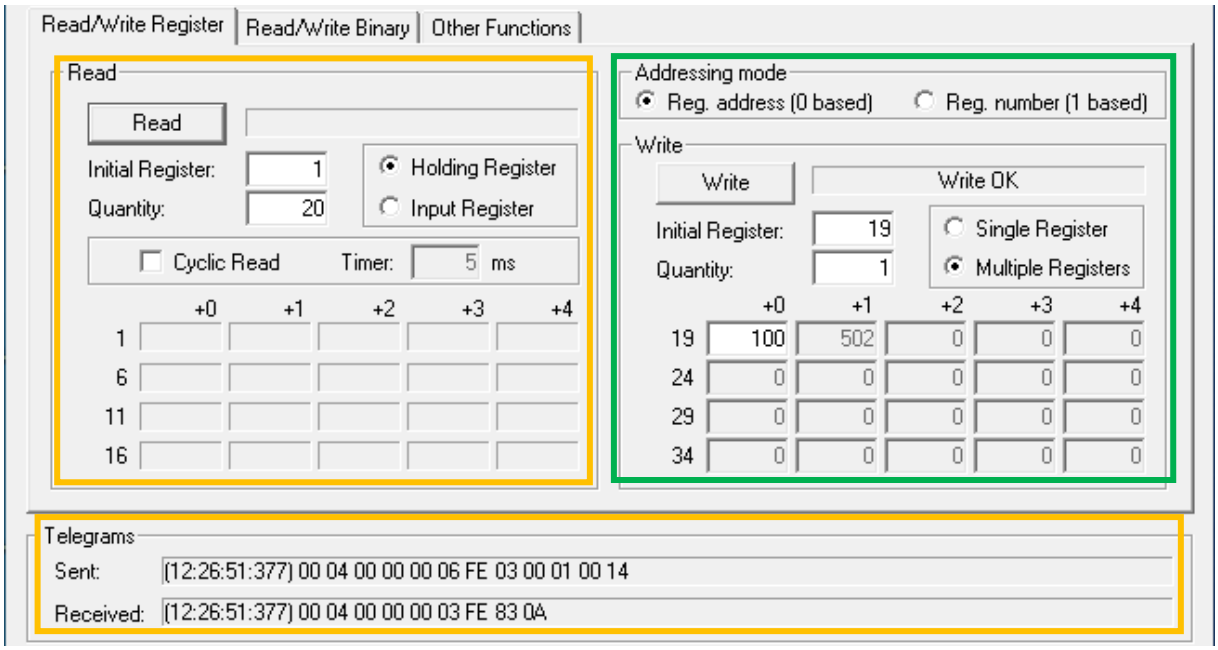
registradores, como potenciais endereços para a *Unit ID* e para a porta Modbus/TCP, internacionalmente padronizada com o valor 502.

Figura 73 – MultiCom2, Write Multiple Register e Read Holding Register

Fonte: Elaborado pelo autor.

Como próximo passo, realiza-se a escrita com sucesso do valor 100 no registrador 19, via função *Write Single Register* (Figura 74 em verde).

Figura 74 – MultiCom2, Alteração do Unit ID



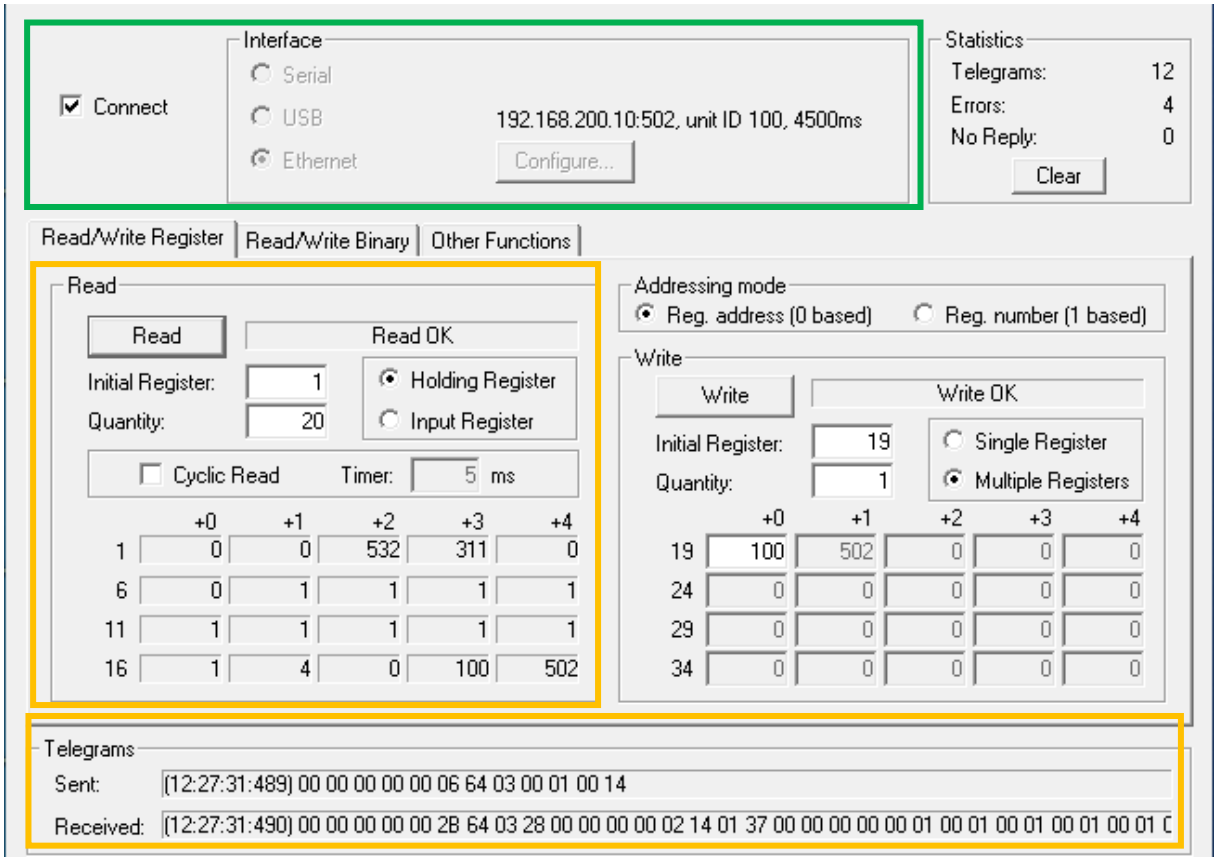
Fonte: Elaborado pelo autor.

Ao tentar realizar a leitura dos registradores novamente (Figura 74 em alaranjado). Valida-se que realmente se tratava do registrador com o *Unit ID* do escravo, pois recebe-se como retorno uma exceção com código 10 (0x0A), caminho do *gateway* indisponível (*Gateway Path Unavailable*).

Ao alterar o MultiCom2 para o novo *Unit ID*, verifica-se que agora o protótipo está disponível no novo endereço (Figura 75 em verde). Ao tentar novamente realizar a leitura dos 20 primeiros registradores, valida-se que o computador não confiável novamente tem acesso aos registradores do protótipo (Figura 75 em alaranjado).

Mas tal alteração afeta a comunicação dos demais dispositivos, gerando impacto ao IACS, e deixa o protótipo sob o domínio do computador não confiável, até que uma intervenção seja realizada.

Figura 75 – MultiCom2, Conexão com o novo Unit ID



Fonte: Elaborado pelo autor.

A Figura 76 apresenta todas as mensagens trocadas entre o computador não confiável IP 192.168.200.100 e o protótipo 192.168.200.10 durante o ensaio. Estas foram capturadas com o auxílio do programa de computador Wireshark.

Figura 76 – Pacotes trafegados entre o protótipo e o computador não confiável

Source	Protocol	Destina	Info
192.168.200.100	TCP	502	54097 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.200.10	TCP	54097	502 → 54097 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1446
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 0; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	54097	Response: Trans: 0; Unit: 254, Func: 3: Read Holding Registers
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=13 Ack=50 Win=64191 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
192.168.200.10	Modbus/TCP	54097	Response: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers. Exception returned
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=66 Ack=59 Win=64182 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 2; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	54097	Response: Trans: 2; Unit: 254, Func: 3: Read Holding Registers
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=78 Ack=108 Win=64133 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 3; Unit: 254, Func: 16: Write Multiple Registers
192.168.200.10	Modbus/TCP	54097	Response: Trans: 3; Unit: 254, Func: 16: Write Multiple Registers
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=93 Ack=120 Win=64121 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 4; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	54097	Response: Trans: 4; Unit: 254, Func: 3: Read Holding Registers. Exception returned
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=105 Ack=129 Win=64112 Len=0
192.168.200.100	TCP	502	54097 → 502 [FIN, ACK] Seq=105 Ack=129 Win=64112 Len=0
192.168.200.10	TCP	54097	502 → 54097 [ACK] Seq=129 Ack=106 Win=1943 Len=0
192.168.200.10	TCP	54097	502 → 54097 [FIN, ACK] Seq=129 Ack=106 Win=1943 Len=0
192.168.200.100	TCP	502	54097 → 502 [ACK] Seq=106 Ack=130 Win=64112 Len=0
192.168.200.100	TCP	502	54594 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.200.10	TCP	54594	502 → 54594 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1446
192.168.200.100	TCP	502	54594 → 502 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 0; Unit: 100, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	54594	Response: Trans: 0; Unit: 100, Func: 3: Read Holding Registers
192.168.200.100	TCP	502	54594 → 502 [ACK] Seq=13 Ack=50 Win=64191 Len=0

Fonte: Elaborado pelo autor.

4.4.2 Cenário 2 – Protótipo com controle de acesso

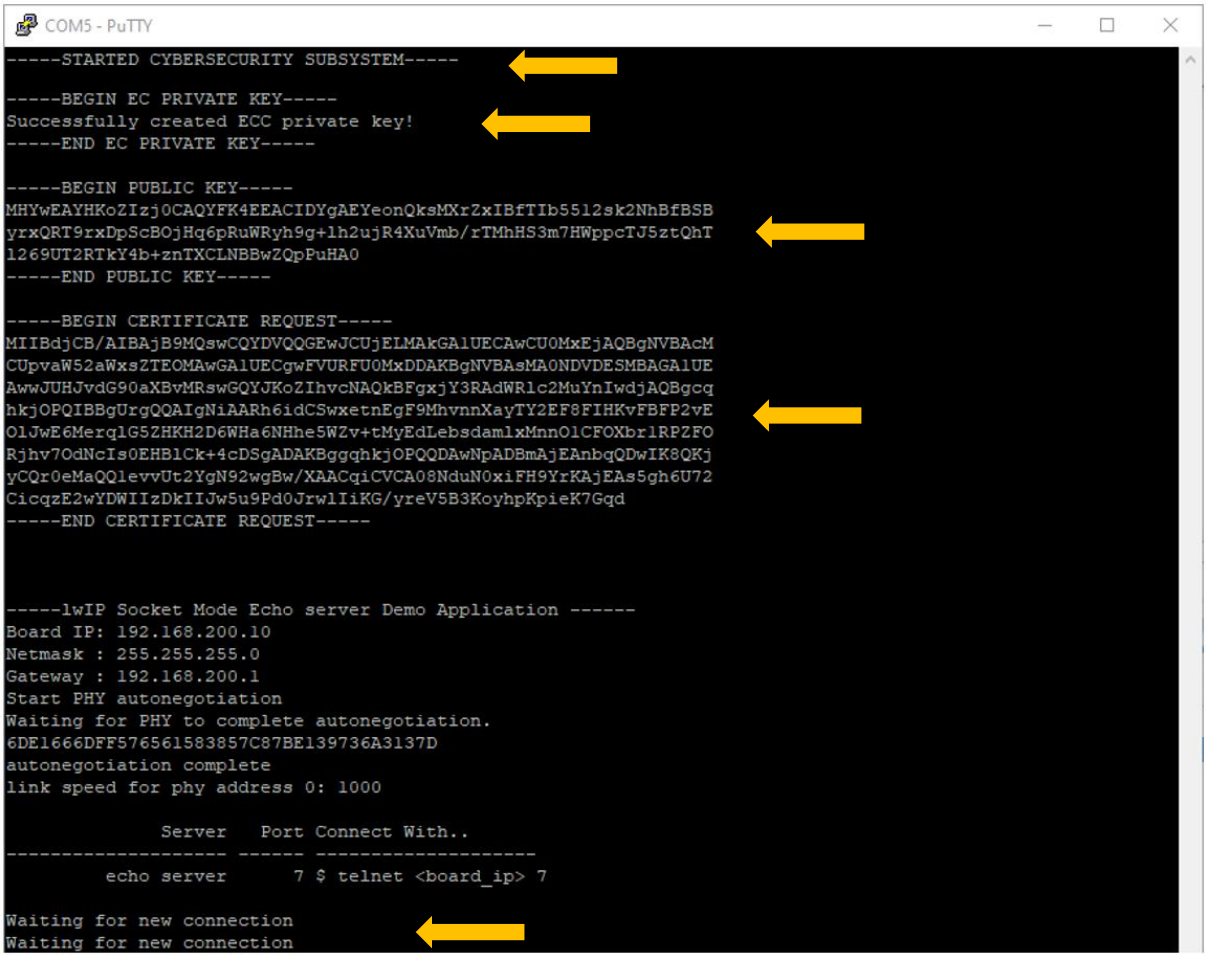
Neste cenário o protótipo é inicializado com o SSC habilitado. O ensaio tem como objetivo, validar o controle de acesso para dispositivos que se comunicam através o protocolo Modbus/TCP padrão, ou seja, sem acesso as funções proprietárias desenvolvidas por este trabalho.

A Figura 77 apresenta a inicialização do protótipo, a primeira mensagem de saída disponibilizada pelo terminal, informa que o SSC está habilitado no protótipo. A primeira vez que o subsistema é habilitado ele cria o par de chaves e o CSR pode ser utilizado para a criptografia do canal de comunicação. A chave pública e o CSR podem ser visualizados, já a chave privada fica armazenada de forma segura no dispositivo.

Também pode-se observar que o protótipo inicializa, disponibilizando duas interfaces de conexão, uma para o protocolo Modbus/TCP porta 502 e outra para o Modbus/TLS porta 802, para uso do programa WPS com suporte a criptografia.

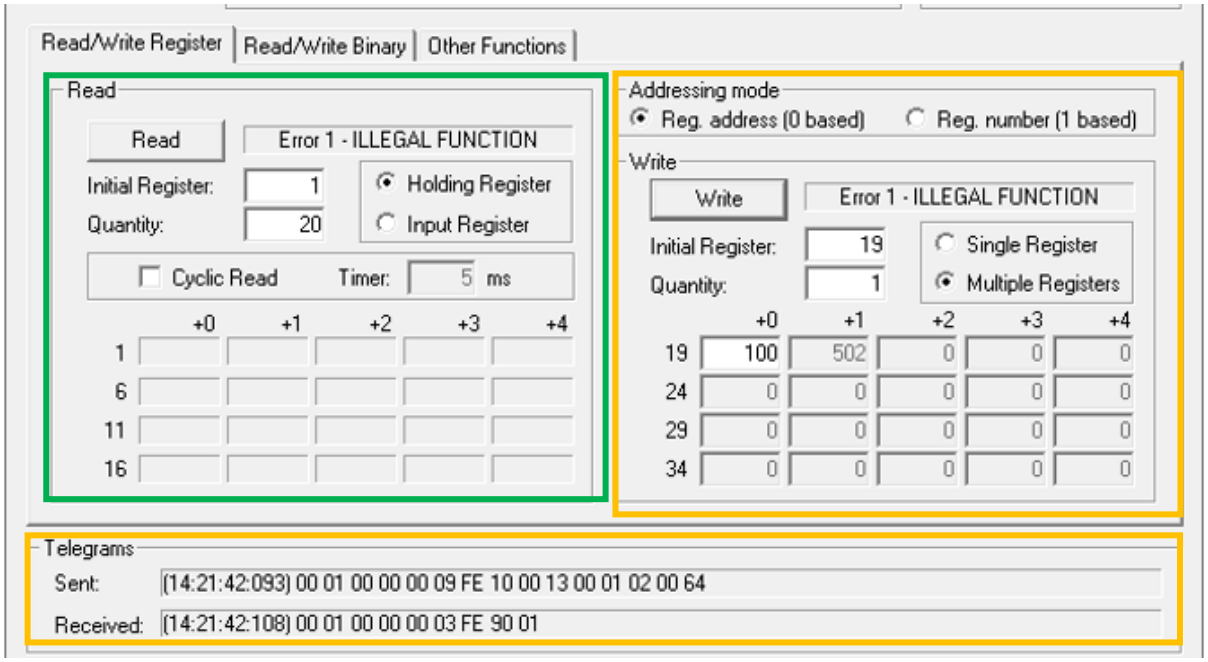
Uma vez, o protótipo inicializado com o SSC habilitado, tenta-se reproduzir as mesmas ações anteriormente realizadas pelo computador não confiável. Ao tentar realizar a leitura dos primeiros 20 registradores, ao invés de ter sucesso na leitura destes registradores, o computado não confiável recebe como retorno, uma exceção do tipo *Illegal Function* (Figura 78em verde). O mesmo acontece para a operação de escrita (Figura 78 em alaranjado).

Figura 77 – Inicialização do protótipo com o SSC habilitado



Fonte: Elaborado pelo autor.

Figura 78 – Exceção para ler e escrever nos registradores



Fonte: Elaborado pelo autor.

Portanto, com o controle de acesso habilitado, o computador não confiável, nem tem acesso de leitura e escrita aos registradores do protótipo.

Agora configura-se o computador utilizado nos ensaios, com o endereço IP do *gateway* (Figura 79).

Figura 79 – Endereço IP do *gateway*

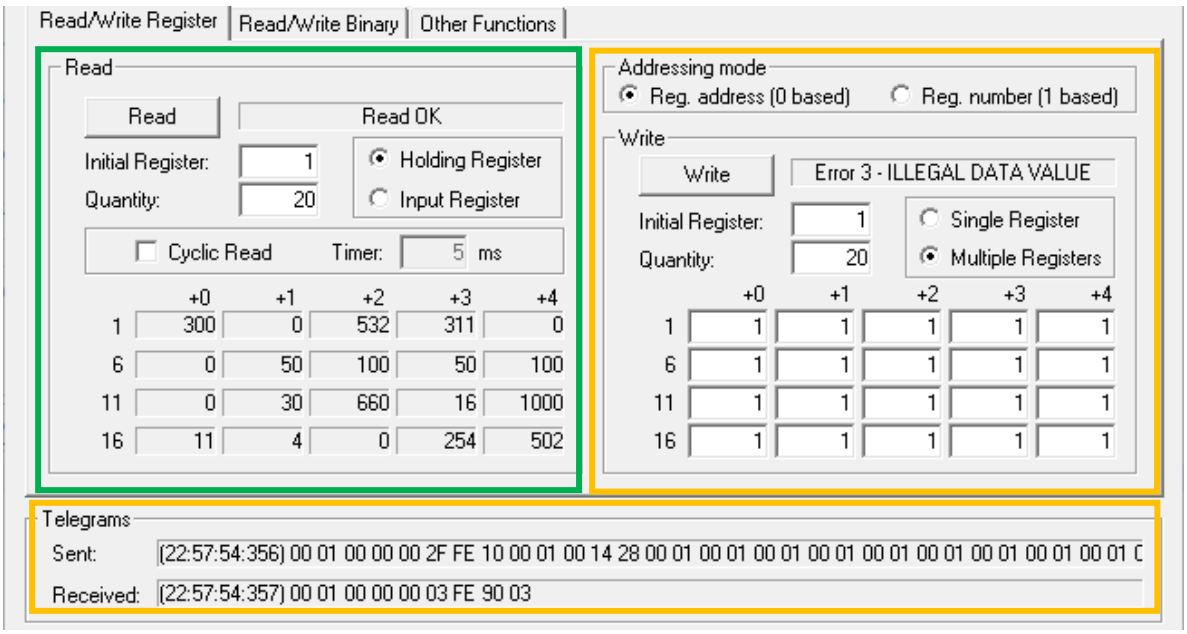
```
Adaptador desconhecido OpenVPN Wintun:

   Estado da mídia. . . . . . . . . . . . . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . . :

Adaptador Ethernet Ethernet 3:

   Sufixo DNS específico de conexão. . . . . . . :
   Endereço IPv4. . . . . . . . . . . . . . . . : 192.168.200.200
   Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . . :
```

Fonte: Elaborado pelo autor.

A função Operador foi criada e atribuída ao identificador do *gateway*, no Modbus/TCP equivale ao endereço IP do *gateway*. Conforme apresentado na Tabela 3, a função Operador, possui somente acesso à leitura de todos os parâmetros do protótipo.

Ao realizar uma requisição de leitura dos 20 primeiros registradores através do programa MultiCom2, o computador recebe com sucesso os valores destes registradores (Figura 80 em verde). Porém, ao tentar escrever um valor unitário nestes mesmos registradores, o computador recebe uma exceção do tipo *Illegal Data Value* como resposta (Figura 80 em alaranjado).

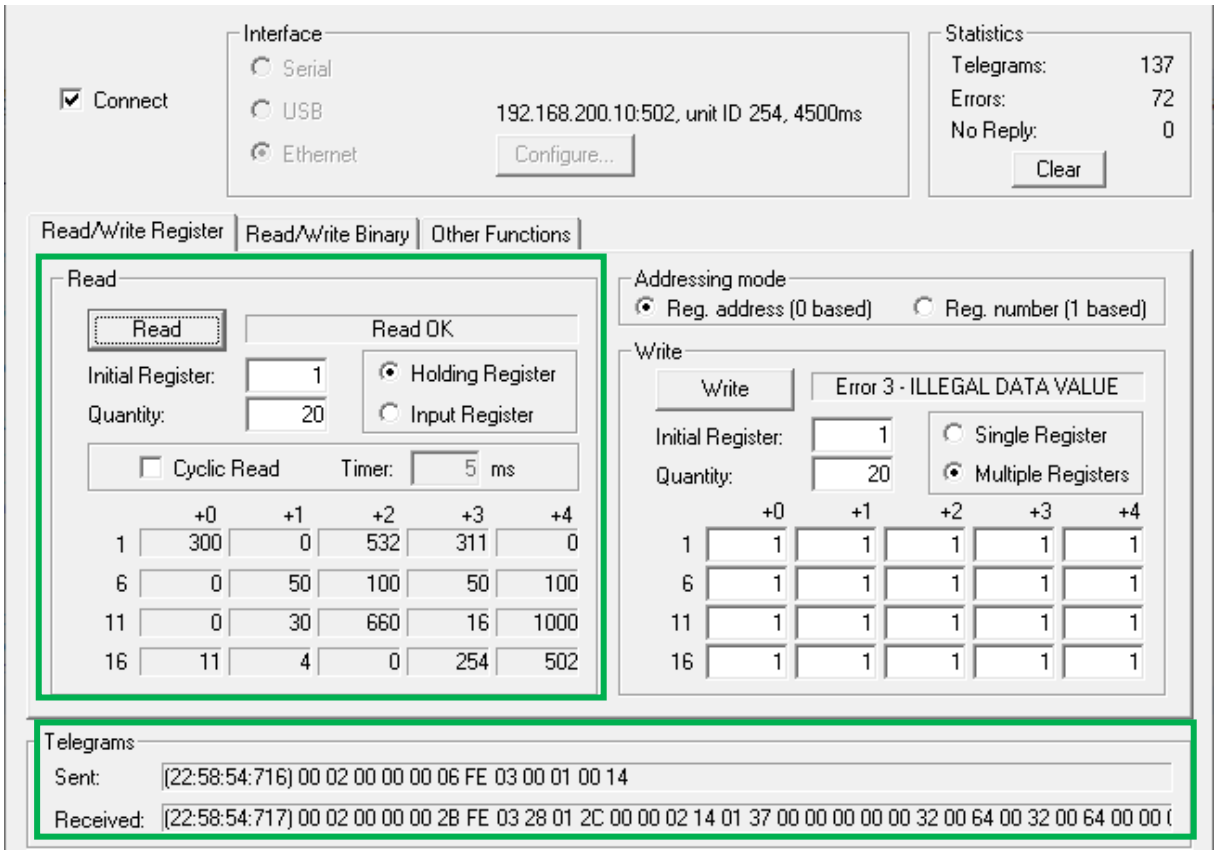
Figura 80 – Escrita e leitura múltiplos registradores com endereço do *gateway*



Fonte: Elaborado pelo autor.

A atuação do controle de acesso é validada através de uma nova requisição de leitura destes 20 registradores, como pode ser observado na Figura 81 em verde. Nenhum teve seu valor alterado, pelo comando realizado com o endereço IP do *gateway*.

Figura 81 – Validação de acesso somente leitura para o endereço do *gateway*



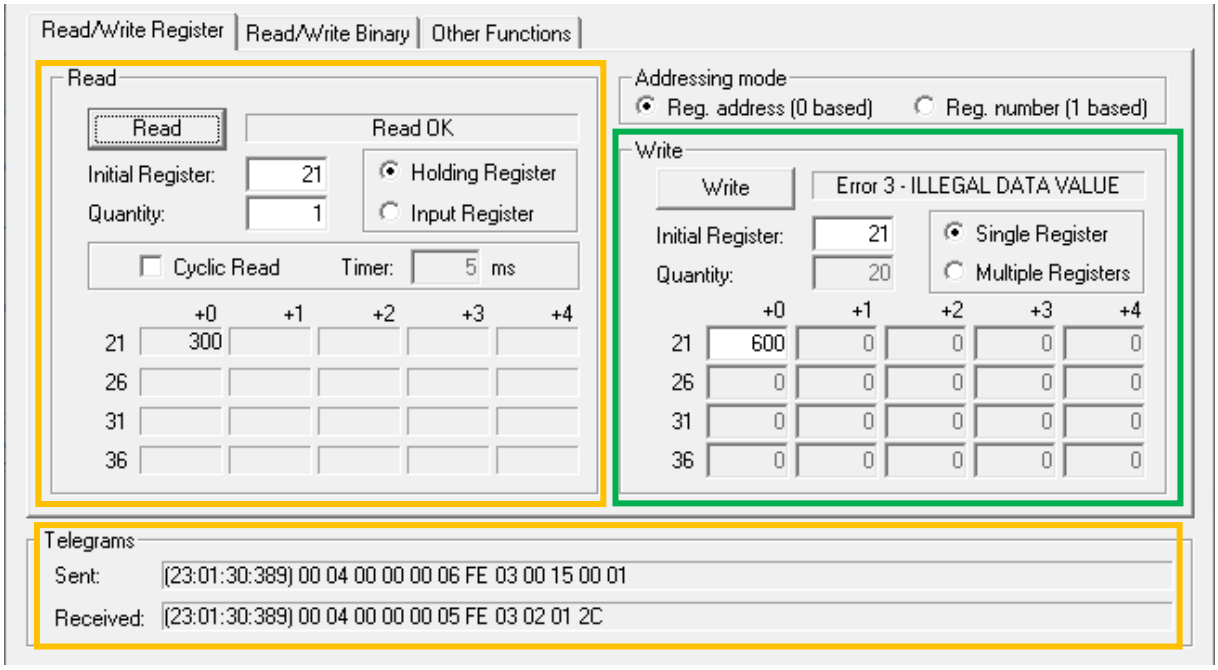
Fonte: Elaborado pelo autor.

Em uma nova tentativa de escrita, no entanto agora utilizando a função *Write Single Register*, tenta-se alterar a velocidade do motor controlado pelo conversor, escrevendo o valor 600 (equivale a 60 Hz) no registrador 21, responsável pela referência de velocidade do conversor. Novamente a mesma exceção *Illegal Data Value* é recebida pelo computador (Figura 82 em verde).

Ao realizar a leitura deste registrador, valida-se que o controle de acesso atuou novamente e não permitiu a escrita no respectivo registrador, mantendo o valor de referência da velocidade do conversor em 300 (Figura 82 em alaranjado).

Todas as mensagens trocadas entre os dispositivos envolvidos, computador não confiável IP 192.168.200.100, *gateway* IP 192.168.200.200 e o protótipo 192.168.200.10 durante o ensaio, foram capturadas com o auxílio do programa de computador Wireshark e são apresentadas na Figura 83.

Figura 82 – Validação exceção para escrita em um único registrador



Fonte: Elaborado pelo autor.

Figura 83 – Pacotes trafegados entre dispositivos durante ensaio do cenário 2

Source	Protocol	Destina	Info
192.168.200.100	TCP	502	64309 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.200.10	TCP	64309	502 → 64309 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1446
192.168.200.100	TCP	502	64309 → 502 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 0; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	64309	Response: Trans: 0; Unit: 254, Func: 3: Read Holding Registers. Exception returned
192.168.200.100	TCP	502	64309 → 502 [ACK] Seq=13 Ack=10 Win=64231 Len=0
192.168.200.100	Modbus/TCP	502	Query: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
192.168.200.10	Modbus/TCP	64309	Response: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers. Exception returned
192.168.200.100	TCP	502	64309 → 502 [ACK] Seq=28 Ack=19 Win=64222 Len=0
192.168.200.100	TCP	502	64309 → 502 [FIN, ACK] Seq=28 Ack=19 Win=64222 Len=0
192.168.200.10	TCP	64309	502 → 64309 [ACK] Seq=19 Ack=29 Win=2020 Len=0
192.168.200.10	TCP	64309	502 → 64309 [FIN, ACK] Seq=19 Ack=29 Win=2020 Len=0
192.168.200.100	TCP	502	64309 → 502 [ACK] Seq=29 Ack=20 Win=64222 Len=0
192.168.200.200	TCP	502	64597 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.200.10	TCP	64597	502 → 64597 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1446
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.200.200	Modbus/TCP	502	Query: Trans: 0; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	64597	Response: Trans: 0; Unit: 254, Func: 3: Read Holding Registers
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=13 Ack=50 Win=64191 Len=0
192.168.200.200	Modbus/TCP	502	Query: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
192.168.200.10	Modbus/TCP	64597	Response: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers. Exception returned
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=66 Ack=59 Win=64182 Len=0
192.168.200.200	Modbus/TCP	502	Query: Trans: 2; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	64597	Response: Trans: 2; Unit: 254, Func: 3: Read Holding Registers
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=78 Ack=108 Win=64133 Len=0
192.168.200.200	Modbus/TCP	502	Query: Trans: 3; Unit: 254, Func: 6: Write Single Register
192.168.200.10	Modbus/TCP	64597	Response: Trans: 3; Unit: 254, Func: 6: Write Single Register. Exception returned
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=90 Ack=117 Win=64124 Len=0
192.168.200.200	Modbus/TCP	502	Query: Trans: 4; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	64597	Response: Trans: 4; Unit: 254, Func: 3: Read Holding Registers
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=102 Ack=128 Win=64113 Len=0
192.168.200.200	TCP	502	64597 → 502 [FIN, ACK] Seq=102 Ack=128 Win=64113 Len=0
192.168.200.10	TCP	64597	502 → 64597 [ACK] Seq=128 Ack=103 Win=1946 Len=0
192.168.200.10	TCP	64597	502 → 64597 [FIN, ACK] Seq=128 Ack=103 Win=1946 Len=0

Fonte: Elaborado pelo autor.

Para o próximo ensaio, configura-se o computador com o endereço IP do PLC (Figura 84). O identificador do PLC está configurado com a função PLC, criada especificamente para

que ele tenha acesso de leitura e escrita no parâmetro 21, conforme Tabela 3, possibilitando-o a controlar a referência de velocidade do conversor e consequentemente do motor.

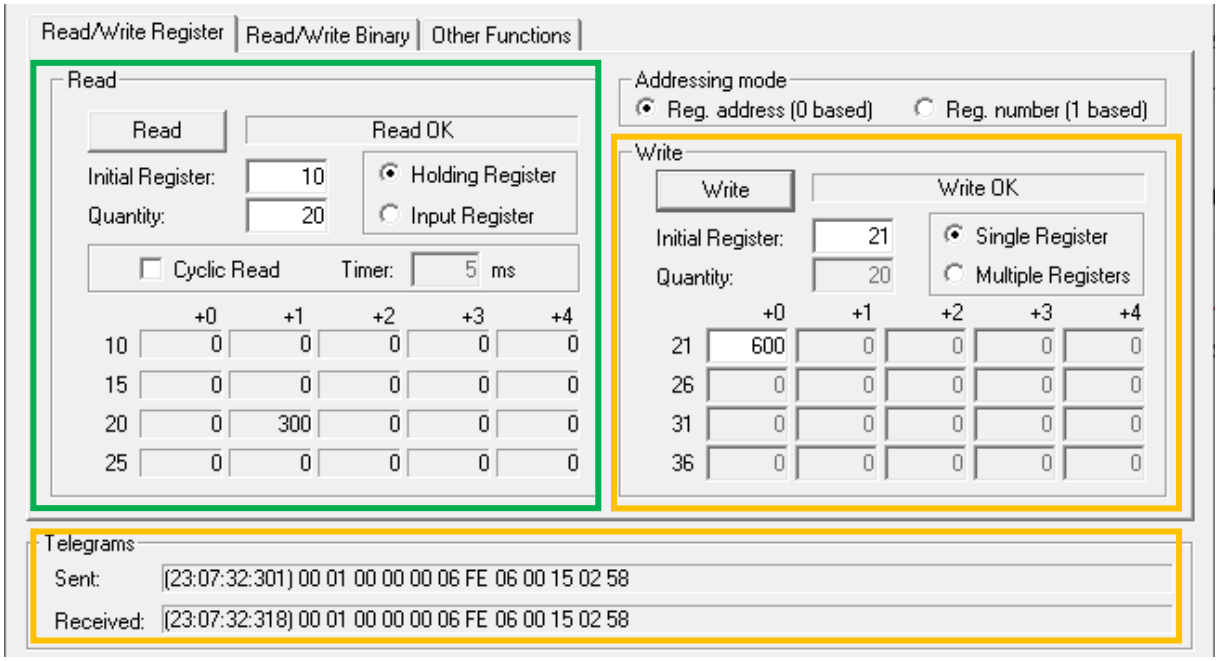
Figura 84 – Endereço IP do PLC

```
Adaptador desconhecido OpenVPN Wintun:

   Estado da mídia. . . . . . . . . . . . . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . . :

Adaptador Ethernet Ethernet 3:

   Sufixo DNS específico de conexão. . . . . . . :
   Endereço IPv4. . . . . . . . . . . . . . . . : 192.168.200.210
   Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . . :
```

Fonte: Elaborado pelo autor.

Conforme pode ser observado pela Figura 85 em verde, ao realizar uma requisição de leitura de 20 registradores a partir do decimo registrador, através da função *Read Holding Register*. O computador tem acesso, somente ao valor do registrador 21. Ao tentar realizar a mesma requisição que não era permitida para a função Operador, ou seja, a escrita no registrador 21, através da função *Write Single Register*, o computador tem como retorno que sua requisição foi realizada com sucesso (Figura 85 em alaranjado).

Figura 85 – Leitura e escrita do registrador 21

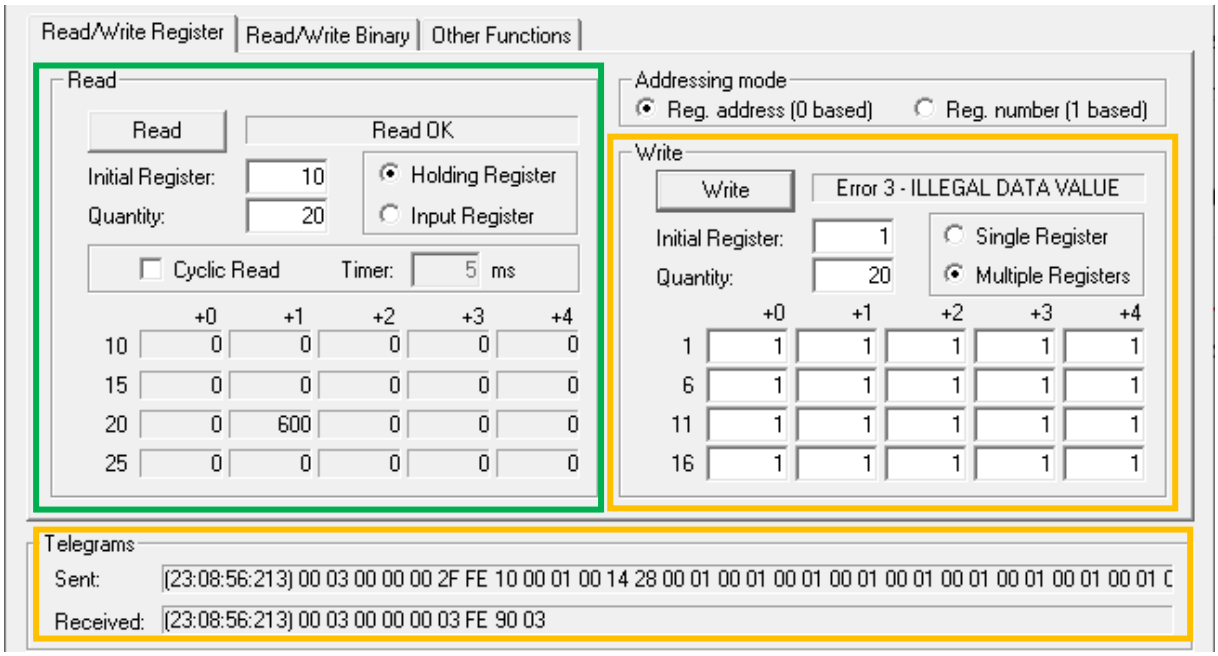


Fonte: Elaborado pelo autor.

Ao repetir a requisição de leitura comprova-se que o registrador realmente foi alterado com sucesso (Figura 86 em verde). Porém, ao tentar escrever um valor unitário nos primeiros

20 registradores, conforme pode ser observado na Figura 86 em alaranjado, o computador recebe uma exceção do tipo *Illegal Data Value*, ou seja, não tem acesso de leitura e nem de escrita nos demais registradores.

Figura 86 – Sem acesso à leitura e escrita dos registradores



Fonte: Elaborado pelo autor.

As mensagens trocadas entre o PLC endereço IP 192.168.200.210 e o protótipo 192.168.200.10 durante o ensaio, também foram capturadas com o programa Wireshark e são apresentadas pela Figura 87.

Figura 87 – Pacotes trafegados entre PLC e protótipo no cenário 2

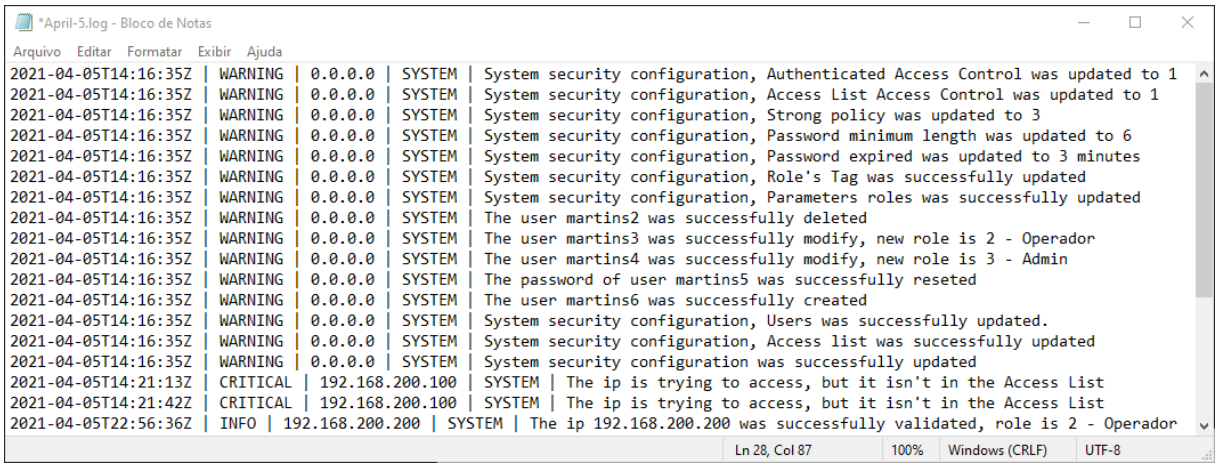
Source	Protocol	Destina	Info
192.168.200.10	Modbus/TCP	64597	Response: Trans: 4; Unit: 254, Func: 3: Read Holding Registers
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=102 Ack=128 Win=64113 Len=0
192.168.200.200	TCP	502	64597 → 502 [FIN, ACK] Seq=102 Ack=128 Win=64113 Len=0
192.168.200.10	TCP	64597	502 → 64597 [ACK] Seq=128 Ack=103 Win=1946 Len=0
192.168.200.10	TCP	64597	502 → 64597 [FIN, ACK] Seq=128 Ack=103 Win=1946 Len=0
192.168.200.200	TCP	502	64597 → 502 [ACK] Seq=103 Ack=129 Win=64113 Len=0
192.168.200.210	TCP	502	65116 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.200.10	TCP	65116	502 → 65116 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1446
192.168.200.210	TCP	502	65116 → 502 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.200.210	Modbus/TCP	502	Query: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	65116	Response: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
192.168.200.210	TCP	502	65116 → 502 [ACK] Seq=25 Ack=79 Win=64162 Len=0
192.168.200.210	Modbus/TCP	502	Query: Trans: 5; Unit: 254, Func: 6: Write Single Register
192.168.200.10	Modbus/TCP	65116	Response: Trans: 5; Unit: 254, Func: 6: Write Single Register
192.168.200.210	TCP	502	65116 → 502 [ACK] Seq=73 Ack=201 Win=64040 Len=0
192.168.200.210	Modbus/TCP	502	Query: Trans: 6; Unit: 254, Func: 3: Read Holding Registers
192.168.200.10	Modbus/TCP	65116	Response: Trans: 6; Unit: 254, Func: 3: Read Holding Registers
192.168.200.210	TCP	502	65116 → 502 [ACK] Seq=85 Ack=250 Win=63991 Len=0
192.168.200.210	Modbus/TCP	502	Query: Trans: 7; Unit: 254, Func: 16: Write Multiple Registers
192.168.200.10	Modbus/TCP	65116	Response: Trans: 7; Unit: 254, Func: 16: Write Multiple Registers. Exception returned
192.168.200.210	TCP	502	65116 → 502 [ACK] Seq=138 Ack=259 Win=63982 Len=0

Fonte: Elaborado pelo autor.

A Figura 88, apresenta os eventos de auditoria, gerados e armazenados pelo SSC do protótipo. Pode-se observar que na inicialização do protótipo, houve uma atualização das configurações de segurança, pois havia no protótipo um arquivo de configuração com o mesmo *hash* do arquivo de configuração do sistema, procedimento descrito na Seção 4.3.7 e representado na Figura 67.

Na sequência foram registrados outros 5 eventos. Dois eventos críticos, devido as tentativas de leitura e escrita do computador não confiável endereço IP 192.168.200.100. E três eventos de informação, um para registar que o identificador do *gateway* realizou requisições ao sistema e dois para avisar que o identificador do PLC, foi identificado pelo SSC e realizou uma requisição de escrita no registrador 21 do conversor.

Figura 88 – Registro de eventos para auditoria cenário 2



Fonte: Elaborado pelo autor.

4.4.3 Cenário 3 – Controle de acesso autenticado através do programa WPS

Neste cenário realiza-se requisições autenticadas ao protótipo, através do programa WPS. O objetivo deste ensaio é validar o acesso autenticado, com a identificação única de cada usuário. O programa WPS está instalado em um computador confiável, pertencente ao IACS. Seu endereço IP é 192.168.200.50, conforme apresentando pela Figura 89.

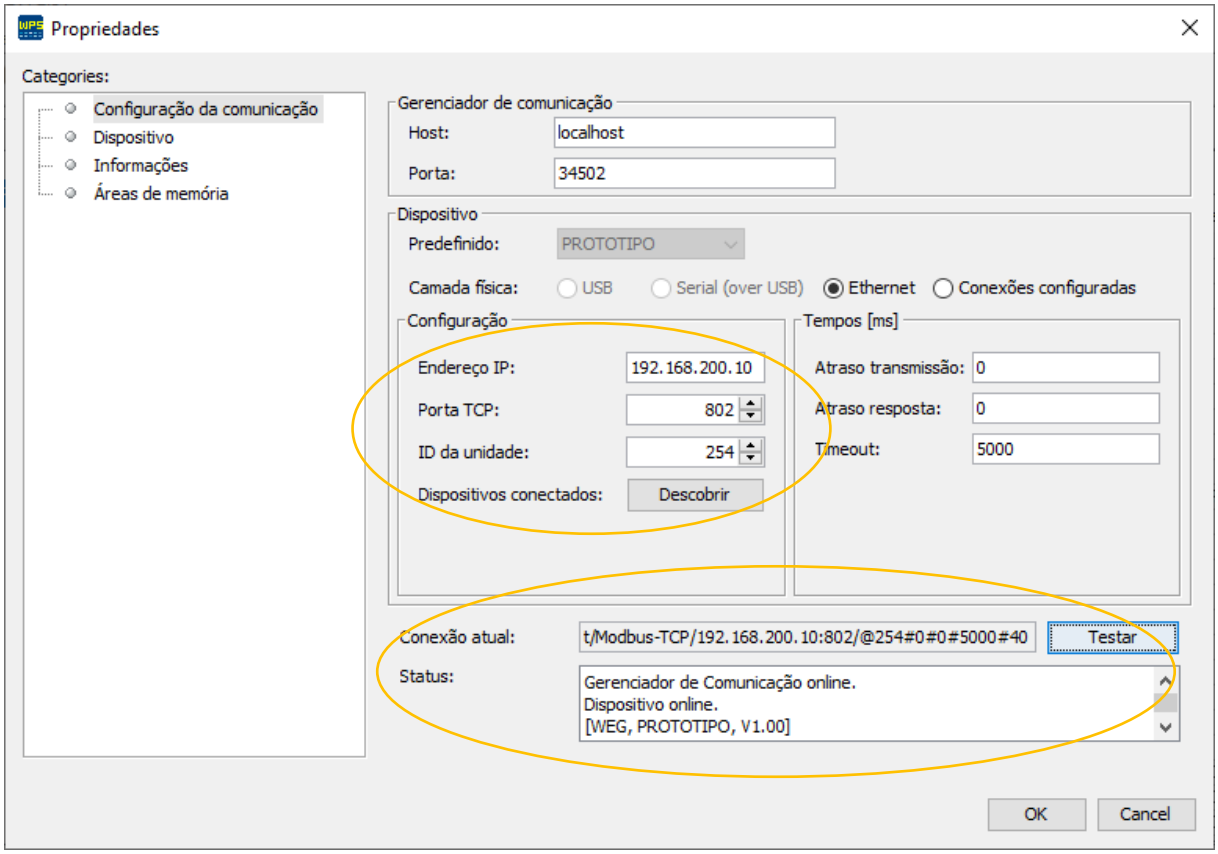
Ao invés de se conectar a porta padrão para o Modbus/TCP, o programa WPS agora se conecta à porta 802, especificada por [130] para uso com TLS. A Figura 90 apresenta a janela do programa WPS, utilizada para a configuração da comunicação com os dispositivos.

Figura 89 – Endereço IP do computador confiável

```
Configuração de IP do Windows


Adaptador desconhecido OpenVPN Wintun:

   Estado da mídia. . . . . . . . . . . . . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . . :

Adaptador Ethernet Ethernet 3:

   Sufixo DNS específico de conexão. . . . . . . :
   Endereço IPv4. . . . . . . . . . . . . . . . . : 192.168.200.50
   Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . . :
```

Fonte: Elaborado pelo autor.

Figura 90 – Janela do programa WPS para configuração da comunicação

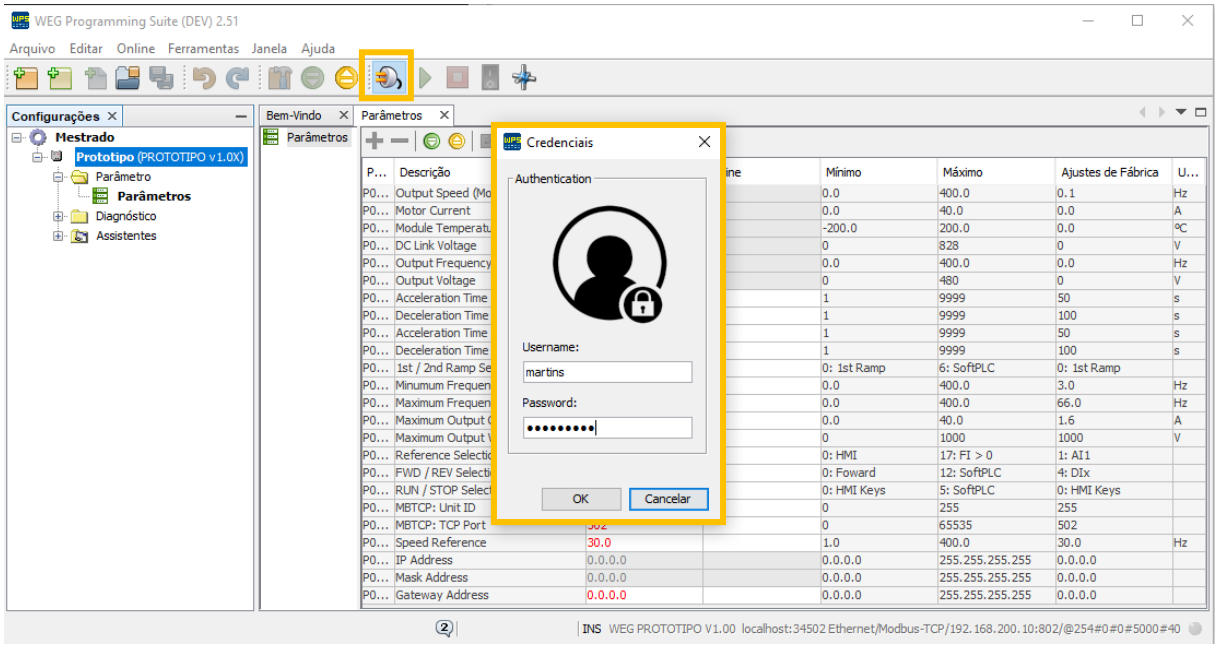


Fonte: Elaborado pelo autor.

Ao clicar no botão para iniciar a monitoração dos parâmetros do protótipo, o programa WPS identifica que o protótipo está com o SSC habilitado e disponibiliza ao usuário a janela de autenticação (Figura 91).

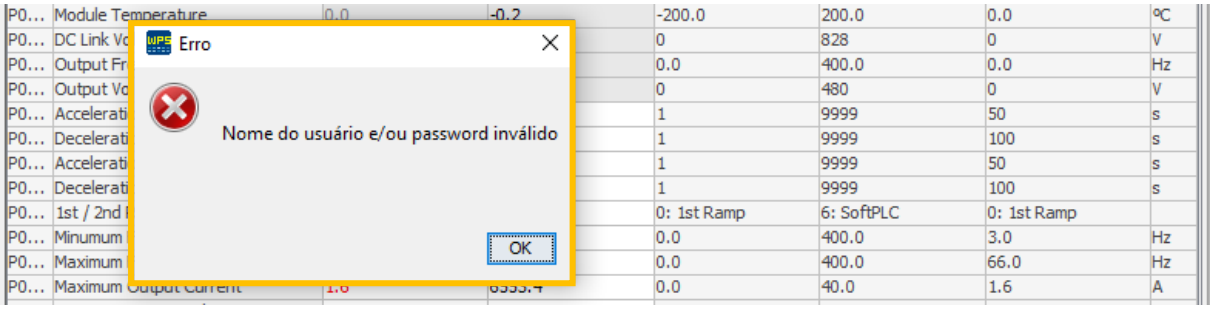
Caso o usuário entre com um autenticador invalido, seja o nome do usuário ou sua senha, uma janela de erro é apresentada a este utilizador (Figura 92). Ao clicar no botão “OK”, uma nova janela é disponibilizada para autenticação (Figura 93).

Figura 91 – Programa WPS, janela monitoração de parâmetros



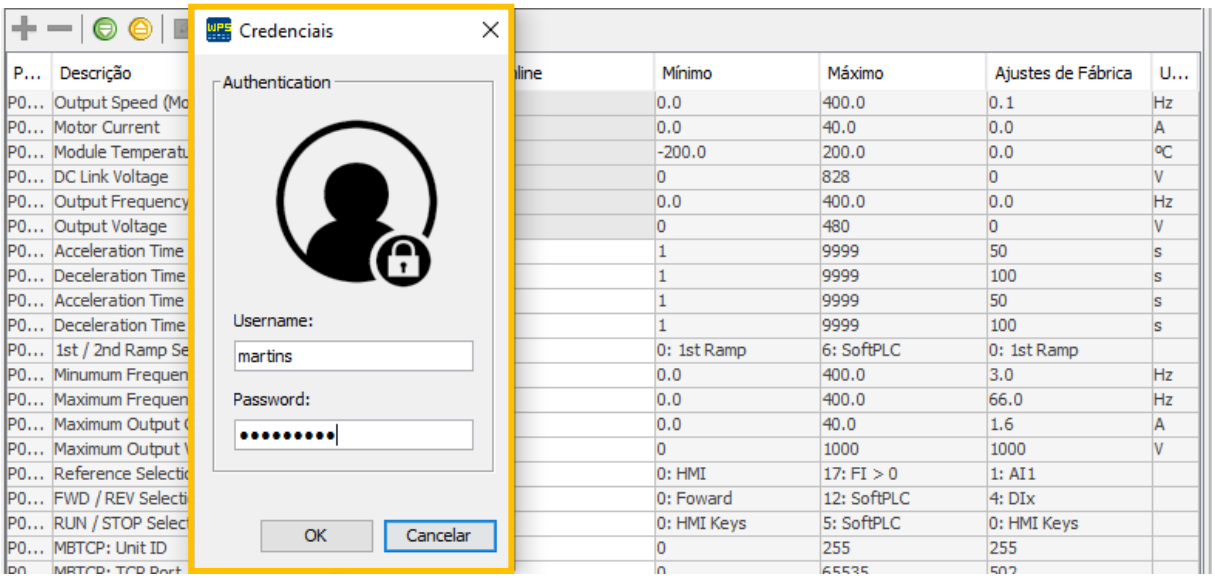
Fonte: Elaborado pelo autor.

Figura 92 – Programa WPS, alerta credenciais inválidas



Fonte: Elaborado pelo autor.

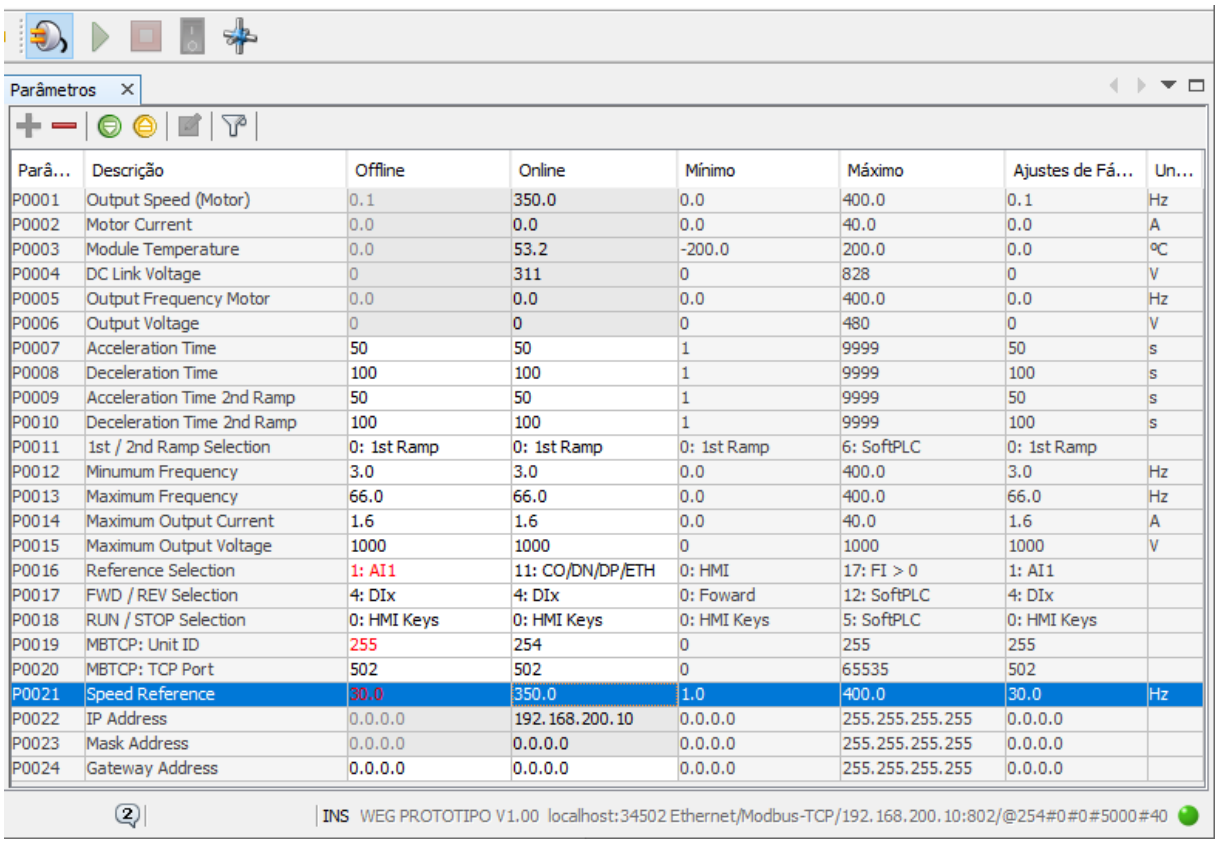
Figura 93 – Programa WPS, janela autenticação



Fonte: Elaborado pelo autor.

Caso o autenticador informado pelo usuário, seja validado pelo SSC, os parâmetros do protótipo são atualizados, na janela de monitoração de parâmetros (Figura 94). O usuário “martins” tem atribuída a sua conta uma função do tipo Admin com acesso total de escrita e leitura a todos os parâmetros do conversor. E consegue escrever o valor 350 no parâmetro 21, referência de velocidade.

Figura 94 – Programa WPS, monitoração dos parâmetros



Parâmetros

Parâ...	Descrição	Offline	Online	Mínimo	Máximo	Ajustes de Fá...	Un...
P0001	Output Speed (Motor)	0.1	350.0	0.0	400.0	0.1	Hz
P0002	Motor Current	0.0	0.0	0.0	40.0	0.0	A
P0003	Module Temperature	0.0	53.2	-200.0	200.0	0.0	ºC
P0004	DC Link Voltage	0	311	0	828	0	V
P0005	Output Frequency Motor	0.0	0.0	0.0	400.0	0.0	Hz
P0006	Output Voltage	0	0	0	480	0	V
P0007	Acceleration Time	50	50	1	9999	50	s
P0008	Deceleration Time	100	100	1	9999	100	s
P0009	Acceleration Time 2nd Ramp	50	50	1	9999	50	s
P0010	Deceleration Time 2nd Ramp	100	100	1	9999	100	s
P0011	1st / 2nd Ramp Selection	0: 1st Ramp	0: 1st Ramp	0: 1st Ramp	6: SoftPLC	0: 1st Ramp	
P0012	Minumum Frequency	3.0	3.0	0.0	400.0	3.0	Hz
P0013	Maximum Frequency	66.0	66.0	0.0	400.0	66.0	Hz
P0014	Maximum Output Current	1.6	1.6	0.0	40.0	1.6	A
P0015	Maximum Output Voltage	1000	1000	0	1000	1000	V
P0016	Reference Selection	1: AI1	11: CO/DN/DP/ETH	0: HMI	17: FI > 0	1: AI1	
P0017	FWD / REV Selection	4: DIx	4: DIx	0: Foward	12: SoftPLC	4: DIx	
P0018	RUN / STOP Selection	0: HMI Keys	0: HMI Keys	0: HMI Keys	5: SoftPLC	0: HMI Keys	
P0019	MBTCP: Unit ID	255	254	0	255	255	
P0020	MBTCP: TCP Port	502	502	0	65535	502	
P0021	Speed Reference	30.0	350.0	1.0	400.0	30.0	Hz
P0022	IP Address	0.0.0.0	192.168.200.10	0.0.0.0	255.255.255.255	0.0.0.0	
P0023	Mask Address	0.0.0.0	0.0.0.0	0.0.0.0	255.255.255.255	0.0.0.0	
P0024	Gateway Address	0.0.0.0	0.0.0.0	0.0.0.0	255.255.255.255	0.0.0.0	

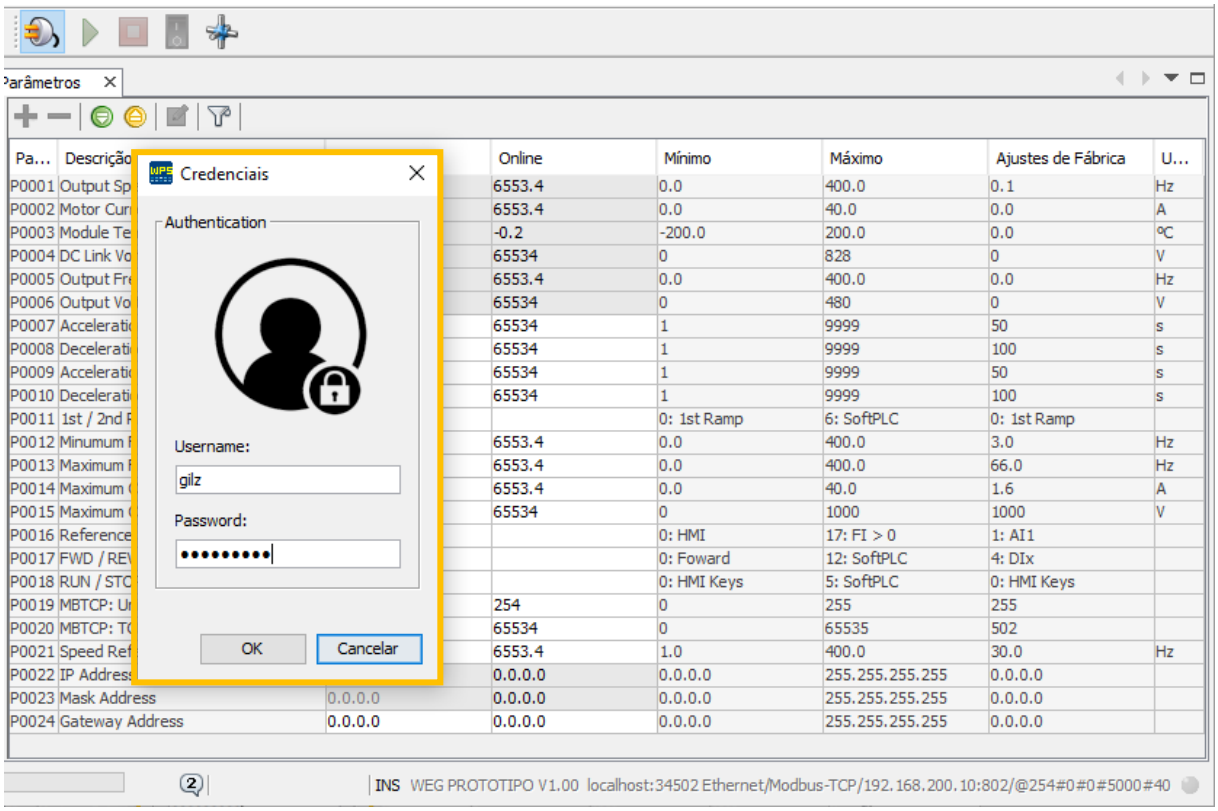
INS WEG PROTOTIPO V1.00 localhost:34502 Ethernet/Modbus-TCP/192.168.200.10:802/@254#0#0#5000#40

Fonte: Elaborado pelo autor.

Ao encerar a monitoração dos parâmetros do protótipo e iniciá-la novamente, através do botão de monitoração, uma nova janela de autenticação é apresentada. Desta vez, entra-se com o autenticador do usuário “gilz”, esta conta de usuário tem a função Operador, ou seja, somente acesso à leitura dos parâmetros (Figura 95)

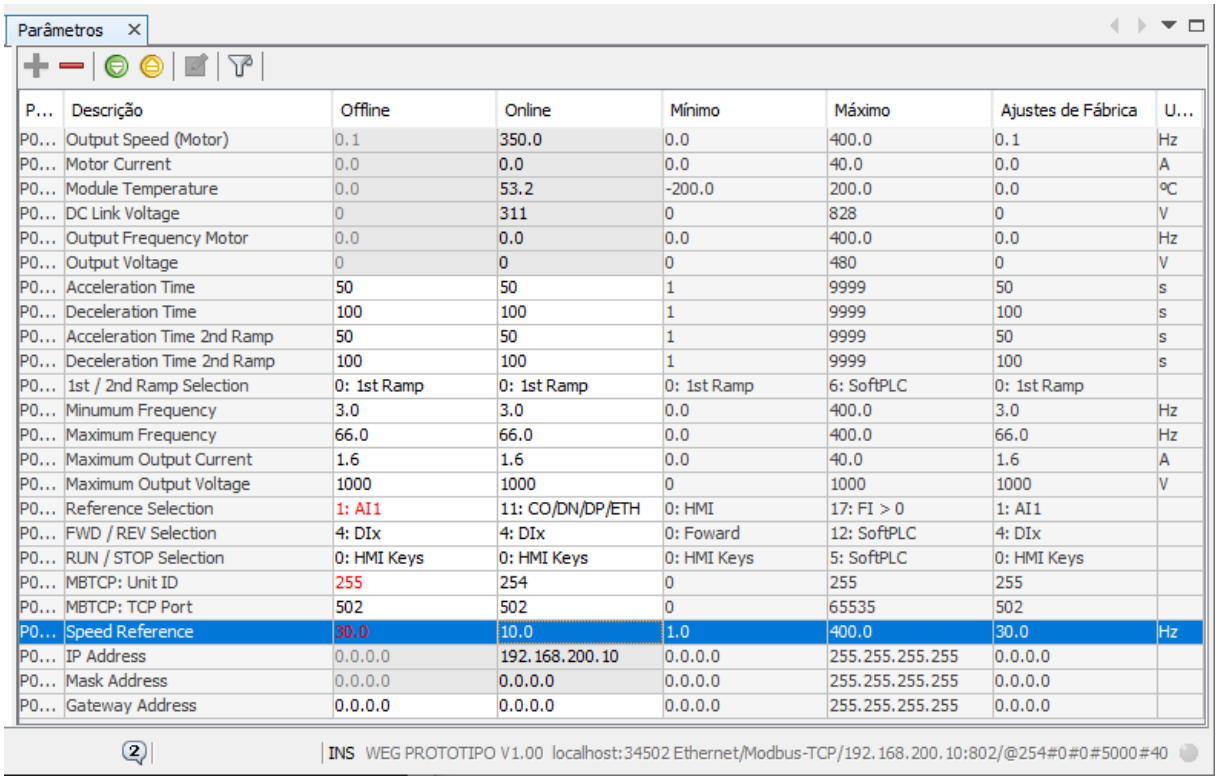
Uma vez autenticado o usuário “gilz” terá acesso total a leitura dos parâmetros, no entanto, não conseguirá alterar a referência de velocidade. Ao tentar alterar o parâmetro 21 para o valor 10, pode-se observar pela Figura 96, que o parâmetro 1, velocidade de saída continua com o valor 350, e o parâmetro 21 retornará para 350 no próximo ciclo de leitura realizado pelo WPS.

Figura 95 – Programa WPS, nova autenticação



Fonte: Elaborado pelo autor.

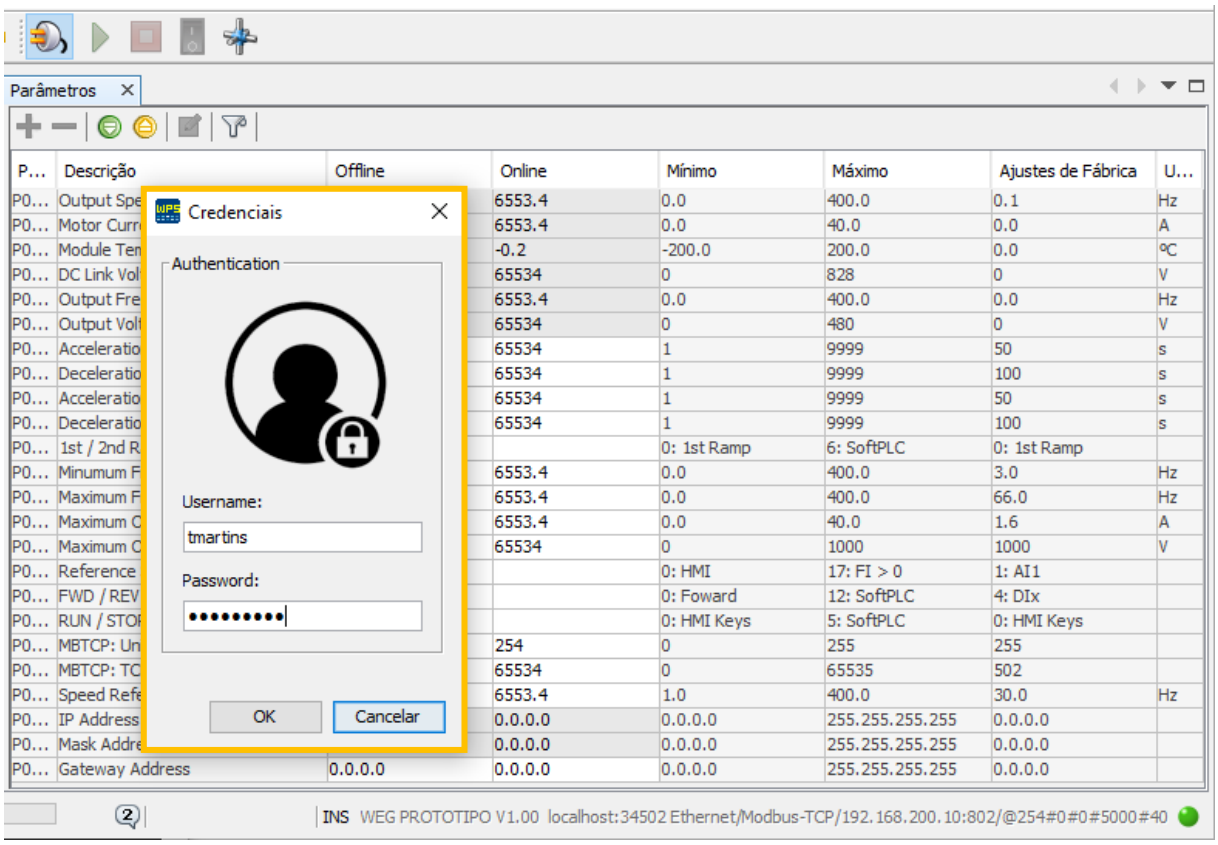
Figura 96 – Programa WPS, sem acesso de escrita



Fonte: Elaborado pelo autor.

Finalizando a monitoração e iniciando ela novamente, após um determinado período. Ao entrar novamente com o autenticador do usuário “martins” (Figura 97). O SSC identifica que o autenticador deste usuário está expirado, forçando-o a atualizá-lo.

Figura 97 – Programa WPS, nova autenticação após um determinado período



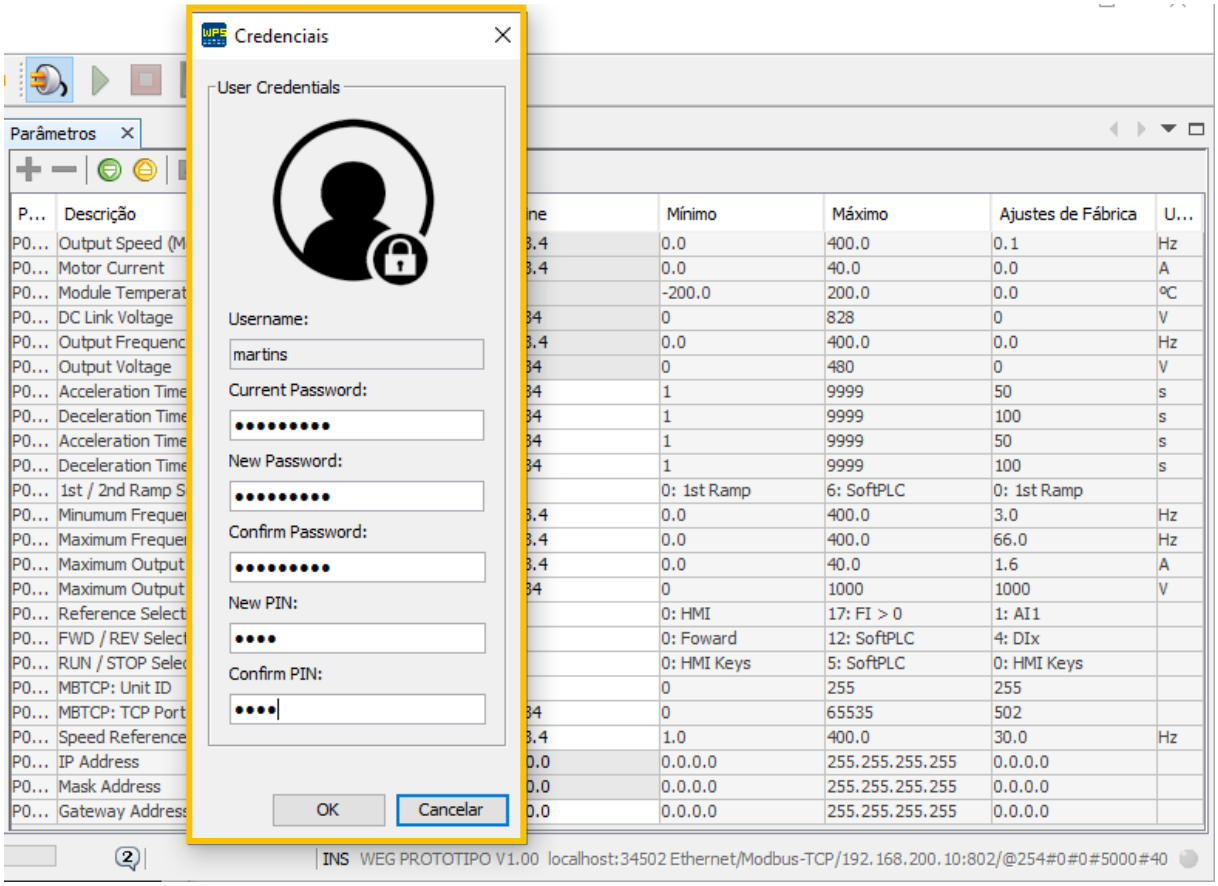
Fonte: Elaborado pelo autor.

Procedimento realizado através da janela apresentada na Figura 98. O usuário deverá entrar com sua senha atual e escolher uma nova senha e um PIN, para serem utilizados a partir de agora como autenticadores para a sua respectiva conta.

Se o usuário entrar com a senha atual incorreta ou com uma nova senha que não atenda as políticas de segurança configuradas para o SSC, o subsistema retornará uma exceção e uma nova janela de atualização de credenciais será disponibilizada para o usuário.

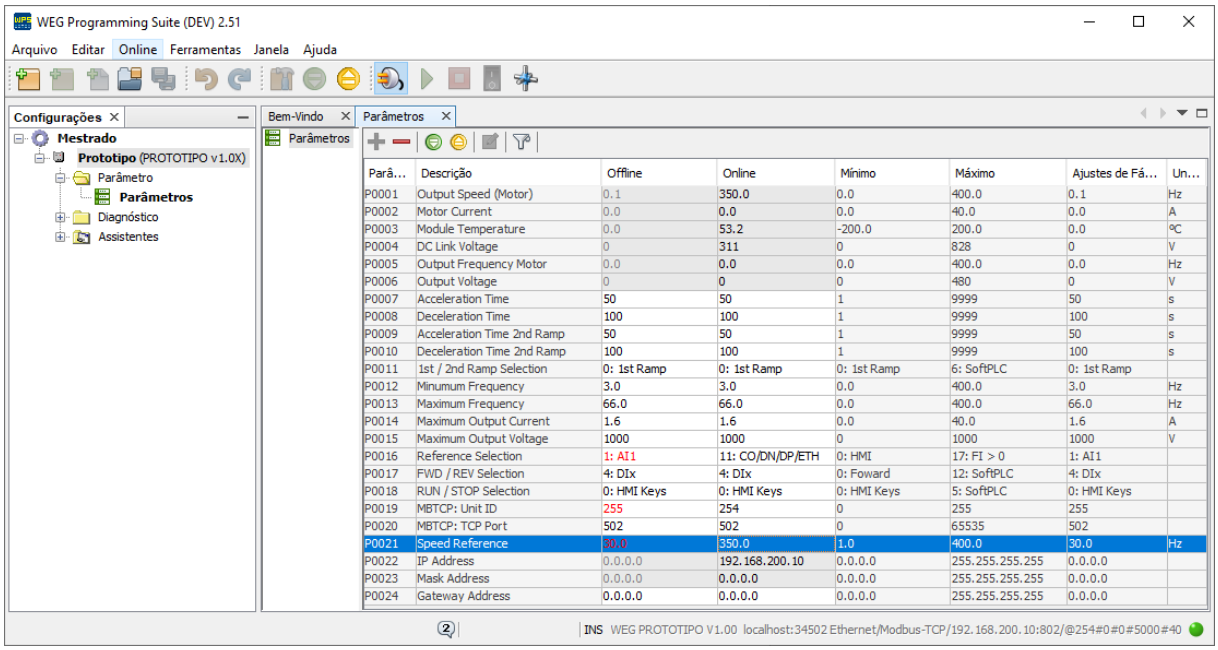
Como neste ensaio a senha atendeu a política de segurança, ou seja, foi atualizada com sucesso pelo SSC, o subsistema realiza a autenticação do determinado usuário na mesma requisição de atualização. E a janela de monitoração, com a informações dos parâmetros para o qual a função respectiva do usuário tem direito de acesso são mostradas (Figura 99).

Figura 98 – Programa WPS, janela atualizações de credenciais



Fonte: Elaborado pelo autor.

Figura 99 – Programa WPS, monitoração após atualização de credencial



Fonte: Elaborado pelo autor.

A Figura 100 apresenta os novos eventos de auditoria, gerados durante ensaio do controle de acesso autenticado junto ao programa WPS. O primeiro evento registrado pelo SSC, foi o evento de alerta (*warning*), registrado devido a falha de autenticação do usuário “martins”, pelo programa WPS no computador confiável com endereço IP 192.168.200.50. Na sequência os registros de informação: o primeiro registrando a autenticação com sucesso do usuário “martins”, o segundo informando que o parâmetro 21 foi alterador e um terceiro informando que uma nova autenticação foi realizada mais agora para o usuário “gilz”.

Ao realizar a nova autenticação com o usuário “martins”, houve a necessidade de atualizar as credenciais. Portanto, o SSC registou dois eventos de alerta, um informando que houve uma tentativa de autenticação com um autenticador expirado e outro informando que este autenticador foi atualizado com sucesso. Também no mesmo carimbo de tempo, foram registrados outros dois eventos informativos, um para informar que o usuário se autenticou com sucesso, ou seja, autenticou na mesma requisição de atualização e um último informando que o usuário “gilz” foi desregistrado da lista de identificadores registrados, ou seja, seu *hash* não será mais valido forçando-o a realizar uma nova autenticação.

Figura 100 – Eventos registrados durante ensaio com programa WPS

```
*April-5.log - Bloco de Notas
Arquivo  Editar  Formatar  Exibir  Ajuda
2021-04-05T14:16:35Z | WARNING | 0.0.0.0 | SYSTEM | The password of user martins5 was successfully reseted
2021-04-05T14:16:35Z | WARNING | 0.0.0.0 | SYSTEM | The user martins6 was successfully created
2021-04-05T14:16:35Z | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Users was successfully updated.
2021-04-05T14:16:35Z | WARNING | 0.0.0.0 | SYSTEM | System security configuration, Access list was successfully updated
2021-04-05T14:16:35Z | WARNING | 0.0.0.0 | SYSTEM | System security configuration was successfully updated
2021-04-05T14:21:13Z | CRITICAL | 192.168.200.100 | SYSTEM | The ip is trying to access, but it isn't in the Access List
2021-04-05T14:21:42Z | CRITICAL | 192.168.200.100 | SYSTEM | The ip is trying to access, but it isn't in the Access List
2021-04-05T22:56:36Z | INFO | 192.168.200.200 | SYSTEM | The ip 192.168.200.200 was successfully validated, role is 2 - Operador
2021-04-05T23:06:54Z | INFO | 192.168.200.210 | SYSTEM | The ip 192.168.200.210 was successfully validated, role is 4 - PLC
2021-04-05T23:07:32Z | INFO | 192.168.200.210 | SYSTEM | Write in parameter (netID) 21
2021-04-05T23:21:27Z | WARNING | 192.168.200.50 | SYSTEM | User martins authenticate fail, invalid password.
2021-04-05T23:22:06Z | INFO | 192.168.200.50 | SYSTEM | The user martins was successfully authenticated, role is 3 - Admin
2021-04-05T23:22:50Z | INFO | 192.168.200.50 | martins | Write in parameter (netID) 21
2021-04-05T23:24:09Z | INFO | 192.168.200.50 | SYSTEM | The user gilz was successfully authenticated, role is 2 - Operador
2021-04-05T23:27:27Z | WARNING | 192.168.200.50 | SYSTEM | The password of user martins is expired
2021-04-05T23:28:01Z | WARNING | 192.168.200.50 | SYSTEM | The password of user martins was successfully updated.
2021-04-05T23:28:01Z | INFO | 192.168.200.50 | SYSTEM | The user martins was successfully authenticated, role is 3 - Admin
2021-04-05T23:28:01Z | INFO | 192.168.200.50 | SYSTEM | The user gilz was unregistered
Ln 28, Col 87   100%   Windows (CRLF)   UTF-8
```

Fonte: Elaborado pelo autor.

Todas as mensagens trocadas entre o programa WPS e o protótipo durante este ensaio usavam criptografia através do protocolo TLS. A Figura 101 apresenta o processo de *handshake* e detalhes sobre a mensagem *Certificate*, enviada pelo servidor da conexão (protótipo) durante o *Server Hello*. Pode-se observar, que o algoritmo de criptografia utilizado foi o ECDSA-SHA384.

Figura 101 – Mensagens trocadas durante *handshake* do TLS

No.	Delta T	Source	Destination	Protocol	Length	Source	Destina	Info
7	0.010	192.168.200.50	192.168.200.10	TLSv1.2	198	55876	802	Client Hello
8	0.000	192.168.200.10	192.168.200.50	TLSv1.2	133	802	55876	Server Hello
10	0.000	192.168.200.10	192.168.200.50	TLSv1.2	818	802	55876	Certificate
13	0.155	192.168.200.10	192.168.200.50	TLSv1.2	238	802	55876	Server Key Exchange
15	0.000	192.168.200.10	192.168.200.50	TLSv1.2	63	802	55876	Server Hello Done
16	0.001	192.168.200.50	192.168.200.10	TLSv1.2	129	55876	802	Client Key Exchange
19	0.000	192.168.200.10	192.168.200.50	TLSv1.2	60	802	55876	Change Cipher Spec
21	0.000	192.168.200.10	192.168.200.50	TLSv1.2	139	802	55876	Encrypted Handshake Message
22	0.000	192.168.200.50	192.168.200.10	TLSv1.2	123	55876	802	Application Data
23	0.000	192.168.200.10	192.168.200.50	TLSv1.2	155	802	55876	Application Data
25	1.139	192.168.200.50	192.168.200.10	TLSv1.2	123	55876	802	Application Data

```
> Frame 10: 818 bytes on wire (6544 bits), 818 bytes captured (6544 bits) on interface \Device\NPF_{353
> Ethernet II, Src: Xilinx_00:01:02 (00:0a:35:00:01:02), Dst: RealtekS_68:3a:fb (00:e0:4c:68:3a:fb)
> Internet Protocol Version 4, Src: 192.168.200.10, Dst: 192.168.200.50
> Transmission Control Protocol, Src Port: 802, Dst Port: 55876, Seq: 80, Ack: 145, Len: 764
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 759
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 755
        Certificates Length: 752
      v Certificates (752 bytes)
          Certificate Length: 749
        v Certificate: 308202e93082026fa00302010202010300a06082a8648ce3d040303308189310b300906… (id
          > signedCertificate
          > algorithmIdentifier (ecdsa-with-SHA384)
```

Fonte: Elaborado pelo autor.

4.5 RESULTADOS

Conforme apresentado na Seção 1.4, o escopo do controle de acesso implementado neste trabalho antecedeu a publicação da IEC 62443-4-2, baseado no conceito Autenticação, Autorização e Auditoria (AAA). Porém, após se ter acesso a norma, verificou-se que seus requisitos fundamentais Identificação e Autenticação, Controle de uso e Respostas estavam alinhados.

A IEC 62443-4-2 qualifica o nível de segurança alcançado pelo componente, através dos quatro níveis de segurança por esta especificados para cada um dos seus requisitos fundamentais. A Tabela 4, visa apresentar estes níveis e suas características de forma geral.

Por exemplo, se todos os requisitos de componente (CRs) e os requisitos específicos para dispositivos embarcado (EDRs) do nível de segurança SL 1 forem alcançados, de acordo com a norma pode-se considerar, que o componente estará protegido contra tentativas de uso e acesso não autorizados casuais, utilizando meios simples, baixo nível de recursos, conhecimento genérico em IACS e baixa motivação.

Tabela 4 – Níveis de segurança especificados pela IEC 62443-4-2

Nível de segurança	Acesso não autorizado	Meios de ataque	Nível de Recursos	Habilidade em IACS	Motivação
SL 1	Casual	Simples	Baixos	Genérica	Baixa
SL 2	Intencional	Simples	Baixos	Especifica	Baixa
SL 3	Intencional	Sofisticados	Moderados	Especifica	Moderada
SL 4	Intencional	Sofisticados	Avançados	Especifica	Alta

Fonte: Adaptado de IEC. [6]

Com o intuito de quantificar e qualificar os resultados alcançados, estes são apresentados em relação aos requisitos fundamentais (FRs). A Tabela 5 apresenta o resultado para o requisito fundamental controle de identificação e autenticação. No qual este trabalho atendeu 100% dos requisitos especificados para os níveis de segurança SL 1 e SL 2, 84% para o SL 3 e 85% dos requisitos especificados para o nível máximo de segurança (SL 4) especificado pela IEC 62443-4-2.

Tabela 5 – FR 1, Controle de identificação e autenticação

Requisito	Descrição	SL 1	SL 2	SL 3	SL 4
CR 1.1	Identificação e autenticação de usuários humanos	Sim	Sim	Sim	Sim
CR 1.1 (1)	Identificação e autenticação única para usuários humanos	-	Sim	Sim	Sim
CR 1.1 (2)	Autenticação multifator para todas as interfaces	-	-	Não	Não
CR 1.2	Identificação e autenticação de dispositivos e processos	-	Sim	Sim	Sim
CR 1.2 (1)	Identificação e autenticação única	-	-	Não	Não
CR 1.3	Gerenciamento de contas	Sim	Sim	Sim	Sim
CR 1.4	Gerenciamento do identificador	Sim	Sim	Sim	Sim
CR 1.5	Gerenciamento do autenticador	Sim	Sim	Sim	Sim
CR 1.5 (1)	Segurança baseada hardware para autenticadores	-	-	Não	Não
CR 1.7	Força da autenticação baseada em senha	Sim	Sim	Sim	Sim
CR 1.7 (1)	Gerador de senha e expiração da senha para humanos	-	-	Sim	Sim
CR 1.7 (2)	Expiração de senha para todos tipos de usuários	-	-	-	Sim
CR 1.8	Certificados PKI	-	Sim	Sim	Sim
CR 1.9	Força da autenticação baseada em PKI	-	NA	NA	NA
CR 1.9 (1)	Segurança baseada em hardware para PKI	-	-	NA	NA
CR 1.10	Feedback do autenticador	Sim	Sim	Sim	Sim
CR 1.11	Tentativa de autenticação sem sucesso	Sim	Sim	Sim	Sim
CR 1.12	Notificação de uso do sistema	NA	NA	NA	NA
CR 1.14	Força da autenticação baseada em chaves simétricas	-	NA	NA	NA
CR 1.14 (1)	Segurança baseada em hardware para chaves simétricas	-	-	NA	NA
%	Porcentagem de cobertura por nível de segurança	100%	100%	84%	85%

Fonte: Adaptado de IEC. [6]

A identificação de usuários foi realizada em combinação com mecanismos de autenticação para implementar o controle de acesso ao conversor. Esta verificação se fez necessária, para evitar o acesso por usuários não autorizados. Conforme descrito neste trabalho, todos os usuários humanos são identificados e autenticados através do *software* WPS ou da HMI, bem como, são identificados os demais dispositivos e tecnologias de comunicação.

O gerenciamento das contas é realizado nativamente pelo SSC, que utiliza como identificador, o nome do usuário ou um identificador da tecnologia, por exemplo endereço IP. O autenticador suporta mudanças, gerencia novas contas e impõe políticas de segurança, mascarando as informações das credencias durante sua utilização.

Certificados de infraestrutura de chave pública foram usados de acordo com padrões internacionalmente reconhecidos, foi utilizado em conjunto com o protocolo TLS 1.2 e sua chave privada armazenada com base no conceito de RoT. Como chaves públicas e simétricas não são utilizadas para autenticação, considera-se que o SSC cobriu tais requisitos, pois a norma especifica requisitos para quando estes são utilizados. Quanto aos certificados PKI, emprega-se o uso de certificados com prazo de validade limitado. Opção especificada pela norma, para casos nos quais a capacidade de revogação não é fornecida.

Após identificar e autenticar cada usuário, o SSC restringi as ações permitidas ao uso autorizado do conversor. O requisito fundamental controle de uso, protege o conversor contra ações não autorizadas, verificando se os privilégios necessários foram concedidos, antes de permitir que um usuário execute tais ações. Para este FR conforme Tabela 6, este trabalho atendeu 100% dos requisitos especificados para o nível de segurança SL 1, 87% para SL 2, 68% para o SL 3 e 57% para o SL 4.

A aplicação de autorização para todos usuários do conversor, com base na regra do privilégio mínimo para a atribuição das suas responsabilidades, garante o controle de uso para todos os usuários e o não repúdio aos usuários autenticados, fornecendo a capacidade de determinar se um determinado usuário humano executou tal ação. Funções não são limitadas às hierarquias aninhadas e fixas, nas quais, faz parte de função de nível superior, um conjunto de uma função menos privilegiada. As regras das funções criadas no SSC, podem ser customizadas para melhor coerência com a atividade fim do usuário. O bloqueio de sessão de usuário, protege contra acesso posterior, após um período de inatividade configurável, e permanece em vigor até que o usuário humano desta sessão, ou outro usuário humano autorizado, restabeleça o acesso usando procedimentos apropriados de identificação e autenticação.

Eventos relevantes para auditoria sobre a segurança cibernética do conversor são armazenados, com carimbos de data e hora, possibilitando a auditoria futura. Para isto, diariamente são criados arquivos, que são sobrescritos anualmente ou de forma antecipada, caso seja alcançada a capacidade total de armazenamento destinada para o registro destes eventos.

Tabela 6 – FR 2, Controle de uso

Requisito	Descrição	SL 1	SL 2	SL 3	SL 4
CR 2.1	Aplicação de autorização	Sim	Sim	Sim	Sim
CR 2.1 (1)	Aplicação de autorização para todos tipos de usuários	-	Sim	Sim	Sim
CR 2.1 (2)	Mapeamento de permissão para funções	-	Sim	Sim	Sim
CR 2.1 (3)	Substituição do supervisor	-	-	Não	Não
CR 2.1 (4)	Dupla aprovação	-	-	-	Não
CR 2.2.	Controle de uso sem fio	NA	NA	NA	NA
CR 2.3	Controle de uso para dispositivos móveis e portáveis	-	-	-	-
EDR 2.4	Código móvel	NA	NA	NA	NA
EDR 2.4 (1)	Verificação de autenticidade do código móvel	-	NA	NA	NA
CR 2.5	Bloqueio de sessão	Sim	Sim	Sim	Sim
CR 2.6	Encerramento de sessão remota	-	Sim	Sim	Sim
CR 2.7	Controle de sessões concorrentes	-	-	Não	Não
CR 2.8	Eventos auditáveis	Sim	Sim	Sim	Sim
CR 2.9	Capacidade de armazenamento para auditoria	Sim	Sim	Sim	Sim
CR 2.9 (1)	Avisar quando o limite de capacidade for atingido	-	-	Não	Não
CR 2.10	Resposta a falhas de processamento de auditoria	Sim	Sim	Sim	Sim
CR 2.11	Carimbo de tempo	Sim	Sim	Sim	Sim
CR 2.11 (1)	Sincronização de tempo	-	Não	Não	Não
CR 2.11 (2)	Proteção da integridade da fonte de tempo	-	-	-	Não
CR 2.12	Não repúdio	Sim	Sim	Sim	Sim
CR 2.12 (1)	Não repúdio para todos os tipos de usuários	-	-	-	Não
EDR 2.13	Uso de interface de teste e diagnostico físico	-	Não	Não	Não
EDR 2.13 (1)	Monitoração ativa	-	-	Não	Não
%	Porcentagem de cobertura por nível de segurança	100%	87%	68%	59%

Fonte: Adaptado de IEC. [6]

Finalmente, a acessibilidade destes eventos foi projetada para ser realizada através do recurso de *upload* do *software* WPS. O que garante ao trabalho nível de segurança SL 1 para o requisito fundamental resposta a eventos, cobertura de 50% dos requisitos para o nível de segurança SL 2 e 33% para os níveis SL 3 e SL 4 (Tabela 7).

Tabela 7 – FR 6, Resposta a eventos

Requisito	Descrição	SL 1	SL 2	SL 3	SL 4
CR 6.1	Acessibilidade dos eventos de auditoria	Sim	Sim	Sim	Sim
CR 6.1 (1)	Acesso programático a registros de auditoria	-	-	Não	Não
CR 6.2	Monitoração continua	-	Não	Não	Não
%	Porcentagem de cobertura por nível de segurança	100%	50%	33%	33%

Fonte: Adaptado de IEC. [6]

O resultado consolidado junto ao resultado individual de cada requisito fundamental é apresentado na Tabela 8. Conforme pode ser observado, considera-se que o SSC proposto neste trabalho, apresenta 72% de aderência ao nível de segurança SL 1, 61% para o SL 2, 51% para o SL 3 e 49% para o nível máximo de segurança (SL 4) especificado pela IEC 62443-4-2. Por não estarem diretamente relacionados ao escopo deste trabalho, os demais requisitos fundamentais com seus CRs e EDRs são detalhados no ANEXO C.

Tabela 8 – Resultado consolidado dos requisitos fundamentais

Requisito	Descrição	SL 1	SL 2	SL 3	SL 4
FR 1	Controle de identificação e autenticação	100%	100%	84%	85%
FR 2	Controle de uso	100%	87%	68%	59%
FR 3	Integridade do Sistema	33%	28%	25%	23%
FR 4	Confidencialidade dos dados	100%	67%	40%	40%
FR 5	Fluxo de dados restrito	0%	0%	0%	0%
FR 6	Resposta a eventos	100%	50%	33%	33%
FR 7	Disponibilidade de recurso	50%	33%	30%	30%
%	Porcentagem de cobertura por nível de segurança	72%	61%	51%	49%

Fonte: Adaptado de IEC. [6]

5 CONCLUSÃO

Com a evolução industrial (indústria 4.0) e devido a transformação digital, conversores e demais ativos que compõe um sistema de automação e controle industrial, estão cada vez mais sofisticados, conectados e monitorados. No entanto, incidentes cibernéticos na infraestrutura de tecnologia operacional estão cada vez mais recorrentes, ao mesmo tempo que conversores estáticos continuam com controles de acessos simples e disponibilizam suporte a protocolos industriais que não contemplam segurança cibernética.

O presente trabalho teve como objetivo principal estudar a segurança cibernética para a área de eletrônica de potência na era da Indústria 4.0 e sua aplicabilidade em conversores estáticos aplicados em acionamentos elétricos.

A validação do conceito de raiz de confiança (RoT), com a inicialização segura, através da verificação da assinatura do *firmware* principal e do armazenamento seguro das chaves criptográficas, possibilitou maior confidencialidade e integridade ao dispositivo e a construção de um canal de comunicação seguro, com a utilização dos protocolos TLS e Modbus.

O modelo de controle de acesso proposto, baseado em funções (RBAC), possibilitou o controle de uso e a segregação dos direitos de acesso, a customização com a possibilidade de se criar perfis de acordo com a função de cada usuário ou dispositivo no IACS e escalabilidade, devido aos direitos de acesso estarem atribuídos a funções e estas poderem ser atribuídas a uma quantidade significativa de usuários.

Os ensaios realizados e apresentados, evidenciaram a fragilidade do controle de acesso atual e validaram que o controle de acesso proposto, elevou a maturidade da segurança cibernética do conversor, tanto para usuários autenticados através do programa WPS, quanto para demais dispositivos conectados através do protocolo de comunicação Modbus/TCP.

Limitações foram identificadas devido ao gerenciamento de contas realizada de forma nativa pelo conversor, o modelo proposto e implementado pode se tornar complexo e resultar em vulnerabilidades, caso seja aplicado para um IACS com uma quantidade significativa de conversores. Deste modo faz-se necessária, sua evolução para um gerenciamento de contas centralizado, junto ao controle da identidade do conversor e o uso de tecnologias de hardware como o TPM. A possiblidade de criar e atribuir funções especificas para identificadores de dispositivos não autenticados, como para o caso do endereço IP do protocolo Modbus/TCP, permite o controle de uso destes dispositivos, mas não impedem que estes sejam vulneráveis a ataques de **spoofing**. Sendo assim, cabe a cada usuário administrador, criar e aplicar funções

especificas que limitam o acesso do determinado dispositivo, com base no princípio do menor privilégio.

Independentemente destas limitações, conclui-se que os objetivos específicos propostos para este trabalho foram alcançados, bem como, os resultados obtidos demostram aderência a norma IEC 62443-4-2, o que possibilita no futuro a busca pela sua conformidade.

5.1 TRABALHOS FUTUROS

Conforme apresentado por este trabalho a segurança cibernética não é um estado binário, precisa ser contínua, pois nunca um sistema estará totalmente protegido contra ameaças cibernéticas. Neste contexto nesta seção são apresentadas sugestões para a evolução de trabalhos que visam a segurança cibernética na área de eletrônica de potência e em conversores estáticos:

a) estudo e desenvolvimento de um sistema controle de acesso centralizado para aplicação a conversores estáticos, deve-se levar em consideração que conversores aplicados em acionamentos elétricos nem sempre estarão 100% do tempo conectados a redes de comunicação;
b) estudo de soluções de segurança baseada em *hardware* para a construção de mecanismos de segurança cibernética, comparando-as com as soluções de *software* desenvolvidas;
c) estudo da inicialização segura medida, verificação das funcionalidades de segurança e a integridade da informação continua após a inicialização do sistema;
d) estudo da proteção física do conversor, controle das interfaces para periféricos e acessórios (serial, USB, etc), visando impedir a conexão não autorizada de periféricos, detectar e relatar qualquer alteração no *hardware* e bloquear a instalação de componentes não homologados;
e) estudo de mecanismos para detecção e proteção contra ataques cibernéticos e de negação de serviço (DoS), desenvolvimento de saídas determinísticas, garantindo um estado mínimo de funcionamento para o conversor mesmo sob ataque;
f) estudo sobre *shack attack*, ataque com equipamentos de baixo custo, tendo acesso físico ao conversor no qual pode-se depurar através da interface JTAG, escanear I/O, etc;
g) estudo sobre *lab attack*, no qual utilizam-se laboratórios, com equipamentos especiais, possibilitando a engenharia reversa do dispositivo.

REFERÊNCIAS

[1] 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.

[2] 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.

[3] INDUSTRIAL INTERNET CONSORTIUM. **Industrial Internet of Things Volume G4:** Security Framework. Ind. Internet Consort, p. 1-173, 2016.

[4] 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.

[5] SANS. **About SANS Institute.** Disponível em: https://www.sans.org/about/?msc=main-nav. Acesso em: 25 jan. 2021.

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443-4-2: Security for industrial automation and control systems-Part 4-2: Technical security requirements for IACS components. 1.0 ed. Geneva: Iec, 2019.

[7] FILKINS, Barbara; WYLIE, Doug; DELY, A. J. Sans 2019 state of ot/ics cybersecurity survey. **SANS Technology Institute**, 2019

[8] BASSETT, Gabriel et all. 2020 Data Breach Investigations Report. **Verizon RISK Team,** 2020.

[9] FYRBIAK, Marc et al. Hardware reverse engineering: Overview and open challenges. In: **2017 IEEE 2nd International Verification and Security Workshop (IVSW)**. IEEE, 2017. p. 88-94.

[10] BECKER, Steffen et al. An exploratory study of hardware reverse engineering—technical and cognitive processes. In: **Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020).** 2020. p. 285-300.

[11] MARTINS, Tiago; OLIVEIRA, Sérgio Vidal Garcia. Cybersecurity in the Power Electronics. **IEEE Latin America Transactions**, v. 17, n. 08, p. 1300-1308, 2019.

[12] HARTMANN, Brian; KING, William P.; NARAYANAN, Subu. Digital manufacturing: The revolution will be virtualized. McKinsey Digital, ago. 2015.

[13] WEG. **WEG Drive Scan**. Disponível em: https://www.weg.net/catalog/weg/BR/pt/Automa%C3%A7%C3%A3o-e-Controle-Industrial/Dispositivos-para-Conectividade-e-Monitoramento/Gateways-e-Edge-Devices/WEG-Drive-Scan/WEG-Drive-Scan-para-Baixa-Tens%C3%A3o/WCD-ED300-DSLV/p/MKT_WDC_BRAZIL_EDGE_DEVICE_DRIVE_SCAN_BT. Acesso em: 01 mar. 2020.

[14] ABB. **ABB Ability Condition Monitoring for drives**. Disponível em: https://new.abb.com/drives/services/advanced-services/condition-monitoring. Acesso em: 24 nov. 2020.

[15] SIEMENS. **Drive technology is now going digital**. Disponível em: https://new.siemens.com/global/en/products/drives/digitalization-in-drive-technology.html. Acesso em: 29 nov. 2020.

[16] YÜLEK, Murat A. The industrialization process: A streamlined version. **How Nations Succeed: Manufacturing, Trade, Industrial Policy, and Economic Development.** Palgrave Macmillan, Singapura, 2018, p. 171-182.

[17] ACETO, Giuseppe; PERSICO, Valerio; PESCAPE, Antonio. A survey on information and communication technologies for Industry 4.0: state-of-the-art, taxonomies, perspectives, and challenges. **IEEE Communications Surveys & Tutorials**, v. 21, n. 4, p. 3467-3501, 2019.

[18] RÜßMANN, Michael et al. Industry 4.0: The future of productivity and growth in manufacturing industries. **Boston Consulting Group**, v. 9, n. 1, p. 54-89, 2015.

[19] THAMES, Lane; SCHAEFER, Dirk. Software-defined cloud manufacturing for industry 4.0. **Procedia CIRP**, v. 52, p. 12-17, 2016.

[20] COSTA, Cesar da. Indústria 4.0: o futuro da indústria nacional. **POSGERE – Pós-Graduação em Revista**, vol. 1, nº 4, pp. 5-14, 2017.

[21] MONOSTORI, László et al. Cyber-physical systems in manufacturing. **Cirp Annals**, v. 65, n. 2, p. 621-641, 2016.

[22] LOPEZ, Javier; RUBIO, Juan E. Access control for cyber-physical systems interconnected to the cloud. **Computer Networks**, v. 134, p. 46-54, 2018.

[23] ZHOU, Keliang; LIU, Taigang; ZHOU, Lifeng. Industry 4.0: Towards future industrial opportunities and challenges. In: **2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)**. IEEE, 2015. p. 2147-2152.

[24] ROBLEK, Vasja; MEŠKO, Maja; KRAPEŽ, Alojz. A Complex View of Industry 4.0. **Sage Open**, v. 6, n. 2, abr. 2016. SAGE Publications. http://dx.doi.org/10.1177/2158244016653987.

[25] POSADA, Jorge et al. Visual computing as a key enabling technology for industrie 4.0 and industrial internet. **IEEE computer graphics and applications**, v. 35, n. 2, p. 26-40, 2015.

[26] WEYRICH, Michael; EBERT, Christof. Reference architectures for the internet of things. **IEEE Software**, v. 33, n. 1, p. 112-116, 2015.

[27] ITU-T. Y.2060: Overview of the Internet of things 2013. **Telecommunication Standardization Sector of ITU.** 2012. Disponível em: https://www.itu.int/rec/T-REC-Y.2060-201206-I/en. Acesso em 20 setembro 2019.

[28] INDUSTRIAL INTERNET CONSORTIUM. **Industrial Internet.** 2015. Disponível em: https://www.iiconsortium.org/images/case-study-posters/Industrial-Internet-Infographic.jpg. Acesso em 20 set. 2019.

[29] DE CARVALHO, Daniel Mendes. Sistema de Segurança para Ambientes com Atmosfera Explosiva. **Revista Brasileira de Mecatrônica**, v. 1, n. 2, p. 14-25, 2018.

[30] MUNDIAL, Foro Económico. Global risks report 2019. **Ginebra: Foro Económico Mundial**, 2019

[31] WILBANKS, Linda. Cybersecurity: Welcome to my world. **IT Professional**, v. 9, n. 2, p. 61-64, 2007.

[32] MEULENBROEK, H et al. Cyber security in energy automation. **Petroleum and Chemical Industry Conference Europe (PCIC Europe)**. 2018.

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

[34] BROCKLEHURST, Katherine. **CRASHOVERRIDE**: First Malware Platform Designed to Take Down Electric Grids. Belden. v. 9, 2017. Disponível em: https://www.belden.com/blog/industrial-security/crashoverride-first-malware-platform-designed-to-take-down-electric-grids. Acesso em: 20 ago. 2018.

[35] Cherepanov, Anton. **GREYENERGY**: A successor to BlackEnergy. ESET. 2018. Disponível em: https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf. Acesso em: 09 out. 2020.

[36] CHEN, Ping; DESMET, Lieven; HUYGENS, Christophe. A study on advanced persistent threats. In: **IFIP International Conference on Communications and Multimedia Security**. Springer, Berlin, Heidelberg, 2014. p. 63-72.

[37] SCHWAB, Wolfgang; POUJOL, Mathieu. **The State of Industrial Cybersecurity 2018**, KASPERSKY. 2018. Disponível em: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf. Acesso em: 23 ago. 2019.

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

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

[40] MILLER, Charlie; VALASEK, Chris. Remote exploitation of an unaltered passenger vehicle. **Black Hat USA**, v. 2015, p S 91, 2015.

[41] VERA, Amir; LYNCH, Jamiel; CARREGA, Christina. **Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says**. 2021. CNN. Disponível em: https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html. Acesso em: 09 abr. 2021.

[42] NEWMAN, Lily Hay. **That Dallas Siren Hack Wasn't Novel, It Was Just Really Loud**: emergency alert systems get hacked all the time. consider this one a wake-up call. Emergency alert systems get hacked all the time. Consider this one a wake-up call. 2017. WIRED. Disponível em: https://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud/. Acesso em: 04 out. 2020.

[43] SHOHET, Yoni. **Ransomware Attacks Hit Manufacturing – Are You Vulnerable?**: Norsk Hydro is latest victim.. Norsk Hydro is latest victim. 2019. Industry Week. Disponível em: https://www.industryweek.com/technology-and-iiot/article/22027363/ransomware-attacks-hit-manufacturing-are-you-vulnerable. Acesso em: 05 out. 2020.

[44] GEIGER, Marcus et al. An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. **25th IEEE INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGIES AND FACTORY AUTOMATION (ETFA)**, 25., 2020, Vienna, Austria. 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). S.L.: IEEE, 2020. p. 1537-1543.

[45] HOFFMAN, Mike; WINSTON, Tom. **Recommendations Following the Colonial Pipeline Cyber Attack**. Dragos Blog. Disponível em: https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/. Acesso em: 10 maio 2021.

[46] TI SAFE. **Ministério de Minas e Energia cria grupo de trabalho para discutir segurança cibernética no setor elétrico**. 2021. Disponível em: https://www.tisafe.com/index.php/pt-br/blog/item/469-ministerio-de-minas-e-energia-cria-grupo-de-trabalho-para-discutir-seguranca-cibernetica-no-setor-eletrico. Acesso em: 09 abr. 2021.

[47] INDUSTRIAL INTERNET CONSORTIUM. **About Industrial Internet Consortium.** 2018. Disponível em: https://www.iiconsortium.org/about-us.htm. Acesso em 5 out. 2018.

[48] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001:2013:** Information technology-Security techniques-Information security management systems-Requirements.. International Organization for Standardization, 2013.

[49] INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 62443-2-4**: Security for industrial automation and control systems-Part 2-4: Security program requirements for IACS service providers. 1.1 ed. Geneva: Iec, 2017.

[50] INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 62443-4-1**: Security for industrial automation and control systems-Part 4-1: Secure product development lifecycle requirements 1.0 ed. Geneva: Iec, 2018.

[51] INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC/TS 62443-1-1**: Preview of Security for industrial automation and control systems-Part 1-1: Terminology, concepts and models. 1.0 ed. Geneva: Iec, 2009. Disponível em:

https://webstore.iec.ch/preview/info_iects62443-1-1%7Bed1.0%7Den.pdf. Acesso em: 20 abr. 2021.

[52] INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 62443-3-3**: Security for industrial automation and control systems-Part 4-2: System security requirements and security levels. 1.0 ed. Geneva: Iec, 2013.

[53] REGULATION, **General Data Protection. Regulation EU 2016/679**. European Parliament and of the Council of 27 April 2016. Official Journal of the European Union. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 7 nov. 2018.

[54] GOVERNMENT OF CANADA. **Personal Information Protection and Electronic Documents** Act S.C. 2000, c. 5, 2000. Justice Laws Website**.** Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html. Acesso em: 18 out 2018.

[55] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais**.** Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 out. 2020.

[56] AICPA. **SOC for Service Organizations: Information for Service Organizations**. Disponível em: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganizationsmanagement.html. Acesso em: 26 mar. 2021.

[57] SCHOLTEN, Bianca. **The road to integration**: a guide to applying the isa-95 standard in manufacturing. EUA: INTERNATIONAL SOCIETY OF AUTOMATION. 2017, Cap. 1. p. 25-64.

[58] ZHAO, Kai; GE, Lina. A survey on the internet of things security. In: **2013 Ninth international conference on computational intelligence and security**. IEEE, 2013. p. 663-667.

[59] AL-OMARY, Alauddin et al. Survey of hardware-based security support for IoT/CPS systems. **KnE Engineering**, p. 52–70-52–70, 2018.

[60] ARM. **ARM Security Technology**: building a secure system using trustzone technology. Building a Secure System using TrustZone Technology. 2009. Disponível em: https://documentation-service.arm.com/static/5f1ffa25bb903e39c84d7e98?token=. Acesso em: 21 mar. 2020. ARM, Building a Secure System using TrustZone Technology, 2009.

[61] BOTTENBERG, Agknaton Luís. **Conversor matricial indireto para acionamento de motor de indução trifásico.** 2010. 115 f. Dissertação (Mestrado) – Curso de Mestrado em Engenharia Elétrica, Universidade Regional de Blumena, Blumenau, 2010. Disponível em: https://bu.furb.br//docs/DS/2010/348555_1_1.pdf. Acesso em: 25 abr. 2020.

[62] WEG. **História**. Disponível em: https://www.weg.net/institutional/BR/pt/history. Acesso em: 04 mar. 2021.

[63] WEG. **Inversor de frequência CFW300**: manual do usuário. Jaraguá do Sul: Weg, 2019. Disponível em: https://static.weg.net/medias/downloadcenter/hce/h5d/WEG-CFW300-user-manual-10003325037-en-es-pt.pdf. Acesso em: 12 out. 2019.

[64] SMA. **Whitepaper Cyber Security**: statement by sma solar technology ag on the cyber security of pv inverters (horus scenario). Disponível em: https://www.sma.de/fileadmin/content/global/specials/documents/cyber-security/Whitepaper-Cyber-Security-AEN1732_07.pdf. Acesso em: 24 mar. 2020.

[65] NIST. **Framework for Improving Critical Infrastructure Cybersecurity**. 2018. National Institute of Standards and Technology. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Acesso em: 04 abr. 2020.

[66] DANFOSS. **Programming Guide VLT AQUA Drive FC 202**. Disponível em: https://files.danfoss.com/download/Drives/MG20OB02.pdf. Acesso em: 23 nov. 2020.

[67] ABB. **Programa primário de controlo do ACS880**: manual de firmware. Manual de firmware. Disponível em: https://library.e.abb.com/public/43143ff588034177b547709747fdb136/PT_ACS880_FW_manual_T_A4.pdf?x-sign=POsbUtymx5y8A+4uJhfBEp4PcUhwLEScyztrytJmU9mene2ilPUUfD1n/FhuQfSa. Acesso em: 24 nov. 2020.

[68] YASKAWA. **YASKAWA AC Drive GA700 Technical Manual**. Disponível em: https://www.no.yaskawa.eu.com/Global%20Assets/Downloads/Technical_Documentation/Inverter_Drives/GA700/TOEP_C710617_17D_GA700_InitSteps_EN.pdf.

[69] SMA. **Public Cyber Security**: guidelines for a secure pv system communication. Guidelines for a Secure PV System Communication. Technical Information. Disponível em: https://files.sma.de/downloads/CyberSecurity-TI-en-10.pdf. Acesso em: 05 abr. 2020.

[70] SIEMENS. **SINAMICS G120 Smart Access**: Operating instructions. Siemens. 2018. Disponível em: https://cache.industry.siemens.com/dl/files/122/109758122/att_953519/v1/G120_smart_access_op_instr_0418_en-US.pdf. Acesso em: 06 maio 2020.

[71] HUAWEI. **User Manual**: smartlogger3000. SmartLogger3000. Huawei Technologies. 2021. Disponível em: https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100108365&partNo=6001&mid=SUPE_DOC&_t=1616594032000. Acesso em: 1 abr. 2021.

[72] ROCKWELL AUTOMATION. **Rockwell Automation Improves Security, Performance and Commissioning with PowerFlex 755T AC Drive Enhancements**. Disponível em: https://ir.rockwellautomation.com/press-releases/press-releases-details/2021/Rockwell-Automation-Improves-Security-Performance-and-Commissioning-with-PowerFlex-755T-AC-Drive-Enhancements/default.aspx. Acesso em: 05 abr. 2021.

[73] ODVA. **CIP Security**. Open Device Vendor Association. Disponível em: https://www.odva.org/technology-standards/distinct-cip-services/cip-security/. Acesso em: 05 abr. 2021.

[74] ISO. **Date and time**: Representations for information interchange – Part 1: Basic rules. 2019. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:8601:-1:ed-1:v1:en. Acesso em: 04 mar. 2021.

[75] PEARSON, Siani. **Trusted Computing Platforms, the Next Security Solution**. 2002. HP Laboratories. Disponível em: https://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf. Acesso em: 09 mar. 2020.

[76] HOELLER, Andrea; TOEGL, Ronald. Trusted platform modules in cyber-physical systems: On the interference between security and dependability. In: **2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)**. IEEE, 2018. p. 136-144.

[77] O'NEILL, Ken; NEWELL, G. Richard; ODIGA, Sathish Kumar. Protecting flight critical systems against security threats in commercial air transportation. In: **2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC).** IEEE, 2016. p. 1-7.

[78] ABB. **Technical guide Cybersecurity for ABB drives**. Disponível em: https://library.e.abb.com/public/e033f84022a4422fad29bcfd9109ada3/EN_Cybersecurity_guide_B_A4.pdf. Acesso em: 07 jan. 2021.

[79] CHECKPOINT. **CHECKPOINT 1200R Rugged Appliance Datasheet**. Disponível em: https://www.checkpoint.com/downloads/product-related/datasheets/ds-1200R-rugged-appliance.pdf. Acesso em: 02 mar. 2021.

[80] XILINX. **UltraFast Embedded Design Methodology Guide.** 2018. Disponível em: https://www.xilinx.com/support/documentation/sw_manuals/ug1046-ultrafast-design-methodology-guide.pdf. Acesso em: 29 mar. 2020

[81] EKBERG, Jan-Erik; KOSTIAINEN, Kari; ASOKAN, N. The untapped potential of trusted execution environments on mobile devices. **IEEE Security & Privacy**, v. 12, n. 4, p. 29-37, 2014.

[82] TEXAS INSTRUMENTS. **M-Shield Mobile Security Technology**: making wireless secure. making wireless secure. Disponível em: https://www.ti.com/pdfs/wtbu/ti_mshield_whitepaper.pdf. Acesso em: 25 fev. 2020.

[83] INTEL. **Software Guard Extensions (Intel SGX)**: what is intel sgx? Disponível em: https://www.intel.com.br/content/www/br/pt/architecture-and-technology/software-guard-extensions.html. Acesso em: 11 fev. 2020.

[84] SHADRIN, Alexander; NIKISHIN, Andrey. **Modern OSs for embedded systems**: A review from KasperskyOS developers. Disponível em: https://securelist.com/modern-oss-for-embedded-systems/86109/. Acesso em: 30 abr. 2020.

[85] WEG. **WEG Programming Suite (WPS)**. Disponível em: https://www.weg.net/catalog/weg/BR/pt/Automa%C3%A7%C3%A3o-e-Controle-Industrial/Drives/Softwares/WEG-Programming-Suite-%28WPS%29/WEG-Programming-Suite-%28WPS%29/p/MKT_WDC_BRAZIL_SOFTWARE_WPS. Acesso em: 11 out. 2020.

[86] SIEMENS. **TIA Portal drive integration with SINAMICS Startdrive.** 2020. Disponível em: https://new.siemens.com/global/en/products/drives/selection-and-engineering-tools/sinamics-startdrive-commissioning-software.html. Acesso em: 30 nov. 2020

[87] WEG. **Inversor de Frequencia CFW300**: catalogo do produto. Jaraguá do Sul: Weg, 2019. Disponível em: https://static.weg.net/medias/downloadcenter/h59/h52/WEG-CFW300-inversor-de-frequencia-50066189-pt.pdf. Acesso em: 02 fev. 2020.

[88] FPGAKEY. **ZedBoard System Architecture**. Disponível em: https://www.fpgakey.com/tutorial/section365. Acesso em: 20 fev. 2021.

[89] DIGILENT. **ZedBoard Zynq-7000 ARM/FPGA SoC Development Board**. Disponível em: https://store.digilentinc.com/zedboard-zynq-7000-arm-fpga-soc-development-board/. Acesso em: 27 out. 2020.

[90] XILINX. **Zynq**: zynq-7000 soc product advantages. Zynq-7000 SoC Product Advantages. Disponível em: https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html. Acesso em: 03 fev. 2021.

[91] MAXIM. **DS3231 Datasheet**: extremely accurate i2c-integrated rtc/tcxo/crystal. Extremely Accurate I2C-Integrated RTC/TCXO/Crystal. Disponível em: https://pdf1.alldatasheet.com/datasheet-pdf/view/254832/MAXIM/DS3231.html. Acesso em: 26 maio 2020.

[92] MICROCHIP. **24C32 Datasheet**: 32k 5.0v i2c smart serial eeprom. 32K 5.0V I2C Smart Serial EEPROM. Disponível em: https://pdf1.alldatasheet.com/datasheet-pdf/view/194592/MICROCHIP/24C32.html. Acesso em: 20 maio 2020.

[93] EWALD, Wolfgang. **DS3231 – Real-time clock**. Wolles Elektronikkiste. Disponível em: https://wolles-elektronikkiste.de/en/ds3231-real-time-clock. Acesso em: 24 mar. 2021.

[94] XILINX. **Vivado HLx Editions**: bringing ultra high productivity to mainstream systems & platform designers. Bringing Ultra High Productivity to Mainstream Systems & Platform Designers. Disponível em: https://www.xilinx.com/support/documentation/backgrounders/vivado-hlx.pdf. Acesso em: 25 fev. 2021.

[95] XILINX. **Xilinx Software Development Kit (XSDK).** Disponível em: https://www.xilinx.com/products/design-tools/embedded-software/sdk.html. Acesso em: 21 mar. 2021.

[96] WOLFSSL. **WolfSSL Embedded SSL/TLS Library**. Disponível em: https://www.wolfssl.com/products/wolfssl/. Acesso em: 03 maio 2020.

[97] FREERTOS. **About FreeRTOS Kernel.** Disponível em: https://www.freertos.org/RTOS.html. Acesso em: 05 maio 2020.

[98] CROCKETT, Louise H. et al. First Designs on Zynq. In: CROCKETT, Louise H. et al. **The zynq book tutorials for zybo and zedboard**. Glasgow: Strathclyde Academic Media, 2015. Cap. 1. p. 1-34.

[99] CROCKETT, Louise H. et al. Next Steps in Zynq Soc Design. In: CROCKETT, Louise H. et al. The zynq book tutorials for zybo and zedboard. Glasgow: Strathclyde Academic Media, 2015. Cap. 2. p. 35-66.

[100] D9 TECH BLOG. **How to export Zynq peripherals (I2C, SPI, UART and etc) to PMOD connectors of ZedBoard using Vivado 2013.4**. Disponível em: https://blog.idv-tech.com/2014/03/22/howto-export-zynq-peripheralsi2c-spi-uart-and-etc-to-pmod-connectors-of-zedboard-using-vivado-2013-4/. Acesso em: 12 abr. 2020.

[101] TAYLOR, Adam. **Meet the Zynq MIO**: adam taylor⁝s microzed chronicles part 9. Adam Taylor's MicroZed Chronicles Part 9. Xilinx. Disponível em: https://forums.xilinx.com/t5/Xcell-Daily-Blog-Archived/Meet-the-Zynq-MIO-Adam-Taylor-s-MicroZed-Chronicles-Part-9/ba-p/386661. Acesso em: 20 jun. 2021.

[102] METZ, Christopher. AAA protocols: authentication, authorization, and accounting for the Internet. **IEEE Internet Computing**, v. 3, n. 6, p. 75-79, 1999.

[103] ZHANG, Peng; LIU, Joseph K.; YU, F. Richard; SOOKHAK, Mehdi; AU, Man Ho; LUO, Xiapu. A Survey on Access Control in Fog Computing. **Ieee Communications Magazine**, S.L., v. 56, n. 2, p. 144-149, fev. 2018. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mcom.2018.1700333.

[104] SAHAFIZADEH, Ebrahim; PARSA, Saeed. Survey on access control models. In: **2nd International Conference on Future Computer and Communication. IEEE**, 2010. p. V1-1-V1-3.

[105] CAI, Fangbo et al. Survey of access control models and technologies for cloud computing. **Cluster Computing**, v. 22, n. 3, p. 6111-6122, 2019.

[106] MAW, Htoo Aung et al. A survey of access control models in wireless sensor networks. **Journal of Sensor and Actuator Networks**, v. 3, n. 2, p. 150-180, 2014.

[107] FERRAIOLO, David F. et al. Proposed NIST standard for role-based access control. **ACM Transactions on Information and System Security (TISSEC)**, v. 4, n. 3, p. 224-274, 2001.

[108] LU, Yuqian et al. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. **Robotics and Computer-Integrated Manufacturing**, v. 61, p. 101837, 2020.

[109] NATIONAL INSTRUMENTS. **The Modbus Protocol In-Depth**. Disponível em: https://www.ni.com/en-us/innovations/white-papers/14/the-modbus-protocol-in-depth.html. Acesso em: 04 mar. 2020.

[110] MODBUS ORGANIZATION. **MODBUS Application protocol specification**. Hopkinton: Modbus Organization, 2012. Disponível em: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf. Acesso em: 03 abr. 2020.

[111] RAMBUS. **Hardware Root of Trust**: Everything you need to know. Disponível em: https://www.rambus.com/blogs/hardware-root-of-trust/. Acesso em: 02 mar. 2021.

[112] INFINEON. **OPTIGA TPM SLB 9670 TPM2.0 Datasheet**. Disponível em: https://www.infineon.com/dgdl/Infineon-SLB%209670VQ2.0-DataSheet-v01_04-EN.pdf?fileId=5546d4626fc1ce0b016fc78270350cd6. Acesso em: 03 fev. 2021.

[113] SECTIGO. **What Is Code Signing Certificate and How Does It Work?** Disponível em: https://sectigostore.com/page/what-is-code-signing-certificate/. Acesso em: 04 abr. 2021.

[114] BLAKE-WILSON, Simon et al. **RFC8422**: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier. 2018. Disponível em: https://www.rfc-editor.org/rfc/rfc8422. Acesso em: 01 fev. 2021.

[115] PORNIN, Thomas. **RFC6979**: Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). 2013. Disponível em: https://datatracker.ietf.org/doc/html/rfc6979. Acesso em: 01 fev. 2021.

[116] THE GUARDIAN. **PlayStation Network hackers access data of 77 million users**. Disponível em: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data. Acesso em: 03 fev. 2021.

[117] BUCHANAN, William. **Not Playing Randomly: The Sony PS3 and Bitcoin Crypto Hacks**: watch those random number generators. Watch those random number generators. 2018. Disponível em: https://medium.com/asecuritysite-when-bob-met-alice/not-playing-randomly-the-sony-ps3-and-bitcoin-crypto-hacks-c1fe92bea9bc. Acesso em: 01 fev. 2021.

[118] BITCOIN. **Android Security Vulnerability**. 2013. Disponível em: https://bitcoin.org/en/alert/2013-08-11-android. Acesso em: 01 fev. 2021.

[119] AARON RUSSELL. **What Is a Certificate Authority (CA)?** Disponível em: https://www.ssl.com/faqs/what-is-a-certificate-authority/. Acesso em: 30 out. 2020.

[120] BAETONIU, Catalin. **High speed true random number generators in xilinx fpgas**.2016 Disponível em: http://forums.xilinx.com/xlnx/attachments/xlnx/EDK/27322/1/HighSpeedTrueRandomNumberGeneratorsinXilinxFPGAs.pdf, Acesso em: 01 fev. 2020

[121] DIERKS, Tim; ALLEN, Christopher. **RFC2246**: The TLS Protocol Version 1.0. 1999. Disponível em: https://tools.ietf.org/html/rfc2246. Acesso em: 01 fev. 2021.

[122] DIERKS, Tim; RESCORLA, Eric. **RFC4346**: The Transport Layer Security (TLS) protocol version 1.1. 2006. Disponível em: https://tools.ietf.org/html/rfc4346. Acesso em: 01 fev. 2021.

[123] DIERKS, Tim; RESCORLA, Eric**. RFC5246**: The Transport Layer Security (TLS) protocol version 1.2. 2008. Disponível em: https://tools.ietf.org/html/rfc5246. Acesso em: 01 fev. 2021.

[124] RESCORLA, Eric; DIERKS, Tim. **RFC8446**: The transport layer security (TLS) protocol version 1.3. 2018. Disponível em: https://tools.ietf.org/html/rfc8446. Acesso em: 01 fev. 2021.

[125] JOSEFSSON, Simon; LIUSVAARA, Ilara. **RFC8032**: Digital Edwards-Curve Signature Algorithm (EdDSA). 2017. Disponível em: https://tools.ietf.org/html/rfc8032. Acesso em: 25 jan. 2021.

[126] TECH SCHOOL. **A complete overview of SSL/TLS and its cryptographic system**. 2020. Disponível em: https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd. Acesso em: 25 jan. 2021.

[127] RESCORLA, Eric. **HTTP over TLS**, May 2000. Disponível em: https://tools.ietf.org/html/rfc2818 Acesso em: 01 fev. 2021.

[128] FORD-HUTCHINSON, Paul. **Securing FTP with TLS**, 2005. Disponível em: https://tools.ietf.org/html/rfc4217 Acesso em: 01 fev. 2021

[129] HOFFMAN, Paul. **SMTP Service Extension for Secure SMTP over Transport Layer Security**, 2002. Disponível em: https://tools.ietf.org/html/rfc3207 Acesso em: 01 fev. 2021

[130] MODBUS. **MODBUS/TCP Security Protocol Specification.** Disponível em: https://modbus.org/docs/MB-TCP- Security-v21_2018-07-24.pdf Acesso em: 27 jan. 2021.

[131] MCAFEE. **What Is Security Information and Event Management (SIEM)?** Disponível em: https://www.mcafee.com/enterprise/pt-br/security-awareness/operations/what-is-siem.html. Acesso em: 02 mar. 2021.METZ, Christopher. AAA protocols: authentication, authorization, and accounting for the Internet. **IEEE Internet Computing**, v. 3, n. 6, p. 75-79, 1999.

GLOSSÁRIO

Checksum: é uma função de verificação que resulta em um hash, geralmente usada para verificar se há erros ou se os dados foram alterados. Ex. função SHA256.

Feedback: resposta a um estímulo oferecida como uma forma de avaliação, tem objetivo de levar o emissor deste estimulo a entender como o seu comportamento foi interpretado ou recebido pelo demais componentes do sistema.

Hash: identificador único, resultado de uma operação criptográfica aplicada a uma determinada informação conhecida. Ex. resultado de uma função SHA256.

Insight: é capacidade de obter uma compreensão intuitiva precisa e profunda de uma coisa, ou seja, traz uma maneira totalmente nova de pensar ou enxergar um determinado assunto.

Spoofing: é a técnica na qual, um ator de ataque cibernético se disfarça como um usuário ou dispositivo confiável. No spoofing de IP, o ator tenta obter acesso não autorizado, enviando mensagens com um endereço IP de uma fonte confiável mascarado.

ANEXO A - EXEMPLO CR 1.1 DA NORMA IEC-62443-4-2

Identificação e autenticação de usuários humanos

Os componentes devem fornecer a capacidade de identificar e autenticar todos os usuários humanos e em todas as interfaces capazes de fornecer acesso a eles. Esse recurso deve identificar e obrigar a autenticação do usuário humano, possibilitando a segregação de funções e privilégio mínimo de acordo com as políticas e procedimentos de segurança aplicáveis. Esta capacidade pode ser fornecida localmente pelo componente ou através da integração com sistemas que possuam tal capacidade.

Justificativa e contextualização

Todos os usuários humanos precisam ser identificados e autenticados. A autenticação da identidade desses usuários deve ser realizada por meio de métodos como senhas, *hashes*, biometria, etc. Esse requisito deve ser aplicado para acesso local e remoto ao componente

As interfaces com capacidade de acesso de usuário humano são interfaces de usuário locais, como telas sensíveis ao toque, botões, teclados, bem como protocolos de rede projetados para interações humanas do usuário, como protocolo de transferência de texto, exemplo HTTP e HTTPS, protocolo de transferência de arquivos, exemplo FTP e SFTP, protocolos usados para ferramentas de configuração de dispositivos, proprietários e ou abertos. Também a identificação e autenticação do usuário não deve impedir ações de emergência locais.

Aprimoramento dos requisitos

Os aprimoramentos de requisitos para o CR 1.1 são:

a) identificação e autenticação únicas, os componentes devem fornecer a capacidade de identificar e autenticar de forma única todos os usuários;
b) autenticação multifator para todas as interfaces, os componentes devem fornecer a capacidade de empregar autenticação multifator para todos os acessos do usuário ao componente.

Níveis de segurança do componente

Os 4 níveis de segurança do componente (SL-C) relacionados ao CR 1.1 são:

1 CR 1.1

2 CR 1.1 (a)

3 CR 1.1 (a)(b)

4 CR 1.1 (a)(b)

ANEXO B - CERTIFICADO X.509V3 COM FUNÇÃO (ROLE)

```
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number: 4135 (0x1027)
Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=STATE, L=LOCAL, O=ORG, OU=SUBORG, CN=INTER-CA
    Validity
        Not Before: Oct 27 12:58:27 2017 GMT
        Not After : Oct 27 12:58:27 2018 GMT
    Subject: C=US, ST=STATE, L=LOCAL, O=ORG, OU=SUBORG, CN=ModbusSecurityClient
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:be:3d:4d:9e:8c:fe:1e:06:e6:19:cd:52:68:07:
                54:c6:d3:b3:cd:bb:da:dd:29:29:b5:2d:2f:3b:bf:
                b9:3c:c7:c2:f4:a9:98:ce:6e:47:f5:64:7d:6d:e8:
                a3:6b:02:da:4c:e9:05:b8:aa:30:d9:95:13:1f:14:
                58:3e:c1:dc:a7:21:ca:c0:90:c9:e5:80:70:2b:8d:
                4d:0a:78:96:c0:9e:1f:f1:1d:e7:e8:24:be:06:a1:
                b8:6a:67:d3:7f:1c:d4:cb:c3:85:5a:f8:a7:ef:d1:
                e0:df:30:60:44:29:a3:4d:63:24:d2:7f:e9:45:29:
                2d:e9:fa:53:3d:be:f8:cd:72:64:08:dc:7e:b0:e9:
                d1:c2:e7:52:de:eb:9d:b0:60:b1:73:62:24:ac:ba:
                08:5f:65:23:9a:38:b5:48:53:08:bc:79:ae:b1:55:
                fd:b1:f3:6f:c9:fa:ac:aa:89:aa:f9:59:ca:bf:fe:
                7a:12:cf:88:20:5b:5e:8b:b5:b1:58:04:41:19:2c:
                26:91:0d:ce:86:38:93:32:a0:ab:57:01:38:5a:41:
                36:77:ae:2b:89:28:8e:22:48:84:b6:18:b9:31:aa:
                52:c3:72:3a:19:41:65:21:87:32:4b:c0:53:3e:aa:
                36:dd:d6:40:09:55:e3:65:2c:f9:d4:61:24:6d:60:
                64:87
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Subject Key Identifier:
            B3:09:92:E3:60:44:DE:F5:5B:30:8B:3B:D3:EA:78:FF:CE:DA:E3:48
        X509v3 Key Usage: critical
            Digital Signature, Non Repudiation, Key Encipherment
        RoleOID:1.3.6.1.4.1.50316.802.1:
            Operator
        X509v3 Subject Alternative Name:
            IP Address:192.168.2.12, IP Address:192.168.2.22
Signature Algorithm: sha256WithRSAEncryption
    4f:a2:ca:1f:ea:11:b8:55:89:97:6a:b8:f2:bc:a6:30:e4:6a:
    d7:1e:25:8e:db:cb:f1:54:23:9a:ce:39:e4:dd:96:5f:ce:2a:
    0c:73:43:23:06:7d:a4:fa:33:48:2c:86:42:a7:eb:d8:d4:fa:
    d1:08:07:e9:b1:9c:51:b6:78:9c:e7:2e:fb:22:cc:89:28:ef:
    8f:7a:30:a9:73:e8:28:9a:ab:a4:f2:d5:ec:29:e8:dc:77:a7:
    f5:e1:71:8a:0f:76:4c:78:a5:5c:b7:ea:4e:86:c7:fe:01:17:
    8c:4a:b1:7c:11:d7:f7:a6:81:d4:1c:bb:86:af:d5:20:fe:05:
    ec:0f:de:8d:d1:c0:76:40:31:0f:15:23:65:4d:5c:7c:52:d3:
    cd:c7:81:a5:8a:4f:51:e1:2b:07:9a:8b:83:0d:95:91:97:37:
    6d:59:c5:ca:2e:5d:82:a8:ac:1c:f8:0a:56:06:dc:47:93:db:
    bc:c6:21:94:dd:55:ee:90:3f:ad:f8:15:22:16:99:cf:3f:bc:
    2f:af:aa:04:16:0d:e6:89:c2:f4:af:cb:0e:27:fc:5c:d9:3f:
    5c:5a:b7:4b:aa:d9:a5:eb:0a:3e:53:16:1a:3f:10:20:7b:52:
    ea:93:ed:b8:21:43:b3:dd:cb:38:1f:d9:38:d1:10:09:c0:25:
    df:bf:6a:b7
```

ANEXO C - RESULTADO GERAL DE ADERÊNCIA A IEC 61443-4-2

Na tabela abaixo apresenta-se o resultado geral levando em consideração os requisitos de componente (CR) e os requisitos específicos para dispositivos embarcados (EDR) especificados na IEC 62443-4-2. Não são analisados os requisitos para sistemas (SAR), servidores de hospedagem (HDR) e dispositivos de rede (NDR).

Tabela – Aderência a IEC 61443-4-2

Item	Requisito	Descrição	SL 1	SL 2	SL 3	SL 4
FR 1	CR 1.1	Identificação e autenticação de usuários humanos	Sim	Sim	Sim	Sim
FR 1	CR 1.1 (1)	Identificação e autenticação única para humanos	-	Sim	Sim	Sim
FR 1	CR 1.1 (2)	Autenticação multifator para todas as interfaces	-	-	Não	Não
FR 1	CR 1.2	Identificação e autenticação de dispositivos e processos	-	Sim	Sim	Sim
FR 1	CR 1.2 (1)	Identificação e autenticação única	-	-	Não	Não
FR 1	CR 1.3	Gerenciamento de contas	Sim	Sim	Sim	Sim
FR 1	CR 1.4	Gerenciamento do identificador	Sim	Sim	Sim	Sim
FR 1	CR 1.5	Gerenciamento do autenticador	Sim	Sim	Sim	Sim
FR 1	CR 1.5 (1)	Segurança baseada hardware para autenticadores	-	-	Não	Não
FR 1	CR 1.7	Força da autenticação baseada em senha	Sim	Sim	Sim	Sim
FR 1	CR 1.7 (1)	Gerador de senha e expiração da senha para humanos	-	-	Sim	Sim
FR 1	CR 1.7 (2)	Expiração de senha para todos tipos de usuários	-	-	-	Sim
FR 1	CR 1.8	Certificados PKI	-	Sim	Sim	Sim
FR 1	CR 1.9	Força da autenticação baseada em PKI	-	NA	NA	NA
FR 1	CR 1.9 (1)	Segurança baseada em hardware para PKI	-	-	NA	NA
FR 1	CR 1.10	Feedback do autenticador	Sim	Sim	Sim	Sim
FR 1	CR 1.11	Tentativa de autenticação sem sucesso	Sim	Sim	Sim	Sim
FR 1	CR 1.12	Notificação de uso do sistema	NA	NA	NA	NA
FR 1	CR 1.14	Força da autenticação baseada em chaves simétricas	-	NA	NA	NA
FR 1	CR 1.14 (1)	Segurança baseada em hardware para chaves simétricas	-	-	NA	NA
FR 2	CR 2.1	Aplicação de autorização	Sim	Sim	Sim	Sim
FR 2	CR 2.1 (1)	Aplicação de autorização para todos tipos de usuários	-	Sim	Sim	Sim
FR 2	CR 2.1 (2)	Mapeamento de permissão para funções	-	Sim	Sim	Sim
FR 2	CR 2.1 (3)	Substituição do supervisor	-	-	Não	Não
FR 2	CR 2.1 (4)	Dupla aprovação	-	-	-	Não
FR 2	CR 2.2.	Controle de uso sem fio	NA	NA	NA	NA
FR 2	CR 2.3	Controle de uso para dispositivos móveis e portáveis	-	-	-	-
FR 2	EDR 2.4	Código móvel	NA	NA	NA	NA
FR 2	EDR 2.4 (1)	Verificação de autenticidade do código móvel	-	NA	NA	NA
FR 2	CR 2.5	Bloqueio de sessão	Sim	Sim	Sim	Sim
FR 2	CR 2.6	Encerramento de sessão remota	-	Sim	Sim	Sim
FR 2	CR 2.7	Controle de sessões concorrentes	-	-	Não	Não
FR 2	CR 2.8	Eventos auditáveis	Sim	Sim	Sim	Sim
FR 2	CR 2.9	Capacidade de armazenamento para auditoria	Sim	Sim	Sim	Sim
FR 2	CR 2.9 (1)	Avisar quando o limite de capacidade for atingido	-	-	Não	Não
FR 2	CR 2.10	Resposta a falhas de processamento de auditoria	Sim	Sim	Sim	Sim
FR 2	CR 2.11	Carimbo de tempo	Sim	Sim	Sim	Sim
FR 2	CR 2.11 (1)	Sincronização de tempo	-	Não	Não	Não
FR 2	CR 2.11 (2)	Proteção da integridade da fonte de tempo	-	-	-	Não
FR 2	CR 2.12	Não repúdio	Sim	Sim	Sim	Sim
FR 2	CR 2.12 (1)	Não repúdio para todos os tipos de usuários	-	-	-	Não
FR 2	EDR 2.13	Uso de interface de teste e diagnostico físico	-	Não	Não	Não
FR 2	EDR 2.13 (1)	Monitoração ativa	-	-	Não	Não

Fonte: Adaptado de IEC 62443-2-4

Tabela – Aderência a IEC 61443-4-2

(conclusão)

Item	Requisito	Descrição	SL 1	SL 2	SL 3	SL 4
FR 3	CR 3.1	Integridade da comunicação	Sim	Sim	Sim	Sim
FR 3	CR 3.1 (1)	Autenticação de comunicação	-	Não	Não	Não
FR 3	EDR 3.2	Proteção contra códigos maliciosos	Não	Não	Não	Não
FR 3	CR 3.3	Verificação das funcionalidades de segurança	Não	Não	Não	Não
FR 3	CR 3.3 (1)	Verificação CR 3.3 durante operação normal	-	-	-	Não
FR 3	CR 3.4	Integridade da informação e do programa	Não	Não	Não	Não
FR 3	CR 3.4 (1)	Autenticidade da informação e do software	-	Não	Não	Não
FR 3	CR 3.4 (2)	Notificação automatizada das violações de integridade	-	-	Não	Não
FR 3	CR 3.5	Validação da entrada	Não	Não	Não	Não
FR 3	CR 3.6	Saída determinística	Não	Não	Não	Não
FR 3	CR 3.7	Manipulação de erros	Sim	Sim	Sim	Sim
FR 3	CR 3.8	Integridade da sessão	-	Sim	Sim	Sim
FR 3	CR 3.9	Proteção da informação de auditoria	-	Não	Não	Não
FR 3	CR 3.9 (1)	Registros gravados em mídia de escrita única	-	-	-	Não
FR 3	EDR 3.10	Suporte para atualização	Não	Não	Não	Não
FR 3	EDR 3.10 (1)	Autenticidade e integridade da atualização	-	Não	Não	Não
FR 3	EDR 3.11	Resistência e detecção de violação física	-	Não	Não	Não
FR 3	EDR 3.11 (1)	Notificação de tentativa de adulteração	-	-	Não	Não
FR 3	EDR 3.12	Provisionamento da RoT do fornecedor de produtos	-	Sim	Sim	Sim
FR 3	EDR 3.13	Provisionamento da RoT do proprietário do ativo	-	Não	Não	Não
FR 3	EDR 3.14	Integridade do processo de inicialização	Sim	Sim	Sim	Sim
FR 3	EDR 3.14 (1)	Autenticidade do processo de inicialização	-	Não	Não	Não
FR 4	CR 4.1	Confidencialidade da informação	Sim	Sim	Sim	Sim
FR 4	CR 4.2	Persistência da informação	-	Não	Não	Não
FR 4	CR 4.2 (1)	Apagar recursos de memória compartilhada	-	-	Não	Não
FR 4	CR 4.2 (2)	Apagar verificação	-	-	Não	Não
FR 4	CR 4.3	Uso de criptografia	Sim	Sim	Sim	Sim
FR 5	CR 5.1	Segmentação de rede	Não	Não	Não	Não
FR 6	CR 6.1	Acessibilidade dos eventos de auditoria	Sim	Sim	Sim	Sim
FR 6	CR 6.1 (1)	Acesso programático a registros de auditoria	-	-	Não	Não
FR 6	CR 6.2	Monitoração continua	-	Não	Não	Não
FR 7	CR 7.1	Proteção contra negação de serviço (DoS)	Não	Não	Não	Não
FR 7	CR 7.1 (1)	Gerenciar a carga de comunicação do componente	-	Não	Não	Não
FR 7	CR 7.2	Gerenciamento de recursos	Não	Não	Não	Não
FR 7	CR 7.3	Backup do sistema de controle	Sim	Sim	Sim	Sim
FR 7	CR 7.3 (1)	Verificação de integridade de backup	-	Não	Não	Não
FR 7	CR 7.4	Recuperação e reconstituição do sistema de controle.	Sim	Sim	Sim	Sim
FR 7	CR 7.5	Emergência de energia	-	-	-	-
FR 7	CR 7.6	Definições de configuração de rede e segurança	Não	Não	Não	Não
FR 7	CR 7.6 (1)	Relatórios legíveis das configurações de segurança	-	-	Não	Não
FR 7	CR 7.7	Menor funcionalidade	Sim	Sim	Sim	Sim
FR 7	CR 7.8	Inventário de componentes do sistema de controle	-	Não	Não	Não

Fonte: Adaptado de IEC 62443-2-4

Legenda:

FR Requisito fundamental.

CR Requisito do componente.

EDR Requisito para dispositivos embarcados.

NA Não se aplica ao escopo, são requisitos somente em casos de tais funcionalidades estarem presentes ao escopo do projeto. Para a contabilização considera-se como um requisito atendido, ou seja, um sim.