CENTRO UNIVERSITÁRIO SENAI CIMATEC

PROGRAMA DE POS-GRADUAÇÃO STRICTO SENSU

MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA INDUSTRIAL

MAYER FERNANDES DOS SANTOS SILVA

ASTRIS – UMA PROPOSTA DE MÉTODO PARA AVALIAÇÃO DE RESILIÊNCIA QUANTO À CIBERSEGURANÇA EM REDES DE INTERNET DAS COISAS INDUSTRIAIS

Salvador - BA

2022

MAYER FERNANDES DOS SANTOS SILVA

ASTRIS – UMA PROPOSTA DE MÉTODO PARA AVALIAÇÃO DE RESILIÊNCIA QUANTO À CIBERSEGURANÇA EM REDES DE INTERNET DAS COISAS INDUSTRIAIS

Exame de Defesa de Dissertação apresentado ao Programa de Pós-Graduação Stricto Sensu do Centro Universitário SENAI CIMATEC como requisito parcial para a obtenção do título de Mestre em Gestão e Tecnologia Industrial

Orientador: Prof. Dr. Herman Augusto Lepikson

Salvador - BA
2022

Ficha catalográfica elaborada pela Biblioteca do Centro Universitário SENAI CIMATEC

S586a Silva, Mayer Fernandes dos Santos

ASTRIS – uma proposta de método para avaliação de resiliência quanto à cibersegurança em redes de internet das coisas industriais / Mayer Fernandes dos Santos Silva – Salvador, 2022.

121 f. : il., color.

Orientador: Prof. Dr. Herman Augusto Lepkison.

Dissertação (Mestrado em Gestão e Tecnologia Industrial) – Programa de Pós-Graduação, Centro Universitário SENAI CIMATEC, Salvador, 2022.
Inclui referências.

1. Internet das coisas industrial. 2. Estrutura de risco - Cibersegurança. 3. Resiliência cibernética. 4. WirelessHART. I. Centro Universitário SENAI CIMATEC. II. Lepikson, Herman Augusto. III. Título.

CDD 658.478

NDI - 04

Sistema FIEB | SENAI CIMATEC
PELO FUTURO DA INOVAÇÃO

CENTRO UNIVERSITÁRIO SENAI CIMATEC

Mestrado Profissional em Gestão e Tecnologia Industrial

A Banca Examinadora, constituída pelos professores abaixo listados, aprova a Defesa de Mestrado, intitulada **"ASTRIS – UMA PROPOSTA DE ESTRUTURA DE AVALIAÇÃO DE RESILIÊNCIA QUANTO À CIBERSEGURANÇA EM REDES DE INTERNET DAS COISAS INDUSTRIAIS**" apresentada no dia 16 de maio de 2022, como parte dos requisitos necessários para a obtenção do Título de Mestre em Gestão e Tecnologia Industrial**.**

Assinado eletronicamente por:
Herman Augusto Lepikson
CPF: ***.545.375-**
Data: 17/05/2022 16:58:11 -03:00

Orientador: **Prof. Dr. Herman Augusto Lepikson**
SENAI CIMATEC

Assinado eletronicamente por:
INGRID Winkler
CPF: ***.486.968-**
Data: 17/05/2022 18:29:09 -03:00

Membro Interno: **Prof.ª Dr.ª Ingrid Winkler**
SENAI CIMATEC

Assinado digitalmente por:
Thiago Barros Murari
CPF: ***.984.148-**
Data: 17/05/2022 16:49:13 -03:00

Membro Interno: **Prof. Dr. Thiago Barros Murari**
SENAI CIMATEC

Electronically signed by:
Adriano Cansian
CPF: ***.716.608-**
Date: 5/17/2022 4:58:46 PM -03:00

Membro Externo: **Prof. Dr. Adriano Cansian**
UNESP

Electronically signed by:
Michele Nogueira Lima
CPF: ***.802.023-**
Date: 5/18/2022 2:34:00 PM -03:00

Membro Externo: **Prof.ª Dr.ª Michele Nogueira Lima**
UFMG

Dedico este trabalho aos meus pais, meus irmãos, minha noiva e a todos que sempre demonstraram apoio para esta realização.

Agradecimentos

Agradeço a Deus pela saúde, capacitação e recursos concedidos.

A meus pais Antonio Paulo e Zélia Fernandes pelo apoio, amor incondicional e pela inspiração!

A meus irmãos Myller e Paula Myllane pela parceria, conselhos e inspiração.

Ao meu amor, Fernanda Moreira, que me motiva, suporta e tanto me apoiou neste desafio!

A meu orientador Prof. Dr. Herman Augusto Lepikson pelos direcionamentos e mentoria durante este desafio!

Ao time de docentes do SENAI CIMATEC e banca de avaliação pelos ensinamentos e aprendizados.

A meus colegas de curso e de trabalho pela parceria, empenho e suporte que também foram fundamentais nesta jornada.

Resumo

Em um contexto de alta competitividade e transformação digital, avanços tecnológicos com potencial de elevar a eficiência de unidades industriais estão ocasionando um aumento exponencial do uso de novas tecnologias nestes ambientes. A comunicação sem fio é uma das soluções mais implementadas, permitindo alto nível de interconectividade em diferentes sistemas, inclusive em sistemas críticos responsáveis pelo controle e segurança da produção. O ganho de desempenho com a elevação da conectividade sem fio entre "coisas", contudo, é acompanhado do aumento de vulnerabilidades em função dos diversos tipos de riscos relacionados à segurança deste tipo de comunicação. Neste contexto, este estudo tem o objetivo de apresentar uma proposta de método para análise de resiliência quanto à cibersegurança em redes de Internet das Coisas que permite a identificação e mitigação de riscos em ambiente industrial. A partir do levantamento de ameaças e mecanismos de proteção para redes sem fio descritos na literatura, foi desenvolvido o método ASTRIS (*Area Stack Threat Resilience Implementation & Scalability*) para análise de risco que estrutura as resiliências necessárias para cada camada de redes sem fio, desde o projeto até a sua fase de operação e futuras expansões. A aplicação do método desenvolvido em uma rede IIoT real com protocolo wirelessHART expôs situações de risco até então não visualizadas, contribuindo para a melhoria de resiliência da rede, bem como na conscientização e maturidade em segurança da equipe responsável pela operação e manutenção. Apesar de a rede analisada demonstrar plena capacidade em escalabilidade, apresentou apenas 39% de resiliência perante vulnerabilidades e ameaças, bem como 47% de resiliência para requisitos de operação da rede. Quanto às ações recomendadas para elevação de resiliência, 87% destas representou cerca de 25% do custo de projeto da rede. Estes resultados demonstraram o potencial do método ASTRIS em auxiliar na identificação da resiliência atual de redes IIoT e no reconhecimento de ações necessárias para elevação de maturidade em segurança e robustez para estas redes.

Palavras-chave: Internet das Coisas Industrial; Estrutura de Risco em Cibersegurança; Resiliência cibernética; WirelessHART.

ASTRIS - A PROPOSAL METHOD FOR CYBER RESILIENCE ASSESSMENT OF INDUSTRIAL INTERNET OF THINGS NETWORKS

In a context of high competitiveness and digital transformation, technological advances with the potential to increase the efficiency of industrial units are causing an exponential increase in the use of new technologies in these environments. Wireless communication is one of the most implemented solutions, allowing a high level of interconnectivity in different systems, including critical systems responsible for production control and safety. Performance improvements with the increase in wireless connectivity between "things", however, are followed by the increase in vulnerabilities due to the different types of risks related to the security of this type of communication. This study aims to present a proposal of method for cybersecurity resilience analysis for Internet of Things that allows the identification and mitigation of risks with focus on industrial environments. Through the survey and analysis of threats and protection mechanisms for wireless networks described in the literature, the ASTRIS (Area Stack Threat Resilience Implementation & Scalability) method was developed to analyze risks and resilience required for each layer of wireless networks, from the project to its operational phase and future expansions. The application of the developed method in a real IIoT network operating with wirelessHART protocol exposed previously unseen risk situations, contributing to the improvement of network resilience, as well as the security awareness and maturity of the responsible team. Although the analyzed network demonstrated full capacity in scalability, it was identified only 39% resilience to vulnerabilities and threats, as well as 47% resilience to network operation requirements. For the recommended actions to increase resilience, 87% of these represented around 25% of the network design cost. These results demonstrated the potential of the ASTRIS method to support the identification of current resilience of IIoT networks and recognize the actions needed to ensure proper robustness and security maturity level for critical applications.

Keywords: Industrial Internet of Things; Cybersecurity Risk Framework; Cyber resilience; WirelessHART.

Lista de Tabelas

Lista de Figuras

Lista de Siglas e Abreviaturas

3GPP - 3rd Generation Partnership Project

ACL - Access Control List

ASTRIS – Area Stack Threat Resilience Implementation & Scalability

BLE – Bluetooth Low Energy

CPS – Cyber Physical Systems

CSRF - Cyber Security Risk Framework

CVE - Common Exposures and Vulnerabilities

DOS – Denial Of Service

DDOS – Distributed Denial Of Service

DSSS – Direct Sequence Spread Spectrum

FHSS – Frequency Hopping Spread Spectrum

IA – Inteligência Artificial

ICS – Industrial Control System

IEC – International Etectrotechnical Commission

IEEE - Institute of Electrical and Electronics Engineers

IoT – Internet of Things – Internet das Coisas

IIoT – Industrial Internet of Things

ISA – International Society of Automation

IWSN – Industrial Wireless Sensor Networks

LAN - Local Area Network

LPWAN – Low Power Wide Area Network

LTE – Long Term Evolution

MAC – Medium Access Control

MAN – Metropolitan Area Network

NFC – Near Field Communication

NIST – National Institute of Standards and Technology

OSI Layer – Open System Interconnection Layer

PAN – Process Area Network

PER – Packet Error Rate

RFID – Radio Frequency Identification

PPGGETEC - Pós-graduação em Gestão e Tecnologia Industrial

TI – Tecnologia da Informação

WAN – Wide Area Network

WEP – Wired Equivalent Privacy

WH – WirelessHART

WIFI – Wireless Fidelity

WLAN – Wireless Local Area Network

WPA – Wi-Fi Protected Access

WPAN – Wide Process Area Network

WSN – Wireless Sensor Network

Sumário

1 Introdução

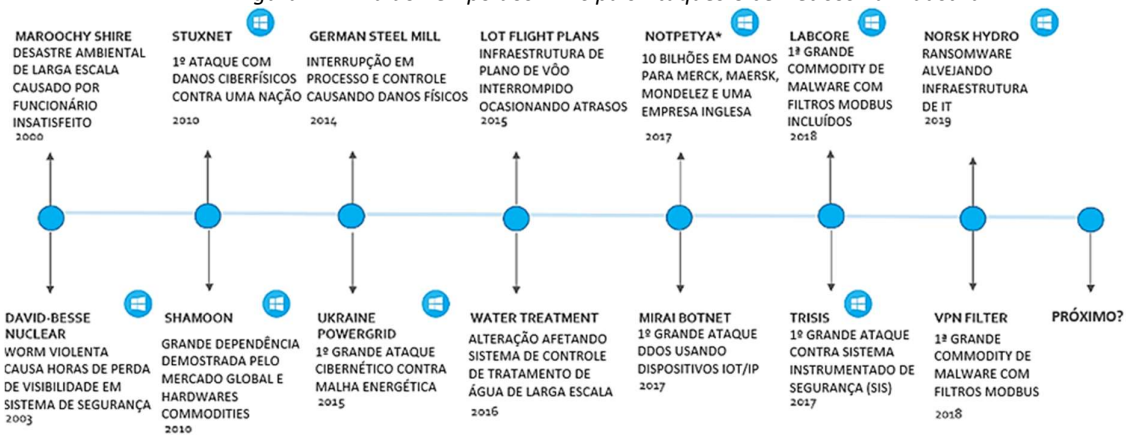
Na revolução digital ora vivenciada, várias áreas em negócios como operação, dados, coordenação e controle foram integradas em redes a dispositivos físicos, compondo ambientes com sistemas denominados ciberfísicos (ou CPS – *Cyber-Physical Systems*). Baseados em novas infraestruturas de computação e comunicação, sistemas de controle e automação industriais evoluíram e passaram a operar em cooperação e colaboração para a otimização de equipamentos, dispositivos e sistemas (JAMAI *et al*., 2020).

Dawson (2018) aborda que implementar manufatura digital na prática, integrando IoT, computação em nuvem e outras tecnologias emergentes gera uma hiper conexão de sistemas, sendo imperativo que a cibersegurança tenha papel definido e vulnerabilidades sejam consideradas e tratadas durante todo o ciclo de vida de sistemas. A crescente aplicação de tecnologias emergentes, principalmente as que são apoiadas nesta interconectividade entre dispositivos e com amplo uso de redes sem fio, por exemplo, ao mesmo tempo que viabilizam o monitoramento de mais variáveis com custo reduzido, por outro lado elevam também de forma exponencial os riscos e vulnerabilidades de segurança de sistemas em relação a sinistros cibernéticos, incluindo riscos de indisponibilidade.

Durante o seu ciclo de vida, sistemas de manufatura são desafiados por diversas ameaças como interrupção de serviços, infiltração, violação de dados, perda de propriedade intelectual, entre outras. A integração de tecnologias emergentes torna a infraestrutura de manufatura ainda mais susceptível a novas formas de ataques que expõem a necessidade de avanços em soluções de segurança e estruturas de defesa (CHHETRI *et al*., 2017). Essa preocupação com estruturas críticas de sistemas de informação e automação geram a demanda por desenvolver *frameworks* de segurança que auxiliem na prevenção de intervenções maliciosas, que podem ter origem em organizações terroristas, crime organizado ou *hackers* patrocinados por organizações ou nações. Por esse motivo, deve-se analisar os impactos econômicos de sinistros envolvendo o comprometimento de dados e de sistemas, bem como estabelecer padrões de segurança com mecanismos rigorosos para medição, controle e gerenciamento de dados e estruturas críticas com abordagens industrialmente aceitáveis (RADANLIEV *et al*., 2020).

Os sistemas de manufatura estão entre os três mais alvejados por ataques do tipo *phishing*. Cerca de 20,1% dos computadores industriais são alvejados por ataques por *malwares* a cada mês. Por este motivo, pesquisadores começaram a ressaltar essas questões e fornecer soluções de segurança para sistemas de manufatura inteligente (CHHETRI *et al.*, 2017). Em dezembro de 2010, uma nova *worm* (tipo de *malware*), chamada Stuxnet alvejou um sistema industrial altamente especializado com impactos e sofisticação sem precedentes, tornando este evento um marco para a área de cibersegurança em softwares e equipamentos industriais. Para muitos, este foi o chamado para acordar para a consciência em segurança cibernética industrial (KARNOUSKOS, 2011). Com o objetivo de ilustrar a crescente diversidade e alcance de ataques cibernéticos na indústria, a Figura 1 contém alguns dos ataques mais relevantes ocorridos nos últimos 20 anos.

Figura 1. Linha do Tempo dos Principais Ataques Cibernéticos na Indústria



Fonte: Verve (2019)

Os riscos envolvidos no uso de sistemas de informação ou de operação dependem da aplicação para o qual são designados. Sistemas críticos devem ser ainda mais robustos e resilientes contra ataques cibernéticos de modo a evitar danos de grandes proporções a patrimônio e a pessoas. A Tabela 1 aborda informações com mais detalhes sobre alguns dos incidentes em redes ICS de maior relevância até o presente momento.

Há aproximadamente 35 bilhões de dispositivos IoT instalados globalmente e mais de 75 bilhões estarão conectados até 2025. Houve um rápido crescimento da transformação digital em 2020 com aumento de conectividade, rede 5G, melhorias em IA (inteligência

artificial) e aprendizado de máquina. O ambiente de manufatura tem experimentado novas capacidades como o monitoramento remoto de maquinário e novos métodos de gestão remota da produção, auxiliando na continuidade dos processos como durante o período pandêmico do Covid19. O uso destas tecnologias continuará aumentando, tornando máquinas, plantas e pessoas cada vez mais conectadas (BANK & FINANCE, 2021).

Tabela 1.Detalhes Sobre Ataques a sistemas ICS de maior relevância

Local Ano Setor	Sistema Alvejado	Meio de Intrusão	Descrição e Impacto	Vulnerabilidades Exploradas	Fonte
2000 Australia Trat. Esgoto	SCADA	Intrusão interna (terceiro)	Marooch Water plant: Perda de controle de 150 estações remotas de bombeamento	1. Controle de ativos e documentação impróprios 2. Acesso wireless configurado de forma insegura 3. Falta de antivírus e políticas de segurança	Slay; Miller, 2007
2010 Iran Nuclear	PLC	ICS *insider* ou engenharia social / MITM (Stuxnet)	Natanz/Iran: 1.000 centrifugas destruídas	1. Engenharia social 2. Exposição física 3. Zero-day 3. MITM	Lindsey, 2013
2015 Ulcrania Elétrico	SCADA	e-mail DoS Killdisk (blackenergy 3)	Desligamento de 30 subestações e 225 mil pessoas sem energia	1. Detalhes de Dispositivos ICS de fornecedores disponíveis publicamente. 2. Acesso VPN sem 2º fator de autenticação. 3. *Firewall* permitiu acesso remoto para o atacante 4. Rede não monitorada.	Lee et Al., 2016
2017 Arabia Saudita Petroquímico	SIS	possível phising ou eng. social (Triton / Trisis / Hatman)	SIS reprogramado e Parada de Planta. (Potencial muito maior)	1. Vulnerabilidade em configuração de certificado de segurança entre workstation e controlador 2. Acesso inadvertido remoto ou físico 3. Infecção com malware	Pinto et Al., 2018

Fontes: (SLAY; MILLER, 2007), (LINDSEY, 2013), (LEE et al., 2016), (LEE et al., 2014) e (PINTO et al., 2018)

Ao conhecer os benefícios oriundos da aplicação da Internet das Coisas (IoT – *Internet of Things*) e outras tecnologias de manufatura digital que esta habilita, como o maior uso de dados, monitoramentos em tempo real, realidade virtual entre outras, organizações de diversos segmentos iniciaram a implementação de programas de manufatura digital e IoT. A preocupação com o aumento de eficiência deve ser acompanhada pela preocupação com segurança ou com a maturidade organizacional em tecnologias IIoT (Internet das Coisas Industrial) no contexto de sua aplicação. No entanto, os modelos consolidados para avaliação de maturidade de segurança em sistemas de informação não consideram riscos específicos da IIoT. Neste contexto, o método ASTRIS (*Area Stack Threat Resilience Implementation & Scalability*) se posiciona, portanto, para auxiliar na solução de uma importante lacuna não resolvida por estruturas conhecidas para análise de risco de sistemas em geral: a avaliação e mitigação de riscos específicos em redes IoT e sem fio em ambiente industrial.

1.1 Objetivo

Apresentar uma proposta de método para análise de resiliência quanto à cibersegurança em redes de Internet das Coisas em ambiente industrial.

1.1.1 Objetivos Específicos

Para alcançar o objetivo do trabalho, foram propostos os seguintes objetivos específicos:

- Analisar as tecnologias de comunicação sem fio e os riscos implicados para sistemas industriais.
- Analisar modelos de gestão de risco cibernético existentes para resiliência em sistemas de internet das coisas.
- Elaborar estrutura para identificação de riscos e resiliências em redes IoT em ambientes industriais.
- Testar o método desenvolvido através de sua aplicação em uma rede IoT operando em uma unidade industrial real.

1.2 Justificativa

Pela exploração da literatura existente e estudos anteriores na área de segurança para sistemas em IIoT é possível identificar que existem lacunas em avaliar a aplicação desta tecnologia em ambientes industriais quanto a aspectos de segurança, bem como em desenvolver abordagens para identificação e gestão do risco para estas redes. Alguns autores utilizam metodologias existentes, ou propõem combinações destas, de modo a encontrar variações e novas formas para avaliação de risco. No entanto, existem oportunidades quanto à identificação de riscos de forma contextualizada através de métodos dedicados para o IoT com foco no ambiente industrial, sobretudo no setor petroquímico.

Unidades industriais são compostas por instalações, equipamentos e sistemas, que formam ambientes diversos em características físicas e diferentes tipos de criticidade. Os sistemas que tornam possível operar uma unidade industrial de forma eficiente e segura operam em ambientes desde salas climatizadas até áreas industriais densas ou remotas, expostas a condições ambientais severas e de difícil controle de acesso ou monitoramento. O crescente uso do IoT em ambientes industriais associado a novas vulnerabilidades e ameaças

inerentes a essa tecnologia adicionam riscos importantes que devem ser considerados durante todo o ciclo de vida de uma instalação industrial. Neste cenário, este estudo aborda os desafios do IIoT desde projetos em fase de engenharia até as etapas de operação e escalabilidade, propondo um novo método para identificação e tratamento destes riscos.

1.3 Organização do Documento

Esta dissertação de mestrado é composta por 5 capítulos, sendo apresentada com a seguinte estrutura:

- **Capítulo 1 – Introdução:** apresenta o contexto da pesquisa e aborda o cenário atual de segurança em redes de internet das coisas em ambientes de manufatura digital. Este capítulo aborda também a importância da pesquisa, bem como o problema central, objetivos desta dissertação e metodologia utilizada.
- **Capítulo 2 – Revisão de Literatura:** este capítulo aborda os principais conceitos e estado da arte para o tema da dissertação através de publicações referências na área na última década de maior aderência ao conteúdo deste estudo.
- **Capítulo 3 – Análise de Vulnerabilidades em Redes IoT:** este capítulo explora aspectos do problema definido nesta dissertação quanto às vulnerabilidades e desafios em redes IoT, mapeando e contextualizando soluções para elaboração do método para análise de resiliência destas redes.
- **Capítulo 4 – Resultados:** Neste capítulo são apresentados detalhes de como vulnerabilidades e soluções identificadas na literatura foram estruturadas para compor o método desenvolvido para avaliar a maturidade de segurança em redes IIoT.
- **Capítulo 5 – Conclusão:** esta seção apresenta as conclusões deste estudo, tendo como referência o problema e objetivos definidos nesta dissertação, bem como apresenta contribuições e oportunidades para estudos futuros na área.

2 Revisão Da Literatura

A integração de dispositivos de automação com outros sistemas em diferentes áreas corporativas tem grande potencial em elevar a capacidade e efetividade do ambiente de produção, sendo cada vez mais necessários e atrativos para as corporações. Para Ambrosio e Widergren (2007), Sociedades modernas dependem de sistemas interoperáveis que ao mesmo tempo em que permitem funções avançadas e maior eficiência em processos, geram riscos e preocupações com segurança. Por este motivo, Neaga e Henshaw (2010) abordam que a interoperabilidade entre sistemas deve possuir requisitos de segurança a serem identificados desde o projeto, de modo a evitar que vulnerabilidades comprometam a integridade e confidencialidade de dados e sistemas.

Com esta crescente convergência entre sistemas de IT e OT, ameaças antes restritas a redes de negócios, hoje possuem cada vez mais capacidade de penetrar também em sistemas operacionais industriais. Propondo minimizar interrupções em redes IoT com equipamentos críticos, Zahran e outros (2021) formularam um sistema para automatização da gestão da rede com base em uma customização das melhores práticas recomendadas por dois métodos de análise de risco existentes (OCTAVE Allegro e ISO/IEC 27030). Embora o sistema ARAS (*Automated Risk Assessment System*) proposto por este autor automatiza a gestão de inventário de ativos, possui base em uma estrutura já existente para análise de riscos em sistemas e não considera etapas do ciclo de vida de redes IIoT diferentes da etapa de operação, como por exemplo projeto, manutenção e escalabilidade. Benias e Markopoulus (2017) abordam que *Industrial Control Systems* (ICS) possuem diferentes requerimentos de desempenho, confiabilidade, gestão de risco e arquitetura de segurança, quando comparados com sistemas de TI (Tecnologia da Informação). Enquanto a gestão de sistemas de TI possui foco na confidencialidade de sistemas e dados, a gestão de sistemas de ICS direciona esforços para garantir a disponibilidade dos sistemas de controle que impactam diretamente o ambiente de produtivo. Com o avanço das tecnologias de redes e da *internet*, dispositivos industriais estão cada vez mais conectados, gerando também o surgimento de novas ameaças para sistemas ICS.

De modo a avaliar a aplicabilidade do método CVSS (*Common Vulnerabilities Score System*) para a identificação de vulnerabilidade em sistemas SCADA (Controle de Supervisão e Aquisição de Dados), Falco e colaboradores (2018) realizaram testes em sistemas SCADA e

não SCADA, onde foi encontrando que há diferenças na distribuição e impactos que ameaças influem para estes diferentes tipos de sistemas, porém que não excluem a aplicabilidade do método também para sistemas SCADA. As vulnerabilidades analisadas neste estudo foram oriundas de fontes internacionais, sendo demonstrado que existem diferenças na força de cada indicador de risco que influencia diretamente na avaliação da probabilidade de exploração de vulnerabilidades para sistemas SCADA. Assim como o *framework* proposto por Zahran e outros (2021), este estudo também possui base em uma estrutura de análise existente, desta vez quantitativa, demonstrando aplicabilidade de uma metodologia amplamente utilizada para sistemas TI também em sistemas SCADA. Deste modo, deixam oportunidades em abordar áreas não contempladas no estudo como etapas de projeto e escalabilidade, bem como importantes desafios técnicos em redes IIoT não considerados, detalhes de ataques e propostas para resiliência customizadas para estas redes aplicadas a setores industriais.

Radanliev e outros (2019) analisaram a literatura existente, mapeando iniciativas, estruturas e os métodos mais consolidados para avaliar o impacto do risco cibernético em sistemas de informação. O resultado foi um novo conjunto de princípios de design apoiado por critérios específicos considerando o risco cibernético da IoT. Os princípios de design propostos contemplam recomendações para melhorias na recuperação da segurança cibernética, permitem a visualização do risco e possibilitam informar organizações sobre melhores práticas para a IoT. Apesar de abordar alguns dos principais *frameworks* existentes para tratamento de riscos em sistemas de informação e IoT, este estudo não envolve um destes métodos no detalhe, deixando oportunidades para outros autores desenvolverem novas visões para segurança em redes *wireless*, de modo mais aprofundado, por não abordar vulnerabilidades específicas destas redes, sobretudo no ambiente industrial.

Abordando cenário mais amplo, Jang e colaboradores (2020) avaliaram as ameaças em redes IoT em microssistemas de malha elétrica (*microgrids*) e propuseram medidas baseadas na estrutura de segurança do NIST. Através da identificação de ativos, riscos e mecanismos de proteção, bem como planos de resposta à incidentes, foram desenvolvidas diretrizes de segurança e gestão para o sistema e políticas organizacionais. Por abordar amplo cenário de ameaças, considerar a rede em ambiente industrial como parte de uma estrutura crítica e utilizar um método para análise de riscos em redes de internet das coisas industrial, este é um

dos estudos que mais se assemelha ao teor desta dissertação. No entanto, o estudo foi designado para *microgrids* (área diferente da proposta desta dissertação) e, como o mesmo menciona, deixa a lacuna em aplicar a metodologia desenvolvida futuramente em um sistema real.

2.1 Segurança e Resiliência em Sistemas IIoT

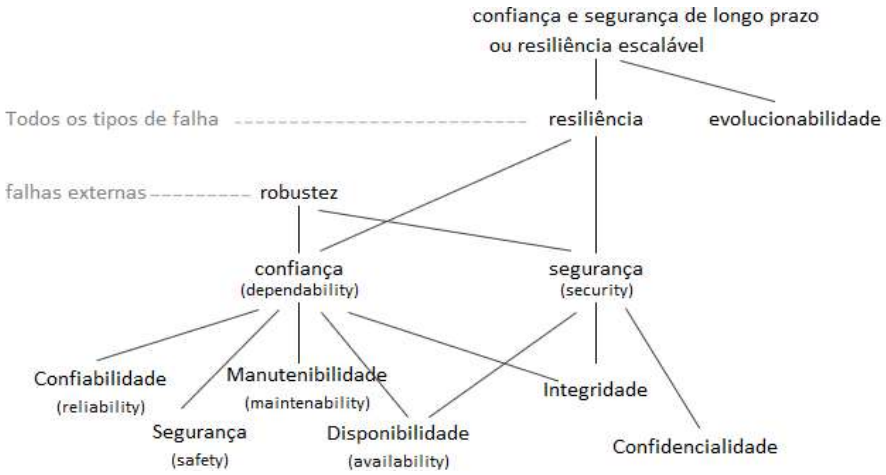
Ratasich *et al.* (2018) abordam que em função do alto nível de interoperabilidade e criticidade de sistemas cibe físicos e da IIoT, existe o desafio em desenvolver continuamente soluções de resiliência para estes ambientes. No entanto, embora amplamente abordada em outras áreas da ciência da computação, no contexto de CPS ainda existe oportunidades em discutir mecanismos de resiliência que podem ser aplicados a estas redes contribuindo para adaptação em cenários desafiadores e mantendo confiabilidade de longo prazo. Em seu estudo, considerando heterogeneidade para estas redes, foi estabelecido que características de confiabilidade e segurança são essenciais para a construção de uma visão geral do estado da arte em resiliência para a IoT integrada a CPS.

Espera-se que sistemas CPS, e seus componentes, sejam confiáveis e seguros durante todo o seu ciclo de vida, apresentando robustez para funcionamento contínuo ainda que sob a presença de falhas em seus componentes. Avizienis et. Al. (2004), define a propriedade de *dependability* (confiança) de um sistema como a combinação de alguns atributos como disponibilidade (prontidão para serviço correto), confiabilidade (continuidade do serviço correto), segurança (no sentido de *safety* - ausência de incidentes severos), integridade (ausência de alterações indevidas) e manutenibilidade (capacidade em passar por modificações e reparos com esforço minimizado). Disponibilidade, integridade e confidencialidade (ausência de divulgações não autorizadas) são tratadas como características inclusas em segurança no sentido de *security*. Essas e outras características são ilustradas na Figura 2, que contém a relação entre os principais atributos no contexto de resiliência cibernética.

Laprie (2008) aborda que um determinado sistema possui robustez quando apresenta habilidade em continuar seu serviço mesmo em condições consideradas não normais, onde quando este consegue ainda lidar com falhas e erros sem impactar o serviço, pode ser

considerado também tolerante a falhas. Este autor define o termo resiliência como a persistência em entregar um serviço de forma confiável ao enfrentar mudanças (como uma falha, ataque ou outro sinistro). Neste contexto, duas importantes propriedades contribuem para a resiliência cibernética e abordam a segurança em diferentes formas: *safety* e *security*. Gunes *et al.*, 2014, refere-se a *safety* (segurança) como a propriedade de um sistema em auxiliar na manutenção da integridade física de pessoas e estruturas, visando evitar danos, perigos e riscos diversos. Um sistema com alto nível de segurança deve possuir conformidade com normas de segurança e possuir mecanismos seguros em caso de falhas.

Figura 2. Relação entre atributos de sistemas no Contexto de resiliência cibernética



Fonte: Ratasich et al. (2018)

Ross *et al.* (2019) aborda que de acordo com o NIST SP800-82, *safety* é definida como "a isenção de condições que podem causar morte, ferimentos, doenças ocupacionais, danos ou perda de equipamento ou propriedade, ou danos ao meio ambiente". A engenharia de segurança possui foco na identificação de comportamentos e interações inaceitáveis em um sistema de modo a garantir que este não entre em um estado inaceitável (ou seja, um estado em que tais comportamentos, interações ou resultados são possíveis, criando uma condição que pode causar um dos danos mencionados). O conjunto de estados inaceitáveis definido pela engenharia de segurança pode constituir uma restrição nas soluções de resiliência cibernética ou pode ser usado em análises de compensação.

A segurança, no sentido de *security*, de acordo com Gunes *et al.* (2014) é a propriedade de um sistema em controlar o acesso aos seus recursos e proteger informações confidenciais de divulgações não autorizadas. Um sistema com alta *security* deve fornecer mecanismos de proteção contra modificação não autorizada de informações e retenção não autorizada de recursos, deve estar ainda livre de divulgação de informações confidenciais em grande medida. Ross *et al.* (2019) menciona *security* como sendo uma propriedade orientada para recursos e danos em sistemas que contêm recursos cibernéticos, no aspecto de perda de ativos ou de capacidade. Neste estudo, o termo segurança quando não seguido de "máquinas" ou "pessoas" refere-se ao significado de *security*.

Ross *et al.* (2019) aborda que grande parte da literatura e muitos profissionais se concentram estritamente nos objetivos de *security* como confidencialidade, integridade e disponibilidade de informações e sistemas de informação. No entanto, este autor mostra que a NIST SP800-37 aborda *security* como proteção de ativos de forma mais ampla, sendo esta "uma condição que resulta do estabelecimento e manutenção de medidas de proteção que permitem a uma organização cumprir sua missão ou funções críticas, apesar dos riscos representados por ameaças ao seu uso de sistemas. As medidas de proteção podem envolver uma combinação de dissuasão, evitação, prevenção, detecção, recuperação e correção que deve fazer parte da abordagem de gestão de risco da organização". Essa definição se sobrepõe à resiliência, mas não a inclui, uma vez que as "medidas de proteção" listadas na definição não cobrem totalmente as estratégias de gerenciamento de risco relacionadas à resiliência cibernética. Nesse contexto, *security* está preocupada principalmente com a proteção de ativos.

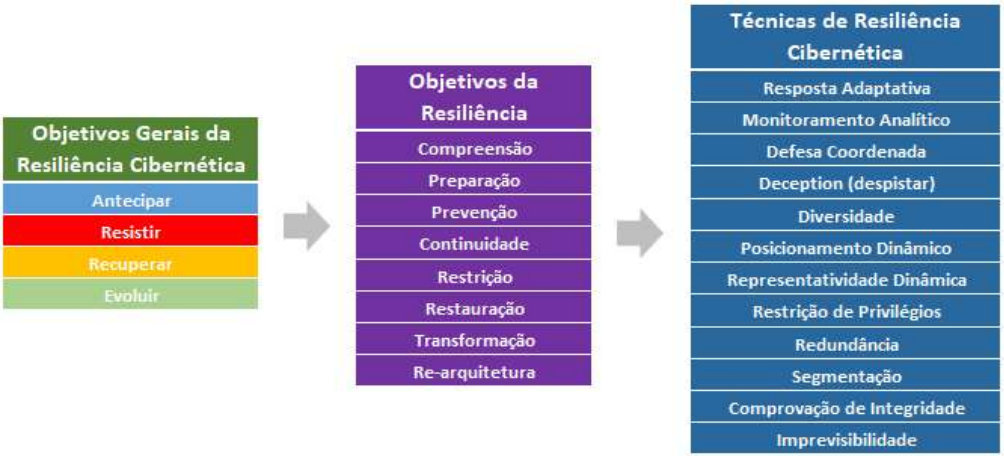
A engenharia de resiliência cibernética considera uma gama mais ampla de efeitos do que a perda de confidencialidade, integridade ou disponibilidade de informações ou de serviços de sistema. De acordo com Gunes *et al.* (2014) resiliência se refere à capacidade de determinado sistema de preservar sua operação e serviços com qualidade aceitável, em caso de exposição a qualquer dificuldade internas ou externas que não excedam seu limite de resistência. Um sistema resiliente deve incluir detecção precoce, autocorreção ou mecanismos de recuperação rápida contra falhas de modo a continuar o atendimento às demandas de serviços. Serviços críticos requerem sistemas altamente resilientes, com operação ininterrupta em todos os níveis como hardware, software, conexões de rede ou

infraestrutura. Por este motivo, exigem uma compreensão completa das falhas e interrupções em potencial.

Ross *et al.* (2019) no NIST Special Publication SP 800-53, aborda que sistemas resilientes são caracterizados por possuírem salvaguardas e medidas de segurança como uma parte da arquitetura do sistema, com capacidade para resistir a ataques e falhas, mantendo sua operação mesmo em estado degradado ou debilitado. Este estudo cita ainda que a resiliência em sistemas de informação é definida como "a capacidade de um sistema de continuar a operar sob condições adversas ou estresse, mesmo se em um estado degradado ou debilitado, enquanto mantém as capacidades operacionais essenciais e se recupera para uma postura operacional eficaz em um período de tempo consistente com as necessidades de sua missão". Esta última é a definição considerada para a condução desta dissertação.

Bodeau e Graubart (2013) retratam que como um veículo para promoção de discussão no espaço da resiliência cibernética, a organização americana MITRE desenvolveu uma estrutura para engenharia da resiliência cibernética (*Cyber Resilience Engineering framework* - CREF). Este grupo, baseia-se em disciplinas de engenharia de resiliência, resiliência de rede, sistemas tolerantes a falhas, intrusão e resiliência de sistemas em infraestruturas críticas com o objetivo de atuar no espaço cibernético e incluir também eventos naturais, erros e diversos vetores de ataques não cibernéticos. A Figura 3 ilustra metas, objetivos e técnicas propostas pelo MITRE, com o objetivo de mapear o espaço de soluções para resiliência cibernética (mais detalhes disponíveis nos Anexos 2 e 3).

Figura 3. Estrutura de Resiliência Cibernética

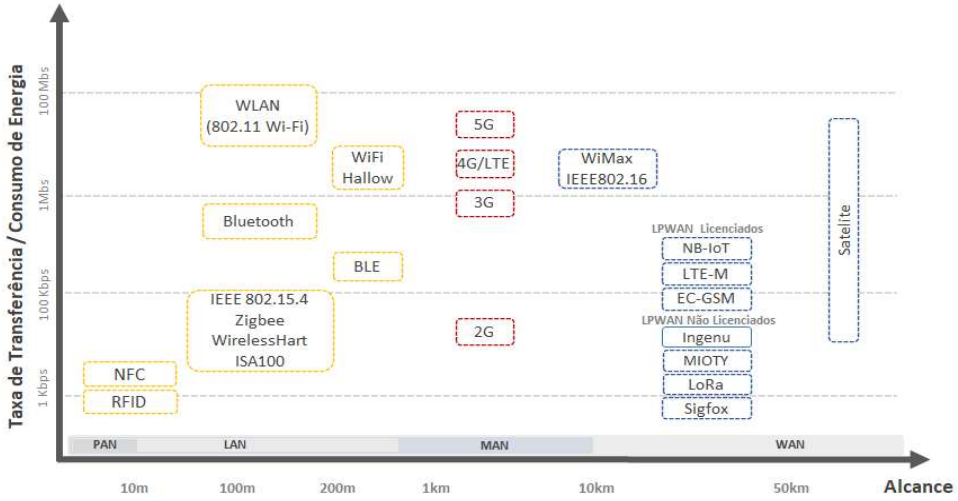


Fonte: Bodeau e Graubart (2013)

2.2 Comunicações Wireless & IoT

A internet das coisas tem o objetivo de possibilitar interconexões de dispositivos de baixo custo através de redes de sensores. Esta tecnologia tem sido aplicada em ambiente de manufatura digital, introduzindo novos conceitos como operação autônoma, personalização de produção em massa, manufatura colaborativa e integração de cadeias produtivas do início ao fim. Dispositivos IoT possuem baixo consumo de energia e podem ser integrados em redes WSN com centenas ou milhares de outros dispositivos (VARGA *et al.*, 2017). Normalmente, a escolha da solução de comunicação depende basicamente da taxa de transferência de dados, do alcance requerido para o sinal e da segurança e confiabilidade. A Figura 4 ilustra diferentes tipos de protocolos de comunicação com suas características de alcance e taxa de transferência de dados.

Figura 4. Redes Wireless – Alcance e Taxa de Transferência de Diferentes Protocolos



Fonte: elaboração própria, adaptado de (BOCCADORO et. Al., 2020), (BEHR, 2018), (STRAND, 2020)

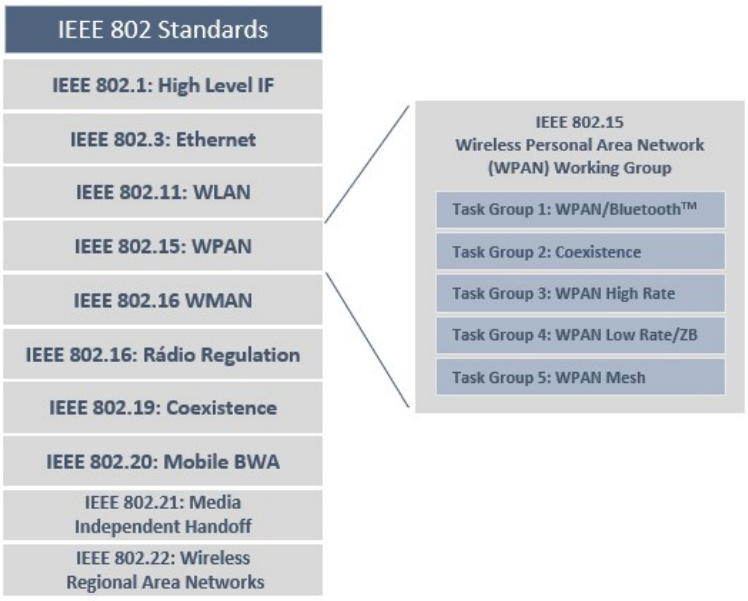
Conforme descrito na Figura 6, as redes wireless são classificadas também quanto ao tipo de área de aplicação e alcance requerido:

- PAN - *Process Area Network*
- LAN - *Local Area Network*
- MAN - *Metropolitan Area Network*
- WAN - *Wide Area Network*

O alcance da rede depende ainda da densidade aérea física e de comunicações da área de aplicação, ou seja, ambientes rurais abertos permitem alcances maiores do que ambientes metropolitanos. Nos últimos anos, o crescente número de tipos de padrões para comunicação *wireless*, na prática, ocasiona heterogeneidade de redes e dispositivos que gera preocupações com segurança, privacidade e confiabilidade. Devido à redução de custos desta tecnologia, dispositivos simples com processamento limitado têm sido conectados entre si e em redes em nuvem (VARGA *et al.*, 2017).

A Figura 5 contém a família de padrões IEEE 802, com destaque para o grupo IEEE 802.15 sobre Redes de Área Pessoal sem fio (*Wireless Personal Area Network* - WPAN) de curta distância. Essas normas também são usadas em vários dispositivos móveis, celulares, assistência digital pessoal (PDAs), eletrônicos de consumo, etc. O grupo de trabalho WPAN foi criado inicialmente como normas IEEE 802.15.1 para Camadas Físicas (*Physical Access*) e de Controle do Meio de Acesso (*Medium Access Control* – MAC) baseadas na tecnologia Bluetooth. Em 1999, foi incluído o grupo WPAN IEEE 802.15.3 e em 2000 foi introduzida a IEEE 802.15.4 WPAN para baixas taxas de transmissão (QURESHI; ABDULLAH, 2014). O Anexo 1 contém as principais normas relacionadas à segurança em sistemas industriais.

Figura 5. Família de Padrões Wireless IEEE802 e IEEE802.15



Fonte: Qureshi e Abdullah (2014)

Com os avanços em tecnologias de comunicação que permitem a integração entre diferentes sistemas em diferentes departamentos e locais físicos, o ambiente industrial e de gestão manufatura vêm se transformando em uma rede cada vez mais conectada com maiores níveis de interoperabilidade e uso de dados que elevam substancialmente a eficiência das operações. O Apêndice 7 ilustra possíveis interfaces dentro de um ambiente corporativo industrial na era digital, incluindo possíveis aplicações de tecnologias IoT.

A comunicação sem fio, antes dedicada a redes e sistemas de informação, passou a ser explorada também em ambientes industriais integrando toda a diversidade de infraestrutura, sistemas e dispositivos. Redes de automação e controle que viabilizam a produção eficiente em diversos segmentos industriais estão integrados com sistemas de gestão da produção em uma estrutura caracterizada por camadas, conforme descrito pela norma ISA 95. De acordo com esta norma, os sensores e atuadores de campo compões a camada L1 (*Level* 1), operando em tempos normalmente inferiores a 1 segundo, e a camada L2 é composta pelo controle e supervisão do processo (operando na casa de segundos). Equipamentos nestas camadas inferiores costumavam ser completamente isolados de redes externas em função da criticidade em segurança e para os negócios, no entanto estão sendo cada vez mais integradas a outros sistemas produtivos.

2.3 Desafios Técnicos da IoT

A implementação de tecnologias IoT possibilita otimizar operações através da aplicação de monitoramentos e controles anteriormente inviáveis, no entanto vem acompanhada de diversos desafios em manter entre dezenas e milhares de dispositivos coexistindo e conectados com eficiência e segurança. Seguem abaixo os principais desafios listados na literatura sobre implementação de redes IoT (BUTUN *et al.*, 2020).

- *Heterogeneidade* – IoT consiste em uma variedade de dispositivos pertencendo a uma mesma rede com *gateways, switches*, sensores, atuadores, aplicações inteligentes e sistemas móveis.
- *Escalabilidade* – desafio em gerar endereços, nomes, gerenciamento e serviços em milhares de dispositivos conectados.

- *Comunicação* – Várias tecnologias são usadas por dispositivos e redes IoT, como comunicações com fio e sem fio em diferentes protocolos de comunicação como Bluetooth, ZigBee, LPWAN.
- *Consumo de Energia* – consiste em um dos maiores desafios para redes IoT. Algoritmos e mecanismos rodando em dispositivos IoT precisam ser projetados para operar com menor carga de processamento.
- *Privacidade de Dados* – privacidade de dados de usuários ao utilizar IoT pode ser um problema em alguns casos específicos. Por exemplo, em modo regular os dispositivos IoT podem fornecer informações de localização a administradores do sistema ou a dispositivos vizinhos, porém quando em modo privado deve-se manter informações como estas de forma secreta.
- *Self-Awareness* – Objetos inteligentes do IoT devem se organizar de forma autônoma para realizar algumas tarefas pré-determinadas em resposta ao ambiente real em que estão inseridos, minimizando necessidades de intervenção humana.
- *Interoperabilidade* – padronização de comunicação entre diferentes dispositivos IoT, permitindo que objetos e redes heterogêneas comuniquem.

Shukla e Tripathi (2018) também abordam desafios relacionados à disponibilidade de dispositivos IoT:

- *Tolerância a falha* – o sistema deve evitar que um nó infectado ou com problema afete todo o sistema. Essa rede também deve conseguir evitar o ataque de exaustão de recursos contra dispositivos de recursos limitados.
- *Disponibilidade* – dispositivos e redes IoT devem estar funcionalmente disponíveis quando necessário, mantendo a continuidade operacional do sistema.

Bekara (2014) traz outras características importantes em aplicações e protocolos de comunicação wireless:

- *Gestão de Confiança (Trust Management)* – Objetos e dispositivos não podem se comunicar sem ao mínimo ter um nível de confiança estabelecido. Estabelecer confiança entre dispositivos de diferentes entidades é um desafio, sobretudo em redes de grande escala.

- *Latência / restrição de tempo* – objetos em redes IoT precisam responder em tempo real a eventos e mensagens. Sistemas SCADA, por exemplo, devem possuir resposta em tempo real a qualquer variação em corrente, tensão ou frequência, além de outros parâmetros meteorológicos que influenciam o funcionamento dos equipamentos.
- *Mobilidade* – o uso de dispositivos móveis, como AGVs (*Automated-Guided Vehicles*) e operações móveis em campo, demanda uma contínua necessidade de autenticação e comunicação segura com um ambiente variável.
- *Limitação de recursos* – vários dispositivos IoT possuem recursos restritos. Atenção especial deve ser direcionada ao desenvolver soluções de segurança, de modo a garantir que seus recursos irão atender às soluções. Isso torna a aplicação de soluções de segurança desafiadora, especialmente aquelas baseadas em criptografia de chave padrão.
- *Bootstrapping* – inicializar de forma eficiente os milhares de dispositivos IoT com recursos necessários para codificação (chaves criptográficas, parâmetros, funções e algoritmos criptográficos, etc.).

Entre os desafios técnicos da implementação de redes IoT está o risco de ataques cibernéticos, onde vulnerabilidades podem ser exploradas por terceiros podendo ocasionar prejuízos físicos ou financeiros. Os ataques em que não há a identificação de intrusão no sistema, são denominados como ataques passivos. Geralmente trata-se de ataques com alvo em dados confidenciais, em que o atacante fica escondido, se inserindo de forma silenciosa na rede. Em ataques ativos, o alvo é não só dados confidenciais como também na integridade dos dados, podendo ocasionar distúrbios no sistema ou na comunicação (BUTUN *et al.*, 2020). O Anexo 4 contém uma lista com os principais tipos de ataques contra redes IoT descritos na literatura.

2.4 Padrões de Rede Sem Fio

Um dos protocolos de comunicação mais utilizados, o WiFi (*Wireless Fidelity*) surgiu na década de 90 pela WiFi Alliance e faz parte da família de padrões IEEE 802.11. Com o seu surgimento, o IEEE 802.11b foi amplamente adotado e incorporado em computadores e laptops (BELDEN, 2021). Ao mesmo tempo que o sucesso do IEEE 802.11 atraiu cada vez mais usuários, aumentou também o potencial de invasões maliciosas. Com o tempo, os ataques sem fio ao IEEE 802.11 se tornaram mais sofisticados e estão evoluindo para transpor

melhorias desenvolvidas para estas redes. Além de perturbações não intencionais através de dispositivos rádio não Wi-Fi, atacantes podem utilizar bloqueadores de Rádio frequência de baixo custo facilmente acessíveis para gerar perturbações na rede. Um atacante *jammer* pode espalhar energia sobre o espectro alvo, se tornando difícil extrair o sinal desejado de sinais de interferência (GARCÍA-VILLEGAS *et al.*, 2014).

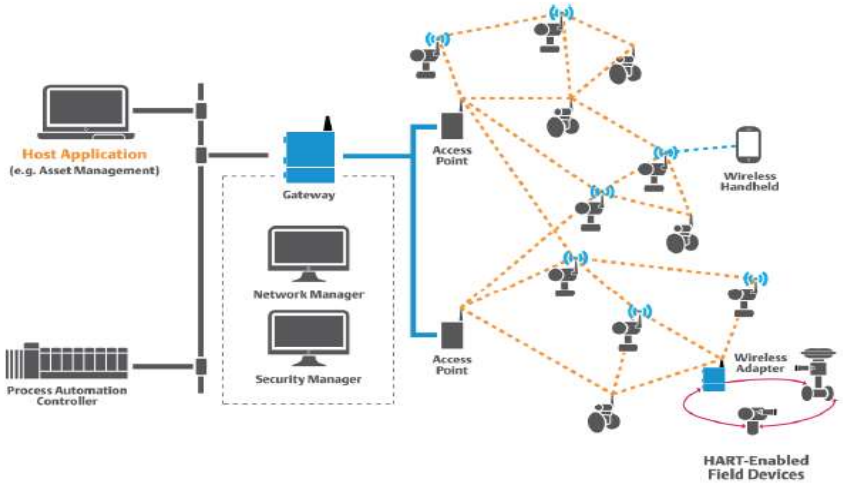
Ren *et al.* (2017) aborda que, ao se utilizar um espaço com limitação em controle de acesso como o ar como meio de propagação da comunicação, dependendo do padrão utilizado é possível identificar e receber pacotes dentro da área de cobertura da rede através da aplicação de uma placa de rede sem fio (especialmente em padrões comuns como 802.11b/g/n/ac). Deste modo, um atacante pode também realizar interceptações de pacotes transmitidos, realizando ataque de *snniffing* (farejamento), e posteriormente realizar roubo ou adulteração informações, sequestro de sessões, bem como adicionar *malwares* e *scripts* na rede. Atacantes podem ainda aproveitar vulnerabilidades relacionadas aos métodos de autenticação de redes wireless, acessá-las e reinstalar chaves de acesso (*key reloading attack*), restaurando padrões iniciais de segurança e se apropriando da rede.

A tecnologia Bluetooth também está entre os protocolos mais utilizados para a realização de comunicações sem fio. Ela oferece uma solução de com baixo custo e baixo consumo de energia para transmissões em rádio de curto alcance. Com estas características, o BLE (*Bluetooth Low Energy*) se tornou uma das tecnologias predominantes para a realização de conexão entre dispositivos IoT como celulares, impressoras, telefones, fones de ouvido, automóveis, entre outros. Embora esta tecnologia ofereça facilidade de uso e conveniência, carece de uma estrutura de segurança centralizada e apresenta sérias vulnerabilidades, sendo necessária a conscientização sobre os riscos de segurança à medida que a tecnologia se torna mais difundida (LONZETTA *et al.*, 2018). Algumas das principais vulnerabilidades do bluetooth que podem ser exploradas de forma maliciosa são abordadas por Scarfone e Padgette (2008), desde senhas fracas e armazenadas em locais impróprios até criptografia não robusta e dispositivos (e serviços) pobres em segurança são características mencionadas por este autor. Detalhes sobre vulnerabilidades deste protocolo estão descritos no Anexo 5.

Como parte da família de padrões de comunicação *wireless* IEEE 802.15.4, amplamente utilizada para comunicação industrial, o WirelessHART (WH) é uma rede de comunicação sem

fio confiável e segura com tecnologia projetada para sensoriamento, monitoramento e controle de processos industriais bem como na interface de gerenciamento de ativos na indústria. Este protocolo é uma extensão do protocolo HART, sendo projetado para ser compatível com versões anteriores e de modo que os segmentos sem fio possam ser adicionados em combinação com segmentos com fio (AKERBERG *et al.*, 2010). A Figura 6 ilustra a disposição e conexões de dispositivos em uma rede WH.

Figura 6. Rede WirelessHART



Fonte: Emerson Process Management, 2016

O WH opera em banda ISM de 2,4 GHz, utilizando ondas com sequência direta de espectro dividido *(Direct Sequence Spread Spectrum* - DSSS) compatível com IEEE 802.15.4, salto de canal e acesso múltiplo por divisão de tempo (*Time Division Multiple Access* - TDMA). Todos os dispositivos estão sincronizados e se comunicam em comprimentos fixos de intervalos de tempo pré-agendados. Considerado robusto para aplicações industriais, este protocolo de comunicação fornece 99,9% de confiabilidade ponta a ponta. Isso é possível devido ao uso do canal com recursos de salto e autocorreção da rede em malha. Quando os caminhos se deterioram ou ficam obstruídos, a propriedade da rede em se autoconsertar garante que a comunicação será ajustada para encontrar caminhos alternativos ao redor das obstruções (AKERBERG *et al.*, 2010).

Akerberg et. Al. (2010) abordam ainda que as medidas de segurança fornecidas pelo WH formam uma solução sempre ativa de várias camadas que é transparente para a aplicação. A entrega de dados é protegida ponta a ponta usando 128-bits AES-*encryption*, assim como a

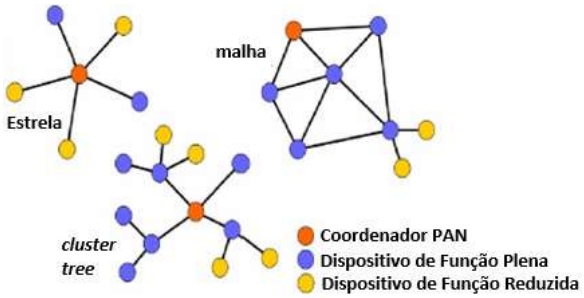
integridade dos dados também é garantida. Todos os dispositivos são autenticados antes de serem autorizados a entrar e participar da rede. Neander et. Al. (2011) adiciona que este protocolo suporta dois tipos de métodos de roteamento: *graph* e *source routing.* O roteamento do tipo *graph* usa grafos pré-construídos para rotear pacotes e o roteamento *source routing* usa rotas de voo construídas. Redes WH devem preferencialmente usar o roteamento de grafo, com vantagens em ter redundância de caminhos e requerer apenas uma sobrecarga de 2 bytes para o pacote (para identificar qual rota o pacote deve seguir). *Source Routing* não suporta caminhos redundantes e cada ID de dispositivo na rota deve ser incluída na sobrecarga do pacote (2 bytes por dispositivo).

Outro protocolo de comunicação sem fio no padrão IEEE 802.15.4 é o ISA-100.11a com topologia em *mesh* aprovada pela ISA Standards & Practices em setembro de 2009. Este protocolo tem o objetivo de fornecer comunicação e operação sem fio seguras para controle de processo e outras aplicações industriais. O foco do comitê ISA SP100 é o padrão ISA100, que é uma família de padrões industriais sem fio cobrindo diferentes aplicações para monitoramento de processo, rastreamento e identificação de ativos, entre outros. O padrão ISA100.11a é o primeiro da família ISA100 com especificação para automação de processos, incluindo o gerenciamento e segurança. Como rigorosa precisão de temporização e alta confiabilidade são crucialmente exigidos por sistemas de processos industriais, de acordo com o padrão de ISA100.11a, é permitido configurar um *backbone* de campo na rede para fins de minimização de latência, largura de banda adicional e QoS mais alto (WANG, 2011).

Operando na banda frequência de rádio não licenciada 2.4 GHz global (disponível também em 915 MHz nas Américas ou 868 MHz na Europa) e transmitindo dados entre 10 e 75 metros (dependendo do meio de aplicação), o ZigBee também opera em padrão IEEE 802.15.4 sendo utilizado para redes de sensores wireless com baixa taxa de comunicação (250 Kb/s), baixo consumo de energia, alcance de até 150 metros e baixo custo (menos de 5 US$). A vida útil de dispositivos de redes ZigBee é de 2 a 6 anos utilizando pilhas AA. Este padrão pode conectar milhares de sensores em ambientes de manufatura para transmitir dados amostrais para sistemas de controle. Este padrão possui autenticação segura na camada MAC e de rede, com topologias do tipo Árvore (*Tree*), malha (*mesh*) ou estrela, dependendo do tipo de aplicação e operação (QURESHI; ABDULAH, 2014).

Embora o ZigBee contenha alguns componentes de serviços e recursos em segurança, possui aplicações ainda vulneráveis a ataques de rede como o de farejar (*sniffing*), já que a chave de rede é enviada em texto simples, por exemplo. Para reduzir o impacto de vulnerabilidades neste protocolo é necessário analisar ameaças de rede para a aplicação específica e sugerir controles e contramedidas para segurança, levando em consideração o comportamento da rede (KHANJI *et al.*, 2019). A Figura 7 ilustra diferentes arquiteturas em redes ZigBee como arranjo em estrela, malha ou em *cluster tree* (grupos de árvore), com diferentes disposições. Mais informações sobre vulnerabilidades deste protocolo disponíveis no Anexo 6.

Figura 7. Modelos de Topologia ZigBee



Fonte: Safaric e Malaric (2006)

Dispositivos ISA100.11a em campo não são obrigados a suportar de forma padrão a função de roteador. Desta forma, redes ISA100.11a podem possuir topologia em estrela enquanto redes WirelessHART operam inerentemente em grafo. A topologia da rede ISA100.11a pode ser influenciada pela escolha de configuração dos dispositivos de campo. Se o usuário for forçado a usar uma topologia em estrela, é muito provável que seja necessário realizar um teste no local para garantir que a rede irá operar de forma satisfatória (NIXON, 2012).

Em relação à segurança, tanto wirelessHART quanto o ISA100.11a definem um conjunto de chaves que são utilizadas para autenticação e comunicação segura de dispositivos na rede. Assim que o dispositivo se conecta à rede, o gerenciador de segurança fornece as chaves para comunicação posterior. O uso da chave de junção é opcional no ISA100.11a. Uma chave global (bem conhecida e sem garantias de segurança) também pode ser usada no

processo de junção para dispositivos que não oferecem suporte a chaves simétricas. O ISA100.11a também permite criptografar mensagens opcionalmente, enquanto o wirelessHART não permite que a segurança seja opcional o que evita que instalações com configurações diferentes das recomendadas possam comprometer o sistema (NIXON, 2012). Mais diferenças e similaridades entre estes padrões estão disponíveis nos Anexos 8 e 9.

Ao contrário do WH e ISA100, o padrão ZigBee não fornece meios de diversidade de frequência, diversidade de caminho ou alta confiabilidade na entrega de mensagens. Interferências e obstáculos persistentes, geralmente inerentes a ambientes industriais, são um grande problema para este protocolo. Desta forma, ZigBee não é adequado para aplicações de processos industriais críticos, uma vez que não atende aos requisitos de confiabilidade e robustez de rede de nível industrial. Por outro lado, os requisitos de segurança e consumo de energia são satisfatórios, conforme descrito na Tabela 2.

Tabela 2. Comparação entre principais protocolos IEEE 802.15.4

	ZigBee	ISA 100.11A	WirelessHart
Segurança	Alta	Muito Alta	Muito Alta
Confiabilidade	Baixa	Muito Alta	Alta
Consumo de Energia	Médio	Baixo	Baixo
Escalabilidade	Média	Alta	Alta
Coexistência	Baixa	Alta	Alta
Salto de Canais	Não	Sim	Sim

Fonte: Sanchez (2011) e Anand et al. (2020)

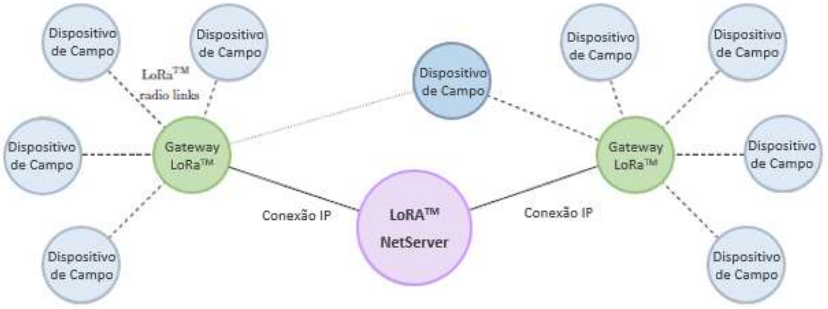
2.4.1 LPWAN e Redes Móveis

Uma tecnologia cada vez mais utilizada para comunicação de dispositivos sem fio é a rede de longa distância de baixa potência, LPWAN (*Low Power Wide Area Networks*), que permite ampliar a comunicação entre sensores a locais remotos em quilômetros de distância. Uma destas tecnologias é o LoRa (de *Long Range*), operando em banda não licenciada abaixo de 1 GHz para operação com link de comunicação de longo alcance. O padrão LoRa possui esquema de modulação de *Spread Spectrum* proprietário que é derivado do *Chirp Spread Spectrum Modulation* (CSS), transferindo dados dentro de um canal com largura de banda fixa. O CSS, que foi desenvolvido na década de 1940, foi tradicionalmente usado em aplicações

militares em função da capacidade de comunicação em longa distância com robustez frente a interferências. LoRa é sua primeira implementação de baixo custo para uso comercial e seu nome vem de sua vantagem na capacidade de longo alcance, que se beneficia do grande *link* fornecido pelo esquema de *Spread Spectrum Modulation* (SINHA *et al.*, 2017).

Outra opção para implementação de internet das coisas com redes de longa distância e baixa potência é a tecnologia SigFox. Trata-se de uma tecnologia baseada em redes públicas com arquitetura em estrela, onde cada sensor envia mensagens para o *gateway* SigFox e, em seguida para a nuvem, onde a mensagem é processada e avaliada pela plataforma IoT, sendo então apresentada aos consumidores (PURNAMA; NASHIRUDDIN, 2020). Como descrito na Figura 8, os dispositivos em uma rede LoRa são gerenciados por um servidor que, por sua vez, está conectado a *gateways* que fazem conexão com dispositivos em uma rede não licenciada. As redes SigFox, por sua vez, possuem conexões entre dispositivos e torres de transmissão integradas com plataformas em nuvem conforme descrito na Figura 9.

Figura 8. Arquitetura de Comunicação LoRaTM



Fonte: Vangelista et al. (2015)

O Sigfox é uma tecnologia que utiliza bandas ultra estreitas (*Ultra Narrow Band* - UNB) não licenciadas de 192 KHz com transmissões em 100 Hz de largura e vantagens em termos de consumo, alta sensibilidade do receptor e baixo custo dos elementos sensores. Comparado com o LoRa e NB-IoT (*Narrow-Band IoT*), Sigfox permite minimizar a troca de pacotes, reduz o consumo de largura de banda, além de limitar o consumo de energia durante as comunicações de rádio. Este padrão requer aproximadamente 6 segundos para cada transmissão, suporta até 140 mensagens de *uplink* por dia (com ciclo de trabalho de 1% e 6 mensagens/hora) e possui carga útil de aproximadamente 12 bytes de *uplink* e 8 bytes no *downlink*. Essas

características permitem que os dispositivos se comuniquem em um intervalo de 10 a 50 km dependendo da frequência de operação (868 MHz na Europa e 902 MHz na América do Norte) com baixo consumo de energia (25 mW a 500 mW na Europa e 158 mW – 4 W nos EUA) (BOCCADORO *et al*., 2020).

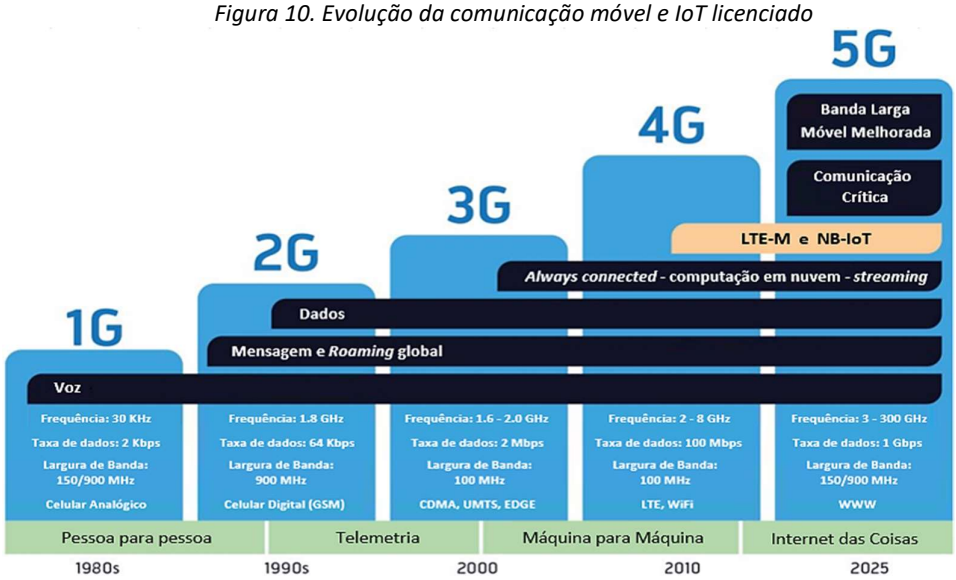
Figura 9. Arquitetura da Tecnologia SigFox

Fonte: Purnama e Nashiruddin (2020)

As redes móveis celulares também permitem comunicação entre dispositivos em longas distâncias e passaram por diversas gerações. A organização de padrões 3GPP (*3rd Generation Partnership Project* - Projeto de Parceria de 3ª Geração), criada em 1998 com o objetivo de desenvolver tecnologias para a terceira geração de redes celulares, trabalhou em um sistema chamado *Long Term Evolution* (LTE). O grupo 3GPP2 desenvolveu sua própria solução chamada *Ultra Mobile Broadband* (UMB) e o IEEE começou a desenvolver um sistema chamado WiMAX. Depois de vários desafios técnicos e soluções, o sistema LTE desenvolvido pelo 3GPP se tornou o padrão 4G predominante, se tornando o padrão global para 4G com cerca de 600 redes LTE lançadas em 189 países em todo o mundo (CASACCIA, 2017).

Baseadas em tecnologia móvel (celular), entraram também no mercado outras duas novas tecnologias: LTE-M e NB-IoT (ambas criadas para serem particularmente adequadas para permitir a conectividade global de IoT). LTE-M e NB-IoT constituem boas opções de conectividade para indústrias que buscam aproveitar as vantagens da tecnologia LPWAN, que aumenta a vida útil da bateria e conecta dispositivos que antes eram difíceis de alcançar. Ambos estão disponíveis hoje, padronizados e construídos na rede 4G, tendo cobertura de rede global e contando com o respaldo dos padrões GSMA e de telecomunicações (TELENOR CONNEXION, 2021). A Figura 10 ilustra a evolução da comunicação móvel (celular e IoT) ao longo do tempo, desde a primeira geração até gerações mais recentes.

Figura 10. Evolução da comunicação móvel e IoT licenciado



Fonte: Telenor Connexion (2021)

Existem, no entanto, diferenças significativas entre os principais padrões de comunicação de longo alcance e baixo consumo de energia. Conhecer estas diferenças descritas na Tabela 3 é crucial para a especificação do protocolo e gestão da segurança da aplicação durante seu ciclo de vida.

Tabela 3. Características de Padrões LPWAN

Característica	Sig Fox	LoRa	NB IoT	LTE-M	LTE Cat0	LTE Cat1
Tipo	PLWAN	PLWAN	DSSS modulation	LTE (celular)	LTE (celular)	LTE (celular)
Baixo Consumo	+++++	++++	++++	+++	++	++
Taxa de Transferência	0.1 Kbps	50 Kbps	100 Kbps	375 Kbps	1 Mbps	10 Mbps
Frequência	915-928 MHz	433-434.8 MHz 902 - 928 MHz		Frequencia 2G, 3G, 4G	Frequencia 2G, 3G, 4G	Frequencia 2G, 3G, 4G
Largura de Banda	ultra-narrow band	Narrowband	Narrowband	Estreita	Larga	Larga
Alcance	50 km	15 km		10 km		
Latência	1 - 30 s	Variável	1.6 - 10s	10 - 15 ms	desconhecido	50 - 100 ms
Padrão	Proprietário	Proprietário	3GPP Rel.13	3GPP Rel.13	3GPP Rel.12	3GPP Rel.8
Disponibilidade	++	+++	++	++	+++++	++++
Spectro	Não Licenciado ISM	Não Licenciado ISM	Licenciado LTE	Licenciado LTE	Licenciado LTE	Licenciado LTE
Complexidade	Muito baixa	Baixa	Muito baixa	Baixa / Media	Baixa	Baixa
Cobertura / range	Média / Alto	Média / Alto	Alto	Alto	Alto	Alto
Vida de Bateria	Muito alta	Muito alta	Alta	Alta	Alta	Alta
necessidade de gateway	Sim	Sim	Não, opcional	Opcional	Opcional	Opcional
penetração de sinal	Alta	Média / Alta	Média / Alta	Média / Alta	Baixa	Baixa
segurança	+++	+++	+++	+++++	++++	++++
Prova para uso futuro	+++	+++	+++++	+++++	+++	+++
Primeiro Projeto	2010	2014		2017		

Fonte: Kani (2017)

Tanto o LTE Cat M1 quanto o NB-IoT possuem coleta e manipulação de dados com uso de torres celulares, de forma semelhante ao LTE de alta velocidade. Uma das principais diferenças entre essas conexões é como os dados dos dispositivos móveis mantém sua comunicação com a internet quando estão em movimento. Por exemplo, ao mover-se de um ponto A para outro mais distante B, cruzando diferentes células de redes, o dispositivo Cat M1 não perde a conexão pois se comporta de forma similar a um telefone celular, refazendo conexões enquanto se move. Já dispositivos NB-IoT, por outro lado, não transferem a conexão e, em vez disso, precisam restabelecer uma nova conexão com uma nova torre de celular cada vez que uma torre é perdida e uma nova torre é detectada (HERNANDEZ, 2018).

2.4.2 Protocolos Wireless Para Segurança de Pessoas e Máquinas

Em aplicações para segurança de pessoas, confiabilidade e pontualidade são os principais requisitos para a comunicação entre sensores e o sistema. Estes sistemas devem possuir mecanismos de comunicação que garantam pontualidade e confiabilidade de entrega dos pacotes de dados dentro de um intervalo de tempo determinado. A maioria dos sistemas aplicados para segurança de pessoas e máquinas possui um modelo de entrega de dados onde o controlador de segurança coleta informações de sensores de forma periódica (PETERSEN; AAKVAAG, 2015).

Os sistemas de segurança de máquinas industriais estão sujeitos ao cumprimento de certos Níveis de Integridade de Segurança (SIL – *Safety Integrity Level*). A norma IEC 61508 define o SIL a partir de um conjunto de requisitos de segurança e integridade cumpridos pelo sistema implementado (*hardware*, *software* e políticas de manutenção). Nem o wirelessHART nem o ISA100.11a suportam diretamente, como parte integrante e especificações, os mecanismos de segurança necessários para operarem com certificação SIL. Uma solução alternativa para isso é usar um protocolo de comunicação ponta a ponta já estabelecido e certificado, como o PROFIsafe, que é projetado para ser implementado no topo do PROFINet *fieldbus*.

O desenvolvimento de um dos primeiros sistemas sem fio para detecção de gás hidrocarboneto no mundo demonstrou que é possível alcançar comunicação de ponta a ponta SIL2 entre um controlador de segurança de máquina e um sensor sem fio por tunelamento

PROFIsafe através do ISA100.11a. Contudo, habilitar este nível de confiabilidade para o protocolo wirelessHART ainda não é possível em função de limitações atuais nos comandos HART disponíveis na camada de aplicação, que torna impossível implementar o mecanismo de tunelamento necessários para o suporte PROFIsafe. Portanto, até que seja realizada uma modificação e uma nova especificação do Protocolo HART, aplicações do PROFIsafe sobre o wirelessHART não estarão disponíveis (PETERSEN; AAKVAAG, 2015).

Os requisitos de confiabilidade para instrumentos industriais dependem da natureza e criticidade da aplicação a que estão direcionadas. A Associação de Usuários para Tecnologias de Automação em Indústrias de Processos (NAMUR) estabelece em seu documento NAMUR NE 124 "*Wireless Automation Requirements*" que existem três classes de aplicações para instrumentação sem fio (Classe A, B e C). Da mesma forma, a *International Society of Automation* (ISA) definiu seis classes de uso para instrumentação *wireless* através de seu documento de especificações ISA100.11a para dispositivos de campo sem fio. A Tabela 4 contém as classes de aplicação em ambientes industriais de acordo com os padrões ISA e NAMUR (PETERSEN; AAKVAAG, 2015).

Tabela 4. Classes de uso de Instrumentação Wireless

APLICAÇÃO	NAMUR	ISA
SEGURANÇA (máquinas e pessoas)	CLASSE A (Segurança Funcional)	CLASSE 0
CONTROLE	CLASSE B (Controle de Processo)	CLASSE 1 (Controle regulatório em malha fechada)
		CLASSE 2 (controle supervisório em malha fechada)
		CLASSE 3 (controle em malha aberta)
MONITORAMENTO	CLASSE C (Monitoramento)	CLASSE 4 (Alerta)
		CLASSE 5 (Logs & Info)

Fonte: Petersen e Aakvaag (2015)

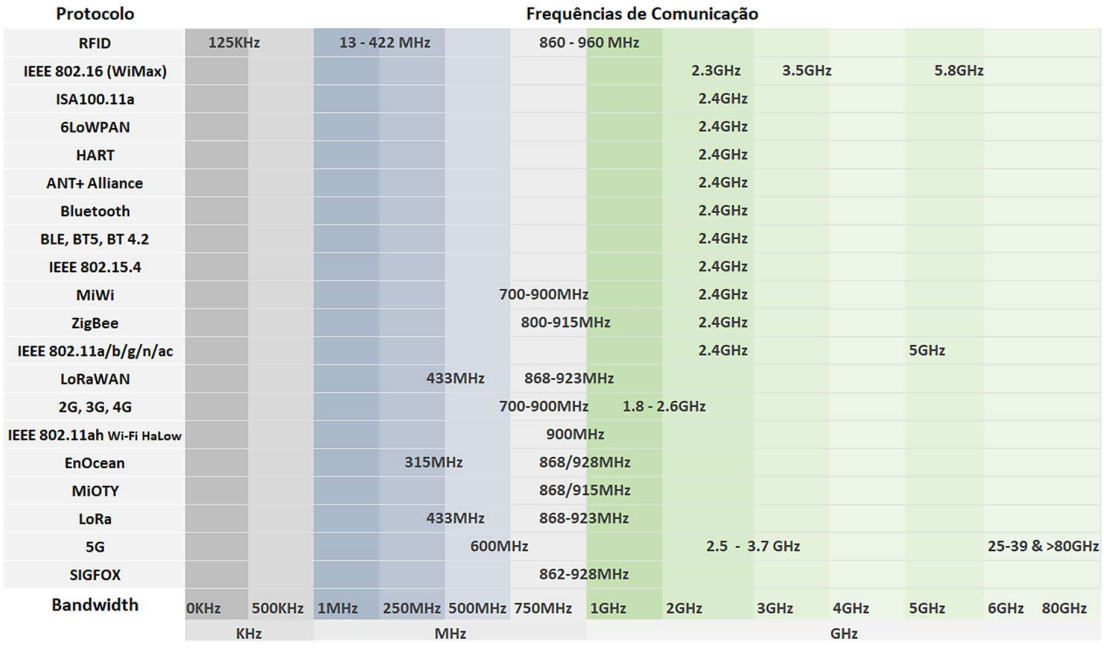
2.5 Coexistência em Redes Wireless

Embora muitas tentativas tenham sido feitas para lançar um padrão único para redes industriais sem fio (por exemplo, dentro das famílias de padrões de rede, como Bluetooth, WiFi e ZigBee), nenhuma conseguiu cumprir todos os requisitos para diferentes aplicações na

indústria. Alguns padrões são capazes de lidar com interferências em níveis mais elevados, mas as técnicas geralmente adotadas tentam evitar colisões ou sugerem pular para canais não utilizados, tornando os procedimentos demorados e reduzindo a taxa de transferência da rede (AUGUSTIN *et al*., 2016).

A gestão de redes deve considerar a possível coexistência de tecnologias heterogêneas de acesso de rádio como parte do paradigma da internet das coisas industrial e facilmente permitir etapas de validação durante projetos e após suas implementações. Problemas de coexistência relevantes podem ocorrer entre redes industriais que utilizam padrões como WirelessHART IEC 62591, IEEE 802.15.4 e IEEE 802.11. Vários cenários de coexistência podem ocorrer ao se aplicar diferentes plataformas de rádio. Para cada caso, existe níveis de interferência toleráveis e limites de sensibilidade em diferentes configurações (WINTER *et al*., 2015).

Figura 11. Frequência de comunicação dos principais protocolos wireless utilizados



Fonte: elaboração própria (adaptado de IVEZIC, 2020)

Como ilustrado através da Figura 11, existe um maior número de padrões possíveis de serem implementados em ambiente industrial operando principalmente em duas zonas de

frequência. Uma Zona situada em 800 - 928 MHz e a outra zona situada em 2.4 – 2.48 GHz. Em ambas, é necessário avaliar os problemas decorrentes da coexistência entre dispositivos nativos, dispositivos e redes futuramente adicionados, bem como a presença de objetos terceiros.

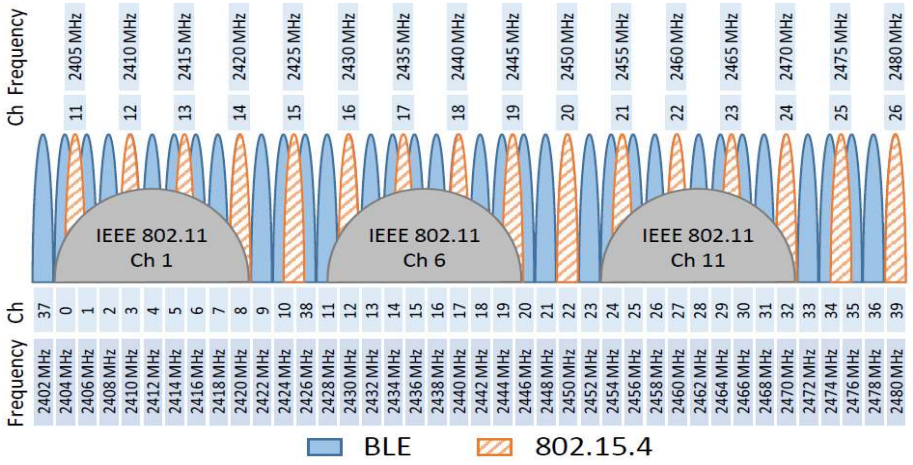
Várias tecnologias de dispositivos sem fio de baixa potência como IEEE 802.15.4 e BLE têm sido desenvolvidas e amplamente adotadas. A banda operacional globalmente permitida para essas tecnologias é a 2,4 GHz ISM não licenciada, que também é usada por outras tecnologias sem fio, como IEEE 802.11 e IEEE 802.15. O resultado é a interferência decorrente da sobreposição de tecnologias que afeta a QoS da rede, especialmente sua confiabilidade e latência, o que pode por sua vez, levar à falha da aplicação. Alcançar coexistência segura de diferentes tecnologias sem fio é, portanto, um grande desafio em projetos de redes IoT (NATARAJAN *et al*., 2016).

Natarajan at. Al. (2016) aborda que Garropo et. Al. (2011) testou a interferência de IEEE 802.11 e Bluetooth clássico em redes IEEE 802.15.4 e vice-versa através de experimentos. Foi encontrado que interferência de redes IEEE 802.11 gera uma taxa de erro de pacotes (*Packet Error Rate* – PER) de 40% em redes IEE 802.15.4 enquanto o Bluetooth gera menos de 10% de erro neste protocolo. Encontrou também efeitos negligenciáveis da interferência do IEEE 802.15.4 nas redes IEEE 802.11 ou Bluetooth. Foi concluído que em geral o BLE é mais afetado pela interferência do IEEE 802.15.4 do que vice-versa. Isso pode ser atribuído ao ganho do processo DSSS e maior ocupação de canais do IEEE 802.15.4 comparado ao BLE. Por outro lado, o BLE é mais resiliente a interferências do IEEE 802.11 do que as redes IEEE 802.14.5 (detalhes disponíveis no Anexo 7). Isto ocorre principalmente em função da ocupação mais curta dos canais do que o IEEE 802.15.4, que o expõe menos a interferências do IEEE 802.11 (NATARAJAN et al., 2016). A Figura 12 ilustra a ocupação e sobreposição de canais para alguns dos principais padrões na banda de frequência de 2,4 GHz.

Krupka *et al.* (2016) concluiu que existem bandas de risco potencial entre LoRa e SigFox, a qual canais de frequência estão sobrepostos (*overlaying*) estando os dispositivos susceptíveis a colisões nestas bandas. A banda de maior risco de colisão está situada em 868.2 MHz. A ocorrência do canal SigFox durante o dia é mais de duas vezes maior que LoRa. Isto é causado pela diferença na política de alcance e vida útil de bateria no custo de velocidade e segurança contra erros de transmissão. A questão da coexistência depende principalmente da

distribuição de frequência e distribuição de tempo dos objetos. A divisão do tempo é composta principalmente de probabilidade de ocorrência de tecnologias individuais e, portanto, a probabilidade de colisões no canal, onde um dos principais limites é o de capacidade potencial máxima de número de dispositivos operando em um mesmo canal.

Figura 12. Banda ISM 2.4 GHz para canais de padrões IEEE 802.15.4, BLE e IEEE 802.11



Fonte: Geil et al. (2017)

A coexistência entre diferentes tecnologias de rede sem fio pode ser classificada em três domínios: espaço, tempo e frequência. Portanto, a coexistência, sem que haja interferências prejudiciais à rede, pode ser alcançada atendendo a um ou mais dos as seguintes condições (NATARAJAN *et al.*, 2016):

- Espaçamento adequado entre as redes
- Controle do compartilhamento de tempo do canal
- Separação de frequência adequada entre as redes

As principais redes sem fio utilizadas em ambientes industriais operam em duas zonas principais de frequência. Uma Zona situada em 800 - 928 MHz e a outra zona situada em 2.4 – 2.48 GHz. Entre os principais padrões que operam na faixa de 800-928 MHz estão os protocolos IEEE 802.11ah, ZigBee, LoRa, RFID e SigFox. Na faixa 2.4-2.48 GHz, entre os principais padrões estão os protocolos IEEE 802.11, IEEE 802.15.4 (ZigBee, WirelessHART, ISA100), 6LoWPAN, BlueTooth LE, Bluetooth.

A ocupação de diferentes padrões dentro de uma mesma banda de frequência e espaço físico pode ocasionar erros de pacote relevantes que prejudica a operação de aplicações que utilizam sinais de dispositivos IoT. As figuras anteriores demonstram que existem diversos padrões de comunicação wireless que operam em faixas de frequência similares. Os diferentes padrões de comunicação possuem diferentes aplicabilidades em função de custo, disponibilidade e segurança envolvida. Aplicações mais críticas envolvendo controle e segurança industrial requerem dispositivos robustos, confiáveis e seguros, que possua risco controlado para operação em ambiente industrial. Enquanto outros dispositivos podem ser utilizados para monitoramento de ativos e outras funções menos críticas onde falhas não levam a um impacto imediato às operações.

2.6 Metodologias para Análise de Risco Cibernético

O risco cibernético (às vezes chamado de risco de TI) é definido como a probabilidade combinada de um evento indesejável e seu nível de impacto. O NIST (Instituto Nacional de Padrões e tecnologia dos EUA) define o risco cibernético como uma função da probabilidade de uma determinada ameaça atuando sob qualquer vulnerabilidade potencial e o impacto resultante desse evento adverso. Riscos são investigados como reflexo da expressão de dois grupos de profissionais: especialistas em cibersegurança e criadores de ontologias pertinentes à cibersegurança. A forma como vulnerabilidades podem ser exploradas por atacantes é objeto de estudo de ambos os grupos. A própria definição da Internet das Coisas (IoT) refere-se a sistemas e dispositivos digitais com a capacidade de transferir dados através de redes sem qualquer interação humano para humano ou humano-computador. Em tais sistemas, em função do espaço, descentralização e modo de operação, espera-se que haja vários tipos de riscos cibernéticos, sendo estes referenciados como riscos de IoT (KANDASAMY *et al.*, 2020).

Ameaças internas podem gerar desafios únicos para o processo de avaliação de risco em ambientes corporativos. Por exemplo, uma simples foto ou vídeo com informações organizacionais confidenciais coletada por um intruso interno pode ser deliberadamente compartilhada a terceiros com objetivos de causar algum dano à organização. É possível ainda que um intruso utilize de dispositivos móveis como USB, *Bluetooth* ou WiFi para se conectar à rede ou provocar algum tipo de infecção por *malware*. A possibilidade de exploração das vulnerabilidades existentes no sistema IoT são tratadas como possíveis ameaças, levando à

necessidade de análise dos riscos do IoT neste ambiente. Por exemplo, o uso de dispositivos IoT para otimizar controles e viabilizar monitoramentos pode também comprometer plantas industriais e centros de informação. Entre os riscos IoT estão o risco ético, risco técnico e o risco de segurança e privacidade (KANDASAMY *et al.*, 2020).

De forma a endereçar o tratamento dos riscos presentes em operações com sistemas de informação, foram criados, ao longo do tempo, alguns métodos de análise de risco cibernético (*Cyber Security Risk Framework* - CSRF) com diferentes abordagens e considerações. A Tabela 8 descreve de forma sumária alguns dos principais *frameworks* usados para análise de risco em sistemas.

A Tabela 5 contém estruturas de análise de risco identificadas na bibliografia, não sendo encontrado um modelo específico e maduro para abordagem dedicada a riscos da IoT. Avaliação de risco por modelos genéricos podem ser utilizados em diversos tipos de sistemas, incluindo IoT, porém não consegue englobar situações específicas e problemas particulares a este tipo de rede. Desta forma, a criação de um modelo de análise de risco específico para tecnologias IoT objeto deste estudo preenche uma lacuna existente na bibliografia e no mercado quanto à consideração ampla e assertiva de riscos IoT em análises de risco que auxiliarão na elevação de maturidade de segurança em sistemas que utilizam a tecnologia.

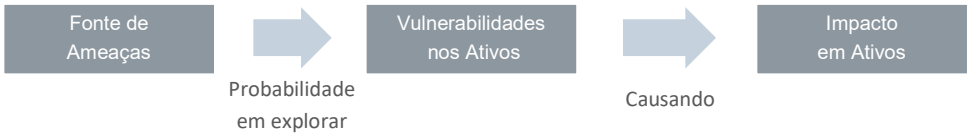
Tabela 5. Estruturas de Análise de Risco em TI

CSRF		DESCRIÇÃO
CVSS	Common Vulnerability Score System	Padrão para avaliar a gravidade das vulnerabilidades cibernéticas na escala de 1 a 10
FAIR	Factor Analysis of Information Risk	Metodologia para quantificar os fatores relativos ao seu risco.
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Avaliação abrangente de risco e procedimento de avaliação com quatro fases, desde a seleção de critérios de medição de risco até a identificação de abordagens de mitigação
CMMI	Capability Maturity Model Integration	Modelo de maturidade de 5 níveis com orientações através dos melhores estudos de caso para a melhoria contínua dos métodos de produção, especialmente no desenvolvimento de software.
TARA	Threat Agent Risk Assessment	Metodologia de identificação / classificação e filtro de ameaças que prioriza mitigações em relação à importância da ameaça
NIST SP800	National Institute of Standards and Technology, Special Publication	Estrutura de risco de segurança cibernética. O NIST SP800 é uma lista abrangente de contramedidas / controle para ameaças cibernéticas.

Fonte: SHEEHAN et al. (2021)

A Abordagem em Avaliação de Risco pode ser realizada de forma quantitativa ou qualitativa. As avaliações quantitativas de risco exigem valores numéricos para fatores de risco, enquanto os métodos qualitativos empregam valores de prioridade ou criticidade não numéricos. Entre as razões para utilizar métodos quantitativos estão a objetividade dos critérios utilizados na avaliação de risco e a facilidade em mensurar o nível de segurança de um sistema de TI em termos dos três pilares comuns de segurança: confidencialidade, integridade e disponibilidade (AKSU *et al.*, 2017). Ilustrando parte do modelo de análise de risco base, a Figura 13 aborda como vulnerabilidades podem ser avaliadas quanto a sua exploração e impacto para ativos.

Figura 13. Modelo para Análise de Risco



Fonte: Aksu et. Al. (2017)

Os elementos básicos tangíveis de risco em um sistema de TI podem ser enumerados como ativos, vulnerabilidades e ameaças. Em seu modelo, Aksu e colaboradores (2017) abordam que um ativo é qualquer computador ou equipamento de rede, físico ou virtual, no qual possam existir vulnerabilidades relacionadas a software. O processo de análise de risco e definição de métricas de maturidade envolve uma sequência de etapas como a (1) identificação de fontes de ameaças, (2) identificação de vulnerabilidades, (3) determinação da probabilidade de ocorrência, (4) determinação da magnitude do impacto e, finalmente, a (5) determinação do risco.

As fontes de ameaças no modelo podem ser hackers atacando da Internet ou usuários mal-intencionados atacando de um local específico dentro da rede que está sendo avaliada, dependendo da capacidade e motivação dos atacantes. A capacidade de uma fonte de ameaça é a medida da capacidade de uma fonte de ameaça em explorar as vulnerabilidades conhecidas. A motivação, por outro lado, mostra até que ponto um invasor está disposto e resoluto em capturar um alvo por meio da exploração das vulnerabilidades (HENRIE, 2013). A

Tabela 6 contém o conceito de vulnerabilidade, ameaça e consequência utilizadas nesta dissertação.

Tabela 6. Parâmetros de Gestão de Risco em Sistemas

Característica	Descrição
Vulnerabilidade	Uma fraqueza no sistema que pode ser explorada
Ameaça	Agentes internos ou externos destinados a perturbar ou causar danos à organização
Consequência	Resultado no sistema se a ameaça explorou com sucesso a vulnerabilidade

Fonte: Henrie (2013)

Assim como Henrie (2013), nesta dissertação o risco é considerado como uma relação entre vulnerabilidades, ameaças e consequências oriundas de eventos intencionais ou não intencionais, sendo necessário uma compreensão organizacional das três variáveis no contexto da análise de resiliência da rede. O aspecto quantitativo do modelo de maturidade, por sua vez, possui maior foco em vulnerabilidades existentes e nas consequências de eventos indesejáveis decorrentes destas. Não é escopo deste estudo abordar de forma quantitativa aspectos em ameaças como motivação e capacidade de atacantes bem como complexidade de explorações das vulnerabilidades analisadas.

3 Metodologia

Segundo Marconi e Lakatos (2003), não há ciência sem o emprego de métodos científicos. Desta forma, o método é composto pelo conjunto de atividades sistemáticas e racionais que permitem alcançar o objetivo esperado com maior segurança e economia, possibilitando aquisição de conhecimentos válidos e verdadeiros com a descrição do percurso percorrido, auxiliando na decisão dos cientistas.

Esta seção destina-se a descrever a metodologia e principais etapas utilizadas neste estudo. Na Tabela 7 são apresentados o tipo de pesquisa, procedimento, natureza das variáveis do estudo e método. Mais adiante é descrito também o desenho da pesquisa abordando etapas realizadas durante a elaboração e desenvolvimento da dissertação.

Quanto ao tipo, pode-se classificar este estudo como exploratório e descritivo, tendo como objetivo o estudo preliminar da área proposta, aprofundando conceitos e características da área de estudo, seguindo por análise qualitativa dos resultados encontrados na literatura.

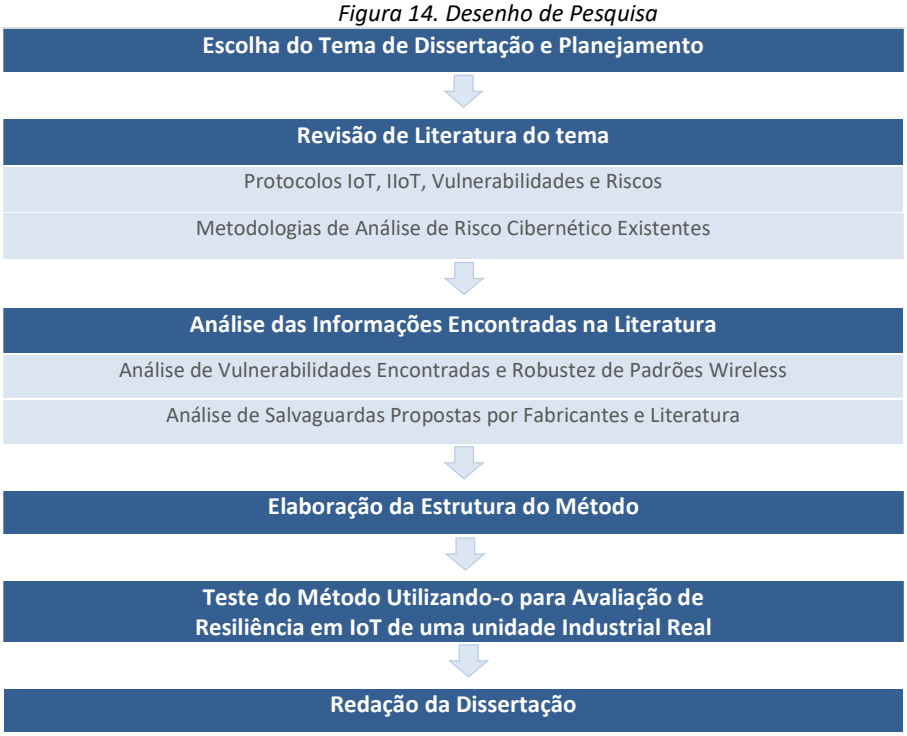
Tabela 7. Descrição Metodológica

Tipo de Pesquisa	**Pesquisa Exploratória e Descritiva**
Procedimento Técnico	**Pesquisa Bibliográfica e Análise de Aplicabilidade**
Natureza das Variáveis	**Qualitativa**
Método e Procedimento	**Comparativo e Estruturalista**

Autor: elaboração própria

Segundo Lando (2020) em uma abordagem qualitativa, é pressuposto que o significado atribuído a um fenômeno possui elevada importância para o entendimento e descrição de determinados contextos. Neste estudo, serão explorados e analisados dados qualitativos sobre a área de pesquisa, de modo a entender as vulnerabilidades existentes e a mecânica de ataques cibernéticos. As vulnerabilidades e desafios encontrados foram identificados, classificados, priorizados e tratados individualmente de forma a encontrar ações práticas que evitem ou mitigue eventos de sinistros em sistemas de produção e TI em ambiente de manufatura digital. A Figura 14 descreve o plano de condução deste estudo, incluindo etapas e atividades:

Figura 14. Desenho de Pesquisa



Autor: elaboração própria

A identificação de parâmetros de segurança em redes IIoT, desde características em tecnologias específicas até estruturas de gestão de risco importantes para uma operação segura compõe os polos teóricos deste estudo. Desta forma, a literatura foi abordada de forma sistemática para composição de elementos teóricos conforme áreas de busca descritas a seguir:

a. Protocolos de comunicação IIoT
b. Vulnerabilidades em redes IIoT
c. Segurança aplicada aos principais protocolos IIoT
d. Estruturas de gestão de risco em sistemas e redes IIoT

Após identificação das áreas, foram definidas as palavras chaves e a fonte de busca, sendo esta o site Google Acadêmico (https://scholar.google.com.br), que traz resultados contidos em outras plataformas como Science Direct, Scielo, IEEExplore, entre outros repositórios de instituições e universidades. Para cada pesquisa, foram analisadas dez páginas de resultado. A Tabela 8 mostra as palavras chaves utilizadas na pesquisa bibliográfica:

Tabela 8. Palavras chaves utilizadas na Revisão Sistemática

Área de Busca	N	Palavra-Chave 1		Palavra-Chave 2		Palavra-Chave 3
1. **Protocolos de comunicação IoT**	1	"Wireless"	AND	“Protocols” OR “Industry” OR “CPS”	AND	“Review”
	2	"IoT"	AND	“Protocols” OR “Industry” OR “CPS”	AND	“Review”
2. **Vulnerabilidades em redes IoT**	3	"Wireless" OR "IoT"	AND	“Vulnerabilities” OR “Problems” OR “Attack”	AND	“Industry” OR “CPS”
3. **Segurança em redes IoT**	4	"Wireless" OR "IoT"	AND	“Security” OR “Resilience”	AND	“Industry” OR “CPS”
4. **Estruturas de gestão de risco em redes IoT**	5	“Wireless” OR “IoT” OR “Cyber”	AND	“Security” OR “Risk”	AND	“Method” OR “Maturity Model”
	6	“Cyber”	AND	“Security” OR “Risk”	AND	“Quantification” OR “Quantitative”

Autor: elaboração própria

A plataforma de busca foi configurada ainda para classificar os resultados por relevância, excluindo patentes e citações. Os estudos encontrados durante a exploração da literatura foram selecionados através da relevância e aderência ao tema desta dissertação que foi aferida através de características como título, palavras-chaves, resumo e exploração do conteúdo.

Com a exploração da literatura encontrada através das palavras chaves descritas na Tabela 9 foi possível avaliar aspectos de segurança da integração de tecnologias IoT em ambientes industriais. Esta etapa suporta este estudo na identificação de tecnologias utilizadas e riscos existentes na comunicação IoT, fornecendo informações para uma pesquisa adicional com o intuito de identificar requisitos específicos de resiliência para os principais padrões de comunicação utilizados. A Tabela 4 indica as palavras chaves utilizadas para a pesquisa específica de diferentes protocolos de comunicação.

Tabela 9. Pesquisa de Protocolos IoT Específicos

Palavras chave 1		Palavra Chave 2
"Wireless Hart"	AND	"Security" OR "Resilience"
"ISA100"		
"ZigBee"		
"WiFi"		
"Bluetooth"		
"LoRa"		
"SigFox"		
"LTE-M"		
"NB-IoT"		

Autor: elaboração própria

Os critérios para a busca específica foram os mesmos já utilizados na exploração inicial da literatura, sendo o site Google Acadêmico (https://scholar.google.com.br) novamente a fonte de pesquisa, analisando dez páginas de resultado.

Esta dissertação se propõe a desenvolver um método que seja aplicável a diferentes ambientes com diferentes tecnologias e cenários operacionais. Neste aspecto, a exploração de vulnerabilidades específicas e as propostas de solução fornecidas na literatura auxiliam na composição de um mapa de riscos com ampla diversidade de cenários e situações. Juntamente com as informações referentes ao cenário macro de risco identificado inicialmente, as informações específicas fornecem elementos adicionais para a estruturação de avaliações e ações em um fluxo lógico que permite elevar a resiliência de redes IoT em ambientes industriais de forma abrangente.

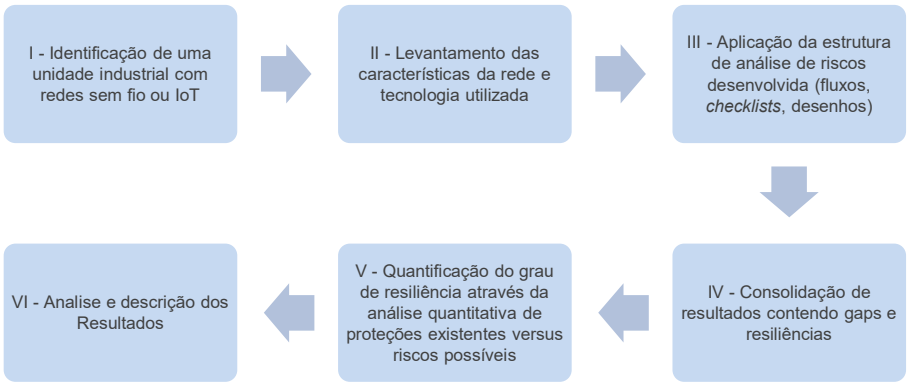
Após o mapeamento das principais tecnologias de comunicação IoT existentes aplicáveis em ambientes industriais, a análise específica de vulnerabilidades e interação destas redes contextualizada em possíveis ambientes físicos e lógicos resulta em uma listagem de pontos mais relevantes relacionados à resiliência para estes sistemas. Esta lista de pontos relevantes associadas a um fluxo lógico de verificação considerando etapas diferentes do ciclo de vida de redes IoT compõe, de forma macro, os elementos utilizados para o desenvolvimento do método proposto por esta dissertação.

Becker *et al*. (2009) aborda que modelos de maturidade na gestão de sistemas de informação devem conter critérios de medição e graus de maturidade que permitam uma compreensão do status atual e forneça uma base para priorização na implementação de ações. Com objetivo de fornecer um meio para quantificar o grau de vulnerabilidade existente através da aplicação do modelo proposto, outros modelos de maturidade e gestão de riscos, assim como artigos desta área, identificados através da pesquisa bibliográfica serão utilizados como referência.

Com o objetivo de avaliar a aderência e aplicabilidade prática do método desenvolvido em uma rede industrial real, o ASTRIS foi testado através da aplicação em uma rede de comunicação sem fio *Wireless*Hart utilizada para medição online de variáveis de processo e equipamentos em uma rede de controle de uma unidade industrial. O teste e análise de aplicação do método foi estruturado em 6 etapas, onde houve: (i) a identificação de uma unidade industrial com redes sem fio ou IoT elegível, (ii) levantamento das características da rede e tecnologia utilizada, (iii) aplicação da estrutura de análise de riscos desenvolvida (fluxos, *checklists*, desenhos), (iv) consolidação de resultados contendo gaps e resiliências, (v) quantificação do grau de resiliência, geral e por etapas, através da análise quantitativa de proteções existentes versus riscos possíveis, (vi) análise dos resultados.

A etapa (iii) do teste do método tem o objetivo de avaliar a aderência prática e contextualização dos riscos identificados na literatura ao ambiente industrial. Nesta fase, é possível realizar ajustes e calibrações no método para foco na identificação e mitigação de riscos relevantes dentro de ambientes industriais. A Figura 15 ilustra as etapas utilizadas no teste do método.

Figura 15. Metodologia para Teste de Aplicação do Método ASTRIS



Autor: elaboração própria

4 Análise de Riscos em Redes IoT

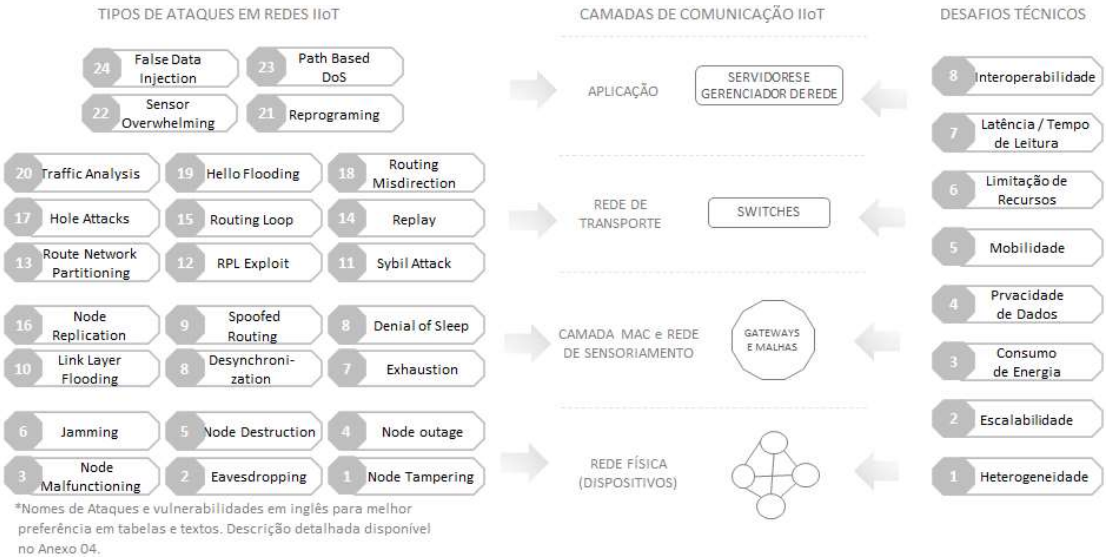
A compreensão de riscos desempenha um papel fundamental na gestão de segurança em sistemas. Vulnerabilidades e necessidades de informações podem variar ao longo do tempo, por esse motivo é importante uma gestão atualizada da rede e reduzir o alto número de vulnerabilidades disponíveis em bases de dados a quantidades utilizáveis. Dois dos principais recursos para compreender as vulnerabilidades são o National Vulnerability Database fornecido pelo NIST e o banco de dados Common Exposures and Vulnerabilities (CVE), que é organizado pelo Departamento de Segurança Interna dos EUA e CISA. Estes bancos de dados permitem identificar não só vulnerabilidades como remediações recomendadas para cenários de ameaças (HUDGENS; MEERS, 2021).

Uma vez definido o problema em identificar, proteger e gerenciar os riscos envolvidos em aplicações IIoT, é essencial compreender o modo de funcionamento destas redes e cada dispositivo utilizado em sua composição. Com base na revisão sistemática da literatura realizada neste estudo, foi possível abordar estas características em redes IIoT bem como informações pertinentes à gestão segura destas redes. Ao identificar que redes IIoT operam através da composição de diferentes camadas de comunicação, com diferentes riscos, é possível abordar as características específicas em cada uma destas camadas e tratar o risco conforme necessidades de cada segmento da rede. O mapeamento de riscos e desafios técnicos em redes IIoT baseados em estudos anteriores foi avaliado quanto à aplicabilidade em diferentes etapas no ciclo de vida destas redes.

Redes de sensoriamento e IoT operam através da composição de diferentes dispositivos que se comunicam, formando camadas de operação conforme descrito na Figura 16. Cada camada está sujeita a uma série de vulnerabilidades conforme características físicas e operacionais. A camada de rede em nível mais baixo, responsável pela medição e transmissão da variável monitorada ou controlada, é a rede física. Esta camada de rede, quando não protegida por controle de acesso, está sujeita a ataques com destruição do dispositivo, acesso ou bloqueio local inadvertido, interferências propositais, entre outros. Este tipo de ataque é possível através de fragilidades na segurança física das instalações, onde um atacante pode acessar nós físicos e realizar ações e acessos.

A Figura 16 ilustra os principais tipos de ataques e desafios técnicos em redes IoT e suas camadas de comunicação. Através da revisão de literatura realizada foi possível ainda identificar também as principais proteções recomendadas para mitigar riscos mencionados, das quais foram consideradas em sua integralidade ou através de seus mecanismos de funcionamento para composição do método ASTRIS proposto.

Figura 16. Ataques e Desafios em Redes IIoT



Autor: Elaboração própria - adaptado de BUTUN et.AL. (2020), SHUKLA e TRIPATHI (2018), BEKARA (2014), KOUTRAS et. Al. (2020), KITANO et. Al. (2014)

As camadas superiores, de link de comunicação sem fio e rede de transporte da informação, estão sujeitas a ataques onde o atacante faz uso de ferramentas para acesso de dispositivos da rede utilizando equipamentos para captura do sinal e envio de informações para nós e rede, na tentativa de obter respostas com algum dado importante sobre a rede ou para exaustão de dispositivos que operam através de bateria. Ataques nestas camadas são possíveis em função de fragilidades em *broadcast* e *advertising* de protocolos onde um nó implantado pode identificar informações da rede, realizando a substituição de um nó existente ou ganhando a confiança da rede, sendo a porta de entrada para diversos tipos de ataques mencionados na Figura 16 (de forma macro) e no Anexo 4 (em detalhes).

As redes IoT existem com o propósito de permitirem monitoramento ou controle de variáveis não viáveis com outras tecnologias de transporte da informação. Deste modo, a

camada de aplicação possui elevada importância para a segurança da rede por ser a parte responsável por disponibilizar as informações ou enviá-las a outros sistemas integrados. Ao longo do ciclo de vida da rede, os servidores que hospedam a aplicação podem apresentar algumas vulnerabilidades com relação a sua segurança física (em caso de servidor físico) estando sujeito a falha física (discos, placas, etc.), infecção por malware, acesso de terceiros não autorizados, entre outros, devendo possuir meios para recuperação de desastres como backups, procedimentos e documentos. Além dos desafios citados, deve-se garantir a segurança da aplicação e todos os outros sistemas conectados através de segmentação de rede por firewalls e políticas de autenticação segura para evitar uso inadvertido de protocolos como HTTP, MQTT ou outro.

Em um mesmo ambiente industrial pode haver diversas aplicações de redes *wireless*. Além de parâmetros técnicos como alcance, taxa de transferência, entre outros, deve-se levar em consideração a maturidade de segurança e as proteções de protocolos possíveis de serem utilizados e estabelecer políticas de uso seguro para implementação em ambientes corporativos. A Tabela 10 mostra a resiliência de diferentes protocolos de comunicação wireless frente a diferentes tipos de ataques.

Tabela 10. Resiliência de Redes Wireless a Cyber Ataques

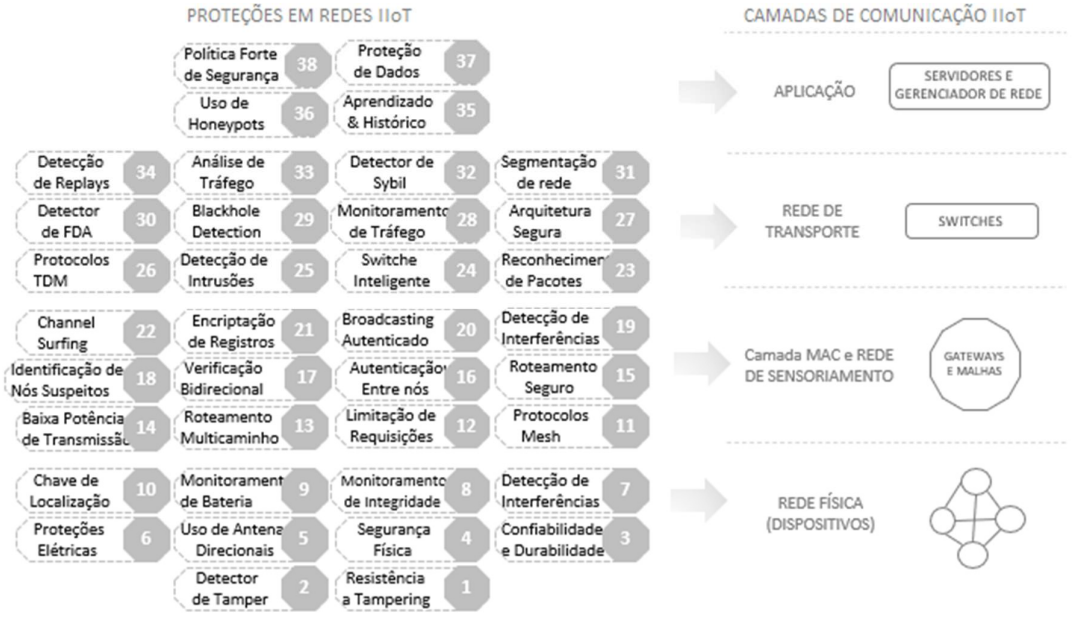
Tipo de Ataque	Camada	W. Hart	ISA100	ZigBee
Eavesdropping	Física	✓	✓	×
Node outage	Física	✓	✓	×
Traffic Analysis	Física	✓	✓	✓
Jamming	Física	✓	✓	✓
Node Tampering	Física	✓	✓	✓
Exhaustion	MAC	✓	✓	×
BlackHole	Network	✓	✓	✓
SinkHole	Network	✓	×	×
Wormhole	Network	✓	✓	×
Sybil Attack	Network	✓	×	✓
DoS	Aplicação	✓	✓	×
Spoofing	**Aplicação**	✓	×	×
Replay	**Aplicação**	✓	×	×
Sniffing	**Network**	✓	✓	✓

× - Foi encontrado um ou mais estudos com vulnerabilidade explorada ou mencionada.
✓ - Foi encontrado um ou mais estudos mencionando segurança para o ataque mencionado e não foi encontrado artigo com possibilidade de exploração do referente ataque no respectivo protocolo.

Autor: Elaboração própria - compilado de Emerson (2016), Raza et. Al. (2009), Raza et. Al. (2010), Kitano et. Al. (2014), Alcaraz e Lopez (2010), FAN et. Al. (2017), Radmand et. Al. (2010), Tournier et. Al (2020), Basu e Mohapatra (2020), Smile et. Al. (2019), Koutras et. Al. (2020), Coman et. Al. (2019), Chackp e Deepu (2018), Zaraket et. Al. (2021), Campillo (2017), Zou et. Al. (2016).

Em função da ampla diversidade de aplicações, resiliência e maturidade de redes wireless, faz-se necessário avaliar os tipos de proteções nativas, dispositivos adicionais de segurança e políticas de uso que habilitem estes protocolos para uso seguro e confiável de acordo com a criticidade do ambiente ou sistema aplicado. De modo a identificar salvaguardas nativas ou que podem ser adicionadas para resiliência de redes wireless contra ataques, os achados de literatura foram decompostos em elementos com o intuito de estabelecer relações de causa e efeito dentro do contexto de aplicação, ilustradas através Figura 17. Neste âmbito, foi realizada a correlação de elementos entre diferentes fontes bibliográficas com a necessidade de suposições técnicas parte embasada pela interpretação da bibliografia e parte embasada pela experiência do autor na gestão de redes industriais.

Figura 17. Proteções em Redes IIoT

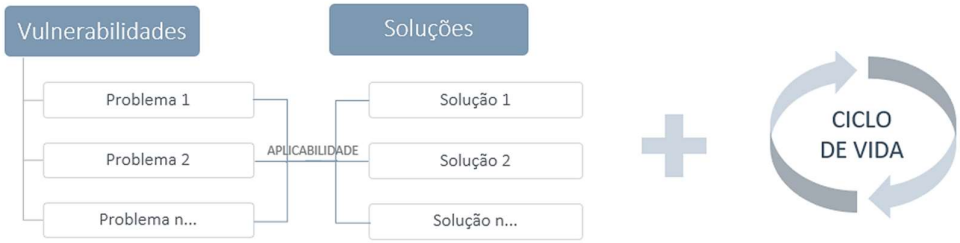


Autor: Elaboração própria - adaptado de Emerson (2016), Raza et. Al. (2009), Raza et. Al. (2010), Kitano et. Al. (2014), Alcaraz e Lopez (2010), Fan et. Al. (2017), Radmand et. Al. (2010), Tournier et. Al (2020), Basu e Mohapatra (2020), Smile et. Al. (2019), Koutras et. Al. (2020), Coman et. Al. (2019), Chackp e Deepu (2018), Zaraket et. Al. (2021), Campillo (2017), ZOU et. Al. (2016).

Como representado através da Figura 18, após correlação entre vulnerabilidades e soluções, cada elemento encontrado na bibliografia foi associado a uma determinada fase no ciclo de vida, estruturando um fluxo para verificação deste elemento durante análise de resiliência da rede IIoT. A análise das ameaças e vulnerabilidades no contexto de redes IIoT,

abordando estas em camadas, permite considerar particularidades não consideradas por *frameworks* existentes, enquanto a abordagem através do ciclo de vida como um todo permite considerar ações mais abrangentes e consistentes para a segurança da rede.

Figura 18. Vulnerabilidades, Soluções e Ciclo de Vida do IoT



Fonte: elaboração própria

A segurança e disponibilidade de redes IoT está diretamente ligada ao tratamento das vulnerabilidades e desafios identificados durante o ciclo de vida destas redes. Em ambientes industriais, existem diferentes tipos de redes com diferentes tipos de criticidade. Redes de sensoriamento sem fio em zonas ICS deverão coexistir com outras tecnologias e sistemas em ambiente corporativo (fora da ICS) que também utilizam ondas de rádio para se conectarem à suas bases de dados e aplicações. Aplicações em redes conectadas a sistemas de controle são mais críticas e, por este motivo, devem possuir critérios de classificação que auxiliem na análise de resiliência requerida para estas redes durante seu ciclo de vida (precisão, latência e integridade, entre outros).

Com frequência cada vez maior, diferentes tipos de aplicações estão presentes em redes diferentes e com protocolos de comunicação sem fio diferentes. Sendo assim, se faz necessário aplicar medidas para controlar a coexistência entre esses padrões e garantir a confiabilidade da rede. Entre as medidas que visam permitir a confiabilidade de redes em ambientes heterogêneos estão:

- Diversidade de frequência e espaço;
- Testes de Coexistência;
- Gestão de espectro (*Greylisting*);
- Documentação e Políticas de Gestão;

De forma a suportar a implementação das medidas mencionadas e evitar problemas com a heterogeneidade de dispositivos IoT, sugere-se criar uma gestão do espaço e espectro em ambientes industriais, dedicando bandas de frequência para diferentes padrões quando houver o risco de interferência. As duas faixas de coexistência mais prováveis com diferentes padrões estão na banda de 2.4 GHz e 900 MHz, portanto é possível, por exemplo, realizar gestão que considere essas faixas de frequência, na ordem de MHz e de GHz.

Escalabilidade segura também é uma propriedade importante, à medida que visa manter o nível de resiliência mediante expansões, garantindo a capacidade de um sistema em lidar com cargas de trabalho crescentes. Sistemas IoT crescem em escala e serão potencialmente compostos por bilhões de interações distribuídas e serviços que abrangem vários domínios administrativos dispersos geograficamente e, por este motivo, analisar os impactos da expansão de redes IoT é uma preocupação relevante. Além da escalabilidade funcional que abrange o número de serviços compostos em um sistema IoT, há também a escalabilidade vertical e a horizontal. A escalabilidade vertical se refere à adição ou remoção de recursos de computação em um único nó, enquanto a escalabilidade horizontal envolve a adição ou remoção de nós (MOLINA, 2019).

Em função do grande número de nós distribuídos muitas vezes em regiões de alta densidade e grande escala, é importante determinar o número de colisões de pacotes que podem ocorrer sem afetar a rede. Cada padrão possui um número máximo de nós que podem se comunicar através de um *gateway* e diferentes capacidades de canais de comunicação, deste modo essas são importantes características a serem consideradas na implementação e expansões de soluções IoT (LAVRIC; POPA, 2018).

Uma eficiente gestão da escalabilidade durante ciclo de vida de sistemas IoT pode requerer técnicas e recursos de suporte. Entre os recursos de suporte à escalabilidade estão hardware, software (ferramentas de análise), rede e expertise (interna ou externa). Entre as técnicas de controle para escalar redes IoT, estão o *bootstrapping* automatizado e o desenvolvimento de arquitetura de microsserviços. Em um sistema escalável, se os requisitos de memória do sistema aumentam conforme há um aumento na quantidade de dados, então ele não cresce a níveis não suportados. Além disso, o dispositivo opera sem problemas e com parâmetros aceitáveis, independentemente do tamanho do dispositivo. Portanto, a

capacidade em ser escalonável é importante para tornar soluções IoT mais eficientes para uso presente e futuro (GUPTA *et al.*, 2017).

Por precisar operar por anos até que necessite de manutenção em baterias de dispositivos, redes IoT demandam sensores com baixo consumo de energia, reduzindo a necessidade de intervenções durante o ciclo de vida do dispositivo. Operar por anos sem necessitar de trocas de bateria é possível através de tecnologias de processamento de baixo consumo de energia (na ordem de mW em potência) e outras medidas de economia de energia, como o tempo em que o dispositivo pode ficar em *stand-by* durante o seu ciclo de vida.

O tempo de vida útil da bateria dos dispositivos depende dos fatores mencionados acima e de forma variável de acordo com o seu uso. Embora este tempo em determinados padrões possa ser estimado de acordo com sua aplicação, não é possível realizar esta avaliação de forma precisa em função de diversos fatores envolvidos e variando com o tempo. Desta forma, a abordagem mais adequada para gestão de autonomia em energia dos dispositivos IoT ocorre através de monitoramento preditivo da carga dos dispositivos e de saúde da rede. Alertas de bateria baixa que informem ao gestor da rede ou time operacional e manutenção sobre necessidade de troca de baterias, com tempo previsto de vida útil do dispositivo até a sua falha, permitem a otimização do consumo das baterias e do processo de manutenção relativo à energia dos dispositivos.

Desde a escolha do padrão a ser utilizado até a gestão de ciclo de vida de redes IoT e seus nós, considerar os fatores que influenciam o tempo de vida útil das células de energia dos dispositivos, bem como o formato de gestão da rede permite reduzir a probabilidade de haver problemas de disponibilidade e segurança por conta de nós em falha ou mal funcionamento.

5 Resultados

Através da metodologia proposta nesta dissertação, com levantamento e análise das tecnologias *wireless* aplicáveis em ambiente industrial, bem como ameaças e vulnerabilidades é possível estabelecer uma estrutura para identificação e caracterização de riscos IIoT que auxiliam na compreensão de estruturas de resiliência para estas redes. Este capítulo destina-se à descrição dos resultados e discussões geradas durante o desenvolvimento desta estrutura, denominada ASTRIS.

5.1 A Abordagem ASTRIS Para Avaliação de Segurança em IIoT

A aplicação de tecnologias IoT em diferentes ambientes adiciona uma série de desafios para que o seu uso ocorra de forma segura e eficiente, conforme designado. Com o objetivo de reunir elementos que suportem de forma sistematizada a consideração destes itens em novos projetos ou avaliação de bases instaladas, tais desafios foram agrupados em diferentes dimensões, conforme exposto na Tabela 11.

Tabela 11. Problemas advindos da aplicação de tecnologias IoT e wireless.

Problemas / Características	Dimensão
Coexistência, interferência, vida útil, alcance, sinal, classificação de área, mobilidade, densidade aérea	ÁREA
Confiabilidade, disponibilidade, latência, privacidade, criticidade	ZONA
Padrões, segurança, robustez, acessos	CAMADAS (STACK)
Ataques externos, ataques internos, problemas de confiabilidade	AMEAÇAS &VULNERABILIDADES
Proteções, resiliência, mitigações	RESILIÊNCIA
Treinamentos, gestão de senhas, monitoramento, manutenção	IMPLEMENTAÇÃO E OPERAÇÃO
escalabilidade, Interoperabilidade, gestão de mudanças, ciclo de vida	ESCALABILIDADE

Fonte: autoria própria.

Um dos principais benefícios da tecnologia *wireless* é a viabilização de medições, monitoramentos e trabalho com conexão em qualquer local, podendo ainda ser fixa ou móvel. Instalações industriais são integradas por diferentes áreas, desde ambientes administrativos, áreas abertas e ruas até áreas produtivas compostas por equipamentos, estruturas operacionais e parques de tancagem. Cada ambiente físico possui diferentes características

como tipos de equipamento, densidade aérea e nível de explosividade, que requerem o uso tecnologias adequadas para cada local. Os ganhos de eficiência da integração de cadeias de suprimentos e acessos remotos ocasionam também a integração de ambientes externos a ambientes produtivos, a qual também deve possuir critérios de avaliação quanto à segurança destes ambientes.

Zonas produtivas com sistemas ciberfísicos responsáveis pela automação e segurança funcional de operações industriais possuem alto nível de confiabilidade e disponibilidade requerida. Em função de sua criticidade de custo e segurança para as empresas, bem como pela característica de intervalos de tempo de processamento curtos, estes sistemas são mais sensíveis a características de latência, confiabilidade e concentram ainda informações com classificação restrita relacionadas a segredos operacionais e receitas produtivas. Por este motivo, é necessário realizar considerações diferentes para as diferentes zonas (ou redes) a qual a aplicação IIoT irá operar.

A zona ICS inclui os instrumentos e equipamentos relacionados à medição, controle, segurança e supervisão de processos, conforme ilustrado na Figura 19. A aplicação em outras redes, normalmente separadas da rede ICS por *firewalls*, sendo elas utilizadas para a gestão da produção ou outras áreas corporativas também deve possuir critérios que auxiliem no seu uso, ciclo de vida e a evitar interferências em outras redes.

Figura 19. Zonas de aplicação de tecnologias IIoT

Fonte: autoria própria.

A análise da área física e zona de rede para determinado uso de tecnologias *wireless* deve ser acompanhada da avaliação de como todos os dispositivos da rede, desde o sensoriamento até a aplicação, serão inseridos e operados. Diferentes segmentos de redes IoT possuem diferentes tipos de ameaças e vulnerabilidades. A diversidade de ameaças e vulnerabilidades existentes em cada camada de comunicação, a qual pode operar também em diversidade de áreas físicas e zonas, justifica a existência de análises de segurança dedicadas para cada uma destas camadas.

A definição da área, zona de operação e camadas de comunicação (*stack*) compõe a caracterização do uso da IIoT, que serve como base para análises subsequentes. A identificação de todos os parâmetros envolvidos em cada uma destas dimensões deve ser realizada para garantir que o contexto local foi considerado e que todas as etapas de avaliação de riscos serão ajustadas para a aplicação conforme critérios de criticidade e características dos sistemas locais.

Após a caracterização, deve-se analisar as vulnerabilidades e ameaças aplicáveis para estabelecer ações de resiliência e fortificação da aplicação. Deve-se contemplar os cenários de risco e atender ao máximo possível às ações de resiliência estabelecidas. Nesta etapa, a solução escolhida para a determinada aplicação será avaliada quanto a sua robustez e ações adicionais de resiliência serão estabelecidas. Durante a análise de resiliência para aplicação pode ser identificado que a solução adotada e protocolo escolhido não atendam aos critérios de segurança estabelecidos, devendo ser revista a intenção de aplicação da solução desejada, realizando uma prova de conceito.

Os resultados da análise de vulnerabilidade e ações de fortificação e segurança da aplicação devem ser configurados e testados de modo a garantir que os requisitos de resiliência serão atendidos e mantidos com o passar do tempo. Os benefícios do uso de tecnologias *wireless* estimulam a aplicação de cada vez mais pontos de medição ou conexão com o passar do tempo, com novos dispositivos que devem atender a requisitos técnicos e de segurança que mantenham a confiabilidade de toda a rede. Escalabilidade é, portanto, uma importante dimensão para garantir que expansões ocorram de forma segura.

A análise dos principais problemas de confiabilidade e segurança decorrente da aplicação de redes IIoT leva a estabelecer dimensões que suportam a resiliência destas redes, permitindo a aplicação controlada e consciente desta tecnologia que contribui para um

ecossistema IIoT seguro e maduro. Organizando estas dimensões em um fluxo estruturado que possa ser adaptado para diferentes aplicações industriais foi possível chegar ao modelo de análise de risco ASTRIS, conforme descrito na Figura 20.

Figura 20. ASTRIS - Estrutura de resiliência IIoT

Fonte: autoria própria.

A estrutura ASTRIS para análise de resiliência e fortificação de redes IIoT deve ser acompanhada de políticas de segurança que endereçam questões macro como diretrizes corporativas sobre o uso de tecnologias *wireless*, gestão do espectro espaço aéreo, guia de uso de padrões específicos, política de projetos e infraestrutura, documentação requerida para gestão de IIoT, entre outras.

O método ASTRIS possui aplicabilidade para análise de estruturas e novos projetos IIoT desde a fase de pré-estudo até a fase de escalabilidade, auxiliando no mapeamento e endereçamento de quesitos de resiliência principalmente na etapa onde há maior detalhamento técnico da solução em que se deseja implementar, o projeto básico e detalhado (design). Diversos pontos de análise são considerados para as diferentes etapas do ciclo de vida de projetos e de aplicações IIoT, de forma que o máximo de vulnerabilidades sejam contempladas e avaliadas. A Figura 21 ilustra etapas em projetos IIoT contempladas na metodologia ASTRIS.

Figura 21. Etapas de Projetos IIoT e ASTRIS

Fonte: autoria própria.

Ao amplificar as possibilidades de digitalização e monitoramento que trazem benefícios significativos para empresas, o uso do IoT tem sido cada vez mais estimulado dentro de ambientes corporativos. Pessoas com expertise diferentes em design e segurança de sistemas têm implementado projetos IoT sem o devido cuidado com todas as etapas do ciclo de vida deste tipo de tecnologia descrito na Figura 21. Este é um problema que pode ocasionar perdas como falta de disponibilidade da ferramenta ou até o vazamento de informações e intrusões maliciosas com danos irreversíveis inclusive em outros sistemas. Esse é um dos motivos que justifica a implementação de uma sistemática de avaliação de riscos envolvidos no IIoT e implementação de ações de resiliência para estes sistemas.

5.2 ASTRIS – Fluxo de Análise

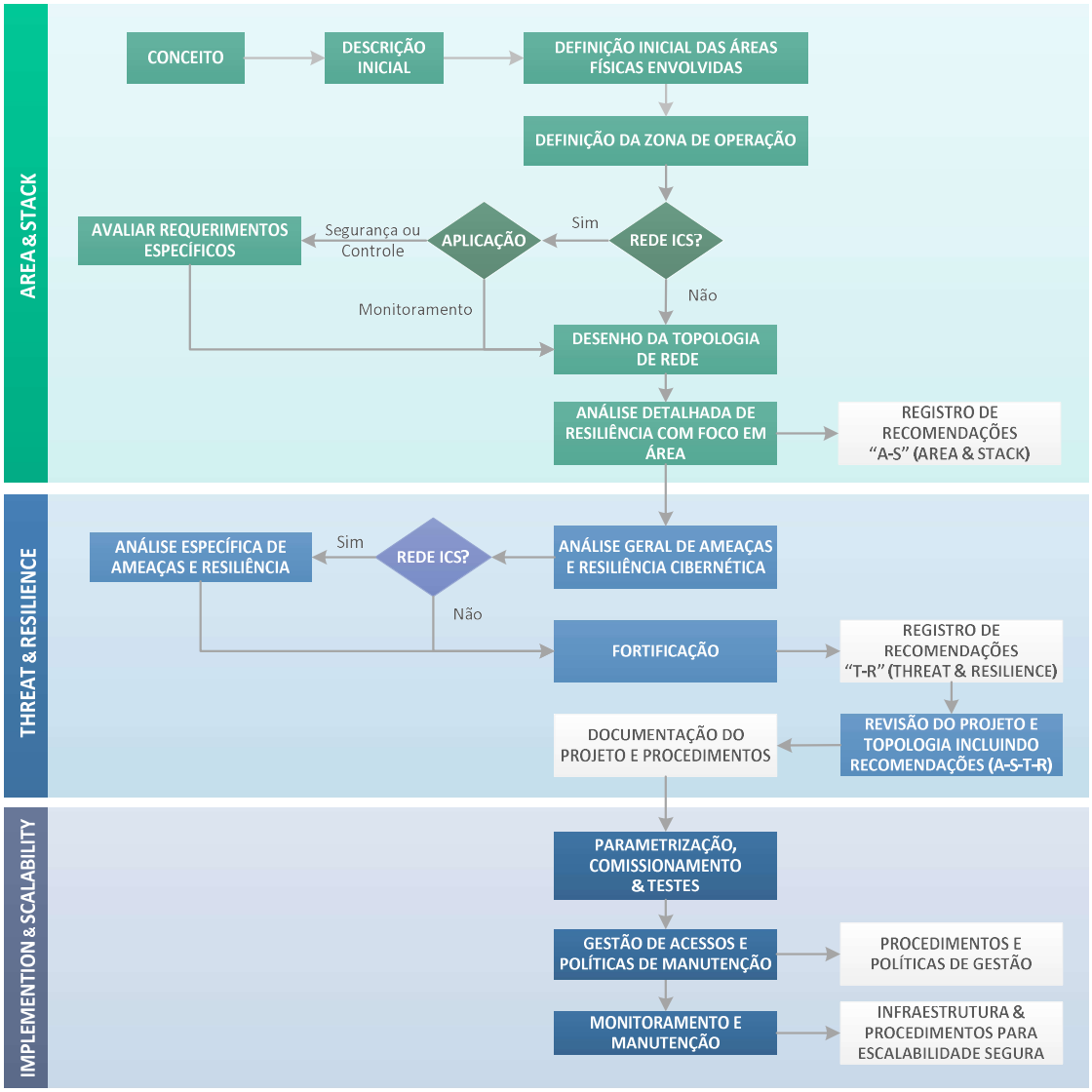
A análise de resiliência de redes *wireless* e projetos IoT através do método ASTRIS proposto inicia com a caracterização do sistema, através da definição da área física de operação, zona de aplicação e descrição inicial da topologia e camadas de comunicação. Após a descrição inicial de áreas e zonas de operação, em caso de aplicação para controle ou segurança em rede ICS deve ser realizada uma análise com requerimentos específicos para analisar inicialmente a aderência da solução estudada aos requisitos técnicos para estas aplicações de maior criticidade. A Figura 22 contém o fluxo de análise de resiliência para redes IIoT incluindo esta e outras etapas.

Caso a aplicação seja direcionada a redes não ICS ou para monitoramento de equipamentos, pode-se partir diretamente para o desenho da topologia e arquitetura de rede que viabilizará a aplicação. Esta caracterização será acompanhada por análise de resiliência para todos os componentes da rede, desde o dispositivo de campo até o usuário, com foco na adequação segura da rede aos espaços físicos que irão ocupar.

A avaliação da aplicação e da arquitetura relacionada ao espaço físico (aéreo ou terrestre) em que o sistema e seus dispositivos ocupam resulta em um primeiro conjunto de recomendações (recomendações de Area e *Stack* – *A&S*), responsável por elevar a confiabilidade de operação da rede. Após a avaliação de área e topologia, deve-se proceder com a análise de resiliência em segurança cibernética. Nesta etapa, a rede é verificada quanto

aos tipos de vulnerabilidades e ameaças existentes aplicáveis para a solução em design. O protocolo é avaliado quanto às proteções nativas e ações adicionais necessárias para a proteção da rede em função de especificidades do sistema ou de sua aplicação.

Figura 22. Fluxo de Análise de Resiliência ASTRIS



Fonte: autoria própria.

A resiliência em redes IoT depende não só da robustez de segurança do protocolo utilizado como também da forma como é implementado. Fazer bom uso das ferramentas de segurança e considerar algumas boas práticas durante a implementação de aplicações IoT

permitem elevar significativamente a resiliência da rede e reduzir riscos corporativos, isso sem necessariamente adicionar custo relevante ao design ou às operações. Ferramentas nativas de autenticação contra explorações de terceiros, *greylisting* de canais evitando o uso de espectro com potencial de interferência ou evitar antenas de alta potência em bordas locais reduzindo a chance de captura de sinal em região externa são algumas das ações de baixo custo e que auxiliam na redução do risco de exploração maliciosa da rede IoT.

Após a análise geral de ameaças e resiliência, especificamente para redes ICS, deve-se analisar também os requisitos específicos para este tipo de rede. Em função de sua maior criticidade, redes ICS devem ser ainda mais robustas frente a possíveis impactos com invasões ou infecções. Esta etapa contém requisitos que podem ser flexibilizados em aplicações menos críticas, evitando que haja superdimensionamento de segurança em tais aplicações com investimento equivocado de tempo e custo.

Após a análise de ameaças (T) e resiliência (R) é realizada a fortificação da rede, que gera um plano de recomendações ao final da etapa. Nesta altura da análise, existem dois registros de recomendações - A&S e T&R. Deve-se reavaliar a topologia definida no início da análise e revisar dispositivos, posicionamento e quaisquer outras ferramentas necessárias para a correta gestão da rede. Conhecendo a topologia requerida para o projeto ou rede IoT resiliente, é possível estabelecer documentação e procedimentos necessários para realizar a configuração e comissionamento da rede, sendo este o próximo passo do projeto (implementação).

Na etapa de implementação, além das recomendações listadas nas etapas anteriores, deve-se configurar os dispositivos da rede para a melhor performance funcional e de segurança. Aspectos como parametrização da aplicação, alarmes, diagnósticos entre outros, devem ser configurados e testados de forma sistematizada através documentos e checklists de startup que representem os requisitos técnicos necessários para a operação e manutenção da rede. A correta operação, monitoramento e manutenção da rede requer também uma equipe capacitada, com elevada cultura de segurança e continuamente atualizada. Estas características são obtidas através de políticas organizacionais, diretrizes corporativas e investimentos voltados para o desenvolvimento de pessoas e infraestrutura. Nesta etapa, o modelo ASTRIS auxilia em algumas destas questões com instruções objetivas sobre

implementação e operação segura de redes IoT, bem como ao definir a necessidade de desenvolvimento de diretrizes e políticas corporativas voltadas para a segurança do IoT.

De modo a fornecer meios para estabelecer níveis, classificações ou escalas de maturidade através do método proposto, modelos de maturidade em segurança devem apresentar uma forma para quantificação de riscos e vulnerabilidades. Após identificação dos principais elementos constituintes do modelo e formulação de um fluxo de análise e verificação, uma abordagem quantitativa para representação da aderência da rede avaliada possui os seguintes benefícios:

i. Desenvolver critérios para priorização e tomadas decisão,
ii. Facilitar a realização de benchmark e comparações entre redes,
iii. Fornecer informações para monitoramento e gestão de riscos,
iv. Identificar e quantificar a resiliência da rede por critérios numéricos e níveis de maturidade.

Uma das formas de quantificar o grau de severidade com que vulnerabilidades e ameaças podem afetar redes IIoT é através da análise de impacto para o funcionamento da rede em caso de exploração inadvertida. Como abordado anteriormente, disponibilidade, integridade, confidencialidade e até segurança de pessoas podem ser impactadas em diferentes formas, conforme matriz de impacto descrita na Tabela 12.

Tabela 12. Matriz de Impacto – para classificação

Impacto	Grau de Impacto	Disponibilidade	Integridade ou Funcionalidade	Confidencialidade	Segurança (safety)
Baixo	1	< 1h	Impacto Parcial Baixo	Vazamento de Informação Interna	Sem danos a pessoas e estruturas
Médio	2	> 1 h e < 1 dia	Impacto Parcial Alto	Vazamento de Informação Restrita	Danos a equipamentos
Alto	3	> 1 dia	Perda Integral de Integridade	Vazamento de Informação Secreta	Segurança de Pessoas

Fonte: elaboração própria

As vulnerabilidades, ameaças e resiliências requeridas foram classificadas individualmente com o grau de impacto para a rede em análise. Os resultados das classificações individuais são somados por área de análise (*Area, Threat, Implementation,*

Scalability) compondo índices de maturidade por área e um índice de maturidade geral para a rede. Estes índices, que vão de 0% a 100%, podem ser utilizados para a tomada de decisão e monitoramento, de modo a garantir nível de resiliência aceitável conforme política de segurança definida pela empresa.

Além dos aspectos de avaliação de resiliência e ações voltadas para a rede, o desenvolvimento de consciência sobre os riscos envolvidos no uso de tecnologias emergentes não deve ser uma barreira para a implementação destas. Entender a ocupação do espaço aéreo, as variáveis envolvidas e a gestão necessária para a operação segura de redes IIoT deve ser um exercício comum para profissionais modernos. Conciliar a extração de benefícios do IIoT com segurança operacional deve ser objeto de desenvolvimento cultural organizacional para a construção de um ambiente maduro neste tipo de tecnologia.

Políticas voltadas para o IIoT devem considerar a gestão de espectro no espaço aéreo dentro do ambiente corporativo, considerando as diferentes características locais, tipos de instalação e regulações. Diretrizes com guias gerais e aceitabilidade para diferentes protocolos em diferentes aplicações podem, junto com procedimentos e manuais específicos, auxiliar na avaliação de requisitos técnicos desde a idealização da solução até a implementação e operação (assim como em expansões futuras). Desta forma, como parte de uma política corporativa voltada para a segurança em redes IIoT, o modelo ASTRIS tem o potencial de auxiliar na elevação de maturidade de segurança destas redes e possibilitar uso cada vez mais amplo, acelerando a transição de sistemas legado para sistemas sem fio sem redução de segurança e confiabilidade.

5.3 Aplicação do ASTRIS em Unidade Real de Planta Industrial

O método ASTRIS tem o objetivo de elevar a maturidade de segurança e resiliência de redes IoT em unidades industriais e reduzir riscos com a sua utilização. Como teste do método proposto, o modelo deve ser avaliado quanto à viabilidade e performance na aplicação a sistemas reais dentro da indústria. Deste modo, a validação do ASTRIS ocorrerá através da avaliação da resiliência atual da rede de sensoriamento *wireless* existente em uma unidade de produção industrial do polo petroquímico de Camaçari, na Bahia. A unidade em estudo conta com sistemas de instrumentação, automação e gestão da produção de acordo com a

ISA 95 e vem aproveitando do baixo custo de tecnologias wireless para adicionar novas medições de processo a seu sistema.

5.3.1 Estudo de Caso – *Wireless*HART

Um dos principais protocolos de comunicação utilizados na indústria para viabilizar a comunicação sem fio entre dispositivos e sistemas de controle e monitoramento é o padrão *Wireless*HART. Embora este protocolo já possua mais de 10 anos de operação e maturidade dentro da indústria química e possua robustez relevante em segurança, empresas fornecedoras da solução e clientes raramente consideram aspectos além de questões funcionais. Na prática, isto ocasiona a existência de diversas aplicações wirelessHART sem a configuração e uso de ferramentas de resiliência nativas, bem como sem a presença de políticas e cultura voltadas para a segurança destas redes.

Com o intuito de avaliar a eficácia do modelo de análise de risco proposto em identificar vulnerabilidades e avaliar a resiliência de aplicações IIoT, o ASTRIS foi utilizado para avaliar os riscos presentes em uma rede de sensoriamento wireless de uma unidade industrial real no polo petroquímico de Camaçari-BA (Figura 23). A aplicação abordada possui o objetivo de monitorar equipamentos industriais através de sensores em campo e comunicação na camada ICS, com o objetivo de possibilitar a transição de manutenção preventiva para manutenção baseada em condição. Os resultados desta análise irão auxiliar não somente na elevação da robustez de segurança da aplicação como na elevação da maturidade no uso do wirelessHART na indústria que o habilitará para maior uso em controles e sistemas críticos.

Figura 23. Polo Petroquímico de Camaçari

Fonte: Prefeitura de Camaçari, 2021

O modelo ASTRIS pode ser dividido em 3 etapas principais: A & S (*area & stack*), T & S (*threat and resilience*) e I & S (*implementation and scalability*). As 3 sessões a seguir desta

dissertação possuem o objetivo de descrever o processo de avaliação da segurança da aplicação mencionada levando em consideração estas etapas. É válido mencionar que o ambiente de análise, ou seja, as instalações e aplicações avaliadas possuem nível moderado de segurança em sistemas de manufatura e patrimonial. Este é um aspecto que influencia significativamente nos resultados da análise.

Implementar ações para mitigação de riscos e ameaças requer analisar o custo e os benefícios que cada proteção adicionada irá apresentar. Tanto no design quanto na avaliação de redes já operacionais, deve-se realizar diferentes medidas em diferentes esferas que minimizam a chance de um incidente envolvendo segurança da rede, bem como um bom plano de recuperação de desastres. De modo a ilustrar a estimativa aproximada dos custos envolvidos em cada ação de proposta através da análise de risco devido à necessidade de configurações, parametrizações, interligações, infraestruturas, hardware, licenças, serviços, entre outros, foram criadas 5 faixas de custo com os símbolos de identificação conforme descrito na Tabela 13.

Tabela 13. Faixas e símbolos utilizados para Representar Custos em Ações de Resiliência

Descrição	Símbolo
Custos com serviços, infraestrutura, licenças, hardware < 3k R$	$
Custos com serviços, infraestrutura, licenças, hardware > 3k R$ e < 10k R$	$$
Custos com serviços, infraestrutura, licenças, hardware > 10k R$ e < 50k R$	$$$
Custos com serviços, infraestrutura, licenças, hardware > 50k R$ e < 100k R$	$$$$
Custos com serviços, infraestrutura, licenças, hardware > 100k R$	$$$$$

Fonte: autoria própria.

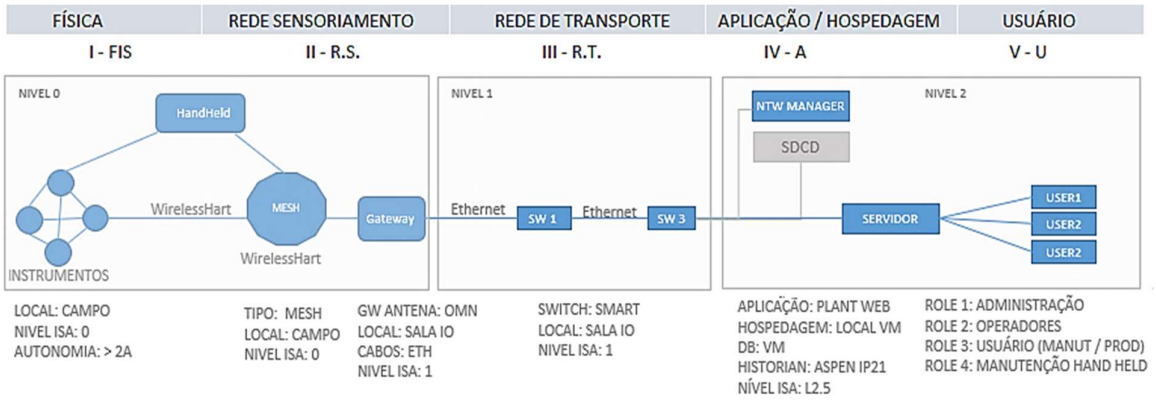
Com objetivo de simplificar a visualização e classificação de investimentos necessários, a tabela acima e a sua aplicação levam em consideração o histórico de custos da referida unidade industrial na implementação de medidas de segurança através de serviços e projetos implementados por equipes locais e terceiras.

5.3.2 A & S – Análise de Área e Stack (Camadas)

Um dos primeiros passos na análise de risco da rede é realizar a descrição da aplicação incluindo as áreas físicas, as camadas de comunicação e a zona de operação (ICS ou não ICS).

A rede WH em estudo opera através de instrumentos sem fio que monitoram variáveis de equipamentos e processo e estão integrados à rede ICS do site. As informações oriundas da rede WSN é enviada para uma aplicação de gestão inteligente de equipamentos localizada na rede DMZ. A Figura 24 ilustra as camadas de comunicação envolvidas na aplicação testada.

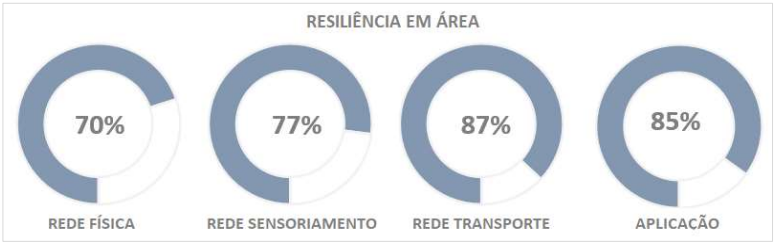
Figura 24. Desenho da Rede e Aplicação



Fonte: elaboração própria

Seguindo o fluxo da análise ASTRIS para área física, é possível identificar pontos fortes como alcance adequado da rede, correto grau de proteção de dispositivos para o meio em que ocupam, proteções elétricas e posicionamento otimizado (distanciamento entre nós, *gateways* e distância mínima de estruturas). Por outro lado, riscos relacionados à coexistência com outros sinais eram desconhecidos, bem como não havia ciência sobre o alcance da rede em locais de risco ou o acesso físico de terceiros a dispositivos físicos, de campo. A Figura 25 representa o grau de resiliência em termos de ocupação física das camadas de comunicação da rede do estudo de caso, através da análise quantitativa de proteções existentes versus riscos possíveis mapeados para esta etapa (em valor percentual).

Figura 25. Aspectos Quantitativos da Resiliência em Área

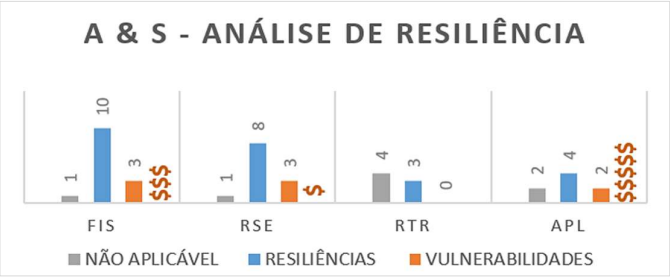


Fonte: autoria própria.

As redes de sensoriamento e de transporte de informação já possuem estrutura robusta com segurança de acessos, testes funcionais e equipamentos inteligentes com portas bloqueadas, entre outras proteções. A camada de aplicação também conta com equipamentos em ambiente controlado e com acessos protegidos, no entanto com ausência de política para *backup* das aplicações sem fio até o momento da análise. Outra oportunidade para melhoria na segurança e uso da rede é a forma de acesso dos usuários finais (engenheiros e técnicos de manutenção) à aplicação, que fica disponível apenas na camada L2 de automação, segundo a ISA 95, compartilhando interligações diretas de rede com o sistema supervisório, não estando disponível na rede de negócios. Isto ocasiona a necessidade de fornecer acesso de usuários a áreas restritas ou não limitar acesso dos usuários à ferramenta, prejudicando os benefícios do seu uso.

Os custos principais relacionados às ações de resiliência oriundas desta etapa distribuídos na Figura 26 se dão devido à necessidade de estabelecimento de gestão de acessos a áreas industriais abertas (referente à segurança da rede física) e à necessidade de estabelecimento de infraestrutura de segurança para disponibilizar a aplicação de forma adequada na rede de negócios, sendo necessário realizar avaliações de riscos , design de rede e aquisição/configuração de *firewalls*.

Figura 26. Vulnerabilidades encontradas na etapa A&S *(Area & Stack)*



Fonte: autoria própria

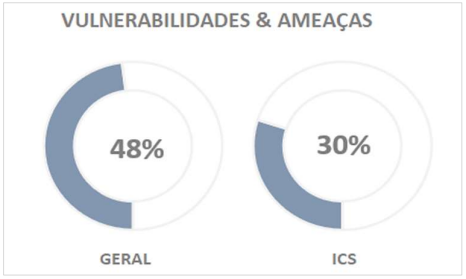
5.3.3 T & R – Análise de Ameaças e Resiliências

Após a caracterização, desenho e análise da área física que cada componente da rede ocupa, desde os elementos sensores até os usuários, parte-se para a análise de robustez da solução proposta mediante a diversas ameaças existentes nas redes IIoT. Utilizando o banco

de ameaças a redes IoT levantado na bibliografia e sua aplicabilidade à rede analisada, é verificado se existe mitigações (nativas ou criadas) para cada item ou se ações de resiliência ou proteção adicionais são requeridas.

Nesta etapa da análise foram identificadas 46 vulnerabilidades, sendo 15 relacionadas a itens gerais mandatórios a qualquer tipo de rede em ambiente industrial (ligado ou não a redes ICS) e 24 específicas para redes *wireless* em ambiente ICS. Adicionalmente 7 ações de fortificação de redes IoT recomendadas não foram consideradas para a rede em análise, não sendo atendidas. A Figura 27 ilustra os resultados quantitativos da análise de resiliência do protocolo perante possíveis vulnerabilidades e ameaças (em valor percentual).

Figura 27. Grau de Resiliência Relacionado a Vulnerabilidades e Ameaças



Fonte: autoria própria.

Entre os pontos analisados a qual a aplicação já apresentava resiliência, estão o robusto controle de acesso de todos os equipamentos da rede em todas as camadas de comunicação, a robustez de criptografia e método de autenticação do protocolo com salto de canais que auxilia na minimização de efeitos de interferência e topologia em *mesh* com rotas alternativas em caso de falha de um nó. Além disso, os dispositivos utilizados possuem amplo uso na indústria, com milhares de horas de operação e, portanto, elevada maturidade para a aplicação mencionada. Durante a instalação, foram seguidas recomendações quanto à distância de equipamentos e estruturas densas, bem como arranjo que possibilita a rede operar com todos os dispositivos com força acima de -75 dB.

Através da análise de ameaças foi identificado que, mesmo o WH possuindo elevada robustez e segurança em seu protocolo, o grau de resiliência geral da sua aplicação na rede perante ataques maliciosos possui é de 47%, como descrito na Figura 30. Foi identificado que

a rede apresentava senha de acesso fraca e sem proteção contra requisições não identificadas, sendo recomendada a alteração do modo de conexão entre os nós e os *gateways* de *Common Access List* para *Access Control List* onde a partir desta configuração, apenas nós de rede com autorização prévia dentro de uma lista de acesso irão conseguir se comunicar com os *gateways*. De modo a evitar a exploração indevida da rede por terceiros, bem como a perda não identificada de algum dispositivo da rede, foi visualizada a oportunidade em realizar monitoramento dos ativos, criar política de conscientização sobre segurança de dispositivos de campo e a implementação de segmentação segura de rede através de *firewalls* para proteção da rede ICS de ambos os lados de interface (tanto da rede *wireless* quanto da rede de negócios, necessária para acesso à aplicação).

O monitoramento de saúde e variáveis operacionais da rede e dos dispositivos *wireless* é uma recomendação que pode ainda solucionar problemas como a não detecção de nós suspeitos, injeção de dados falsos e a não detecção de falhas em baterias que podem levar à indisponibilidade de dispositivos e, consequentemente, buracos na rede que geram vulnerabilidades de segurança. Assim que uma falha ocorre, esta deve ser analisada por uma equipe treinada e deve haver alertas classificados, indicando a criticidade do evento.

O WH é utilizado como meio de comunicação para viabilizar novas medições com custo reduzido. Durante a implementação da aplicação que irá utilizar os dados oriundos de campo através do WH deve-se analisar todos os equipamentos e pessoas envolvidas durante do ciclo de vida da aplicação, desde usuários e operadores até pessoas responsáveis pela manutenção da solução. Este item não foi considerado durante o design da aplicação, sendo necessário realizar a definição de papéis e acessos à rede, bem como prover capacitação técnica e conceitual.

Devido à vulnerabilidade de comunicações *wireless* a ataques do tipo *jamming* e ao potencial de interromper comunicações críticas, é recomendada ainda a implementação de sistemas de prevenção e detecção a intrusões e interferências *wireless*, denominados wIPS (*wireless intrusion prevention system*). Recomenda-se ainda a aplicação combinada de antenas omnidirecionais e direcionais de acordo com a posição interna dos nós, de modo que antenas próximas as bordas da unidade direcionem sinal apenas para a parte interna das instalações físicas, evitando a existência e identificação de sinais fora das fronteiras físicas.

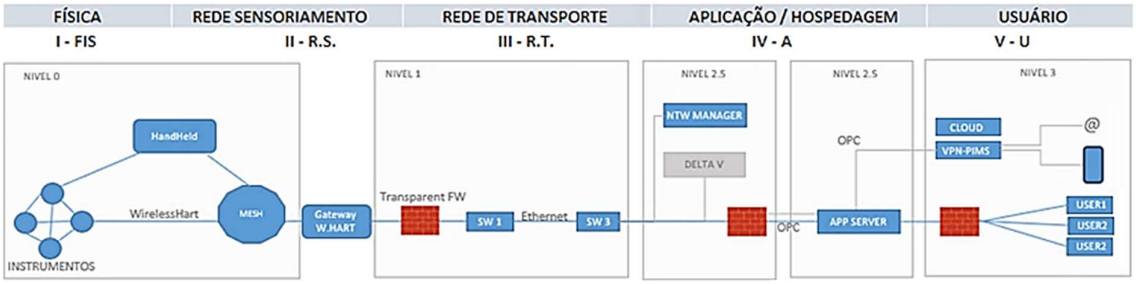
Estas e outras ações estão contabilizadas na análise de resiliência e ações requeridas ilustradas na Figura 28.

Figura 28. Vulnerabilidades encontradas na etapa T&R *(Threat & Resilience)*

Fonte: Autoria Própria

Após a verificação das vulnerabilidades apontadas pelas etapas A-S-T-R e suas respectivas resiliências recomendadas, a arquitetura da solução foi revisada, inserindo novos elementos funcionais e de segurança, conforme ilustrado na Figura 29.

Figura 29. Arquitetura de Rede Após análises de Resiliência



Fonte: Autoria Própria

5.3.4 I & S – Análise de Implementação, Operação e Escalabilidade

A estrutura de análise de resiliência proposta pode ser aplicada tanto a novas aplicações, guiando o projeto de implementação antes de ocorrer, como de instalações existentes, possibilitando a identificação de ameaças e mitigação de riscos. Para o caso em análise de uma rede WH já em operação, a etapa I & S tem o objetivo de especificar metodologia recomendada para a aplicação de novos nós e escalabilidade futura bem como esquematizar a adequação da segurança recomendada nas etapas anteriores de forma sustentável.

Em função da baixa maturidade de segurança presente nos projetos e redes IoT atuais, será comum encontrar número relevante de recomendações relacionadas à estrutura, configuração e gestão destas redes ao realizar a análise através do ASTRIS. Desde empresas pequenas até empresas líderes mundiais no ramo de tecnologia, os projetos de implementação e expansão de redes IIoT possuem foco no funcional e a parte referente à gestão de confiabilidade e segurança da rede é fornecida como escopo adicional (isto quando lembrada), por vezes por equipes diferentes, cabendo ao cliente definir o nível de segurança requerido para a rede que por muitas vezes ainda não é conhecida em detalhes. Isto explica parte da discrepância entre a capabilidade em segurança do protocolo e a segurança real da sua aplicação, decorrente de deficiências durante o processo de implementação da rede conforme descrito na Figura 30.

Figura 30. Aspectos Quantitativos de Resiliência na Implementação da Rede Testada

Fonte: autoria própria.

A continuidade na gestão de segurança da rede IoT é tão importante quanto o projeto e implementação das resiliências definidas. Ao longo do ciclo de vida, ocorre uma série de mudanças relacionadas à estrutura física, sistemas e pessoas, entre outras, que requerem gestão contínua do sistema. Nesta etapa, deve-se identificar os elementos relacionados à parametrização, documentação de projeto e manutenção, procedimentos, monitoramento requerido e capacitação da equipe local para a gestão segura e eficiente da rede.

Nesta etapa, foi identificado que existe oportunidades de cadastro de diagnósticos e detalhes de rede em historiador, bem como a necessidade de criação de uma série de documentos para gestão da rede tais como um mapa geral da unidade com distribuição dos pontos *wireless*, associação entre sensores e *gateways*, parametrização ou *datasheet* com detalhes de cada dispositivo e manual de operação com políticas e requerimentos para o

protocolo utilizado. Adicionalmente, existe oportunidade de criar procedimentos para comissionamento e operação que possuem grande importância na adição de novos dispositivos, bem como auxiliar com o monitoramento e manutenção da rede, incluindo plano de respostas a incidentes.

Infraestrutura, treinamento e procedimentos são alguns dos principais elementos para a operação segura de uma rede IIoT. Na etapa de avaliação da resiliência para a operação do sistema, foram identificadas necessidades como criação de um plano de recuperação de desastres, backups, atualizações, controle de interferências e gestão do espaço aéreo, estratégia para gestão de partes reserva, gestão de acessos e a criação de monitoramento da rede. Foi verificado que existem ferramentas suficientes para a gestão da rede como foi verificado que existem ferramentas suficientes para a gestão da rede como o próprio *network manager*, aplicação para gestão dos ativos e ferramentas para avaliação e design (estes últimos através de serviços do fabricante, em função de não haver ferramentas locais para simulação). Estas ferramentas existentes possuem diversas oportunidades em parametrização e configuração de novas funcionalidades, no entanto estão disponíveis e podem ser utilizadas para melhoria contínua do monitoramento da rede.

Quanto à sua escalabilidade, considerando a base instalada atual da unidade em estudo e a infraestrutura existente, o protocolo de comunicação wirelessHART preencheu todos os requisitos necessários para expansões futuras de forma segura, com alta capacidade em previsibilidade de performance e baixo custo na adição de estruturas (os custos de novos nós ocorrerão em função dos próprios nós adicionados). Fornecedores da tecnologia wirelessHART possuem ferramentas para simulação e análises de performance de rede antes mesmo de suas implementações, permitindo analisar o posicionamento otimizado de novos nós e medidas para otimização de performance da rede, por este motivo este protocolo também é resiliente no que diz respeito à previsibilidade de performance em expansões.

Em relação à escalabilidade da rede de sensoriamento, devido à sua tecnologia de comunicação em *mesh* quanto mais dispositivos na rede, maior a confiabilidade e performance. Em uma unidade industrial, é prevista a instalação de milhares de instrumentos em equipamentos e tubulações. Para a aplicação atual em monitoramento, a capacidade de 100 dispositivos por *gateway* em um range de aproximadamente 200 m da solução atende à

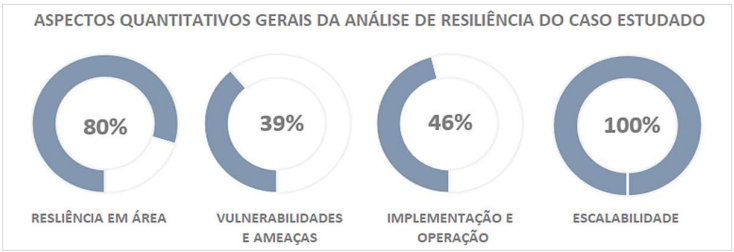
futuras expansões. Os equipamentos das camadas de transporte, rede e aplicação suportam a adição de novos nós, *gateways* e usuários sem impactar performance e com custos apenas das adições de dispositivos funcionais. Estas e outras ações estão contabilizadas na análise de implementação e escalabilidade ilustradas na Figura 31.

Figura 31. Vulnerabilidades encontradas na etapa de Implementação & Stack (I&S)

Fonte: Autoria Própria

Como resultado geral, utilizando o critério de quantificação da resiliência desenvolvido, foi possível identificar que a rede testada está 39% resiliente perante vulnerabilidades e ameaças possíveis, bem como 47% resiliente para as recomendações de segurança em implementação e operação desta rede que, na prática, resulta em processos com menor capacidade de reação e recuperação em caso de ocorrência de sinistros. Enquanto esta rede possui demonstração de 100% de capacidade em ser escalável, possui 80% de resiliência frente a riscos decorrentes de infraestrutura física e arranjo de campo. A disposição física de equipamentos e proteções contra vulnerabilidades decorrente de interferências, acesso de terceiros e condições ambientais adversas é essencial para a confiabilidade da rede. O resultado quantitativo descrito está ilustrado através da Figura 32, onde é possível perceber a resiliência da rede em diferentes perspectivas.

Figura 32. Aspectos Quantitativos Gerais



Fonte: autoria própria.

5.4 Discussões

Através deste estudo foi possível identificar que existe diversas possibilidades para implementação da IoT em ambientes industriais. Diferentes zonas de aplicação requerem diferentes soluções *wireless* com diferentes níveis de confiabilidade e maturidade. Sistemas de Informação (TI) e sistemas de operação (TO) com diferentes requerimentos deverão coexistir com segurança no espaço aéreo, requerendo cuidados durante a implementação de novos projetos. Para operar em redes de automação e controle, os protocolos *wireless* precisam de altos níveis de segurança, confiabilidade e maturidade que podem ser alcançados, por exemplo, pelos padrões *Wireless*HART e ISA100, que são utilizados e homologados pelos principais fabricantes de sistemas de controle e automação mundiais.

O desenvolvimento da estrutura de análise de risco para redes IIoT proposta neste estudo envolveu a exploração de literatura de diversas vulnerabilidades e ameaças em redes sem fio. Incluindo desde o elemento sensor até a aplicação e usuário, considerando todos os equipamentos intermediários e as áreas em que ocupam (incluindo espaço aéreo), foram analisadas como vulnerabilidades podem ser exploradas e causar impactos reais em redes IoT em ambientes industriais. Após análise de literatura sobre vulnerabilidades e ameaças em redes IIoT, foi identificado que estas redes não apresentam resiliências nativas a ataques cibernéticos, sendo necessário aplicar programas de segurança que dependem de uma boa identificação de necessidades e direcionamento quanto a ações de resiliência.

Conhecendo os riscos envolvidos na operação de redes IIoT, buscou-se identificar modelos de gestão e análise de riscos em sistemas de informação, especificamente redes para *wireless* e IoT. Estruturas de análise de risco cibernético de sistemas e redes de TI conhecidas como CVSS, TARA, OCTAVE, NIST SP800 e FAIR, entre outras, foram encontradas e estão disponíveis no mercado com considerável nível de maturidade. No entanto, todas estas estruturas encontradas foram designadas para realização de análise de risco de sistemas de TI em geral, havendo carência de estruturas com foco para análise de sistemas *wireless* ou IoT. Deste modo, o desenvolvimento de uma estrutura como o ASTRIS para avaliação de segurança em redes IIoT se mostrou ainda mais importante em função da escassez de métodos para identificar e mitigar riscos envolvidos nestas redes, bem como suportar a realização de novos projetos de forma segura.

Para diferentes tipos de rede, foram levantados os principais tipos de ataques e possíveis ações de resiliência os quais foram estruturadas em formato e fluxo lógico para análise de risco, possibilitando realizar avaliações objetivas de diferentes tipos de redes IIoT. Em função da diversidade de padrões e cenários de risco que deram origem ao modelo, a sua aplicação é realizada levando sempre em consideração o tipo de ambiente e protocolo sendo avaliado, com o objetivo de verificar os itens aplicáveis e evitar análise de itens não viáveis da sua aplicação. Por exemplo, o requerimento de redes com rotas alternativas de comunicação como em malha (*mesh*) pode não ser viável em redes IIoT menos críticas onde protocolos não atendam a esta característica.

Ao aplicar o método desenvolvido em um sistema IIoT real, foi possível caracterizar e analisar uma rede WirelessHART operando dentro de um ambiente industrial. Desde os dispositivos de campo, passando pela rede de sensoriamento e transporte até a aplicação, foram identificadas vulnerabilidades ainda não visualizadas anteriormente e recomendar uma série de ações para elevar proteções e resiliência da rede, como mudanças em rede, cultura de segurança, procedimentos e documentos.

Utilizando o critério de quantificação da resiliência desenvolvido, foi possível identificar que a rede testada possui deficiências na defesa contra vulnerabilidades e ameaças listadas e quanto a proteção sobre riscos decorrentes de infraestrutura física e arranjo de campo. Apesar de a rede demonstrar plena capacidade em escalabilidade, apresentou apenas 39% de resiliência perante vulnerabilidades e ameaças, bem como 47% de resiliência para as recomendações de segurança em implementação e operação da rede. Quanto às ações recomendadas para elevar a resiliência da rede, 87% destas representou cerca de 25% do custo de projeto da rede (com expansões futuras, este percentual relativo de investimento em segurança será ainda mais reduzido).

Estes resultados demonstram, na prática, a capacidade do método de análise desenvolvido em identificar o grau de resiliência em redes IIoT. Para a rede testada, identificou-se que esta não possuía grau de resiliência de classe mundial, conforme referenciado em padrões internacionais e recomendações baseadas em estudos que abordam o estado da arte para segurança em redes IIoT. Por motivos de confidencialidade, não é possível compartilhar detalhes sobre a rede avaliada e vulnerabilidades específicas encontradas na unidade avaliada através do ASTRIS. No entanto, é possível abordar aspectos

qualitativos e quantitativos gerais, ressaltando os principais pontos de análise em cada uma das etapas do método elaborado, como foi realizado.

Embora a coexistência entre diferentes protocolos de comunicação possa ocasionar alguns desafios conforme mencionados na literatura, este problema não foi identificado para a unidade avaliada. A malha de comunicação *wireless* da unidade em estudo conta com protocolos de comunicação WiFi, *Wireless*HART, Bluetooth, Rádio e telefonia móvel licenciada que ainda não ocupam um mesmo espaço físico em uma mesma banda de frequência, evitando problemas com interferências. Este cenário será bastante diferente em um futuro próximo, à medida que haverá novos pontos de rede WiFi para utilização de dispositivos móveis também em áreas operacionais que hoje são prenominadas pelo protocolo wirelessHART por exemplo (ambas as redes na zona 2.4 GHz de frequência). Prevendo um cenário de operação móvel, haverá também diferentes redes WiFi (redes em TI e TO) coexistindo na área operacional em paralelo com as redes atuais de sensoriamento. Neste sentido, o ASTRIS auxiliou no mapeamento das redes *wireless* do site e construção de documentação e diretrizes de suporte que auxiliam no provisionamento do funcionamento seguro destas redes no futuro desde o design das expansões.

Conforme discutido nesta dissertação e amplamente abordado na literatura e mídia, o número de dispositivos IoT utilizados em diversos segmentos da indústria crescerá de forma exponencial. Por este motivo, a escalabilidade foi um dos pontos principais de discussão e que foi abordado deste a sua origem até possíveis soluções e medidas de maturidade. A rede de campo estudada, com aproximadamente 40 instrumentos *wireless* e 4 *gateways*, possui escalabilidade para até 400 instrumentos sem custo de infraestrutura adicional, em função da capacidade de 100 instrumentos por *gateway*. A rede de transporte, composta por switches com portas reservas e espaços em painéis, bem como a capacidade ociosa do servidor utilizado para *Network Manager* e para a aplicação final, mostraram ter capacidade para elevar em ao menos 100 vezes o número de instrumentos também sem a necessidade de investimento em infraestrutura.

O protocolo WH testado demonstrou alta escalabilidade, em função de o esforço de expansões estar apenas nos dispositivos adicionais e não em alterações em infraestruturas ou em problemas decorrentes de expansões. De modo geral, através do estudo, é possível ainda

observar que a escalabilidade de uma rede IIoT depende não somente da capacidade do protocolo utilizado, mas também do ambiente e infraestrutura onde está implementada, bem como da preparação de fornecedores em avaliar e provisionar o funcionamento da rede em estado futuro.

Através deste estudo foi possível avaliar que a segurança de uma rede de sensoriamento utilizando o protocolo wirelessHART pode ter sérias vulnerabilidades se não instaladas para fazerem uso de todas as ferramentas de resiliência disponíveis. O protocolo é robusto em segurança e possui parâmetros de configuração que, somado a proteções nativas e procedimentos seguros, atendem ao uso em ambiente industrial. Ou seja, embora este seja um protocolo considerado seguro, o seu real nível de segurança vai depender da forma como é implementado e operado. Através da avaliação utilizando o ASTRIS foi possível identificar que a aplicação em estudo possuía vulnerabilidades que tornavam a rede vulnerável a ataques e que poderiam ser corrigidos com simples parametrizações de segurança da rede.

Ainda que possa ser parametrizada para desempenho otimizado de proteção e segurança, através deste estudo foi visualizado que a rede *wireless* avaliada não disponibiliza de forma nativa todas as ferramentas necessárias para monitorar a segurança da rede. A análise identificou que para monitoramento contínuo 24/7 das variáveis de diagnóstico da rede que permitem identificar sinistros e pequenos eventos de forma proativa é necessário customizar parâmetros e comunicações entre redes ICS e sistemas corporativos no nível ISA L3, como o PIMS, utilizando o protocolo OPC / OPC UA. Além dos meios de monitoramento, este estudo sugere a utilização de ferramentas que possibilitem comunicação remota de sinistros como envio automático de e-mails, SMS ou alerta em aplicativos de suporte. Existe, portanto, a oportunidade para que fabricantes de sistemas que operam utilizando o protocolo wirelessHART possam fornecer soluções que atendam de forma integral a princípios de segurança e monitoramento de desempenho da rede em plataforma única sem a necessidade realizar configurações adicionais para adequação à requisitos de segurança (que na prática acabam não ocorrendo no processo de implementação).

Assim como ocorre em monitoramentos de equipamentos críticos e alarmes relacionados a condições ambientais como, por exemplo, a identificação de gases no meio ambiente através de detectores, a identificação de operação anormal em qualquer parte da rede deve ser verificada presencialmente ou através de dispositivos de monitoramento

patrimonial. Sistema de monitoramento e plano de resposta a falhas é essencial para identificar distúrbios e ataques a redes IoT que se tornarão cada vez mais críticos à medida que serão cada vez mais utilizadas em função do custo reduzido destas soluções.

6 Conclusão

Através do levantamento e análise das tecnologias *wireless* aplicáveis em ambiente industrial e dos riscos envolvidos nestas aplicações, foi possível mapear as principais ameaças para estas redes e vulnerabilidades que podem ser exploradas por atacantes, com possibilidade de causar danos em equipamentos e instalações industriais. Ao descrever o paradigma de segurança envolvido em redes IIoT, foi identificada a necessidade de haver uma estrutura de análise de risco com foco em redes *wireless*, abordagem carente na literatura e no mercado. O conceito das estruturas de análise utilizadas para caracterizar os riscos em sistemas de informação tradicionais foi utilizado em conjunto com as vulnerabilidades do IIoT mapeadas para compor uma nova estrutura de análise de risco denominada ASTRIS.

O método ASTRIS se posiciona, portanto, para auxiliar na solução de uma importante lacuna não resolvida por estruturas já consolidadas para análise de risco de sistemas em geral: os riscos específicos de redes IoT e sem fio em ambiente industrial. O método demonstrou-se interessante para identificar vulnerabilidades de redes IoT em ambiente industrial durante todo o seu ciclo de vida, auxiliando na criação de políticas locais para gestão de risco, que reduz o impacto de sinistros ocasionados por agentes internos e externos. O método também possibilita avaliar, de forma antecipada, a maturidade em segurança de tecnologias IoT em ambientes industriais, auxiliando a identificar eventuais configurações adicionais e infraestrutura requerida para mitigar cenários de risco, fornecendo elementos técnicos para escolha de tecnologias e projeto resiliente.

Pela aplicação da estrutura de análise de risco em uma unidade industrial foi possível testar o modelo e avaliar a rede IIoT da unidade em estudo quanto a suas vulnerabilidades e resiliências. Situações de risco, antes não visualizadas, foram expostas através da análise utilizando o modelo proposto, contribuindo com a melhoria de resiliência desta rede, bem como na conscientização e maturidade em segurança da equipe local. Apesar de a rede demonstrar plena capacidade em escalabilidade, apresentou apenas 39% de resiliência perante vulnerabilidades e ameaças, bem como 47% de resiliência para as recomendações de segurança em implementação e operação da rede. Quanto às ações recomendadas para elevar a resiliência da rede, 87% destas representou cerca de 25% do custo de projeto da rede. A aplicabilidade do método para identificação de resiliência visualizada neste estudo,

associado às deficiências encontradas para a rede, demonstra o potencial do método ASTRIS em auxiliar na elevação da maturidade em segurança e robustez para redes IIoT.

A caracterização de cenários de risco de tecnologias de comunicação emergentes em ambiente industrial (como a IoT) associada a políticas de gestão de segurança, incluindo recursos técnicos e humanos, possibilita ainda um ganho de maturidade em cultura de segurança que permite elevar o uso e potenciais benefícios destas tecnologias em ambientes críticos. O método desenvolvido auxilia na transformação de uma cultura de incerteza relacionada à segurança da IIoT para um cenário onde os riscos são conhecidos, abordados e tratados, permitindo a expansão segura desta tecnologia.

6.1 Sugestões para Trabalhos Futuros

Embora a consciência sobre os benefícios e aplicação de dispositivos IoT em ambiente industrial seja cada vez maior, o uso destas ainda é recente e não é comum a presença de redes IIoT verdadeiramente densas nestes ambientes. Ao mesmo tempo em que redes IIoT muito densas ainda não é comum em áreas industriais, estudos envolvendo testes de funcionamento com aplicação de centenas ou milhares de dispositivos para avaliação do comportamento em cenários de alta densidade de rede seriam onerosos e dificilmente acessíveis à pesquisadores independentes. Em função da escassez de estudos nesta área, existem oportunidades em abordar e emular condições decorrentes da escalabilidade de redes para avaliar a performance de diferentes protocolos em cenários de expansões futuras. Parâmetros de performance como latência, consumo de bateria, coexistência, processamento, rotas de comunicação, entre outros, podem ser abordados em cenários de redes com grandes números de nós e, consequentemente, maior dependência deste tipo de comunicação.

O conceito de confiabilidade e disponibilidade em equipamentos industriais possui elevada importância, uma vez que existem equipamentos de segurança e proteção contra acidentes industriais que requerem alto nível de precisão e disponibilidade. Os protocolos mais utilizados em redes de sensoriamento industrial (*wireless*HART e ISA100) não possuem certificação para uso em redes de segurança que requerem garantias de Nível de Integridade (SIL – *Safety Integrity Level*) conforme normas 61508/61511. Embora haja alguns protocolos com uso em segurança em teste e aplicação no mercado, não foram encontrados estudos

suficientes para evidenciar aceitação de protocolos *wireless*HART para aplicação em malhas de segurança que requerem certificação de integridade SIL, sendo, portanto, uma área com oportunidades de estudo para viabilizar a aplicação do IoT também nesta zona (ainda sem soluções *wireless* de mercado maduras).

Referências

ABUHASEL, K. A.; KHAN, M. A. **A secure industrial Internet of Things (IIoT) framework for resource management in smart manufacturing.** IEEE Access, v. 8, p. 117354-117364. DOI: 10.1109/ACCESS.2020.3004711. 2020.

AKERBERG, J.; GIDLUND, M.; NEANDER, J.; LENNVALL, T.; BJÖRKMAN, M. **Deterministic downlink transmission in wirelesshart networks enabling wireless control applications**. In: IECON 2010-36th Annual Conference on IEEE Industrial Electronics Society. IEEE. p. 2120-2125. DOI: 10.1109/IECON.2010.5675281. 2010.

AKSU, M. U., DILEK, M. H., TATLI, E. İ., BICAKCI, K., DIRIK, H. I., DEMIREZEN, M. U., & AYKIR, T**. A quantitative CVSS-based cyber security risk assessment methodology for IT systems.** In: 2017 International Carnahan Conference on Security Technology (ICCST). IEEE. p. 1-8. DOI: 10.1109/CCST.2017.8167819. ISSN: 2153-0742. 2017.

ALCARAZ, C.; LOPEZ, J. **A security analysis for wireless sensor mesh networks in highly critical systems.** IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), v. 40, n. 4, p. 419-428. DOI: 10.1109/TSMCC.2010.2045373. ISSN: 1558-2442. 2010.

AMBROSIO, R; WIDERGREN, S. **A framework for addressing interoperability issues.** In: 2007 IEEE Power Engineering Society General Meeting. IEEE. p. 1-5. DOI: 10.1109/PES.2007.385817. 2017.

ANAND, P.; SINGH, Y; SELWAL, A.; ALAZAB, M.; TANWAR, S.; KUMAR, N. **IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges**. IEEE Access, v. 8, p. 168825-168853. DOI: 10.1109/ACCESS.2020.3022842. 2020.

AUGUSTIN, A.; YI, J.; CLAUSEN, T.; TOWMSLEY, W. A study of LoRa: Long range & low power networks for the internet of things. MDPI, Sensors, v. 16, n. 9, p. 1466, 2016. DOI: https://doi.org/10.3390/s16091466. 2016.

AVIZIENIS, A., LAPRIE, J. C., RANDELL, B.; LANDWEHR, C. **Basic concepts and taxonomy of dependable and secure computing**. IEEE transactions on dependable and secure computing, v. 1, n. 1, p. 11-33, 2004. DOI: 10.1109/ACCESS.2019.2891969.

BANK & FINANCE. **Internet of Things: Four Upcoming trends in 2021.** 2020. Disponível em: https://bfsi.eletsonline.com/internet-of-things-four-upcoming-trends-in-2021/#:~:text=According. Acesso em 12/07/2021.

BASU, D.; GU, T.; MOHAPATRA, P**. Security issues of low power wide area networks in the context of LoRa networks.** Doi: https://doi.org/10.48550/arXiv.2006.16554. 2020.

BEHR TECHNOLOGIES INC. Best Uses of Wireless IoT Communication Technology. 2018. Disponível em: https://industrytoday.com/best-uses-of-wireless-iot-communication-technology/. Acessado em: 10/08/2021.

BEKARA, C. **Security issues and challenges for the IoT-based smart grid.** International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications. Procedia Computer Science, v. 34, p. 532-537. DOI: https://doi.org/10.1016/j.procs.2014.07.064. 2014.

BELDEN. **The Evolution and Progress of Wireless Standards.** 2018. Disponível em: https://www.belden.com/blogs/evolution-and-progress-of-wireless-standards. Acessado em: 17/06/2021.

BENIAS, K.; MARKOPOULUS, A. P. **A Review on the Readiness Level and Cyber-Security Challenges in Industry 4.0** In: 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE. p. 1-5. DOI: 10.23919/SEEDA-CECNSM.2017.8088234. 2017.

BOCCADORO, P.; DANIELE, V.; GENNARO, P. D.; TEDESCHI, P. **Water Quality Prediction on a Sigfox-compliant IoT Device: The Road Ahead of WaterS**. DOI: https://doi.org/10.48550/arXiv.2007.13436. 2020.

BODEAU, D.; GRAUBART, R. **Cyber resiliency and nist special publication 800-53 rev. 4 controls.** MITRE, Tech. Rep., 2013.

BUTUN, I.; OSTERBERG, P. ; SONG, H. **Security of the Internet of Things: Vulnerabilities, Attackes, and Countermeasures.** IEEE Communications Surveys & Tutorials, v. 22, n. 1, p. 616-644. DOI: 10.1109/COMST.2019.2953364. 2019.

CAMPILLO, O. S. **Security Issues in Internet of Things.** Universitat Politécnica de Catalunya. 2017.

CASACCIA, L. **Understanding 3GPP – starting with the basics.** 2017.

CASE, Defense Use. Analysis of the cyber attack on the Ukrainian power grid. **Electricity Information Sharing and Analysis Center (E-ISAC)**, v. 388, p. 1-29, 2016.

CHHETRI, S. R.; RASHID, N.; FAEZI, S.; FARUQUE, M. A. A. **Security Trends and Advances in Manufacturing Systems in The Era of Industry 4.0.** In: 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE. p. 1039-1046. DOI: 10.1109/ICCAD.2017.8203896. 2017.

COMAN, F. L.; MALARSKI, K. M.; PETERSEN, M. N.; RUEPP, S. R. **Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT**. In: 2019 Global IoT Summit (GIoTS). IEEE. p. 1-6. DOI: 10.1109/GIOTS.2019.8766430. 2019.

DAWSON, M. **Cyber Security in Industry 4.0: The Pitfalls of Having Hyperconnected Systems.** Journal of Strategic Management Studies, v. 10, n. 1, p. 19-28. DOI: https://doi.org/10.24760/iasme.10.1_19. 2018.

EMERSON. **Tecnologia Wireless – Implemente e expanda de maneira fácil e econômica suas redes de detecção existentes com wireless.** 2021. Disponível

em :https://www.emerson.com/pt-br/expertise/automation/industrial-internet-things/pervasive-sensing-solutions/wireless-technology. Acesso em: 11/06/2021.

EMERSON. **WirelessHART® and Wi-Fi® Security**. Emerson Wireless Security Technical Note. 2017.

EMERSON PROCESS MANAGEMENT. **System Engineering Guidelines IEC 62591 WirelessHART**. Engineering Guidelines. 2016.

FALCO, G. CALDERA, C. SHROBE, H. **IIoT Cyber Security Risk Modelling for SCADA Systems.** IEEE Internet of Things Journal, v. 5, n. 6, p. 4486-4495, 2018. DOI: 10.1109/JIOT.2018.2822842.

FAN, X. SUSAN, F. LONG, W. LI, S. **Security Analysis of Zigbee**. **MWR InfoSecurity**, p. 1-18, 2017.

GARROPO, R. G.; GAZZARRINI, L.; GIORDANO, S.; TAVANTI, L. **Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices**. 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. IEEE, 2011. p. 1-9. DOI: 10.1109/WoWMoM.2011.5986182.

GEIL, A.; SAGERS, G.; SPAULDING, A. D.; WOLF, J. R. **Cyber Security on The Farm: An Assessment of Cyber Security Practices in the United States Agriculture Industry.** International Food and Agribusiness Management Review, v. 21, n. 3, p. 317-334, 2018. DOI: https://doi.org/10.22434/IFAMR2017.0045.

GUNES, V.; PETER, S.; GIVARGIS, T.; VAHID, F. **A survey on concepts, applications, and challenges in cyber-physical systems.** KSII Transactions on Internet and Information Systems (TIIS), v. 8, n. 12, p. 4242-4268, 2014. DOI: https://doi.org/10.3837/tiis.2014.12.001.

GUPTA, A.; CHRISTIE, R.; MANJULA, R. **Scalability in Internet of Things: Features, Techniques and Research Challenges.** Int. J. Comput. Intell. Res, v. 13, n. 7, p. 1617-1627, 2017. ISSN 0973-1873.

HENRIE, M. **Cyber security risk management in the SCADA critical infrastructure environment.** Engineering Management Journal, 25(2), 38-45. 2013. DOI: https://doi.org/10.1080/10429247.2013.11431973.

HUDGENS, J.; MEERS, T. **Sources for Vulnerability and Threat Information.** 2021. https://pratum.com/blog/328-sources-for-vulnerability-and-threat-information

HERNANDEZ, M. **Connectivity Now and Beyond; exploring Cat-M1, NB-IoT, and LPWAN Connections.** 2018.

ISA GLOBAL CYBERSECURITY ALLIANCE. **Security of Industrial Automation and Control Systems**. 2020.

IVEZIC, M. **IoT Wireless Protocols – Spreadsheet.** Disponível em: https://5g.security/5g-security-privacy/iot-wireless-protocols-spreadsheet/. Acesso em 06/03/2021.

JANG, J. W.; KWON, S.; KIM, S.; SEO, J.; OH, J.; LEE, K. H. **Cybersecurity framework for IIoT-based power system connected to microgrid.** KSII Transactions on Internet and Information Systems (TIIS), v. 14, n. 5, p. 2221-2235, 2020. 1976-7277(eISSN). DOI: https://doi.org/10.3837/tiis.2020.05.020.

JAMAI, I.; AZZOUZ, L. B.; SAIDANE, L. A. **Security Issues In Industry 4.0**. In: 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020. p. 481-488. DOI: 10.1109/IWCMC48107.2020.9148447.

KARNOUSKOS, S. **Stuxnet Worm Impact on Industrial Cyber-Physical System Security.** In: IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2011. p. 4490-4494. DOI: 10.1109/IECON.2011.6120048.

KHANJI, S.; IQBAL, F.; HUNG, P. **ZigBee Security Vulnerabilities: Exploration and Evaluation.** 10th International Conference of Information and Communication Systems. 2019.

KHANJI, S.; IQBAL, F.; HUNG, P. **ZigBee Security Vulnerabilities: Exploration and Evaluation.** In: 2019 10th International Conference on Information and Communication Systems (ICICS). IEEE, 2019. p. 52-57. DOI: 10.1109/IACS.2019.8809115.

KITANO, K. YAMAMOTO, S. **Strong Security Measures Implemented in ISA100.11a Wireless System**. Yokogawa, p. 57, 2014.

KOUTRAS, D.; STEGIOPOULOS, G.; DASAKLIS, T.; KOTZANIKOLAOU, P.; GLYNOS, D.; DOULIGERIS, C. **Security in IoMT Communications: A Survey**. Sensors, v. 20, n. 17, p. 4828, 2020. DOI: https://doi.org/10.3390/s20174828.

KRUPKA, L.; VOJTECH, L.; NERUDA, M. **The Issue of LPWAN Technology Coexistence in IoT Environment.** In: 2016 17th international conference on mechatronics-Mechatronika (ME). IEEE, 2016. p. 1-8.

KANDASAMY, K.; SRINIVAS, S.; ACHUTHAN, K.; RANGAN, V. **IoT cyber risk: a holistic analysis of cyber risk assessment framework, risk vectors, and risk ranking process.** EURASIP Journal on Information Security, v. 2020, n. 1, p. 1-18, 2020.

LANDO, F. **Método de Pesquisa Qualitativa: O que é e como fazer?** Disponível em: https://www.academicapesquisa.com.br/post/m%C3%A9todo-qualitativo-como-fazer. Acesso em 20/11/2021.

LAPRIE, J. **From dependability to resilience**. In: 38th IEEE/IFIP Int. Conf. On dependable systems and networks. 2008. p. G8-G9.

LAVRIC, A.; POPA, V. **Performance Evaluation of LoRaWAN Communication Scalability in Large-Scale Wireless Sensor Networks.** Wireless Communications and Mobile Computing, v. 2018, 2018. DOI: https://doi.org/10.1155/2018/6730719.

LINDSEY, J. R. D. **Stuxnet and The Limits of Cyber Warfare.** 2013.

LINDSAY, Jon R. Stuxnet and the limits of cyber warfare. **Security Studies**, v. 22, n. 3, p. 365-404, 2013. DOI: https://doi.org/10.1080/09636412.2013.816122.

LEE, R. M.; ASSANTE, M. J.; CONWAY, T. **Analysis of the Cyber Attack on the Ulkrainian Power Grid.** Electricity Information Sharing and Analysis Center. 2016.

LEE, M. L.; ASSANTE, J. A.; CONWAY, T. **German Steel Mill Cyber Attack.** Industrial Control Systems, v. 30, n. 62, 2014.

LONZETTA, A. M.; COPE, P.; CAMPBELL, J.; MOHD, B. J.; HAYAJNEH, T. **Security Vulnerabilities in Bluetooth technology as used in IoT.** Journal of Sensor and Actuator Networks, v. 7, n. 3, p. 28, 2018. Doi: https://doi.org/10.3390/jsan7030028.

MANTRAVADI, S.; MOLLER, C. **Na Overview of Next-generation Manufacturing Execution Systems: How important is MES for Industry 4.0?** Procedia manufacturing, v. 30, p. 588-595, 2019. DOI: https://doi.org/10.1016/j.promfg.2019.02.083.

MARCONI, E. V.; LAKATOS, M. A. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MOLINA, D. I. A. **An Algebraic Service Composition Model for the Construction of Large-Scale IoT Systems.** The University of Manchester (United Kingdom), 2020.

NATARAJAN, R.; ZAND, P.; NABI, M. **Analysis of Coexistence between IEEE 802.15.4 BLE and IEEE 802.11 in the 2.4 GHz ISM Band.** 2016.

NEAGA, I. N.; HENSHAW, M. J. DE C. **Modeling the Linkage Between Systems Interoperability and Security Engineering.** In: 2010 5th International Conference on System of Systems Engineering. IEEE, 2010. p. 1-6. DOI**:** 10.1109/SYSOSE.2010.5544056.

NEANDER, J.; LENVALL, T.; GIDLUND, M. **Prolong Wireless HART Network Lifetime Using Packet Aggregation.** In: 2011 IEEE International Symposium on Industrial Electronics. IEEE, 2011. p. 1230-1236. DOI: 10.1109/ISIE.2011.5984334.

NIXON, M. **A comparison of WirelessHART™ and ISA100.11a**. Whitepaper, Emerson Process Management, p. 1-36, 2012.

PINTO, A. D.; DRAGONI, Y.; CARCANO, A. **TRITON: The First ICS Cyber Attack on Safety Instrument Systems.** In: Proc. Black Hat USA. 2018. p. 1-26.

PURNAMA, A. A. F.; NASHIRUDDIN, M. I. **SigFox-based Internet of Things Network Planning for Advanced Metering Infrastructure Services in Urban Scenario.** In: 2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT). IEEE, 2020. p. 15-20. DOI: 10.1109/IAICT50021.2020.9172022.

PETERSEN, S.; AAKVAAG, N. **Wireless Instrumentation for Safety Critical Systems.** Technology, standards, solutions and future trends. 2015.

POWERS, N. **Industrial Protocols Comparison: IIoT Industrial Networks**. Disponível em: https://www.arrow.com/en/research-and-events/articles/industrial-connectivity-protocols#:~:text=The. Acesso em: 15/06/2021.

PREFEITURA DE CAMAÇARI. **Camaçari Parabeniza o Polo Industrial pelos 43 Anos.** 2021. Disponível em: *https://www.camacari.ba.gov.br/camacari-parabeniza-o-polo-industrial-pelos-43-anos/*. Acesso em 21/08/2021.

QURESHI, K. N.; ABDULLAH, A. H. **Adaptation of Wireless Sensor network Industries and Their Architecture, Standards and Application.** World Applied Sciences Journal. 2014.

QURESHI, K. N.; ABDULLAH, A. H. **Adaptation of Wireless Sensor network Industries and Their Architecture, Standards and Application.** World Applied Sciences Journal, v. 30, n. 10, p. 1218-1223, 2014. DOI: 10.5829/idosi.wasj.2014.30.10.14152.

RAMYA, C. M.; SHANMUGARAJ, M.; PRABAKARAN, R. **Study on Zigbee Technology.** In: 2011 3rd International Conference on Electronics Computer Technology. IEEE, 2011. p. 297-301. DOI**:** 10.1109/ICECTECH.2011.5942102.

RATASICH, D.; KHALID, F.; GEISSLER, F.; GROSU, R.; SHAFIQUE, M.; BARTOCCI, E. **A roadmap toward the resilient internet of things for cyber-physical systems.** IEEE Access, v. 7, p. 13260-13283, 2019. DOI: 10.1109/ACCESS.2019.2891969. Electronic ISSN: 2169-3536.

RAZA, S. SLABBERT, A. VOIGT, T. **Security Considerations for the WirelessHART Protocol**. In: 2009 IEEE Conference on Emerging Technologies & Factory Automation. IEEE, 2009. p. 1-8. DOI: 10.1109/ETFA.2009.5347043.

RAZA, S. **Secure Communication in WirelessHART and its Integration with Legacy HART. Swedish Institute of Computer Science**. 2010.

RADMAND, P. DOMINGO, M. SINGH, J. ARNEDO, J. TALEVSKI, A. PETERSEN, S. CARLSEN, S. **ZigBee/ZigBee PRO security assessment based on ompromised cryptographic keys.** In: 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. IEEE, 2010. p. 465-470. DOI: 10.1109/3PGCIC.2010.79.

RADANLIEV, P.; ROURE, D. D.; NURSE, J. R. C.; NICOLESCU, R.; HUTH, M. **Cyber Security Framework for the Internet-of-Things in Industry 4.0.** 2019. DOI: 10.20944/preprints201903.0111.v1.

ROSS, R.; PILLITTERI, V., GRAUBART, R.; BODEAU, D.; McQuaid, R. **Developing cyber resilient systems: a systems security engineering approach**. National Institute of Standards and Technology, 2019. DOI: https://doi.org/10.6028/NIST.SP.800-160v2.

STRAND, H. IoT based monitoring for Power Grid Components. 2020. Disponível em: https://blog.sintef.com/sintefenergy/iot-based-monitoring-for-power-grid-components/. Acessado em: 07/08/2021.

SANCHEZ, J. H. **WirelessHART Network Manager.** KTH The Royal Institute of Technology. 2011.

SCARFONE, K.; PADGETTE, J. **Recommendations of the National Institute of Standards and Technology.** NIST Special Publication. 2008.

REGENSCHEID, Andrew; SCARFONE, Karen. Recommendations of the national institute of standards and technology. **NIST special publication**, v. 800, p. 155, 2011.

SHUKLA, A.; TRIPATHI, S. **Security Challenges and Issues of Internet of Things: Possible Solutions.** In: Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT). 2018. p. 26-27. Disponível em: SSRN:https://ssrn.com/abstract=3166735, DOI:http://dx.doi.org/10.2139/ssrn.3166735.

SLAY, J.; MILLER, M. **Lessons Learned from the Maroochy Water Breach.** In: International conference on critical infrastructure protection. Springer, Boston, MA, 2007. p. 73-82. DOI: https://doi.org/10.1007/978-0-387-75462-8_6.

SHEEHAN, B.; MURPHY, F.; KIA, A. N.; KIELY, R. **A quantitative bow-tie cyber risk classification and assessment framework.** Journal of Risk Research, v. 24, n. 12, p. 1619-1638, 2021. DOI: https://doi.org/10.1080/13669877.2021.1900337.

SINHA, R. S.; WEI, Y.; HWANG, S. **A survey on LPWA technology: LoRa and NB-IoT.** ICT Express, v. 3, n. 1, p. 14-21, 2017. DOI: https://doi.org/10.1016/j.icte.2017.03.004.

TELENOR CONNEXION. **LTE-M vs NB-IoT – A guide exploring the differences between LTE-M and NB-IoT.** 2021. Disponível em: https://www.telenorconnexion.com/iot-insights/lte-m-vs-nb-iot-guide-differences/. Acessado em 25/06/2021.

TOURNIER, J.; LESUEUR, T.; MOUEL, F.; GUYON, L.; BEN-HASSINE, H**. A survey of IoT protocols and their security issues through the lens of a generic IoT stack.** Internet of Things, v. 16, p. 100264, 2021. DOI: https://doi.org/10.1016/j.iot.2020.100264.

VANGELISTA, L.; ZANELLA, A.; ZORZI, Micheli. **Long-Range IoT Technologies: The Dawn of Lora™.** In: Future access enablers of ubiquitous and intelligent infrastructures. Springer, Cham, 2015. p. 51-58. DOI: https://doi.org/10.1007/978-3-319-27072-2_7.

VARGA, P.; SANDOR, P.; SOOS, G. **Security Threats and Issues in Automation IoT**. In: 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). IEEE, 2017. p. 1-6. DOI: 10.1109/WFCS.2017.7991968.

VERVE. **Endpoint Protection and Its Effect on Cyber Security Risk and Intel.** 2019. Disponível em:https://verveindustrial.com/resources/blog/endpoint-protection-and-its-effect-on-cyber-security-risk-and-intel/. Acesso em 14/07/2021.

WANG, G. **Comparison and Evaluation of Industrial Wireless Sensor Networks Standards ISA100.11a and WirelessHART.** Chalmers University, Department of Signals and Systems. 2011.

WINTER, J. M.; MULLER, I.; SOATTI, G.; SAVAZZI, S.; NICOLI, M.; BECKER, L. B.; NETTO, J. C.; PEREIRA, C. E. **Wireless Coexistence and Spectrum Sensing in Industrial Internet of**

Things: An Experimental Study. International Journal of Distributed Sensor Networks, v. 11, n. 11, p. 627083, 2015. DOI: https://doi.org/10.1155/2015/627083.

ZARAKET, C.; PAPAGEORGAS, P.; AILLERIE, M.; AGAVANAKIS, K.; SALAME, C. **Cyber security vulnerabilities of smart metering based on LPWAN wireless communication technologies.** In: AIP Conference Proceedings. AIP Publishing LLC, 2020. p. 020050. DOI: https://doi.org/10.1063/5.0032709.

ZAHRAN, B.; HUSSAINI, A.; ALI-GOMBE, A. **IIoT-ARAS: IIoT/ICS Automated Risk Assessment System for Prediction and Prevention.** In: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy. 2021. p. 305-307. DOI: https://doi.org/10.1145/3422337.3450320.

Produção Técnica e Científica

Artigo: “Resilience Evaluation of Cyber Risks in Industrial Internet of Things” publicado na conferência do IEMTRONICS 2022 (International IOT, Electronics and Mechatronics Conference).

Depósito de Patente: “ASTRIS – Método para Avaliação de Resiliência Cibernética em Redes IIoT”.

Artigo “Aplicação De Técnicas De Inteligência Artificial Em Controle De Processos Em Batelada” publicado no V SIINTEC 2019 (Simpósio Internacional de Inovação e Tecnologia).

Artigo: “ASTRIS – A Proposal Method for Cyber Resilience Assessment of Industrial Internet of Things Networks” a ser publicado após depósito de Patente.

APÊNDICE 1. ASTRIS – CARACTERIZAÇÃO DA APLICAÇÃO IIoT

DESCRIÇÃO DA APLICAÇÃO DO IIoT

DESCRIÇÃO DA APLICAÇÃO	Ex: IMPLEMENTAÇÃO DE INSTRUMENTOS PARA MONITORAMENTO DE EQUIPAMENTOS E PROCESSO
PROTOCOLO DE COMUNICAÇÃO WIRELESS	Ex: WIRELESS HART
TIPO DE INTERFACE APLICAÇÃO	Ex: HTTP / WEB
NOME DA APLICAÇÃO FINAL	Ex: PLANTWEB
USUÁRIOS	Ex: FUNCIONÁRIOS DA MANUTENÇÃO E OPERADORES
CAMADA DE HOSPEDAGEM DA APLICAÇÃO	Ex: ICS L2.5
CONEXÃO COM OUTROS SISTEMAS?	Ex: SIM - DCS
NÚMERO DE DISPOSITIVOS	Ex: 40
ÁREA DE COBERTURA	Ex: 250m2 x 250m2

CARACTERIZAÇÃO DA ÁREA DE OPERAÇÃO DO IIoT

ÁREA DE APLICAÇÃO																		
INTERNA										EXTERNA								
CAMPO / CCM	FI	RS	VIAS / ÁREAS	RS	-	PREDIAL	RT	AP	FORNECEDOR / CLIENTE		-	NUVEM	-	-	REMOTO	US	-	

* FI – Rede Física | RS – Rede de Sensoriamento | RT – Rede de Transporte | AP – Aplicação | US - Usuário

DEFINIÇÃO DA ZONA DE APLICAÇÃO (ICS / N-ICS)

ZONA													
ICS							NÃO ICS						
SEGURANÇA*		I	SUPERVISÃO / IHM MÓVEL		III		MONITORAMENTO DE ATIVOS		V	GESTÃO E PERFORMANCE		VII	
CONTROLE*		II	MONITORAMENTRO		IV		TRABALHO MÓVEL		VI	REALIDADE VIRTUAL / AUMENTADA		VIII	

ANÁLISE PRELIMINAR PARA APLICAÇÕES EM CONTROLE OU SEGURANÇA

REDE	REQUISITO	S	N	NA	CONFORMIDADE	S	N	NA	RESILIÊNCIA REQUERIDA OU EXISTENTE
FÍSICA	SERÁ UTILIZADO ATUADOR WIRELESS?				EXISTE INFRAESTRUTURA ELÉTRICA PARA O ATUADOR?				
FÍSICA	APLICAÇÃO EM PROCESSO?				É CONHECIDA A CONSTANTE DE TEMPO DO PROCESSO?				SCAN DEVE SER 3X MAIS RÁPIDO QUE CTE TEMPO
FÍSICA	APLICAÇÃO REQUER SCAN REDUZIDO?				ANALISADA A VIDA ÚTIL DA BATERIA P/ SCAN REQUERIDO?				
FÍSICA	EXISTE RESTRIÇÕES DE LATÊNCIA?				FOI ANALISADA O IMPACTO DA LATÊNCIA?				
FÍSICA	REDE REQUER ALTA DISPONIBILIDADE?				REDE MADURA E COM NÓS VIZINHOS SUFICIENTES?				
FÍSICA	ALTA CONFIABILIDADE REQUERIDA?				ANALISADA CONFIABILIDADE DOS DISPOSITIVOS?				
FÍSICA	ALTA CONFIABILIDADE REQUERIDA?				ANALISADA REDUNDÂNCIA DE REDE E ENERGIA?				
FÍSICA	APLICAÇÃO EM CONTROLE OU SEGURANÇA?				DEFINIDOS REQUISITOS DE FALHA SEGURA?				
GERAL	APLICAÇÃO EM CONTROLE OU SEGURANÇA?				DISPOSITIVOS FÍSICOS E ARQUITETURA MADURA?				
GERAL	APLICAÇÃO EM CONTROLE OU SEGURANÇA?				DEFINIDOS CRITÉRIOS DE TOLERÂNCIA À FALHA?				
GERAL	APLICAÇÃO EM SEGURANÇA?				DIRETRIZES CORPORATIVAS PERMITEM USO EM SEGURANÇA?				
APLICAÇÃO	APLICAÇÃO EM SEGURANÇA?				LOGIC SOLVER E DISPOSITIVOS CERTIFICADOS P/ APLICAÇÃO?				
GERAL	SIL 1, 2 ou 3 REQUERIDO?				CALCULO DE SIL REALIZADO COMPROVANDO SIL REQ?				REDUNDÂNCIA DE INSTR, GATEWAYS (NTW) E LOGIC SOLVER

**NÃO CONTINUAR ANÁLISE PARA APLICAÇÕES EM CONTROLE E SEGURANÇA, ATÉ QUE SEJAM ATENDIDOS ESSES REQUISITOS

APÊNDICE 2. ASTRIS – ANÁLISE DE ÁREA & STACK

ÁREA DA REDE FÍSICA

	REQUISITO	S	N	NA	CONFORMIDADE	S	N	NA	RESILIÊNCIA REQUERIDA OU EXISTENTE
I.1	INFRAESTRUTURA DE REDE REQUERIDA?				INFRAESTRUTURA EXISTENTE?				
I.2	INFRAESTRUTURA ELÉTRICA REQUERIDA?				INFFRAESTRUTURA ELÉTRICA EXISTENTE?				
I.3	MOBILIDADE REQUERIDA?				COBERTURA DE SINAL NA ÁREA DE MOVIMENTAÇÃO?				
I.4	USO EM ÁREA CLASSIFICADA?				DISPOSITIVOS INTRINSICAMENTE SEGUROS?				
I.5	POTENCIAL DE SOFRER INTERFERÊNCIAS?				REALIZADA ANÁLISE DE COEXISTÊNCIA?				
I.6	POTENCIAL DE CAUSAR INTERFERÊNCIAS?				REALIZADA ANÁLISE DE COEXISTÊNCIA E POTÊNCIA?				
I.7	DENSIDADE AÉREA OU ESTRUTURAL ALTA?				REALIZADA ANÁLISE DE OBSTÁCULOS E BARREIRAS?				
I.8	APLICAÇÃO DE LONGO ALCANCE?				REALIZADO TESTE DE ALCANCE?				
I.9	ESPOSIÇÃO FÍSICA A TERCEIROS?				DESIGNADO MEIO DE PROTEÇÃO FÍSICA DO EQUIPAMENTO?				
I.10	CONDIÇÕES AMBIENTAIS AGRESSIVAS?				GRAU DE PROTEÇÃO ADEQUADOS?				
I.11	PROTEÇÕES ELÉTRICAS REQUERIDAS?				PROTEÇÃO ELÉTRICA NA ESTRUTURA DO EQUIPAMENTO?				
I.12	EXPANSÃO FUTURA PREVISTA?				EQUIPAMENTOS APROPRIADOS PARA EXPANSÃO?				
I.13	EXISTE REQUERIM. DE ALTURA MIÍNIMA?				AVALIADA ALTURA MÍNIMA REQUERIDA?				
I.14	DISTANCIAMENTO DE ESTRUTURA REQ?				AVALIADA DISTÂNCIA DE ESTRUTURAS REQUERIDA?				

*Formulário preenchido não autorizado para divulgação.

ÁREA DA REDE DE SENSORIAMENTO

	REQUISITO	S	N	NA	CONFORMIDADE	S	N	NA	RESILIÊNCIA REQUERIDA OU EXISTENTE
II.1	INFRAESTRUTURA DE REDE REQUERIDA?				INFRAESTRUTURA EXISTENTE?				
II.2	MOBILIDADE REQUERIDA?				COBERTURA DE SINAL NA ÁREA DE MOVIMENTAÇÃO?				
II.3	USO EM ÁREA CLASSIFICADA?				DISPOSITIVOS CERTIFICADOS PARA A. CLASSIFICADA?				
II.4	COEXISTÊNCIA COM OUTROS PADRÕES?				REALIZADA ANÁLISE DE COEXISTÊNCIA?				
II.5	DENSIDADE AÉREA OU ESTRUTURAL ALTA?				REALIZADA ANÁLISE DE OBSTÁCULOS E BARREIRAS?				
II.6	APLICAÇÃO DE LONGO ALCANCE?				REALIZADO TESTE DE ALCANCE?				
II.7	ESPOSIÇÃO FÍSICA A TERCEIROS?				DESIGNADO MEIO DE PROTEÇÃO FÍSICA DO EQUIPAMENTO?				
II.8	CONDIÇÕES AMBIENTAIS AGRESSIVAS?				EQUIPAMENTOS RESISTENTES À ESTAS CONDIÇÕES?				
II.9	PROTEÇÕES ELÉTRICAS REQUERIDAS?				PROTEÇÃO ELÉTRICA NA ESTRUTURA DO EQUIPAMENTO?				
II.10	EXPANSÃO FUTURA PREVISTA?				EQUIPAMENTOS APROPRIADOS PARA EXPANSÃO?				
II.11	PROTEÇÃO FÍSICA A TERCEIROS				ANALISADO MEIOS DE PROTEÇÃO DE ACESSO FÍSICO?				
II.12	DISTANCIAMENTO DE ESTRUTURA REQ?				AVALIADA DISTÂNCIA DE ESTRUTURAS REQUERIDA?				

APÊNDICE 2. ASTRIS – ANÁLISE DE ÁREA & STACK (Continuação)

ÁREA ENVOLVIDA NA REDE DE TRANSPORTE

	REQUISITO	S	N	NA	CONFORMIDADE	S	N	NA	RESILIÊNCIA REQUERIDA OU EXISTENTE
III.1	INFRAESTRUTURA DE REDE REQUERIDA?				INFRAESTRUTURA EXISTENTE?				
III.2	INFRAESTRUTURA ELÉTRICA REQUERIDA?				INFFRAESTRUTURA ELÉTRICA EXISTENTE?				
III.3	MOBILIDADE REQUERIDA?				COBERTURA DE SINAL NA ÁREA DE MOVIMENTAÇÃO?				
III.4	USO EM ÁREA CLASSIFICADA?				DISPOSITIVOS CERTIFICADOS PARA A. CLASSIFICADA?				
III.5	ESPOSIÇÃO FÍSICA A TERCEIROS?				DESIGNADO MEIO DE PROTEÇÃO FÍSICA DO EQUIPAMENTO?				
III.6	CONDIÇÕES AMBIENTAIS AGRESSIVAS?				EQUIPAMENTOS RESISTENTES À ESTAS CONDIÇÕES?				
III.7	PROTEÇÕES ELÉTRICAS REQUERIDAS?				PROTEÇÃO ELÉTRICA NA ESTRUTURA DO EQUIPAMENTO?				

ÁREA ENVOVIDA COM INFRAESTRUTURA DA APLICAÇÃO

	REQUISITO	S	N	NA	CONFORMIDADE	S	N	NA	RESILIÊNCIA REQUERIDA OU EXISTENTE
IV.1	SERÁ UTILIZADO SERVIDOR FÍSICO?				SERVIDOR FÍSICO DISPONÍVEL E PROTEGIDO?				
IV.2	ESPOSIÇÃO FÍSICA SERVIDOR A TERCEIROS?				DESIGNADO MEIO DE PROTEÇÃO FÍSICA DO EQUIPAMENTO?				
IV.3	SERÁ UTILIZADO SERVIDOR VIRTUAL?				EXISTE CAPACIDADE EM HARDWARE ATUAL?				
IV.4	SERÁ UTILIZADO SERVIDOR EM NÚVEM?				AVALIADO REQUISITOS PARA SERVIDOR EM NUVEM				
IV.5	DADOS GERADOS REQUER HISTORIAMENTO?				EXISTE SERVIDOR PARA HISTORIAMENTO DOS DADOS?				
IV.6	APLICAÇÃO REQUER BACKUP (DB)?				LOCALIZAÇÃO DO BACKUP PROTEGIDA?				
IV.7	INTERFACES COM OUTROS LOCAIS				LOCAIS COM ACESSOS PROTEGIDOS?				
IV.8	APLICAÇÃO REQUER REDE RESTRITA?				USUÁRIOS FINAIS POSSUEM ACESSO A ESTA REDE?				

APÊNDICE 3. ASTRIS – ANÁLISE DE THREAT & RESILIENCE

ANÁLISE GERAL DE AMEAÇAS E RESILIÊNCIAS PARA A APLICAÇÃO IIoT

STACK	AMEAÇA / VULNERABILIDADE	ATAQUE RELACIONADO	PROTEÇÃO RECOMENDADA (RESILIÊNCIA)	Aplicável	Resiliente	Mitigação Req	PROTEÇÃO / MITIGAÇÃO ADOTADA
FIS	VIOLAÇÃO DE CONFIDENCIALIDADE	EAVESDROPPING	SEGURANÇA FÍSICA E CONTROLE DE ACESSOS				
FIS	ACESSO A LOGS E INFORMAÇÕES	TAMPERING	ENCRIPTAÇÃO DE REGISTROS				
FIS	VULNERABILIDADE FÍSICA	NODE DESTRUCTION	PROTEÇÃO FÍSICA DE DISPOSITIVOS				
FIS	INFORMAÇÕES EM NÓS FÍSICOS	TAMPERING	ACESSO CONTROLADO OU TAMPER PROOF				
FIS	ACESSO INADVERTIDO AO DISPOSITIVO	TAMPERING	CONTROLE DE ACESSO NO DISPOSITIVO				
MAC	TENTATIVAS DE ACESSOS INADVERTIDOS	EXHAUSTION	LIMITAR NÚMERO DE REQUISIÇÕES				
MAC	TENTATIVAS DE ACESSOS INADVERTIDOS	EXHAUSTION	PROTEÇÃO CONTRA REQUISIÇÕES NÃO IDENTIFICADAS				
MAC	EXPLORAÇÃO DA REDE POR TERCEIROS	EXHAUSTION	PROTEÇÃO DE DADOS NÃO CRIPTOGRAFADOS				
MAC	EXPLORAÇÃO DA REDE POR TERCEIROS	ROUTE SPOOFING	SEGURANÇA DE REDE E ARQUITETURA SEGURA				
MAC	EXPLORAÇÃO DA REDE POR TERCEIROS	EAVESDROPPING	ENCRIPTAÇÃO				
REDE	FALTA DE ROBUSTEZ	EAVESDROPPING	SWITCHES E DISPOSITIVOS INTELIGENTES				
REDE	INTERFERÊNCIAS E INVASÕES	JAMMING	RACIONALIZAR USO DE REPETIDORES E POSIÇÃO DE DEVICES				
REDE	INTRUSÃO NA REDE DE SENSORIAMENTO	HELLO FLOODING	AUTENTICAÇÃO ENTRE NÓS				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK	AVALIAÇÃO DA TOPOLOGIA REQUERIDA				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - GRAYHOLE	RECONHECIMENTO DE PACOTES ENTRE NÓS				
REDE		RPL EXPLOIT	AUTENTICAÇÃO DE TOPOLOGIA				
REDE	PERDA DE SINCRONIA DE REDE	DESYNCHRONIZATION	AUTENTICAÇÃO DE PACOTES DE DADOS				
REDE		MQTT EXPLOIT	POLÍTICAS DE SEGURANÇA				
REDE	SEQUESTRO DE SESSÃO	SESSION HIJACKING	AUTENTICAÇÃO DE ACESSOS				
APP		PATCH BASED DoS	DETEÇÃO DE REPLAY E PACOTES ESPÚRIOS				
APP	PERDA/ROUBO	PERDA	MONITORAMENTO DE ATIVOS				
APP	VIOLAÇÃO DE CONFIDENCIALIDADE	EAVESDROPPING	CONSCIÊNCIA DE PROTEÇÃO				
APP	ACESSO INDEVIDO DE REDES	INTRUSION	AVALIAR SEGREGAÇÃO DE REDES COM *FIREWALL*				

APÊNDICE 3. ASTRIS – ANÁLISE DE THREAT & RESILIENCE (Continuação)

ANÁLISE DE AMEAÇAS E RESILIÊNCIAS PARA A APLICAÇÃO IIoT ESPECÍFICO PARA REDES ICS

STACK	AMEAÇA / VULNERABILIDADE	ATAQUE RELACIONADO	PROTEÇÃO RECOMENDADA (RESILIÊNCIA)	Aplicável	Resiliente	Mitigação	PROTEÇÃO / MITIGAÇÃO ADOTADA
FIS	DEGRADAÇÃO DO DISPOSITIVO	NODE DESDTRUCTION	DISPOSITIVOS CONFIÁVEIS / DURÁVEIS				
FIS	FALHAS NA REDE OU EM NÓS	TAMPERING	MONITORAMENTO DE INTEGRIDADE DE NÓS				
FIS	VULNERABILIDADE FÍSICA	TAMPERING	DETECTOR DE TAMPER MAGNETICO, TAMPA ABERTA, ETC.				
FIS	DESCARGAS ELÉTRICAS	NODE DESDTRUCTION	ATERRAMENTO E PROTEÇÕES ELÉTRICAS ADEQUADAS				
FIS	EXAUSTÃO OU FALHA DA BATERIA	EXHAUSTION	MONITORAMENTO E ALERTA DE SAÚDE DAS BATERIAS				
MAC	INTRUSÃO MALICIOSA	DENIAL OF SLEEP / FLOODING	ANALISADOR DE TRÁFEGO DE DADOS MAC				
MAC	INTRUSÃO MALICIOSA	DENIAL OF SLEEP / FLOODING	IDS - SISTEMA DETECTOR DE INTRUSÃO				
REDE	VIOLAÇÃO DE CONFIDENCIALIDADE	EAVESDROPPING	SEGMENTAÇÃO DE REDE				
REDE	IDENTIFICAÇÃO DE REDE POR INTRUSOR	JAMMING	BAIXA POTÊNCIA DE TRANSMISSÃO				
REDE	INTERFERÊNCIAS NA REDE	JAMMING	DETECÇÃO DE INTERFERÊNCIAS DE RÁDIO				
REDE	INTERFERÊNCIAS E INVASÕES	JAMMING	ADOTAR PROTOCOLOS FHSS				
REDE	INTERFERÊNCIAS E INVASÕES	JAMMING	ANTENAS DIRECIONAIS				
REDE	CONEXÕES NÃO AUTORIZADAS	HELLO FLOODING	VERIFICAÇÃO BIDIRECIONAL ENTRE NÓS				
REDE	FALHAS NA REDE OU EM NÓS	HELLO FLOODING	ROTEAMENTO MULTICAMINHO				
REDE	CONEXÕES NÃO AUTORIZADAS	HELLO FLOODING	PROTOCOLOS COM BROADCASTING AUTENTICADOS				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - WORMHOLE	PACOTES COM LIMITAÇÃO DE LOCALIZAÇÃO E SINCRONIZAÇÃO				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - BLACKHOLE	IDS - SISTEMA DETECTOR DE INTRUSÃO				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - BLACKHOLE	USO DE HONEYPOT				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - BLACKHOLE	ACTIVE TRUST BLACKHOLE DETECTION				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - BLACKHOLE	AUTENTICAÇÃO ENTRE NÓS				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - SINKHOLE	IDENTIFICADOR DE NÓS SUSPEITOS NA REDE				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - WORMHOLE	CHAVE DE LOCALIZAÇÃO				
REDE	PERDA DE NÓS COM DESVIO DE DADOS	HOLE ATTACK - WORMHOLE	PACKET LEASHING				
REDE	REPLICAÇÃO MALICIOSA DE DADOS	NODE REPLICATION	PACOTES COM LIMITAÇÃO DE LOCALIZAÇÃO E SINCRONIZAÇÃO				
REDE	REPLICAÇÃO MALICIOSA DE DADOS	NODE REPLICATION	CHAVE DE LOCALIZAÇÃO				
REDE	REPLICAÇÃO MALICIOSA DE DADOS	NODE REPLICATION	NÚMERO DE CONEXÕES				
REDE	REPLICAÇÃO MALICIOSA DE DADOS	NODE REPLICATION	USO DE INFORMAÇÕES HISTÓRICAS DOS NÓS				
REDE	REPLICAÇÃO MALICIOSA DE ROTAS	REPLAY ROUTING	DETECÇÃO E ISOLAMENTO DE NÓS COM ROTAS INADEQUADAS				
REDE	REPLICAÇÃO MALICIOSA DE ROTAS	REPLAY ROUTING	PROTOCOLO COM ROTEAMENTO SEGURO (SecRout)				
REDE		SYBIL	PROTOCOLOS COM DETECTOR DE ATAQUE SYBIL (ANOMALIAS)				
REDE		MQTT EXPLOIT	UTILIZAR SECURE MQTT (SMQTT)				
APP		CoAP EXPLOIT	UTILIZAR CoAP COM CAMADA ADICIONAL DE SEGURANÇA				
APP	INJEÇÃO DE DADOS FALSIFICADOS	FALSE DATA INJECTION	DETECTOR DE FDA				

APÊNDICE 3. ASTRIS – ANÁLISE DE THREAT & RESILIENCE (Continuação)

MEDIDAS PARA FORTIFICAÇÃO DA SOLUÇÃO IIoT

STACK	FORTIFICAÇÃO	CHECK		NA	
FIS	ESPECIFICAR CONFIGURAÇÃO DE CHAVES ÚNICAS DE AUTENTICAÇÃO ENTRE DISPOSITIVOS				
FIS	VERIFICAR ALTERAÇÃO DE SENHAS DE ACESSO PADRÕES PARA SENHAS ROBUSTAS				
FIS	AVALIAR INSTRUÇÕES DE FABRICANTES QUANTO À PROXIMIDADE COM OUTROS EQUIPAMENTOS E MATERIAIS DURANTE INSTALAÇÃO				
RSE	AVALIAR NECESSIDADE DEUSO DE BAND PASS FILTER (BPFEM SISTEMAS VIA RÁDIO DE ALTA POTÊNCIA) NA UNIDADE				
RSE	EM CASO DE *GATEWAYS* COM MAIS DE UM PROTOCOLO WIRELESS, DESABILITAR PROTOCOLOS NÃO UTILIZADOS				
RSE	VERIFICAR VULNERABILIDADES PARA O PROTOCOLO ESCOLHIDO EM BASES INTERNACIONAIS (CISA, CERT, ETC.) (IDENTIFICAR HISTÓRICO DE SINISTROS)				
TRA	UTILIZAR SWITCHS INTELIGENTES E BLOQUEAR PORTAS NÃO UTILIZADAS				
APP	UTILIZAR ACL (ACCESS CONTROL LIST) SEMPRE QUE POSSÍVEL				
APP	ESPECIFICAR FORMATO E FERRAMENTAS DE GESTÃO DE SAÚDE DA REDE				
APP	AVALIAR SEGMENTAÇÃO DE REDE, PROTEGENDO *GATEWAYS* E EQUIPAMENTOS ICS DE REDES EXTERNAS ATRAVÉS DE *FIREWALL*				
APP	DEFINIR QUAIS TIPOS DE DADOS SERÃO DISPONIBILIZADOS PARA DIFERENTES PAPÉIS (Ex: Operador, mantenedor, gestor, etc.)				
APP	DEFINIR PROTEÇÃO CONTRA *MALWARE* EM ESTAÇÕES E HOSTS				
APP	DEFINIR FORMATO DE MONITORAMENTO DE DISPONIBILIDADE				
APP	AVALIAR RECOMENDAÇÕES DE TOPOLOGIA SEGURA DEFINIDA PELO FABRICANTE DO SISTEMA				

APÊNDICE 4. ASTRIS – ANÁLISE DE IMPLEMENTAÇÃO & SCALABILITY

IMPLEMENTAÇÃO DOPROJETO IoT

SISTEMA E PARAMETRIZAÇÃO

		CHECK		NA	
I1	CONFIGURAÇÃO DE NOS DA REDE (PARÂMETROS, UNIDADES, ALARMES, ETC.)				
I2	ALARME DE SAÚDE DO DISPOSITIVO (FADIGA, DISTANCIA EXCESSIVA, ATENUAÇÕES, DISTORÇOES, INTERFERÊNCIAS)				
I3	CADASTRAR VARIÁVEIS, ALARMES E DIAGNÓSTICOS DE REDE EM HISTORIADOR				
I4	ALARME - SETPOINT - CONSIDERAR A CONSTANTE DE PROCESSO E O TEMPO NECESSÁRIO PAR AO OPERADOR RESPONDER				
I5	PRIORIDADE DO ALARME				

DOCUMENTOS

		CHECK		NA	
I6	DEFINIR E DOCUMENTAR NETWORK ID ÚNICO PARA *GATEWAYS*				
I7	DOCUMENTAR PONTOS WIRELESS POR ÁREA (OU POR FUNCIONALIDADE) EM UM MASTER DRAWING				
I8	CRIAR E DOCUMENTAR DESENHO DA REDE INCLUINDO INFORMAÇÕES DE PROTOCOLOS				
I9	PARAMETRIZAÇÃO E DOCUMENTAÇÃO DE CADA SENSOR				
I10	DOCUMENTAÇÃO COM IDENTIFICAÇÃO DE *GATEWAY* ASSOCIADO A SENSORES				
I11	MANUAL DE OPERAÇÃO COM POLÍTICAS E REQUERIMENTOS OPERACIONAIS PARA O PROTOCOLO EM QUESTÃO				

PROCEDIMENTOS E COMISSIONAMENTO

		CHECK		NA	
I12	PROCEDIMENTO DE TESTE DE EQUIPAMENTOS (FAT/SAT) COM DOCUMENTAÇÃO				
I13	PROCEDIMENTO DE NETWORK CHECKOUT				
I14	TESTES DE MALHA DO INSTRUMENTO E DISPOSITIVOS				
I15	TESTE DE CONEXÃO WIRELESS DE CADA INSTRUMENTO COM CRITÉRIOS DE ACEITAÇÃO (E PROCEDIMENTO)				
I16	PRÉ-COMISSIONAMENTO - VERIFICAR INSTALAÇÕES, BARREIRAS, ENERGIA, FONTES DE INTERFERENCIA				
I17	PROCEDIMENTO DE GESTÃO DA CONFIDENCIALIDADE DOS DADOS DOS DISPOSITIVOS WIRELESS				
I18	ATERRAMENTO DOS EQUIPAMENTOS DA REDE VERIFICADO?				
I19	ENERGIA PARA OS DISPOSITVOS DE REDE É SEGURA, ESTABILIZADA E PROTEGIDA CONTRA SURTOS?				
I20	POLÍTICA DE ACESSO DA APLICAÇÃO				

TREINAMENTOS

		CHECK		NA	
I21	TREINAMENTO EM SEGURANÇA E MANUTENÇÃO PARA USUÁRIOS E EQUIPE DE MANUTENÇÃO				
I22	TREINAMENTOS SOBRE USO DA APLICAÇÃO				

CONFIGURAÇÕES

		CHECK		NA	
I23	CONFIGURAÇÃO DE ROLES E ACESSOS				
I24	TROCA DE SENHAS PADRÕES				
I25	INSTALAÇÃO DE ANTI-VIRUS				

APÊNDICE 5. ASTRIS – ANÁLISE DE IMPLEMENTAÇÃO & SCALABILITY (Continuação)

OPERAÇÃO DA REDE IIoT

MANUTENÇÃO	
O1	PROCEDIMENTOS DE RECUPERAÇÃO DE DESASTRES (FALHAS NOS INSTRUMENTOS, EM *GATEWAYS*, NA APLICAÇÃO E RESTORE...)
O2	DEFINIÇÃO DE ESTRATÉGIA PARA SPARE PARTS DE ACORDO COM MATRIZ DE CRITICIDADE (CRITICO / N-CRITICO)- EX: *GATEWAYS*
O3	GESTÃO DE SENHAS DE ACESSO AOS DISPOSITIVOS DE CAMPO - TRATAR COMO SENHAS AO DCS. NÃO É RECOMENDADO GUARDAR ESTAS SENHAS EM BASES DE PROJETOS
O4	BACKUPS DE APLICAÇÕES E PARÂMETROS DE DISPOSITIVOS
O5	ATUALIZAÇÕES DE ANTI-VIRUS E *PATCHES*
O6	CONTROLE DE INTERFERÊNCIAS - FONTES RADIOATIVAS E OUTRAS
O7	VERIFICAÇÃO PERIÓDICA E APÓS SINISTROS COMO DESLIGAMENTOS

FERRAMENTAS	
O9	FERRAMENTAS/SOFTWARE DE MANUTENÇÃO (ACESSO LOCAL / REMOTO)
O10	FERRAMENTAS/SOFTWARE DE DESIGN
O11	APLICAÇÃO DE GESTÃO DE ATIVOS

MONITORAMENTO	
O12	MONITORAMENTO DE % DISPONIBILIDADE DE CADA NÓ
O13	MONITORAMENTO BATERIA
O14	MONITORAMENTO SAÚDE DA REDE
O15	MONITORAMENTOS

APÊNDICE 6. ASTRIS – ANÁLISE DE IMPLEMENTAÇÃO & SCALABILITY (Continuação)

ESCALABILIDADE DE REDES IIoT

AVALIAÇÃO DE ESCALABILIDADE ESPECÍFICA DO PROTOCOLO:

CUSTO DA ESCALABILIDADE	BAIXA	MÉDIA	ALTA
	>20%	<20%	<10%
CUSTO DA ESCALABILIDADE DA REDE DE SENSORES (GATEW, SENSORES, REPETIDORES)			
CUSTO DA ESCALABILIDADE DA REDE DE TRANSPORTE			
CUSTO DA ESCALABILIDADE DA REDE DE APLICAÇÃO			

CAPACIDADE DE ESCALABILIDADE	BAIXA	MÉDIA	ALTA
CAPACIDADE DO PROTOCOLO EM ESCALABILIDADE DA REDE DE SENSORES			
CAPACIDADE DO PROTOCOLO EM ESCALABILIDADE DA REDE DE TRANSPORTE			
CAPACIDADE DO PROTOCOLO EM ESCALABILIDADE DA APLICAÇÃO			

FERRAMENTAS DE ESCALABILIDADE	NÃO	SIM
SOFTWARE PARA SIMULAÇÃO DE EXPANSÕES DE REDES DISPONÍVEL (Ex: WiNC, SNAPON)		
PROTOCOLO RESILIENTE PARA REDES DENSAS DE COMUNICAÇÃO		
APLICAÇÃO PERMITE VISUALIZAR PERFORMANCE APÓS EXPANSÕES		

AVALIAÇÃO DE ESCALABILIDADE ESPECÍFICA DAS INSTALAÇÕES

	S	N	
INSTALAÇÕES FÍSICAS APROPRIADAS PARA ESCALABILIDADE FUTURA? (INFRA ELÉTRICA, PAINÉIS, SWITCHES, ETC.)			
SISTEMA POSSUI ESCALABILIDADE HORIZONTAL?			
SISTEMA OU DESIGN POSSUI ESCALABILIDADE VERTICAL?			

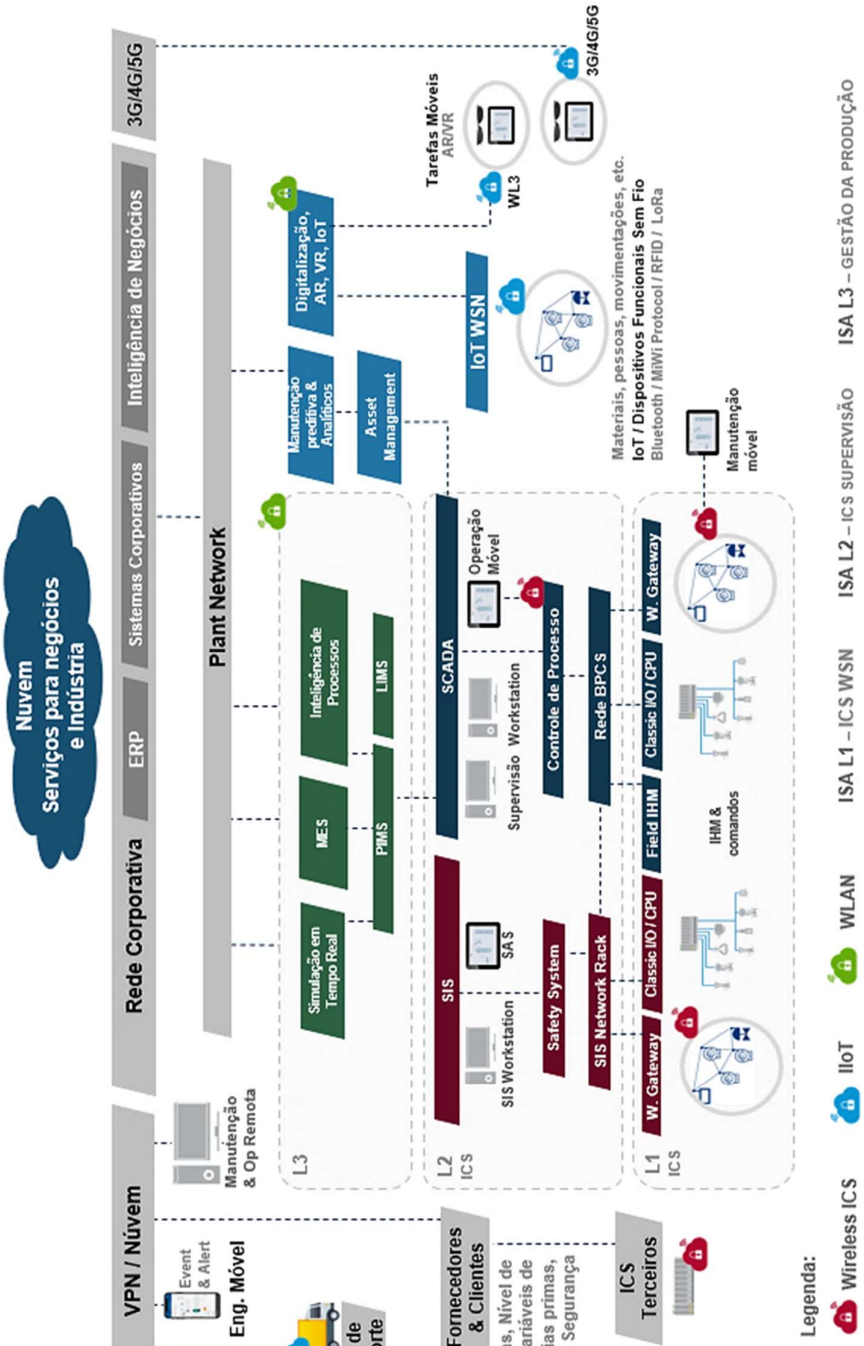
ESCALABILIDADE EM NOVOS PROJETOS

	S	N	
DETERMINAR PROBABILIDADE DE ESCALABILIDADE FUTURA E DESIGNAR SOLUÇÃO ESCALÁVEL EM ACORDO A ESTA POSSIBILIDADE			
CONSIDERAR APLICAÇÕES FUTURAS E MANTER PERCENTUAL DE CAPACIDADE RESERVA PARA A REDE (*GATEWAYS*, ETC.)			

ESCALABILIDADE DE INSTALAÇÕES EXISTENTES

		CHECK	
AVALIAR IMPACTO DA BASE DE SISTEMA EXISTENTE EM FUTURAS EXPANSÕES (MEMÓRIA, ARMAZENAMENTO, PROCESSAMENTO, ETC.)			
REVISAR NUMERO DE *GATEWAYS*, COM POSSÍVEL REARRANJO DE REPETIDORES.			
AVALIAR CUSTO BENEFÍCIO ENTRE ADICIONAR REPETIDOR OU NOVO *GATEWAY*			
MANTER PERCENTUAL DE CAPACIDADE RESERVA PARA A REDE			
REALIZAR ANÁLISE DE PERFORMANCE E DENSIDADE DA REDE FUTURA ATRAVÉS DE MODELAGEM E SIMULAÇÃO			
EM CASO DE REDES MUITO DENSAS, ANALISAR MÉTODOS DE DISTRIBUIÇÃO DE CANAIS E FREQUENCIA PARA EVITAR INTERFERENCIAS			
AVALIAR O IMPACTO DA ESCALABILIDADE SOB OS NÓS EXISTENTES			
MAPEAR INTERLIGAÇÕES E CONFIGURAÇÕES PADRÕES PARA NOVOS NÓS			
REALIZAR E REGISTRAR TESTE DE ALCANCE DE NOVOS DISPOSITIVOS			

APÊNDICE 7. Conexões e Interoperabilidade em Ambiente de Manufatura Digital



ANEXO 1. Principais Normas Técnicas em Segurança de Sistemas Industriais

Norma	Descrição	Norma	Descrição
ISA 60	Control Centers	**ISA 101**	Human-Machine Interface
ISA 84	Instrumented systems Functional Safety in the Process Industries	**ISA 104**	Device Integration
ISA 95*	Enterprise/Control integration Committee	**ISA 108***	Intelligent Device Management
ISA 99*	Industrial Automation and Control Systems Security	**ISA 111**	Unified Automation for Buildings
ISA 100*	Wireless Systems for Automation	**ISA 112**	SCADA Systems
USTAG65A	ISA-administered U. S. Technical Advisory Group (USTAG) for IEC SC65A, System Aspects	**USTAG65C**	ISA-administered U. S. Technical Advisory Group (USTAG) for IEC SC65C, Industrial Networks
USTAG65E	ISA-administered U. S. Technical Advisory Group (USTAG) for IEC SC65E, Devices and Integration in Enterprise Systems	**IEC 60950**	Safety of Information technology Equipment
IEC 60079	Explosive Atmospheres	**IEC 61131**	Programmable Logic Controllers
IEC 60793	Optical Fibre? IEC 60874 (Conectors for Optical Fibre)	**IEC 61158**	Industrial Communication Networks
IEC 61334	Distribution automation using distribution line carrier systems – a standard for low-speed reliable power line communications by electricity meters, water meters and SCADA	**IEC 61514**	Industrial process control systems – Methods of evaluating the performance of valve positioners with pneumatic outputs
IEC 61506	Industrial-process measurement and control – Documentation of application software	**IEC 61588**	Precision clock synchronization protocol for networked measurement and control systems
IEC 61508*	Functional Safety of electrical/electronic/programmable electronic safety-related systems	**IEC 61636**	Software interface for Maintenance Information Collection and Analysis (SIMICA)
IEC 61511*	Functional Safety – safety instrumented systems for the process industry sector	**IEC 61642**	Industrial a.c. networks affected by harmonics – Application of filters and shunt capacitors
IEC 61513	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	**IEC 61907**	Communication network dependability engineering
IEC 61920	Infrared free air applications	**IEC 62002**	Mobile and portable DVB-T/H radio access
IEC 61926	Design automation	**IEC 62040**	Uninterruptible power systems (UPS)
IEC 61987	Industrial-process measurement and control – Data structures and elements in process equipment catalogues	**IEC 62074**	Fibre optic interconnecting devices and passive components – Fibre optic WDM devices
IEC 62232	Determination of RF field strength, power density and SAR in the vicinity of radiocommunication base stations for the purpose of evaluating human exposure	**IEC 62680**	Universal Serial Bus (USB) interfaces for data and power
IEC TR 62263	Live working – Guidelines for the installation and maintenance of optical fibre cables on overhead power lines	**IEC 62682**	Management of alarm systems for the process industries
IEC 62264	Enterprise-control system integration	**IEC/TR 62685**	Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)
IEC/TR 62357	Power system control and associated communications – Reference architecture for object models, services and protocols	**IEC 62734***	Industrial networks – Wireless communication network and communication profiles – ISA 100.11a
IEC 62439	Industrial communication networks – High availability automation networks	**IEC 62769**	Field device integration (FDI)
IEC 62443*	Industrial communication networks – Network and system security	**IEC/TR 62794**	Industrial-process measurement, control and automation – Reference model for representation of production facilities (digital factory)
IEC 62455	Internet protocol (IP) and transport stream (TS) based service access	**IEC/TS 62872**	Industrial-process measurement, control and automation system interface between industrial facilities and the smart grid
IEC 62491	Industrial systems, installations and equipment and industrial products – Labelling of cables and cores	**IEC/PAS 62948***	Industrial networks – Wireless communication network and communication profiles – WIA-FA
IEC 81346	Industrial systems, installations and equipment and industrial products – Structuring principles and reference designations	ISA 106	Procedure Automation for Continuous Process Operations

Fonte: ISA (2021) e IEC (2020)

ANEXO 2. Objetivos e Técnicas em Resiliência Cibernética

Meta	Descrição
Antecipar	Manter um estado de preparação informada para evitar comprometimentos da função da missão de possíveis condições adversas
Resistir	Manter funções essenciais da missão apesar das condições adversas
Recuperar	Restaurar as funções da missão durante e após as condições adversas
Evoluir	Alterar as funções da missão e/ou recursos de suporte, de modo a minimizar os impactos adversos das condições adversas reais ou previstas

Objetivo	Descrição
Entender	Manter representações úteis das dependências da missão e o status dos recursos em relação a possíveis adversidades
Preparar	Manter um conjunto de cursos de ação realistas que abordam adversidades previstas ou antecipadas
Evitar / Evitar	Impedir a execução bem-sucedida do ataque ou a realização de condições adversas
Continuar	Maximize a duração e a viabilidade das funções essenciais da missão durante condições adversas
Restringir	Limite os danos causados por condições adversas
Reconstituir	Reimplantar recursos para fornecer um conjunto de funcionalidades de missão o mais competitivo possível após condições adversas
Transformar	Mudar aspectos do comportamento organizacional em resposta a condições adversas anteriores, atuais ou prospectivas ou ataques

Fonte: Bodeau e Graubart, 2013

ANEXO 3. Técnicas de Resiliência Cibernética

Técnica	Descrição
Adaptativo Resposta	Responder de forma adequada e dinâmica a situações específicas, utilizando contingências operacionais ágeis e alternativas para manter as capacidades operacionais mínimas, a fim de limitar as consequências e evitar a desestabilização, tomando ações preventivas quando apropriado
Analítico Monitoramento	Recolher, fundir e analisar dados continuamente para usar inteligência de ameaças, identificar vulnerabilidades, encontrar indicações de possíveis condições adversas e identificar danos potenciais ou reais
Coordenado Defesa	Coordene vários mecanismos distintos (defesa em profundidade) para proteger recursos críticos, entre subsistemas, camadas, sistemas e organizações
Decepção	Confundir, enganar e enganar o adversário
Diversidade	Use um conjunto heterogêneo de tecnologias, fontes de dados, locais de processamento e caminhos de comunicação para minimizar falhas de modo comum (incluindo ataques que exploram vulnerabilidades comuns)
Dinâmico Posicionamento	Distribua e realoque dinamicamente funcionalidades e ativos
Dinâmico Representação	Apoiar a conscientização e resposta da situação da missão usando representações dinâmicas de componentes, sistemas, serviços, atividades adversárias e outras situações adversas e efeitos de cursos alternativos de ação
Não Persistência	Reter informações, serviços e conectividade por tempo limitado, reduzindo assim a exposição à corrupção, modificação ou usurpação
Privilégio Restrição	Design para restringir privilégios atribuídos a usuários e entidades cibernéticas e definir requisitos de privilégios em recursos com base na criticidade
Realinhamento	Permitir que os recursos sejam alinhados (ou realinhados) com as principais funções da missão, reduzindo assim a superfície de ataque, o potencial de consequências não intencionais e o potencial de falhas em cascata
Redundância	Forneça várias instâncias protegidas de informações e recursos críticos, para reduzir as consequências da perda
Segmentação / Separação	Componentes separados (logicamente ou fisicamente) com base na criticidade e confiabilidade, para limitar a propagação de danos
Comprovado Integridade	Fornecer mecanismos para verificar se serviços críticos, armazenamentos de informações, fluxos de informações e componentes foram corrompidos
Imprevisibilidade	Alterações, com frequência e aleatoriamente, para tornar a superfície de ataque imprevisível

Fonte: Bodeau e Graubart, 2013

ANEXO 4. Tipos de Ataques cibernéticos

Ataques Passivos

N	Ameaça	Descrição
T1	Eavesdropping	Quando um atacante ganha acesso a um canal de comunicação e realiza alterações aos poucos, enviando dados de volta para cada participante. Também chamado de ataque de replay
T2	Node Destruction	Destruição física (com o uso de um surto elétrico, força física ou munição) de um nó por qualquer meio, para que o nó não seja mais operável.
T3	Node Malfunctioning	Mau funcionamento do nó: pode acontecer devido a muitos fatores diferentes, desde sensores defeituosos ou esgotamento de energia devido à sobrecarga do sensor ou outros ataques DoS.
T4	Node Outage	Node Outage: este ataque ocorre sempre que um nó falha em sua funcionalidade normal. Por exemplo, se um cluster head de uma rede heterogênea falha em operação regular, então os protocolos WSN devem ser fortes o suficiente para mitigar os efeitos negativos desse tipo de indisponibilidade de nós, elegendo novos cluster head e/ou fornecendo rotas alternativas para rede.
T5	Traffic Analysis	Análise de tráfego: o padrão de tráfego de uma rede pode ser tão valioso quanto o conteúdo dos pacotes de dados para os adversários. Informações importantes sobre a topologia de rede podem ser obtidas analisando os padrões de tráfego. Em WSNs, os nós mais próximos da estação base, ou seja, o sink, fazem mais transmissões do que os outros nós porque retransmitem mais pacotes do que os nós mais distantes da estação base. Da mesma forma, o clustering é uma ferramenta importante para escalabilidade em WSNs e os chefes de cluster são mais ocupados do que os outros nós da rede.

Ataques Ativos

	N	Ameaça	Descrição
Physical Layer	T6	Jamming	Criação de nós maliciosos de comunicação implantado por hackers
	T7	Node Tampering	Quando alguém realiza mudanças físicas no dispositivo ou no link de comunicação. Elementos do hardware pode ser acessados, identidades roubadas ou substituídas, a qual podem violar a confidencialidade, disponibilidade e integridade.

	N	Ameaça	Descrição
MAC Layer	T8	Collusion	Criação propositada de colisão pode ser considerado como um ataque de Jamming. Comumente alveja redes wireless, tornando a comunicação impossibilitada
	T9	Denial of Sleep	Negação de *sleep*: para dispositivos alimentados por bateria, o ataque de negação e *sleep* resultará em esgotamento de energia. Este ataque pode ser alcançado executando ataques de colisão ou handshaking repetido, ou seja, manipulando continuamente os sinais de controle de fluxo Request to Send (RTS) e Clear to Send (CTS), eventualmente impedindo que o nó entre na fase de *sleep*.
	T10	De-synchronization:	Time Synchronized Channel Hopping (TSCH) é um protocolo de camada MAC apresentado no padrão IEEE 802.15.4e. Ele capacita a consistência extrema e possui pequenos ciclos de trabalho através da sincronização de tempo e técnicas de salto de canal
	T11	Exhaustion	Exaustão de recursos de rede, como buffers e capacidades computacionais
	T12	Link layer Flooding	Nesse tipo de ataque, um nó malicioso abusa da justiça do acesso ao meio enviando pacotes de dados MAC excessivos ou pacotes de controle MAC para seus nós vizinhos. No final, os nós vítimas sofrem de DoS ou a energia de suas baterias se esgota. Além disso, este ataque também pode esgotar os recursos de largura de banda do canal.
	T13	Spoofed Routing Information	Falsificar ou repetir o IP (Replay IP) de determinado dispositivo ou aplicação com intuito de perturbar os dados de uma rede, gerando falsas mensagens de erro, re-roteamento de malhas, encurtamento de rotas. Podem aproveitar que enquanto a carga útil dos pacotes são criptografados, informações de rota e títulos não são.
	T14	Unfairness	ataques aos mecanismos de rede (fairness mechanisms) que monitoram comunicações quanto à parcela de dados que usuários e aplicativos recebem.
	T15	6LoWPAN Exploit	Revisado para a IoT para uso estendido do IPv6 por dispositivos inteligentes. O 6LoWPAN integra infraestruturas baseadas em IP e WSNs, especificando como os pacotes IPv6 devem ser roteados em redes restritas, como redes IEEE 802.15.4, por fragmentação e remontagem de campos de dados de datagramas. Um ataque específico para 6LoWPAN é a duplicação de fragmentos. 6LoWPAN camada se um fragmento se originar da mesma fonte que os fragmentos recebidos anteriormente do mesmo pacote IPv6. Portanto, nenhum mecanismo de autenticação existe no receptor no momento da recepção para verificar se o fragmento recebido é um fragmento duplicado original ou falsificado, esse ataque pode facilmente enganar o receptor. O receptor não pode distinguir fragmentos legítimos de duplicatas falsificadas. Em vez disso, ele deve processar todos os fragmentos que parecem pertencer ao mesmo pacote IPv6 de acordo com o endereço MAC do remetente e a tag de datagrama 6LoWPAN. Assim, um invasor pode fingir ser um nó legítimo e explorar esse ataque de fraqueza, no qual um invasor coloca seus próprios fragmentos no cadeia de fragmentação.

Fonte: Butun et. Al. (2020) e Varga et. Al. (2017)

ANEXO 4. Tipos de Ataques cibernéticos (Continuação)

	N	Ameaça	Descrição
Network Layer	T16	Hello Flooding	HELLO-flooding: Neste tipo de ataque, um invasor (tem maior alcance de transmissão do que os nós normais) transmite mensagens publicitárias para toda a rede e convence outros nós de que está localizado em sua vizinhança.
	T17.1	Hole Attacks - BlackHole	Blackhole: Um nó malicioso pode descartar todos os pacotes que recebe para encaminhamento. Este ataque é especialmente eficaz quando o nó do buraco negro também é um sumidouro. Essa combinação de ataque pode interromper todo o tráfego de dados ao redor do buraco negro. Em alguns textos, esse ataque também é referido como "Selfishness" (Egoísmo).
	T17.2	Hole Attacks - SinkHole	Sinkhole: Um nó malicioso pode anunciar por broadcast para todos os nós vizinhos que é o melhor próximo salto para enviar os pacotes ao seu destino. Quando um nó se torna um sinkhole, ele se torna o hub para sua vizinhança e começa a receber todos os pacotes que vão para a estação base. Todo o tráfego da rede é direcionado para este único nó, mas neste caso, o nó sinkhole não descarta nenhum pacote. Dessa forma, ele espera permanecer indetectável pelo IDS.
	T17.3	GrayHole	Encaminhamento Seletivo (Grayhole): É um tipo especial de ataque de buraco negro, no qual o nó malicioso age de forma mais inteligente e não descarta todos os pacotes que recebe, mas os que seleciona. Dessa forma, o invasor espera não ser detectado pelo IDS. Esse tipo de ataque também é chamado de "ataque de buraco cinza", pois é uma variante do ataque de buraco negro.
	T17.4	Wormhole attack	Wormhole é um link de baixa latência maliciosamente preparado, através do qual o attacker pode repetir mensagens. Os pacotes de informação recebidos em um ponto da rede são entunelados a outro ponto, no qual a informação é repetida de volta para o ponto inicial.
	T18	Node Replication	Copiar a identidade de um nó e criar um outro nó (virtual) com a mesma identidade, a partir do qual pode ser enviado dados falsos em seu nome através de rotas randômicas para perturbar a rede.
	T21.1	Routing - Misdirection	No ataque de direcionamento errado, um invasor encaminha mensagens em andamento para os caminhos errados intencionalmente. Isso pode ser alcançado fabricando anúncios de roteamento falsos e fazendo com que as tabelas de roteamento dos nós vizinhos atualizem essas informações falsas [61]. Esse ataque também é categorizado como ataque DoS, portanto, os nós direcionados são completamente bloqueados e não recebem mais pacotes após o anúncio das informações de roteamento falsas.
	T21.2	Routing - Network Partitioning	Uma rede totalmente conectada é dividida em sub-redes (chamadas sub-redes) nas quais os nós em diferentes sub-redes não podem se comunicar, embora estejam conectados. Por exemplo, em uma rede que consiste em várias sub-redes em que os nós A e B estão localizados em uma sub-rede e os nós C e D estão em outra, uma partição de rede ocorre se o dispositivo de comutação entre as duas sub-redes falhar (ou forçado a falhar). Nesse caso, os nós A e B não podem mais se comunicar com os nós C e D, mas todos os nós A-D retomam a operação normal.
	T21.3	Routing Loop	Roteamento Loop: Um roteamento loop é introduzido em um caminho de rota. Ele é criado falsificando atualizações de roteamento. Suponha um adversário pode determinar que o nó A e o nó B estão dentro do alcance de rádio um do outro. Um adversário pode enviar uma atualização de roteamento forjada para o nó B com um endereço de origem falsificado indicando que veio do nó A. O nó B então marque o nó A como seu pai e retransmita a atualização de roteamento. O nó A ouvirá a atualização de roteamento do nó B e marque B como seu pai. As mensagens enviadas para A ou B serão encaminhadas para sempre em um loop entre o dois deles. Isso leva ao esgotamento de energia e eventual falha de nó/rede. Informações de roteamento falsificadas, alteradas ou repetidas: as informações de roteamento trocadas entre os nós podem ser alterados por nós maliciosos para ter um efeito prejudicial no esquema de roteamento. Especialmente, se os pacotes não forem protegidos por mecanismos de contagem, como nonce, os pacotes podem ser gravados e facilmente usados para reprodução ataques.
	T21.4	Replay Routed Information	Informações de roteamento falsificadas, alteradas ou repetidas: as informações de roteamento trocadas entre os nós podem ser alterados por nós maliciosos para ter um efeito prejudicial no esquema de roteamento. Especialmente, se os pacotes não forem protegidos por mecanismos de contagem, como nonce, os pacotes podem ser gravados e facilmente usados para reprodução ataques.
	22	RPL Exploit	Exploração de RPL: IoT consiste em dispositivos com recursos limitados, como bateria, memória, capacidade de processamento, etc. Para este tipo de rede, um novo protocolo de roteamento da camada de rede é projetado chamado RPL (Routing Protocol for Lowpower and lossy networks). O RPL é leve e não possui todas as funcionalidades dos protocolos de roteamento tradicionais. O RPL foi proposto especialmente para coletores de dados (comunicações multiponto a ponto) e está sendo adotado pela IoT recentemente.
	23	Sybil Attack	Ataque Sybil: Um único nó apresenta várias identidades para outros nós da rede. Isso causa confusão no rede; os nós recebem caminhos de roteamento contraditórios que estão passando pelo invasor. Isso reduz a eficácia dos esquemas de tolerância a falhas e representa uma ameaça significativa aos protocolos de roteamento geográfico. Além desses serviços, também pode afetar o desempenho de outros esquemas, como detecção de mau comportamento, algoritmos baseados em votação, agregação de dados, fusão e armazenamento distribuído.

Fonte: Butun et. Al. (2020) e Varga et. Al. (2017)

ANEXO 4. Tipos de Ataques cibernéticos (Continuação)

	N	Ameaça	Descrição	
Transport Layer	24	De-synchronization	Dessincronização: um invasor interrompe os links reais entre dois nós dessincronizando as transmissões em entre eles. Um exemplo desse tipo de ataque é o envio de mensagens fabricadas, como sequências de sinalizadores defeituosos (transmitindo pacotes forjados com números de sequência falsos ou sinalizadores de controle que dessincronizam os terminais para que eles retransmitam os dados [64]) continuamente para ambos os lados das partes comunicantes, como resultado, para forçá-los a perder sua sincronização.	
	25	MQQT Exploits	MQTT Exploit: O Message Queue Telemetry Transport (MQTT) [83] é um protocolo de conectividade leve de publicação e assinatura destinado a trabalhar em dispositivos com recursos limitados, como sensores incorporados de baixa potência, para permitir que eles se comuniquem. No contexto de IoT, o MQTT é amplamente utilizado para permitir a comunicação entre dispositivos usando uma abordagem de mensagens de publicação e assinatura. No entanto, o MQTT não inclui a camada de segurança por padrão e é responsabilidade do usuário resolver problemas de segurança.	
	26	Session Hijacking	Em ciência da computação, esse ataque é referido como a “exploração de” e “adulteração” de uma sessão de comunicação válida (que também é chamada de chave de sessão) para obter acesso não autorizado a informações ou serviços de um sistema. Por ser uma extensão das redes IP, o sequestro de sessão de mensagens TCP também afetará e será problemático para as redes IoT.	
	27	SYN-flooding	Em um ataque de inundação, um invasor visa esgotar a energia e/ou a memória de um nó, inundando-o com mensagens espúrias. Isso é conseguido, por exemplo, enviando várias solicitações de conexão sem nunca completar a conexão, sobrecarregando o buffer e, eventualmente, fazendo com que o nó seja morto [61], [67]. Mais especificamente, em um ataque de inundação TCP SYN (sincronizar), um adversário envia várias solicitações de conexão TCP sem nunca completar a conexão, sobrecarregando assim o buffer de conexão meio aberto do alvo [64].	

	N	Ameaça	Descrição	
Application layer	28	CoAP Exploit	O Constrained Application Protocol (CoAP) [85] é um protocolo de camada de aplicação projetado como uma replicação do HTTP para os pequenos dispositivos de IoT para fornecer capacidade de comunicação com o resto da Internet. Recentemente, muitas implementações de IoT estão usando CoAP, o que indica que ele terá um papel crucial no futuro das aplicações de IoT. Como mencionado em [86], existem vários desafios relacionados à segurança pela introdução do CoAP. Ele não traduz a funcionalidade completa do HTTP, o que cria problemas de segurança para mensagens multicast.	
	29	False Data Injection	Para influenciar o resultado geral de uma medição ou leitura, os nós capturados injetam intencionalmente dados falsos na RSSF. Portanto, pode-se afirmar que esse ataque acontece em nível semântico, portanto, não afeta nada além da lógica.	
	30	Path-based DoS	Como o nome sugere, esse ataque é um ataque DoS na camada do aplicativo. Neste ataque, um invasor sobrecarrega os nós de uma longa distância inundando um caminho de comunicação de ponta a ponta com pacotes fabricados ou pacotes repetidos [87]. Como resultado, todos os nós ao longo do caminho do invasor ao destino são afetados.	
	31	Re-programming	De vez em quando, cada elemento de rede precisa ser corrigido ou reprogramado para controle de versão, aquisição de código e codificação-decodificação, ao mudar para uma nova versão do programa. Isso também é verdade para RSSFs e IoT. Se esse cronograma de reprogramação (ou gerenciamento de patches em si) não for mantido em segredo, os adversários podem aproveitar esse tempo vulnerável da rede simplesmente enviando mensagens falsas para os nós e empurrando-os para estados instáveis ou mortos [88].	
	32	Sensor Overwhelming:	Atacar ou alterar a sensibilidade das medições do sensor. Sensores de mira com espúrios interferência ou sobrecarregando-os completamente com mensagens falsas e inundando-os com falsos estímulos.	

Fonte: Butun et. Al. (2020) e Varga et. Al. (2017)

ANEXO 5. VULNERABILIDADES DO PROTOCOLO BLUETOOTH

	Security Issue or Vulnerability	Remarks
Versions Before Bluetooth v1.2		
1	**Unit key is reusable and becomes public once used.**	A unit key should be used as input to generate a random key. A key set should be used instead of only one unit key.
2	**Unit key sharing can lead to eavesdropping.**	A corrupt user may be able to compromise the security between two other users if the corrupt user has communicated with either of the other two users. This is because the link key (unit key), derived from shared information, has been disclosed.
Versions Before Bluetooth v2.1		
3	**Short PINs are allowed.**	Weak PINs, which are used for the generation of link and encryption keys, can be easily guessed. People have a tendency to select short PINs.
4	**PIN management is lacking.**	Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems.
5	**Encryption keystream repeats after 23.3 hours of use.**	Per Figure 3-5, the encryption keystream is dependent on the link key, EN_RAND, Master BD_ADDR, and Clock. Only the Master's clock will change during a particular encrypted connection. If a connection lasts more than 23.3 hours, the clock value will begin to repeat, hence generating an identical keystream to that used earlier in the connection.
All Versions		
6	**Link keys are stored improperly.**	Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls.
7	**Attempts for authentication are repeated.**	A limiting feature needs to be incorporated in the specification to prevent unlimited requests. The Bluetooth specification currently requires a time-out period between repeated attempts that will increase exponentially.
8	**Strength of the challenge-response pseudo-random generator is not known.**	The Random Number Generator (RNG) may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.
9	**Encryption key length is negotiable.**	The specification allows devices to negotiate encryption keys as small as one byte. A more robust encryption key generation procedure needs to be incorporated in the specification.
10	**The master key is shared.**	A better broadcast keying scheme needs to be incorporated into the specification.
11	**No user authentication exists.**	Only device authentication is provided by the specification. Application-level security, including user authentication, can be added via overlay by the application developer.
12	**The E_0 stream cipher algorithm used for Bluetooth encryption is weak.**	More robust encryption needs to be incorporated in the specification.
13	**Privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.**	Once the BD_ADDR is associated with a particular user, that user's activities could be logged, resulting in a loss of privacy.
14	**Device authentication is simple shared-key challenge-response.**	One-way-only challenge-response authentication is subject to MITM attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that users and the network are legitimate.
15	**End-to-end security is not performed.**	Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by use of additional security controls.
16	**Security services are limited.**	Audit, nonrepudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.
17	**Discoverable and/or connectable devices are prone to attack.**	Any device that must go into discoverable or connectable mode to pair should only do so for a minimal amount of time. A device should never be in discoverable or connectable mode all the time.

Fonte: Scarfone e Padgette, 2008

ANEXO 6. ZIGBEE AMEAÇAS

Ataques em diferentes camadas do ZigBee

Camada	Descrição
Transport Layer Attacks	esta camada é utilizada para apoiar links de comunicação de sensores recém inseridos na rede. Os ataques podem incluir flooding e desynchronization; onde o nó alvo é inundado por um grande número de solicitações de estabelecimento de conexões inválidas (ataque de inundação), e forjar pacotes para um ou ambas as extremidades da conexão para que o host solicite retransmitir os frames de pacotes perdidos (ataque de dessincronização)
Network Layer Attacks	esta camada é responsável pelo processo de roteamento e tráfego de rede também. Ataques pode incluir buracos de minhoca e encaminhamento seletivo ataques. No ataque do buraco de minhoca, há dois nós maliciosos que estão localizados em diferentes saltos da rede. Quando um nó emissor transmite um quadro de dados, um nó malicioso canaliza esses dados para o outro nó malicioso e pelo qual ele irá enviá-lo para os nós vizinhos, por sua vez. Consequentemente, o nó remetente é enganado de forma que nós maliciosos estão próximos de um ou dois saltos onde esses dois nós maliciosos podem estar fora de range
MAC Layer Attacks	incorpora o cabeçalho MAC que ajuda o receptor a saber o tamanho do pacote, retransmite os quadros em caso de erros e aloca recursos para nós recém ligados. *Link Layer Jamming* é um exemplo de ataques de camada MAC que é lançado para criar DoS interrompendo a troca de mensagens entre transmissores e receptores. Isso gera a consequente degradação e redução do desempenho da rede
Physical Layer Attacks	exploram o sinal de rádio comum através de *jamming* para observar silenciosamente (*eavesdrop*) ou adulterar (*tamper*) os quadros de pacotes de dados

Métodos de Ataques

Método	Descrição
Active Attacks	este ataque requer interceptação real da rede onde o adversário pode modificar os dados, injetar frames em falha (*fault frames*). Consequentemente, o desempenho da rede é afetado negativamente. Além disso, a integridade e confidencialidade dos dados são comprometido
Passive Attacks	ao contrário dos ataques ativos, não há nenhuma interceptação do fluxo de comunicação, mas sim o atacante monitora o tráfego de dados sem afetar sua integridade. Contudo, a confidencialidade da informação é exposta como informações confidenciais que podem ser coletadas com intenção maliciosa

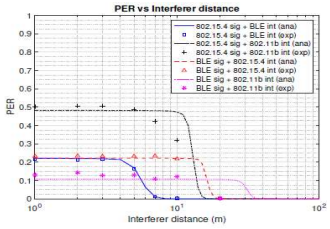
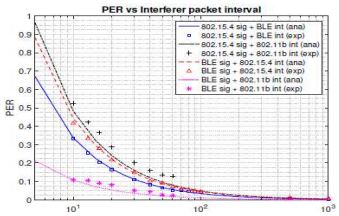
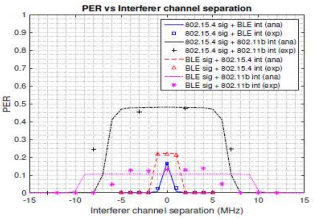
Alvos de Ataques

Camada	Descrição
Sink Attacks	*Sinkhole* ou simplesmente o ataque de afundamento (*sink*) pode acontecer quando um nó malicioso anuncia uma rota para ser o caminho mais curto. E uma vez que todos os algoritmos de roteamento selecionam o caminho mais curto, atrairá mais tráfego de rede para ser escavada em direção a ele. Normalmente, este ataque é combinado com ataque de buraco de minhoca
Source Attacks	Nestes ataques, o adversário compromete um nó legítimo para atuar como um nó buraco negro. Este nó descarta seletivamente os pacotes recebidos ou todos os pacotes recebidos para enganar outros nós vizinhos, induzindo-os a procurar outra rota.
Neighbour Attacks	Este tipo de ataque explora o processo de descoberta de outros nós vizinhos através da transmissão de mensagens HELLO. Um nó malicioso envia mensagem HELLO com alta potência de transmissão, e em consequência, os outros nós (r*eceivers*) consideram este nó como seu vizinho e enviarão os pacotes de dados sensíveis em retorno. Consequentemente, uma grande quantidade de energia será desperdiçada, podendo ocorrer uma consequente congestão na rede.
Member Attacks	as vezes são chamados de párias ou de ataques internos. No caso de ataques de párias (outcast), o nó atacante não faz parte (não é membro) da rede, mas é autorizado a inserir ameaça à rede. Por outro lado, o ataque interno (membro) ocorre quando um nó malicioso faz parte da rede e compromete a rede ou quando o invasor carregou um perfil falso e conseguiu entrar na rede
Energy Depletion Attacks	O atacante envia mensagens falsas para atrair o nó a esgotar intencionalmente a sua energia por redundância relacionada a cálculos de segurança. Isso vai reduzir a vida útil do nó e permitir que o invasor lance vários ataques pós-esgotamento como em DoS e ataques de Replay

Fonte: Abuhasel e Khan (2020)

ANEXO 7. TESTE DE COEXISTÊNCIA WIRELESS (ESTUDO DE CASO)

Testes de interferência nos protocolos IEE 802.15.4 e BLE

	Distância	Intervalo de Pacotes	Separação de Canais
Resultados dos Testes			
Descrição	Distância do interferente: Neste cenário, a distância do interferente para o do receptor d varia de 1 a 100 m. O intervalo de pacote interferente LIper é fixado em 20 ms para o IEEE 802.15.4 e o BLE, e 10 ms para IEEE 802.11b. O transmissor e os canais de interferência são escolhidos da seguinte forma: IEEE 802.15.4 no canal 12 (2410 MHz), BLE no canal 3 (2410 MHz) e IEEE 802.11b no canal 1 (2.412 MHz), constituindo portanto interferência co-canal. Todos os outros parâmetros são fixados.	Intervalo de pacote do interferente: neste cenário, o intervalo de pacote do interferente LI,per por varia de 5ms a 1s. A distancia do interferente d é fixada em 5m e os canais interferentes são escolhidos da seguinte forma: IEEE 802.15.4 no canal 12 (2410 MHz), BLE no canal 3 (2410 MHz) e IEEE 802.11b no canal 1 (2.412 MHz), constituindo assim interferência co-canal. Todos os outros parâmetros são fixados.	Separação de canal do interferente: neste cenário, a separação de canal do interferente para o transmissor varia de -15 a 15 MHz, constituindo assim interferência de canal adjacente. A distância interferente d é fixada em 5m. O intervalo de pacote do interferente LI,per é fixado em 20 ms para IEEE 802.15.4 e BLE, e 10 ms para IEEE 802.11b. Todos os outros parâmetros são fixos.
Conclusão	A rede BLE é afetada mais pela interferência IEEE 802.15.4 do que vice-versa. A rede IEEE 802.15.4 atinge 1% de PER com distancia do interferente BLE em cerca de 7 m, enquanto a rede BLE requer uma distancia de 17m da IEEE 802.15.4 para atingir 1% de PER. Uma razão para essa diferença é ganho de processo DSSS (cerca de 9 dB) na rede IEEE 802.15.4. Outra razão é a maior ocupação de canal do IEEE 802.15.4 no tempo de transmissão de pacotes BLE em comparação com pacotes IEEE 802.15.4. Isso aumenta a probabilidade de que o sinal BLE possa evitar colisão com o interferente IEEE 802.11b.	A rede BLE é afetada marginalmente mais pela rede IEEE 802.15.4 do que vice versa. A rede IEEE 802.15.4 atinge 10% PER com interferente BLE com intervalo de pacote em cerca de 35 ms, enquanto a rede BLE atinge 10% PER com interferente IEEE 802.15.4 com Intervalo de pacotes de cerca de 45 ms. As razões para esta diferença são o ganho do processo DSSS e a maior ocupação do canal da rede IEEE 802.15.4. Outra observação é que a rede BLE é afetada muito menos (cerca de 5 vezes) por interferência IEEE 802.11b do que pela interferência IEEE 802.15.4, apesar da potencia superior de transmissão do interferente IEEE 802.11b (20 dBm) em comparação com IEEE 802.15.4 (0 dBm). Há duas razões para isso. Primeiro, o interferente IEEE 802.15.4 tem uma maior ocupação de canal em comparação com o interferente IEEE 802.11b. Em segundo lugar, o poder de interferencia do IEEE 802.11b diminui conforme a interferencia da banda do IEEE 802.11b passa pela banda estreita do filtro do receptor do BLE.	A rede BLE é mais uma vez afetada mais pela rede IEEE 802.15.4 do que vice-versa. Em uma separação de canal do interferente em 1 MHz, a rede BLE tem um PER de cerca de 22%, enquanto o PER da rede IEEE 802.15.4 cai para cerca de 1%. Em separação de canal de 2 MHz, o PER cai para quase zero em ambas configurações. No caso de interferência IEEE 802.11b, ambas as redes IEEE 802.15.4 e BLE são severamente afetadas a cerca de 10 MHz de separação de canal, após o qual o PER cai para quase zero.

Fonte: Natarajan et. Al. (2016)

ANEXO 8. COMPARAÇÃO ENTRE WirelessHART E ISA100 STACKS

CAMADA		IEC 62591 (Wireless HART)	ANSI/ISA100.11a
Físico (PHY)		Rádio IEEE 802.15.4 2.4GHz DSSS	Rádio IEEE 802.15.4 2.4GHz DSSS
Camada de acesso de mídia (MAC)		Compatível com os serviços MAC e MAC 802.15.4-2006	Baseado em uma versão modificada e não compatível do IEEE 802.15.4-2006 MAC
Camada de enlace de dados (DLL)		Salto de canal com intervalo de tempo Reconhecimentos seguros Propagação do relógio Segurança: integridade de dados salto a salto	Salto de canal com intervalo de tempo Reconhecimento seguro Propagação de relógio Segurança: integridade e criptografia de dados salto a salto Roteamento de fonte e gráfico Opções de junção* para: salto lento e salto lento/rápido híbrido Reconhecimento duplo Tamanhos de slot de tempo baseados em configuração Notificação explícita de congestionamento
Camada de rede		Roteamento de gráfico e fonte. As rotas gráficas incluem o "1 a n Pontos de Acesso" permitindo conexões redundantes/múltiplas às redes backbone. Isso permite que uma única rede dê suporte a uma taxa de transferência muito alta. Juntando-se à segurança: criptografia de ponta a ponta e integridade de dados	IETF IPv6 e 6LoWPAN Fragmentação e remontagem em roteador backbone. Observe que, se a fragmentação e a remontagem forem usadas, a rota do gráfico deve terminar e remontar as mensagens em um único roteador de backbone, introduzindo um único ponto de falha.
Camada de transporte		Serviço sem conexão Entrega confiável com um serviço de reconhecimento	Serviço UDP sem conexão Segurança: ponta a ponta criptografia e integridade de dados
Camada de aplicação	Controle do processo	HART 7	Sem camada de aplicação de processo e controle
	Gerenciamento	Diagnósticos Configuração de rede centralizada de links de superframes e rotas Junção	Diagnósticos Configuração de rede centralizada de links de superframes e rotas Opções de junção* para: Configuração de rede distribuída
	Segurança	Gerenciamento de chaves	Gerenciamento de chaves
	Subcamada de aplicativo	Estrutura de comando e resposta Codificação de dados Segurança: Criptografia e integridade de dados	Estrutura de serviços de objeto e método Codificação de dados

Fonte: Nixon (2012)

ANEXO 9. OUTRAS DIFERENÇAS ENTRE WIRELESS HART E ISA100

Característica	IEC 62591 (Wireless HART)	ANSI/ISA100.11a	Comentários
Tipos de dispositivo e funções	WirelessHART define dispositivo que inclui dispositivo de campo, ponto de acesso, gateway, gerenciador de rede, gerenciador de segurança, adaptador e dispositivo portátil	ISA100.11a define funções que IO, roteador, provisionamento, roteador de backbone, gateway, gerenciador de sistema, gerenciador de segurança e fonte de tempo do sistema	Há uma diferença fundamental no nível do instrumento de campo; Os dispositivos ISA100.11a não são necessários para dar suporte à função de roteador. Por esta razão, será muito provável que vejamos redes ISA100.11a que são apenas Star vs. redes WirelessHART que são inerentemente mesh
Provisionamento	Todos os dispositivos de campo e pontos de acesso devem oferecer suporte a solicitações de associação	O ISA100.11a define uma função de provisionamento específica, o que significa que nem todos os dispositivos serão capazes de provisionar outros dispositivos para ingressar na rede.	A escolha dos dispositivos ISA100.11a terá uma influência significativa na topologia que pode ser implantada. Se o usuário for forçado a usar uma topologia em estrela, também é bastante provável que eles precisem de pesquisas de site para garantir que a rede se forme
Espaço de endereço	WirelessHART é limitado a cerca de 30K dispositivos por rede WirelessHART	O ISA100.11a usa IPv6 e, como tal, possui um espaço de endereço muito maior.	O limite prático do número de dispositivos por ponto de acesso e gateway é de algumas centenas e alguns milhares. Como os DCSs são totalmente capazes de se conectar a muitos gateways, essa limitação de espaço de endereço é interessante, mas não limitante
Dimensionamento de uma única malha (pontos de estrangulamento)	WirelessHART suporta vários pontos de acesso por rede local. Para taxas de dados de E/S aumentadas, podem ser adicionados pontos de acesso adicionais. Para plantas grandes, mais de um gateway pode ser usado.	O ISA100.11a suporta 1 ou mais roteadores de backbone por rede local. Se uma área local exceder a largura de banda de um rádio, serão adicionados roteadores de backbone adicionais.	Esta é uma diferença fundamental entre a arquitetura de duas redes.
Fragmentação e Remontagem	WirelessHART suporta fragmentação e remontagem na camada de aplicação. Uma função específica, transferência de dados de bock, é definida para esta finalidade.	O ISA100.11a suporta fragmentação e remontagem no nível da rede. Esta capacidade é inerentemente fornecida pelo 6LoWPAN.	Embora o ISA100.11a suporte fragmentação e remontagem, o que não está definido é como vários roteadores de backbone coordenam a remontagem de pacotes. Sem essa função, um gráfico deve terminar em um roteador de backbone que introduz um único ponto de falha.
Redundância	WirelessHART é uma rede mesh; por design, todos os caminhos devem ser definidos para serem redundantes. No backbone, vários pontos de acesso podem ser usados.	ISA100.11a é definido para suportar opcionalmente a tecnologia mesh. Os roteadores de backbone podem ser projetados para suportar DUO-CAST.	O ISA100.11a DUOCAST é uma tecnologia muito capaz, mas não é totalmente especificada, levando a implementações proprietárias. Ambos os esquemas devem funcionar bem em ambientes reais de plantas.
Camada de enlace de dados	WirelessHART usa um tempo de slot de 10ms. Um único algoritmo para salto de canal é definido. Os códigos MIC são sempre de 4 bytes. As redes são coordenadas pelo Absolute Slot Time (AST).	ISA100.11a suporta um tamanho de slot de tempo configurável, 10 é apenas um tamanho de slot que pode ser suportado. O System Manager configura o horário do slot quando um dispositivo ingressa na rede. Três sequências de salto de canal são definidas e 5 padrões de salto são definidos. Os padrões de salto de canal são fornecidos ao gerenciador do sistema quando o dispositivo se junta à rede. Os códigos MIC podem ter de 4 a 16 bytes. As redes são coordenadas pelo tempo TAI. O ISA100.11a também oferece suporte ao roteamento na DLL.	O suporte padrão ISA100.11a de tamanhos de slot configuráveis e padrões de salto de canal é muito flexível. A desvantagem de seu padrão de salto lento é que o receptor deve permanecer ligado por períodos muito mais longos, o que aumenta o uso de energia. Ao contrário da definição de DLL do modelo OSI, isso significa que o roteamento de rede mesh é feito no nível da DLL versus a camada de rede. Todas as opções ISA100.11a significam que nem todos os dispositivos ISA100.11a irão interoperar.

Fonte: Nixon (2012)

ANEXO 9. OUTRAS DIFERENÇAS ENTRE WIRELESS HART E ISA100 (Continuação)

Característica	IEC 62591 (Wireless HART)	ANSI/ISA100.11a	Comentários
Camada de rede	WirelessHART suporta roteamento, junção e criptografia/descriptografia na camada de rede.	ISA100.11a suporta IETF IPv6 e 6LoWPAN na camada de rede.	As camadas de rede nos dois padrões são muito diferentes. Enquanto o WirelessHART usa a camada de rede para dar suporte ao roteamento pela rede mesh, o ISA100.11a usa a camada de rede para dar suporte ao roteamento pelo backbone. Como o roteamento pelo backbone usa IPv6, a camada de rede também implementa 6LoWPAN. Incluído como parte do 6LoWPAN está o suporte para fragmentação e remontagem e compressão de cabeçalho IPv6.
Roteamento de backbone	O WirelessHART não exige uma tecnologia de backbone. O HARTOver-IP pode ser usado para o backbone.	ISA100.11a usa IPv6 para o backbone para rotear pacotes entre sub-redes	O roteamento de backbone é projetado para dimensionar redes. O WirelessHART consegue isso adicionando pontos de acesso e gateways adicionais. O ISA100.11a usa IPv6 que pode ou não estar disponível em uma rede da planta.
Camada de transporte	WirelessHART suporta serviços reconhecidos e não reconhecidos. O serviço com reconhecimento permite que os dispositivos enviem pacotes e obtenham uma confirmação na entrega, enquanto os serviços não reconhecidos permitem que os dispositivos enviem pacotes sem a exigência de reconhecimento de ponta a ponta, portanto, sem qualquer garantia de transmissão de pacotes bem-sucedida.	O ISA100.11a TL fornece serviços sem conexão por meio do User Datagram Protocol (UDP) sobre IPv6 com compactação opcional conforme definido pela especificação IETF 6LoWPAN. A extensão inclui verificações de integridade de dados melhores do que as disponíveis usando a soma de verificação UDP e mecanismos adicionais de autenticação e criptografia. ISA100.11a TL não suporta transações reconhecidas.	No ISA 100.11a, a camada de rede usa os formatos IETF IPv6 e 6LoWPAN, e a camada de transporte fornece serviço UDP IPv6 sem conexão com portas de origem e destino compactadas ou não compactadas. Os pacotes ISA 100.11a podem viajar pela Internet e são transparentes para os nós de roteamento. No entanto, o cabeçalho de segurança, a carga útil do aplicativo e o MIC formam a carga útil da mensagem do UDP. Portanto, qualquer nó final da Internet que envie e/ou receba essas mensagens DEVE entender esses três componentes. Em outras palavras, deve seguir o protocolo de segurança ISA100.11a. Ele deve saber como configurar a segurança ISA100.11a com seu par e como usá-la. Isso significa que os aplicativos baseados na Internet devem ser projetados para serem compatíveis com ISA100.11a – as coisas não são tão abertas como parecem ser.
Camada de aplicação	WirelessHART utiliza o HART AL. O AL, conforme definido e apoiado pela HART Communication Foundation (HCF), é extenso. O AL inclui Comandos Universais (definidos pela IEC 61158-5-20 e IEC 61158-6-20). Os Comandos Universais definem o suporte mínimo que deve ser implementado por um dispositivo. Esses comandos melhoram a operação geral do dispositivo. Os dispositivos WirelessHART são definidos usando EDDL e totalmente suportados pelos handhelds existentes.	ISA100.11a AL define objetos de software para modelar objetos do mundo real. Ela é dividida em duas subcamadas: a AL superior (UAL) e a subcamada de aplicação (ASL). O UAL contém os processos de aplicação para o dispositivo e pode ser usado para lidar com hardware de entrada e/ou saída, suportar encapsulamento de protocolo ou executar uma função computacional. O ASL fornece os serviços necessários para que o UAL execute suas funções, como comunicação baseada em objeto e roteamento para objetos dentro de um processo de aplicação de usuário (UAP) na rede.	Esta é a diferença mais significativa entre os dois padrões. Embora o WirelessHART suporte totalmente o HART, o ISA100.11a adota uma abordagem mais aberta e permite, mas não define, protocolos de aplicação.

Fonte: Nixon (2012)

ANEXO 9. OUTRAS DIFERENÇAS ENTRE WIRELESS HART E ISA100 (Continuação)

Característica	IEC 62591 (Wireless HART)	ANSI/ISA100.11a	Comentários
Segurança	WirelessHART suporta chaves de junção, chaves de rede e chaves de sessão. As chaves de sessão são alocadas para comunicações de dispositivo para dispositivo. Todos os dispositivos devem usar uma chave de junção. Todas as comunicações devem ser criptografadas usando chaves de sessão. As chaves de junção são provisionadas usando um dispositivo portátil. Chaves simétricas AES-128 são suportadas. As chaves podem ser giradas	1a Revisão 1.0, Data de lançamento: 23 de setembro de 2012 Página 24 de 39 Segurança FINAL WirelessHART suporta chaves de junção, chaves de rede e chaves de sessão. As chaves de sessão são alocadas para comunicações de dispositivo para dispositivo. Todos os dispositivos devem usar uma chave de junção. Todas as comunicações devem ser criptografadas usando chaves de sessão. As chaves de junção são provisionadas usando um dispositivo portátil. Chaves simétricas AES-128 são suportadas. As chaves podem ser giradas. O ISA100.11a suporta chaves de junção, chaves de rede e chaves de sessão. As chaves de sessão são alocadas para comunicações de dispositivo para dispositivo. As chaves de junção são opcionais, assim como as chaves de sessão. As chaves de junção são provisionadas usando o provisionamento aéreo. Chaves simétricas AES-128 são suportadas. ISA100.11a também define opcionalmente chaves assimétricas para o processo de junção. As chaves podem ser giradas.	Tanto o WirelessHART quanto o ISA100.11a definem um conjunto de chaves de segurança que são usadas para garantir uma comunicação segura. A criptografia simétrica depende de ambos os terminais de comunicação usando a mesma chave ao se comunicar com segurança. Os invasores que não compartilham as chaves não podem modificar as mensagens sem serem detectados e não podem descriptografar as informações de carga útil criptografada. Comum a ambos os padrões é que um novo dispositivo é provisionado com uma chave de ingresso antes de tentar ingressar em uma rede. A chave de junção é usada para autenticar o dispositivo para uma rede específica. Assim que o dispositivo se conectar com sucesso à rede, o gerente de segurança fornecerá chaves para comunicação adicional. O uso da chave de junção é opcional no ISA100.11a. Uma chave global, uma chave bem conhecida sem garantias de segurança, também pode ser usada no processo de junção para dispositivos que não suportam chaves simétricas. O ISA100.11a permite a criptografia opcional de mensagens. ISA100.11a OTAP em combinação com chaves assimétricas é útil para escalar redes. O WirelessHART não permite que a segurança seja opcional o que evita erros que podem comprometer o sistema
Gerente de segurança	A função do Security Manager é definida. Comandos e API para Security Manager não estão definidos.	O ISA100.11a fornece uma especificação para o Security Manager.	Como a funcionalidade do Security Manager tende a ser fornecida em conjunto com o Network Manager, para redes de pequeno e médio porte há pouco a ganhar descrevendo o gerenciador de segurança em detalhes. Para redes maiores, um caso pode ser feito para um gerenciador de segurança mais completamente definido
Gerenciador de Rede / Sistema	WirelessHART contém uma extensa descrição e um conjunto de comandos para o Network Manager.	O ISA100.11a contém uma extensa descrição e um conjunto de serviços para o System Manager.	Existem muitas diferenças entre o Network Manager e o System Manager. As diferenças começam a aparecer quando se observam os detalhes de diagnóstico, configuração e ativação de superframes e links, rotas, contratos e horários. O System Manager ISA100.11a também deve acompanhar as funções que os dispositivos específicos suportam e deve ser capaz de provisionar e gerenciar corretamente esses dispositivos. Isso torna o System Manager mais complicado de usar.
Padrão internacional	IEC 62591-1 em março 2010 HART7 a partir de 2007	ANSI/ISA100.11a2011	WirelessHART é um padrão internacional desde março de 2010-. A ISA100.11a está avançando rumo ao padrão internacional (IEC 62734).

Fonte: Nixon (2012)

ANEXO 9. OUTRAS DIFERENÇAS ENTRE WIRELESS HART E ISA100 (Continuação)

Característica	IEC 62591 (Wireless HART)	ANSI/ISA100.11a	Comentários
Interoperabilidade (capacidade dos dispositivos e gateways construídos por diferentes fabricantes para trabalhar juntos)	A interoperabilidade entre dispositivos WirelessHART é exigida pelo HCF. O HCF realiza testes de interoperabilidade com vários fabricantes' Dispositivos e gateways WirelessHART para a pilha de comunicação e o aplicativo HART7.	O teste de conformidade de pilha é realizado pelo WCI. O foco da ISA100.11a está na flexibilidade da especificação que leva a opções algumas das quais não estão totalmente definidas. As opções ISA100.11a não estão definidas para que, quando implementadas, interoperem com dispositivos que não`não os use	Os dispositivos ISA100.11a podem passar no teste WCI e ainda não funcionarem juntos – depende de como as opções foram usadas Não há teste de interoperabilidade de automação de processo para dispositivos ISA100.11a.
Coexistência	Sim	Sim	Recurso de camada física, salto de canal e TDMA
Número de fabricantes que atualmente fornecem produtos	Emerson, Siemens, ABB, Endress+Hauser, Pepperl+Fuchs, MacTech e outros (cerca de 13 fornecedores suportam WirelessHART, muitos outros das 240 empresas membros da HCF estão trabalhando em produtos).	Honeywell e Yokogawa suportam ISA100.11a	O número de fornecedores que suportam WirelessHART e o número de produtos WirelessHART enviados excedem em muito seus equivalentes para ISA100.11a. WirelessHART tem uma vantagem de 2 anos, suporta uma camada de aplicação totalmente definida, tem um conjunto muito mais extenso de fornecedores e tem um número significativo de redes implantadas em todo o mundo.
Camada Física e Pilha de Comunicações	IEEE 802.15.4 – 2006. As pilhas de comunicações incluem: Linear Technology, WiTECK, Nivis e AwiaTech	IEEE 802.15.4 – 2006. As pilhas de comunicações incluem: Nivis.	
Protocolo de pacote básico	HART7	ISA100.11ª	O ISA100 deve ser capaz de encapsular HART7 por meio de seu protocolo básico, mas os métodos necessários para a interoperabilidade ainda não foram padronizados.
Adaptadores HART que permitem que dispositivos HART com fio se conectem à rede sem fio.	Sim, atualmente sendo fornecido por um grande número de fabricantes.	Possível, mas ainda não disponível.	Os adaptadores são parte fundamental do WirelessHART. Eles permitem que dispositivos HART 5 e 6 mais antigos se comuniquem em uma rede WirelessHART.

Fonte: Nixon (2012)