MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SISTEMAS DE CONTROLE E ELETRICIDADE DE NAVIOS

TRABALHO DE CONCLUSÃO DE CURSO

SOLUÇÕES DE SISTEMA DE CONTROLE E AUTOMAÇÃO PARA NAVIOS:
Evolução tecnológica e desafios em segurança cibernética.

1ºTen PEDRO VITOR MATTOS COSTA

Rio de Janeiro
2023

1ºTen PEDRO VITOR MATTOS COSTA

SOLUÇÕES DE SISTEMA DE CONTROLE E AUTOMAÇÃO PARA NAVIOS:
Evolução tecnológica e desafios em segurança cibernética.

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Sistemas de Controle e Eletricidade de Navios.

Orientadores:
D. Sc. Alessandro Jacoud Peixoto
M. Sc. Warlley Paulo Freire

CIAA
Rio de Janeiro
2023

FOLHA DE APROVAÇÃO

1ºTen PEDRO VITOR MATTOS COSTA

SOLUÇÕES DE SISTEMA DE CONTROLE E AUTOMAÇÃO PARA NAVIOS:
Evolução tecnológica e desafios em segurança cibernética.

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Sistemas de Controle e Eletricidade de Navios.

Aprovada em 24 de novembro de 2023

Banca Examinadora:

Alessandro Jacoud Peixoto, D. Sc – UFRJ

Warlley Paulo Freire, M. Sc. – MB.

Luiz Philipe Souza Cavalcanti, M. Sc. – MB.

CIAA
Rio de Janeiro
2023

À minha amada esposa Isabella, que está grávida de nosso filho Miguel, por serem minha inspiração constante.

AGRADECIMENTOS

Após um longo período de estudos, de mais uma etapa acadêmica, faz-se necessário reconhecer a importância daqueles que me incentivaram e de alguma forma contribuíram para o andamento desta pesquisa. Aos meus orientadores agradeço o tempo empregado em reuniões e conversas acerca do tema, que agregaram de sobremaneira para o desenvolvimento deste trabalho. Estendo ao Coordenador do curso e docente das disciplinas de Controle I e II, Prof. Cesar Lampe, que com seus ensinamentos pôde nortear significativamente as análises realizadas.

Agradeço em especial, ao meu orientador técnico, Capitão-Tenente Paulo Freire, contemporâneo das épocas de Colégio Naval e Escola Naval, além de grande amigo, compartilhando os conveses da Fragata Liberal. Seu incessante entusiasmo nas conversas sobre *Blockchain* e segurança cibernética, sem dúvida foi um dos motivadores na minha escolha pelo tema, que por fim culminou na sorte de tê-lo como orientador deste trabalho acadêmico.

Aos meus familiares e amigos, sou grato por ao longo desses mais de 12 anos de carreira sempre terem ficado ao meu lado, em especial a minha mãe, Mauricéia, meu pai, Jorge e minha irmã, Patrícia. Aos meus companheiros de turma e de sala de aula, agradeço a competição saudável e camaradagem, que sempre nos fazem persistir em seguir adiante, mesmo diante das dificuldades.

Por fim, à minha amada esposa Isabella, que durante este curso teve sobre ela a graça de Deus, que em seus planos nos reservou a alegria de um filho, nosso Miguel, nos trazendo uma felicidade que vai além de qualquer coisa que poderíamos planejar para nossas vidas. Agradeço por ser minha companheira paciente e maior incentivadora, mesmo nos dias mais difíceis em que tive que me ausentar para me dedicar as minhas obrigações. Saiba que todos os dias me esforçarei para fazer de vocês dois, as pessoas mais amadas e felizes do mundo.

Desta forma, agradeço a Deus por tudo que pude viver nesse período, pois cada uma das escolhas e sacrifícios me conduziram até este momento.

“Se eu vi mais longe, foi por estar sobre ombros de gigantes.”
Isaac Newton

SOLUÇÕES DE SISTEMA DE CONTROLE E AUTOMAÇÃO PARA NAVIOS:
Evolução tecnológica e desafios em segurança cibernética.

Resumo

O panorama industrial para soluções de sistemas de controle e automação vem mudando rapidamente ao longo dos últimos anos. O uso do processamento digital, com recursos de linguagem de programação e protocolos de rede, vem crescendo de maneira contínua sob a égide da quarta revolução industrial, também conhecida como Industria 4.0. Com a introdução de conceitos como sistemas de controle em rede, que preveem a conexão de sensores, atuadores e controladores por meio de uma infraestrutura de comunicação, os protocolos de rede tem assumido uma importância cada vez maior no *design* das instalações industriais. Paralelamente, as infraestruturas navais vêm se tornando cada vez mais complexas desde a metade do último século. O desenvolvimento da microeletrônica, com computadores cada vez menores, permitiu a integração destes dispositivos aos sistemas navais, auxiliando no monitoramento e controle, a fim de assistir as tripulações e engenheiros em suas atividades. Como resultado, a operação de navios mercantes e militares tornou-se mais eficiente e segura, aumentando a produtividade, mesmo com um número reduzido de pessoal. Nesse contexto, a convergência entre os domínios operacional e cibernético pode representar uma ameaça sem precedentes as instalações industriais e sistemas navais. Isso pode ser amplificado pela utilização de protocolos de rede de comunicação, nos níveis operacionais de sistemas de controle e automação de infraestruturas complexas. Desta forma, este trabalho busca apresentar análises de sistemas, como o *SCADA Systems,* e um estudo de caso do ataque cibernético "Stuxnet", como forma de representar as vulnerabilidades dos sistemas de controle em rede. Além disso, inclui uma simulação de ataque de degradação de serviço a uma planta de propulsão naval, com discussões sobre como o ataque proposto pode ser efetivo, destacando a necessidade de enfatizar a mentalidade de segurança cibernética nos ambientes industrial e marítimo.

Palavras-chave: Industria 4.0; Sistemas de Controle em Rede; Protocolos de Rede; Segurança Cibernética.

SOLUTIONS FOR SHIP CONTROL AND AUTOMATIONS SYSTEMS:
Technological advancements and Cybersecurity challenges.

Abstract

The industrial landscape for control and automation systems solutions has been changing rapidly over the past few years. The use of digital processing, as programming languages and network protocols, has been continuously growing under the aegis of the Fourth Industrial Revolution, also known as Industry 4.0. Since the introduction of concepts such as Networked Control Systems, which foresee the connection of sensors, actuators, and controllers through a communication infrastructure, network protocols have assumed increasing importance in the design of industrial facilities. Simultaneously, naval infrastructures have become progressively more complex since the last half-century. The development of microelectronics, with ever-smaller computers, has enabled the integration of these devices into naval systems, assisting in monitoring and control to support crews and engineers in their activities. As a result, the operation of merchant and military vessels has become more efficient and secure, increasing productivity, even with reduced personnel quantity. In this context, the convergence of operational and cyber domains can pose an unprecedented threat to industrial facilities and naval systems. This can be amplified using communication network protocols at the operational levels of complex control and automation systems. Thus, this work seeks to present analyses of systems such as SCADA Systems and a case study of the cyber-attack "Stuxnet" as a means of representing the vulnerabilities of Networked Control Systems. It also includes a simulation of a service degradation attack on a naval propulsion plant, with discussions on how the proposed attack can be effective, emphasizing the need to underscore the cybersecurity mindset in both industrial and maritime environments.

Key words: Industry 4.0; Networked Control Systems; Network Protocols; Cybersecurity.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

A/D	*Analog-to-Digital Converter*
ADU	*Application Data Unit*
BSA	*Backtracking Search Optimization Algorithm*
PLC	*Programmable Logical Control*
CAN	*Control Area Networked*
CIP	*Control and Information Protocol*
CPI	*Cyber-physical Intelligence*
CPS	*Cyber-Physical Systems*
D/A	*Digital-to-Analog Converter*
DC	*Digital Computer*
DCS	*Distributed Control System*
DoS	*Denial-of-Service*
EA	*Evolutionary Algorithm*
EPA	*Enhanced Performance Architecture*
Ethernet/IP	*Ethernet/ Industrial Protocol*
FTMA	Função de Transferência de Malha Aberta
FTMF	Função de Transferência de Malha Fechada
HMI	*Human Machine Interface*
HPC	Hélice de passo controlado
ICS	*Industrial Control System*
ICT	*Information and Communication Technology*
IED	*Intelligent Electronic Devices*
IIoT	*Industrial Internet of Things*
IT	*Information Technology*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IMO	*International Maritime Organization*
ISO	*International Organization for Standardization*
IP	*Internet Protocol*
IoT	*Internet of Things*
LAN	*Local Area Network*

MTS	*Maritime Transport System*
MIMO	*Multiple Input Multiple Output*
MitM	*Man-in-the-middle*
MTU	*Master Terminal Unit*
MBAP	*ModBus Application Protocol*
NCP	*Network Control Protocol*
NCS	*Networked Control System*
OSI	*Open Systems Interconnection*
OT	*Operational Technology*
PLC	*Programmable Logical Control*
PDU	*Protocol Data Unit*
PID	Controladores Proporcional-Integral-Derivativo
PSI	*Passive System Identification*
RTE	*Real-Time Ethernet*
RTU	*Remote Terminal Unit*
SD	*Service Degradation*
SISO	*Single Input Single Output*
SCADA	*Supervisory Control and Data Acquisition*
SoS	*System of a System*
TCP	*Transmission Control Protocol*
WAN	*Wide Area Network*
z.o.h.	*Zero-order-hold*

LISTAS DE SÍMBOLOS

$F(s)$	Função no domínio da frequência (Transformada de Laplace)
$F(z)$	Função no domínio do tempo (Transformada Z)
$f(kT)$	Função que descreve o sinal discretizado.
T	Período de amostragem (em s).
k	Número de ciclos de amostragem (0,1,2,3...).
$\hat{y}(k)$	Resposta da função estimada do BSA
$y(k).$	Resposta da planta de controle
$f_{p,j}$	Função aptidão ou objetivo
p_j	Coordenada de um individuo da população do BSA
$s(k)$	Amostra de dados
S	Sequência de amostras de dados
W_{fw}	Palavra de ataque do *loop* de controle
W_{fb}	Palavra de ataque do *feedback*
$N(t)$	Variação de velocidade de rotação do eixo
$Q(t)$	Variação de torque no eixo
$\phi(s)$	Ajuste de passo do hélice
$f(s)$	Variação do fluxo de combustível
$\boldsymbol{G(s)}$	Matriz que descreve a FTMA da planta propulsiva
$g_{11}(s), g_{12}(s),$ $g_{21}(s)\ e\ g_{22}(s)$	Funções de Transferência da planta propulsiva
$k_1(z), k_2(z)\ e\ k(z)$	Compensadores da planta propulsiva
ω	frequência de oscilação amortecida
f_s	Taxa de amostragem ideal para Sistema digital
$r_1(s)$	*Set point* do torque do eixo
$R_1(s)$	*Set point* de velocidade do eixo
N(t)	Resposta da FTMF
$\hat{n}(k)$	Resposta da FTMF à palavra de ataque W
$n(k)$	Curva objetivo da função aptidão

SUMÁRIO

1 INTRODUÇÃO

Cyber-physical systems (CPS)[1] é o ambiente necessário para promover a integração de computadores digitais e plantas físicas. A tecnologia atual permite que através da comunicação entre atuadores, sensores, protocolos de rede e unidades de processamento de dados, possa-se construir uma sofisticada infraestrutura capaz de realizar o controle e automação de processos que se tornam cada vez mais complexos (Kessler e Shepard, 2022).

Monitoramento médico, veículos autônomos e plantas industriais são alguns dos exemplos das mais diversas aplicações destes sistemas de controle digitais e, como fica evidente, as soluções apresentadas por esses recursos estão presentes em sistemas cada vez mais críticos e essenciais para a sociedade. Com isso, pode-se observar que o panorama industrial mudou rapidamente ao longo das últimas décadas, como resultado do processo de digitalização e de outros avanços tecnológicos, consequência direta da concomitante evolução da engenharia computacional e das telecomunicações desde a década de 1950 (Kessler e Shepard, 2022).

Com a introdução da microeletrônica e desenvolvimento dos computadores pessoais, a partir da década de 1970, a digitalização tornou-se mais presente no dia a dia da indústria e da sociedade. Um simples exemplo, presente no dia a dia, são os celulares, que passaram a ser dispositivos que não só permitem a comunicação entre pessoas, mas também outras atividades integradas como tirar fotos, realizar transações bancárias, bem como controlar e automatizar outros dispositivos eletrônicos em casa (Kessler e Shepard, 2022).

A implementação dos protocolos de rede, obtenção de dados em tempo real e disseminação da internet proporcionaram a indústria uma maior integração vertical, entre os dispositivos pessoais presentes nos escritórios, até os níveis das máquinas e operadores, no chão de fábrica, melhorando os processos de tomada de decisão e otimizando as etapas do ciclo de produção (Ferrari *et al.*, 2020). O *Ethernet*[2], como é conhecido o principal protocolo de redes de informação, tornou-se amplamente utilizado em redes domésticas ou empresariais, permitindo que diversos dispositivos se comuniquem e tenham acesso compartilhado aos dados e recursos físicos disponíveis (Peschle, 2006).

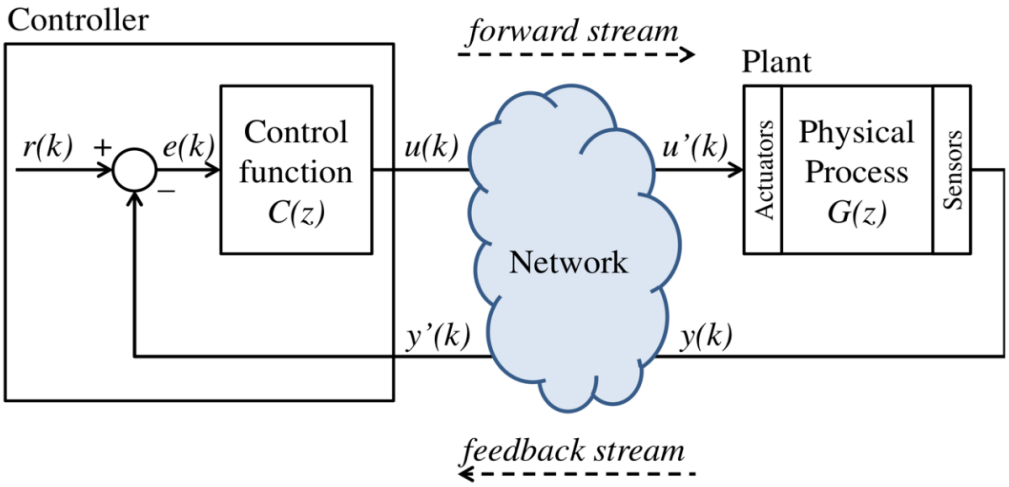
Essa constante associação dos processos físicos e digitais tem se tornando cada vez mais comum na chamada Industria 4.0, que faz alusão a Quarta Revolução Industrial. Esta nova era

[1] *Cyber-physical systems* (CPS), termo em inglês para Sistemas que realizam a interação entre o ambiente do domínio físico e cibernético.

[2] *Ethernet*, protocolo que define a estrutura de redes para a tecnologia de redes de computadores.

da indústria busca permitir a conexão entre plantas industriais, controladores e sensores, a uma estrutura de tecnologia de informação e comunicação (ICT)[3] sem precedentes, seja através de redes locais (LAN)[4], ou por meio da internet e redes de longa distância (WAN)[5].

FIGURA 1.1 – Networked Control System (NCS)



Fonte: Ferrari *et al.*, 2020.

O aumento constante da implementação de avanços tecnológicos na indústria, em especial no setor de telecomunicações, com o uso de conexões sem fio, como o Wi-Fi, e o desenvolvimento da conexão 5G, é uma tendência evidente. Como resultado, os sistemas de controle em rede (NCS)[6] estão passando por atualizações contínuas, à medida que a chamada Internet das Coisas (IoT)[7] se torna parte da realidade industrial. A IoT representa a infraestrutura que possibilita o controle e gerenciamento de processos físicos por meio de dispositivos digitais (Wollschlaeger *et al.*, 2017).

Tudo indica que, a integração entre as redes 5G e os protocolos de informação já existentes, como o Ethernet, podem trazer mais mudanças a essa estrutura de forma a permitir uma maior aplicabilidade desses recursos na Industria IoT (IIoT)[8]. Essas mudanças tecnológicas estão moldando a forma como a indústria está passando a operar, o que torna automação e conectividade uma parte essencial de seus processos e sistemas de controle, com busca a uma maior eficiência e produtividade (Wollschlaeger *et al.*, 2017).

---

[3] Do inglês, *Information and Communication Technology.*
[4] Do inglês, *Local Area Network*.
[5] Do inglês, *Wide Area Network.*
[6] Do inglês, Networked Control Systems.
[7] Do inglês, *Internet of Things*, o termo coisas (*Things*) representa os dispositivos do domínio físico que podem ser remotamente controlados, através de algum tipo de conexão de rede, por outros dispositivos eletrônicos.
[8] Do inglês, Industrial Internet of Things.

Desta forma, os novos aspectos tecnológicos das soluções de sistema de controle e automação, introduzem diversas possibilidades futuras de integração e melhorias das operações industriais. Com isso, possibilita-se o aumento do fluxo de dados entre os processos físicos e as unidades de processamento responsáveis por seu controle.

No início dos anos 2000, com aumento na demanda industrial por redes com maior capacidade de processamento, foram apresentadas soluções técnicas que permitiram o incremento dos protocolos de redes utilizados até então. O RTE (Real-Time Ethernet)[9] trouxe benefícios como aumento da capacidade de transmissão de dados, taxas de amostragem menores e mais precisas, além de ser pautado em protocolos tradicionais, já utilizados em tecnologia de informação (Lagouvardou, 2018).

Entretanto, surfando nos ganhos operacionais com a indústria 4.0 e prezando pela continuidade da produção, sem tempo para *upgrades* e atualizações, a segurança das redes foi colocada em segundo plano. Estes fatos, por consequência, acabaram por expor de maneira sem precedentes todos esses sistemas críticos envolvidos, tornando-os cada vez mais vulneráveis a ataques cibernéticos. Processos que antes estavam protegidos, por estarem isolados das ameaças presentes no domínio cibernético, agora tornaram-se integrados. Portanto, apesar de todos os aspectos positivos que a integração das conexões IT/OT[10] podem trazer, há de se voltar os olhos para a importância de se desenvolver mecanismos que possam incrementar a segurança destes sistemas (Ferrari *et al.*, 2020).

1.1 Apresentação do Problema

A complexidade do Sistema de Transporte Marítimo (MTS)[11] é proporcional a sua relevância no cenário global. Na estrutura do MTS está envolvida a interconexão de vários outros setores, o que o faz se comportar como um sistema de sistema (SoS)[12], que pode ser composto pelos mais diversos subsistemas dependendo de sua área de atuação, como: embarcações, empresas de transporte marítimo, portos, transportes intermodais, logística e

[9] ***Real-Time Ethernet*:** Estende os princípios do protocolo *Ethernet* tradicional para possibilitar suportar comunicações em tempo real. Tecnologia amplamente utilizada para conectar dispositivos em uma rede local, facilmente integrável a plantas de automação industrial.

[10] Do inglês, ***Informational Technology* (IT) *e Operational Technology* (OT)**, o termo IT representa as tecnologias que processam informação, que compreende hardware, software e redes dos sistemas de computação em geral. Por outro lado, enquanto o OT se refere a tecnologia do campo operacional, que é utilizado para monitorar e controlar processos físicos industriais.

[11] Do inglês, *Maritime Transport System*.

[12] Do inglês, *System of a System*.

manutenção, passageiros. Outrossim, ambiente marítimo é compartilhado com diversos outros elementos, entre eles: Navios de guerra, patrulhamento costeiro, segurança publica, barcos pesqueiros, veleiros e embarcações de recreio.

Notavelmente, parte da sociedade não tem a correta dimensão da importância do MTS para a Força marítima e economia de uma nação. A nível global, aproximadamente 90% das transações comerciais fluem pelos mares, são cerca de 90,000 navios responsáveis por transporte de carga e passageiros, que levam de um ponto a outro mais de 19 trilhões de dólares de carga por ano (Kessler e Shepard, 2022). Estes números demonstram o quanto o domínio marítimo é relevante para economia global, e reafirmam a importância de se buscar operar com o foco voltado para a produtividade, de maneira cada vez mais eficiente e segura.

Após a metade do último século, acompanhando o desenvolvimento de boa parte dos sistemas de controle e automação na indústria, navios de carga e passageiros passaram por um profundo processo de digitalização. A complexidade envolvida nas suas operações passou por avanços tecnológicos significativos, com incrementos consideráveis na execução das suas tarefas, proporcionando maior segurança e produtividade (Lagouvardou, 2018).

Conforme as unidades de processamento se tornaram pequenas o suficiente para serem incorporadas nas embarcações, mecanismos de controle e automação foram implementados para auxiliar a tripulação na operação e monitoramento dos mais diversos sistemas de bordo. Isso inclui, por exemplo: sistema de navegação, sistema de propulsão, sistema de geração de energia, sistema de armas, sistema de carga (Lagouvardou, 2018).

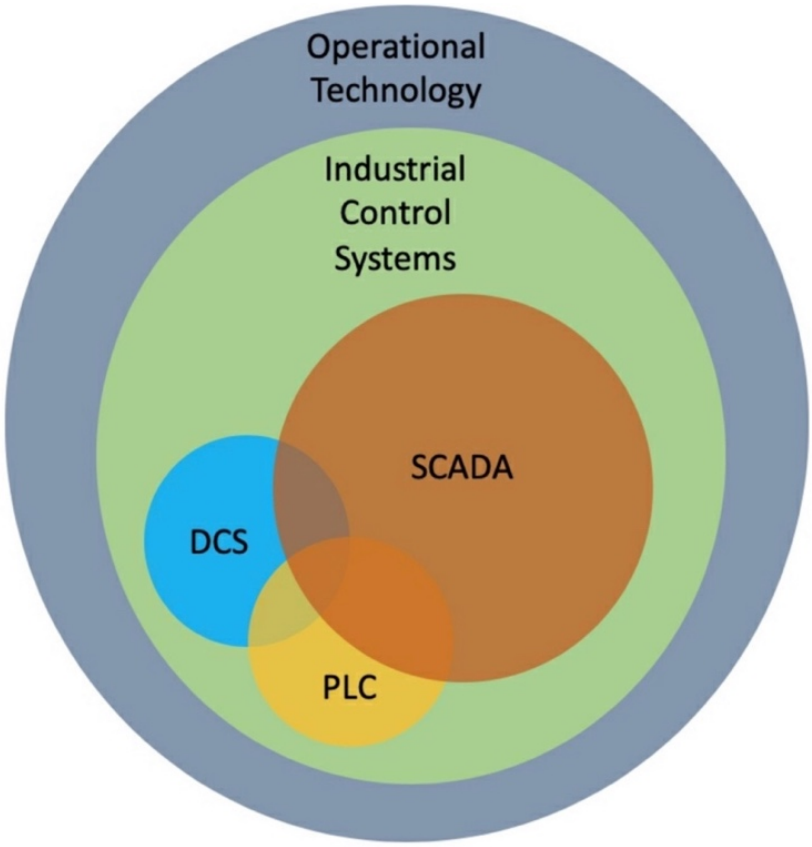
Como era esperado, bem como nas plantas industriais, observou-se um grande incremento em confiabilidade na operação de processos críticos em navios. Isso resultou em ganhos consideráveis de eficiência, levando a redução substancial da necessidade de quantitativo de pessoal a bordo e à manutenção de níveis precisos na execução e verificação dos processos, algo que não pode ser alcançado apenas com a intervenção humana (Kessler e Shepard, 2022).

Sistemas de Controle Industrial (ICS), Controlador Lógico Programável (PLC) e Sistemas de Controle Distribuídos (DCS)[13] são termos amplamente utilizados na Industria 4.0. Através dessas novas definições, estão comprimidos diversos recursos que estão presentes nos sistemas OT, como pode-se observar na Figura 1.2. Dentro desta estrutura, os ICS podem promover o controle em tempo real, de vários equipamentos, tais como: bombas, válvulas,

[13] Do inglês, *Industrial Control System (ICS), Programmable Logical Controller (PLC), Distributed Control System (DCS).*

motores, geradores, disjuntores, e diversos outros atuadores e dispositivos mecânicos, elétricos, hidráulicos, além do monitoramento de diversos parâmetros, através de sensores de temperatura, pressão, humidade, movimento (Kessler e Shepard, 2022).

FIGURA 1.2 – Classificação dos dispositivos OT.



Fonte: Kessler e Shepard, 2022.

O *Supervisory Control and Data Acquisition system (SCADA System),* presente nas mais diversas plantas industriais, é utilizado para operar e monitorar infraestruturas complexas. O SCADA permite o gerenciamento dos processos, funcionando como uma estrutura central para operar subsistemas e protocolos. O sistema permite o fluxo de dados entre o *Mainframe*[14], passando pelos processamentos distribuídos dos DCS, que comportam diversos PLC em sua estrutura, que podem executar diversas tarefas independentes, até chegar aos vários dispositivos que atuam nas plantas físicas (Parcharidis, 2018).

A abordagem de segurança cibernética apresentada pela indústria naval, por um longo período, seguiu o que era conhecido na indústria como *air gap,* pois seus sistemas críticos encontravam-se isolados fisicamente das ameaças do domínio cibernético. Com a crescente

[14] *Mainframe:* Unidade de processamento que centraliza o fluxo de dados.

evolução do processo de digitalização e aumento da conectividade nas infraestruturas marítimas, os navios também passaram a ser um conglomerado de sistemas críticos, interconectados por computadores e protocolos de rede (Kessler e Shepard, 2022).

Desta forma, com a incorporação de NCS e redes IoT presentes na indústria, os sistemas navais passaram a ter aberturas para ameaças cibernéticas, por razões semelhantes aos sistemas IT/OT. Adicionalmente, um fator que torna um sistema OT embarcado um caso excepcional, é que qualquer ameaça pode vir a infligir danos físicos aos equipamentos, podendo gerar risco a integridade física da tripulação, prejudicar a operação, causar danos permanentes aos sistemas integrantes, além de outros possíveis danos externos a estrutura (Lagouvardou, 2018).

Nesse contexto, a simbiose existente entre os sistemas voltados para Tecnologia Operacional e as estruturas de protocolos de rede inicialmente voltadas para Tecnologia da Informação, impulsionada pelas vantagens de se utilizar uma infraestrutura de rede já existente e mais econômica, trouxe consigo algumas deficiências na capacidade de resposta a ameaças cibernética. Como, por exemplo, ferramentas inadequadas de autenticação e poucos mecanismos de criptografia. Através dessa exposição, a implementação de sistemas OT marítimos enfrenta riscos potenciais de segurança semelhantes ao de qualquer computador ou sistema IoT, mas com o agravante de poder afetar plantas físicas de sistemas críticos de extrema importância (Kessler e Shepard, 2022).

A próxima geração de Soluções de Sistema de Controle e Automação terá pela frente inovações significativas. No entanto, o maior desafio que se apresenta é o monitoramento de ameaças cibernéticas, o que é evidenciado pelo crescimento de casos de ataques a plantas industriais nos últimos anos. Dessa forma, isso exigirá o desenvolvimento de novas estruturas e arquiteturas de sistemas que permitam a detecção de anomalias e invasões, com o objetivo de proteger os sistemas críticos envolvidos (Rosa *et al.*, 2021).

1.2 Justificativa e Relevância

Entre os dias 23 e 29 de março de 2021, o Navio Porta-Contêiner Ever Given ficou encalhado, bloqueando o Canal de Suez. Esta é uma das principais rotas marítimas do mundo, por onde passam cerca de 12% do comércio global (Ibrahim, 2021). Desastres como este ocorrem por uma variada gama de fatores, desde causas naturais até falhas humanas e dos equipamentos, mas as consequências, sejam de caráter econômico, ambiental ou político, podem se tornar globais.

Apesar de o cenário apresentado não ter sido comprovadamente fruto de algum tipo de ataque cibernético malicioso, as literaturas De Sá *et al.* (2017), Parcharidis (2018) e Ferrari *et al.* (2020), são capazes de demonstrar, através de simulações e modelos, que o domínio cibernético pode vir a ser uma porta para que sistemas sensíveis tornem-se um canal de possíveis ameaças. O *SCADA system*, por exemplo, que é amplamente utilizado em plantas industriais e navais, em sua geração mais atual, funciona estabelecendo exatamente esta relação entre sistemas IT/OT.

Nestes casos, quando se trata de sistemas críticos, qualquer manipulação de um atuador através de seus dispositivos controladores, pode vir a causar perda de eficiência relevante, ou até mesmo levar ao limite de funcionamento de determinado equipamento ou planta. Consequentemente, a depender do contexto em que estão inseridos, tem potencial para ocasionar situações de risco ou desastres ainda maiores, como o observado no caso do Ever Given.

Em 2017, a Organização Marítima Internacional (IMO)[15], percebendo o crescente emprego de sistemas computacionais nos mais diversos setores que englobam desde as embarcações até diversas outras infraestruturas marítimas, produziu o documento *Guidelines on Maritime Cyber Risk Management***,** onde destaca sua preocupação com as possíveis ameaças no ambiente marítimo e cibernético. A medida se deu, principalmente, por conta do crescente número de casos de ataques cibernéticos, sejam eles a plantas industriais que utilizam sistemas semelhantes, ou a plataformas navais, o que torna este assunto cada vez mais relevante e estratégico. A iniciativa se revelou como uma medida de estratégia global, posteriormente sendo acompanhado por nações com estimada relevância no cenário marítimo internacional, através do *National Maritime Cybersecurity Plan* (EUA, 2020) e do *Code of Practice: Cyber Security for Ships* (Reino Unido, 2017).

Nesse cenário, fica evidente a importância do tema abordado para o ambiente marítimo global, desde o contexto operacional das empresas, com possibilidades de ataques motivados por fatores financeiros ou sabotagens, até o ponto de vista estratégico, com ameaças ao comércio marítimo, danos ao meio ambiente e pirataria. Desta forma, o presente estudo busca demonstrar a considerável evolução tecnológica apresentada através da digitalização dos processos no campo de Sistemas de Controle e Automação, especialmente nas últimas décadas com a introdução da Industria 4.0. Além de associar a importância dessas soluções serem incorporadas a indústria naval, a fim de tornar as operações mais eficientes, sem perder de vista

[15] Do inglês, *International Maritime Organization*.

que todas essas evoluções tecnológicas no domínio cibernético podem trazer consigo vulnerabilidades de segurança cibernética.

1.3 Objetivos

Este trabalho de conclusão de curso tem como objetivo geral, diante do exponencial avanço tecnológico dos últimos anos, que promoveu o domínio cibernético a uma ferramenta de destaque na otimização de processos industriais, explorar as Soluções em Sistema de Controle e Automação com foco na indústria naval. Outrossim, analisar como os avanços proporcionados pela Industria 4.0, com a implementação dos sistemas digitais e protocolos de rede, promovem novos desafios, passando pela necessidade de se desenvolver uma maior mentalidade de segurança cibernética, ao se identificar as vulnerabilidades que estes sistemas apresentam.

Com o intuito de alcançar os resultados acima, seguir-se-á os objetivos específicos:

a) Apresentar as evoluções do sistema de controle e automação, com ênfase nos sistemas de controle digitais, além de trazer a adequação para aplicação destes sistemas, a realidade da Industria Naval atual, no monitoramento e automação dos processos executados em navios através de suas plantas de propulsão e geração de energia.

b) Com a evolução da conectividade e integração dos processos, através da indústria 4.0, por meio da implementação das linguagens de programação e protocolo de redes, expor os ganhos adquiridos com as novas tecnologias em termos de conectividade que propiciam uma melhor automação dos processos críticos e verticalização das plantas industriais aos escritórios.

c) Apresentar um dos principais sistema de controle distribuídos em rede, o SCADA *system*, utilizado na Industria e em Navios, com uma breve descrição técnica e possibilidades de integração com protocolos de rede, a fim de expor suas vulnerabilidades a ameaças cibernéticas. Adicionalmente, apresentar como estudo de caso, um ataque cibernético real: o caso “Stuxnet”, que é um dos precursores nos estudos de mentalidade de segurança cibernética na indústria.

d) Apresentar descrever e analisar as simulações, através do MATLAB, de como um ataque furtivo a uma malha de controle de uma planta propulsiva, com pequenas alterações em seus pacotes de dados, pode ocasionar danos críticos aos processos executados, reduzindo eficiência ou até mesmo impedindo o cumprimento do objetivo.

e) Discutir soluções de forma a mitigar as vulnerabilidades dos Sistemas de Controle e Automação de Navios, desde o implemento da mentalidade de Segurança Cibernética até o desenvolvimento de algoritmos capazes de identificar e neutralizar os ataques.

1.3.1 Tema

A pesquisa tem enfoque nas Soluções de Sistema de Controle e Automação para navios, compreendendo os avanços tecnológicos da indústria e desafios em segurança cibernética.

1.3.2 Delimitação do Tema

São apresentadas Soluções em Sistemas de Controle Digitais voltados para o Monitoramento e Automação de sistemas críticos, como os presentes em Sistemas de Propulsão e Geração de Energia de Navios. Será dado ênfase na evolução da indústria 4.0, permitindo maior conectividade e integração nas mais variadas gamas de processos industriais, através dos protocolos de rede e linguagens de programação. Outrossim, descrever as vulnerabilidades a ameaças cibernéticas, as quais essas plantas passam a ser expostas, através de ataques furtivos a seus processos de controle, passando pela Industria, até chegar nos meios navais.

1.4 Etapas do Trabalho

O presente Trabalho de Conclusão de Curso encontra-se estruturado conforme descrito a seguir:

O capítulo 1, INTRODUÇÃO, tem o intuito de apresentar o problema abordado, sua justificativa e contextualizar o assunto a ser tratado, além de expor os objetivos da pesquisa cientifica delineada.

O capítulo 2, REFERENCIAL TEÓRICO, promove a compreensão de assuntos considerados essenciais para o entendimento do trabalho. Sendo apresentados, primeiramente, a evolução dos Sistemas de Controle e Automação, elementos para modelagem e análise da performance de um sistema, culminando nos sistemas digitais. Por fim, aborda-se os elementos básicos de Protocolos de rede e suas vulnerabilidades a ameaças cibernéticas.

O capítulo 3, METODOLOGIA DE PESQUISA, apresenta a classificação da pesquisa, quanto aos fins e quanto aos meios, além de dissertar sobre os métodos para coleta de dados e suas limitações.

O capítulo 4, ANÁLISE DAS VULNERABILIDADES DE SISTEMAS DE CONTROLE, apresenta uma análise técnica das vulnerabilidades do SCADA system, com base em manuais, artigos e estudos, além de um estudo de caso sobre o ataque cibernético real conhecido como "*Stuxnet worm*".

O capítulo 5, SIMULAÇÃO DE ATAQUE CIBERNÉTICO A PLANTA PROPULSORA, descreve um ataque cibernético furtivo a um modelo de planta propulsora de sistema naval, além de analisar os resultados das simulações.

Por fim, o capítulo 6, CONCLUSÃO, completa o estudo realizado, apresentando as considerações finais, bem como as sugestões para trabalhos futuros.

2 REFERÊNCIAL TEÓRICO

Com o intuito de melhor desenvolver os objetivos mencionados neste trabalho, o presente capítulo busca realizar uma revisão de literatura, para promover um panorama conceitual dos principais tópicos necessários para compreensão das análises e discussões que virão nas seções a seguir. São apresentados os principais conceitos dos Sistemas de Controle e Automação, de maneira evolutiva, culminando nos Sistemas de controle digital, posteriormente, uma passagem pelos Protocolos de Rede que permitem que os NCS se comuniquem com os atuadores e sensores nas plantas industriais. Por fim, correlacionar os assuntos com as peculiaridades da Industria Naval, e com determinados aspectos dos avanços tecnológicos que podem estar expondo os sistemas a certas vulnerabilidades no domínio cibernético.

2.1 Sistema de Controle e Automação

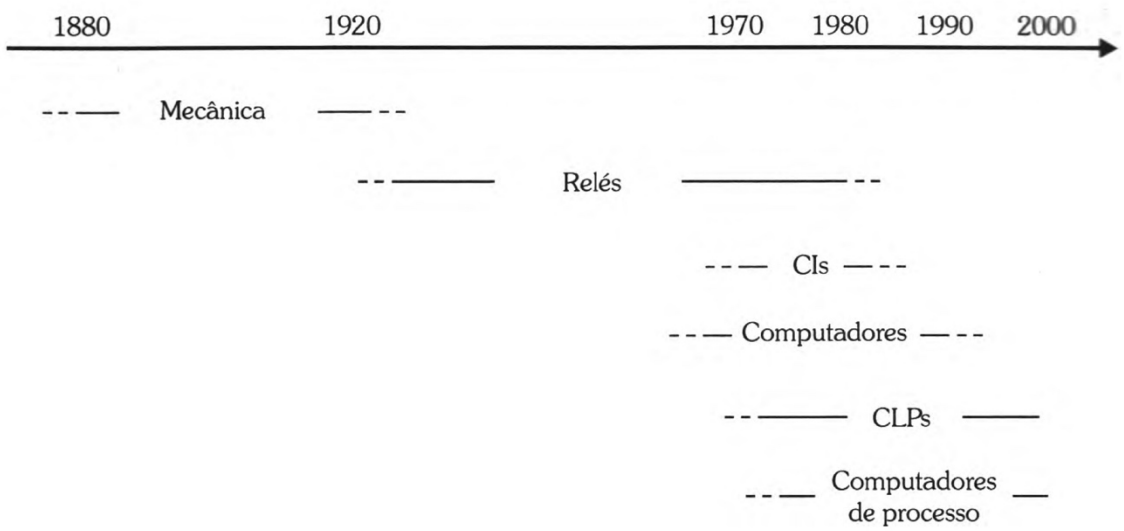
Historicamente, os sistemas de controle e automação desempenham um papel fundamental na indústria, sempre buscando impulsionar a eficiência, a produtividade e aprimoramento dos processos industriais. Seria inviável falar da evolução desses sistemas, sem mencionar os avanços tecnológicos das Revoluções Industriais, caracterizada pela substituição da produção manual e artesanal pela mecanização dos processos. Os processos de controle e automação, inicialmente se dariam a partir das máquinas a vapor[16] (Primeira Revolução Industrial), atuando ainda de maneira mecânica. Posteriormente, passando por avanços tecnológicos significativos de engenharia como a eletrificação, que permitiria vários incrementos de controle com a lógica de relés e circuitos integrados (Segunda Revolução Industrial). Até, por fim, culminar na introdução das tecnologias de informação e da computação, por ocasião da Revolução Digital (Terceira Revolução Industrial) (Franchi e Camargo, 2008).

Como citado, as soluções de sistemas de controle e automação evoluíram concomitantemente com os avanços das Revoluções Industriais. À medida que as tecnologias se desenvolviam, permitindo que os dispositivos de controles evoluíssem, as demandas da indústria por processos de controle mais precisos, complexos e eficazes tornavam-se realidade.

[16] O regulador centrifugo, de James Watt, foi um dos primeiros trabalhos significativos de controle, que permitia realizar o controle de velocidade de uma máquina a vapor, ainda no século XVIII (Ogata, 2010).

Os primeiros sistemas, ainda no final do século XIX, eram manipulados por dispositivos meramente mecânicos, que detinham a capacidade de desempenhar tarefas repetitivas e foram muito utilizados nas linhas de montagem que se estabeleciam na época (Franchi e Camargo, 2008).

FIGURA 2.1 – Linha do tempo da evolução Sistemas de Controle



Fonte: Franchi e Camargo, 2008.

A partir da década de 1920, com o avanço da engenharia elétrica, incorporando dispositivos como relés[17] e contatoras, houve um progresso significativo no desenvolvimento de funções lógicas cada mais elaboradas. Como exemplo, os servomecanismos a relé, capazes de monitorar as entradas nas plantas e atuadores com maior precisão. Além de, métodos que possibilitaram o projeto de sistemas lineares de malha fechada, permitindo uma observação mais precisa das respostas dos sistemas por meio de *feedbacks* dos sensores. Neste contexto, ocorreram várias mudanças substanciais que se encontram presentes em boa parte da indústria até os dias de hoje. Mais adiante, no início de 1940, Ziegler e Nichols desenvolveram regras que vieram a permitir a sintonização de controladores PID[18] (Ogata, 2010).

A partir de 1960, com o surgimento da Revolução Digital, as até então predominantes lógicas baseadas em relés, compostas por circuitos integrados, passaram a ser complementadas

[17] Uma das vantagens da utilização de relés é que, através de suas bobinas, permitem que circuitos controlados com níveis de tensão e corrente elevados, possam ser acionados por uma corrente e muito pequena. Enquanto as contatoras são normalmente utilizadas para cargas de alta potência (Lamb, 2015).

[18] Controladores Proporcional-integral-derivativo (PID) são compensadores que podem atuar no sistema permitindo ações de controle, podem ser formados por combinações de um circuito elétrico integrado ou através de logica de programação em um sistema digital (Nise, 2020)

ou substituídas por computadores, marcando mais um avanço significativo nos sistemas de controle. Através da linguagem de programação, possibilitou-se a análise de sistemas cada vez mais complexos, com múltiplas entradas e saídas, e seus cada vez mais críticos processos, com aplicação em diversos setores da indústria que estavam em pleno desenvolvimento na época: como no setor espacial, militar, e não obstante, nas embarcações e infraestruturas marítimas (Ogata, 2010).

Os sistemas de controle digitais, com ferramentas como o Controle Lógico Programável (PLC)[19], foram desenvolvidos a partir da necessidade de atender a indústria em processos cada vez mais críticos e mutáveis. Sua implementação permitiu a constante programação e reprogramação das plantas nas linhas de montagem, aumento da confiabilidade, redução das dimensões, interfaces cada vez mais integradas aos operadores, além da possibilidade de integração de banco de dados (Franchi e Camargo, 2008).

Desta forma, os sistemas de controles modernos tornaram-se cada vez mais robustos, com mais dispositivos, atuadores e sensores integrados, modelando sistemas suscetíveis a distúrbios ou mudanças de suas variáveis internas. A Teoria de controle moderno foi se adaptando a estas novas demandas da indústria, e mais uma vez, aproveitando-se dos recursos tecnológicos atuais, como a grande capacidade de processamento dos computadores e conectividade cada vez mais rápidas (Ogata, 2010).

2.1.1 Configurações de Sistemas de Controle

Para compreensão dos tópicos que serão abordados a seguir, faz-se necessário um certo nivelamento de conhecimento no que diz respeito a certas definições e propriedades de Sistema de Controle e Automação. Com isso, primeiramente irá se discutir as duas principais configurações de arquiteturas de sistemas de controle: malha aberta e malha fechada*,* através de diagrama de blocos[20] que descrevam sua estrutura.

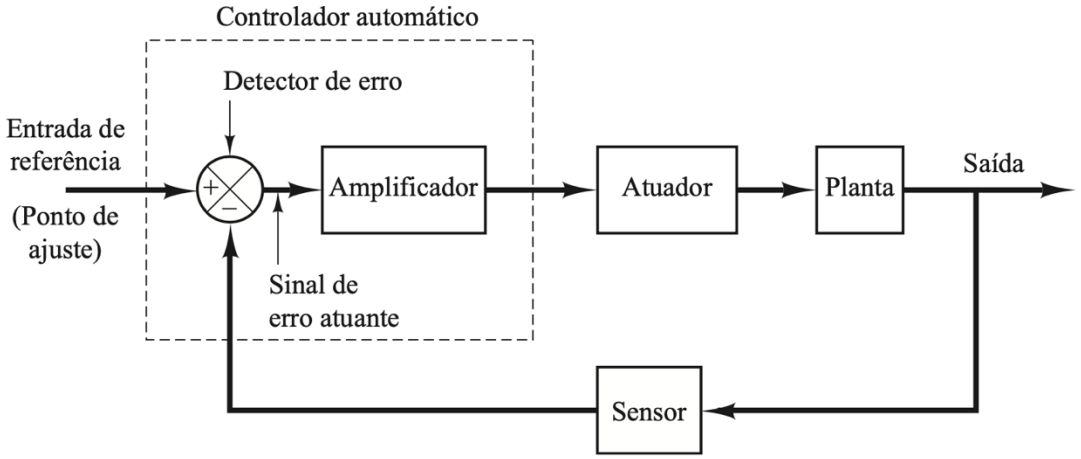
Os sistemas de controle de malha aberta são aqueles que o sinal de saída não realimenta o comando de entrada com nenhuma informação, ou seja, não possui sensores ou medidores coletando os dados da planta para efeito de comparação. Desta forma, como a saída não é

[19] O PLC, através de seus microprocessadores, utiliza uma memória programável para armazenar as funções lógicas que antes eram construídas fisicamente nos circuitos (Lamb, 2015).

[20] Diagrama de blocos é a representação gráfica de um sistema, com as funções desempenhadas por cada componente e linhas de fluxos entre eles. Com isso, o bloco é a operação matemática que é aplicada a sua entrada, que produz posteriormente um sinal de saída (Ogata, 2010).

comparada ao sinal de entrada, cada entrada de referência corresponde a uma operação pré-definida na resposta, sem correções a qualquer distúrbio que possa afetar o processo. Um exemplo deste tipo de controle são aqueles baseados em temporizadores, que executam tarefas em uma sequência de tempo (Ogata, 2010).

FIGURA 2.2 – Modelo de sistema de controle industrial de malha fechada.



Fonte: Ogata, 2010.

Já nos sistemas que possuem o *feedback*[21], que são os sistemas de malha fechada, o sinal de erro atuante, que é a diferença do sinal de entrada de referência e do sinal de realimentação, como pode-se observar na Figura 2.2, serve de alimentação para o controlador, de modo a procurar sempre corrigir o erro presente na saída. Com isso, sistemas de controles realimentados são muito úteis para plantas que estejam suscetíveis a distúrbios, pois permitem que sejam verificados e corrigidos os erros na resposta, atualizando as informações da sua entrada. As vantagens e desvantagens de cada um deles irá depender dos objetivos que irão determinar a configuração da planta, caso seja uma operação que tolere erros ou não sofra com distúrbios ao longo do processo, a malha aberta mesmo que mais simples, pode ser uma opção menos custosa (Ogata, 2010).

2.1.2 Modelagem e análise do comportamento de um sistema

Nesta seção, conforme apresentado pelas literaturas Nise (2019) e Ogata (2010), serão estabelecidos uma sequência de procedimentos para se realizar a modelagem e análise do

[21] *Feedback*: termo em inglês para sinais de realimentação em sistemas de controle de malha fechada.

controle de uma planta, realizados por um sistema de controle de malha fechada. Para tal, serão definidos alguns passos a serem seguidos, desde as determinações das especificações físicas e requisitos de resposta da planta, até sua modelagem e testes de desempenho.

i. **Descrição do sistema físico e seus principais requisitos:** Compreende a identificação dos principais componentes do sistema, bem como das suas interações físicas. Por exemplo, o potenciômetro que aciona um motor de indução produzindo um aumento ou redução de velocidade na sua rotação. Pode-se observar uma componente de entrada atribuindo um ângulo θ, e no outra ponto a saída de uma velocidade angular ω no eixo do rotor. Desta forma, é um processo de observação preliminar dos elementos que interagem entre si, além disso, permite-se verificar o comportamento das respostas transitórias e em regime permanente, ainda que superficialmente, com base nos requisitos de um sistema de controle para determinada planta.

ii. **Transformar sistemas físicos em uma representação esquemática:** Os sistemas de controle consistem em uma combinação de componentes elétricos, mecânicos, fluídicos e térmicos, que tornam sua análise de caráter multidisciplinar. Neste contexto, consiste em melhor descrever os fenômenos que ocorrem em cada uma dessas interações, como as forças que agem sobre um bloco ou os elementos que interagem em um circuito elétrico, através das leis da física que regem o comportamento do sistema físico. O engenheiro responsável realizará aproximações adequadas aos objetivos do sistema para facilitar que se extraia, nas próximas fases, equações matemáticas que permitam modelar a sua execução.

iii. **Desenvolver um modelo matemático:** De posse das representações esquemáticas, utilizam-se as leis da física, tais como as Leis de Newton, para sistemas mecânicos e as Leis de Kirchoff, para circuitos elétricos, para elaborar as equações que descrevem o sistema dinâmico. Com isso, podem ser realizadas simplificações ou suposições matemáticas que reduzam a complexidade do modelo observado, sem comprometer os requisitos do sistema.

Sem algumas dessas simplificações, o modelo matemático poderia vir a ter equações diferenciais de uma ordem maior ou até mesmo não ser linear, e consequentemente dificultaria a modelagem do sistema, bem como sua análise de seu comportamento.

Como a análise de sistemas dinâmicos pode apresentar equações diferenciais com alto grau de complexidade. A transformada de Laplace, para sistemas lineares invariantes no tempo[22], pode ser utilizada para descrever um sistema em equações algébricas mais fáceis de se resolver. Conforme definido nas equações abaixo.

[22] Sistemas lineares são aqueles que obedecem ao princípio da superposição, onde a resposta produzida por duas funções aplicadas simultaneamente é a soma das suas respostas individuais. Enquanto, os sistemas invariantes no tempo são em que todos os coeficientes das equações são constantes, e não se alteram em função do tempo.

$$\mathcal{L}[\,f(t)\,] = F(s) = \int_{0-}^{\infty} f(t)e^{-st}dt\,, \tag{2.1}$$

$$s = \sigma + j\omega \text{ (domínio da frequência).} \tag{2.2}$$

A ideia fundamental por trás da **transformada de Laplace**[23] é converter uma função no domínio do tempo, em uma função de variável complexa, no domínio da frequência. Com isso, transforma operações com equações diferenciais em multiplicações simples, além de se permitir inferir características do sistema de forma mais objetiva.

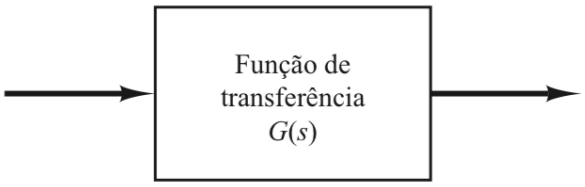
A partir do modelo matemático, aplicando-se a transformada de Laplace, pode-se isolar os termos matemáticos de entrada e saída do sistema, conforme apresentado na equação 2.3.

$$\text{Função de transferência} = G(s) = \frac{\mathcal{L}[saida]}{\mathcal{L}[entrada]} \tag{2.3}$$

$$G(s) = \frac{b_0 s^m + b_1 s^{m-1} + \cdots + b_{m-1} s + b_m}{a_0 s^n + a_1 s^{n-1} + \cdots + a_{n-1} s + a_n}. \tag{2.4}$$

A razão de polinômios no domínio de Laplace, onde o numerador representa a saída e o denominador a entrada, é denominada **Função de Transferência**[24], ilustrada na Figura 2.3.

FIGURA 2.3 – Função de transferência.



Fonte: Ogata, 2010

Outro modelo de representação, para sistemas que apresentem mais variáveis de entrada e saída, ou que não possam ser simplificados, é o **espaço de estados**[25]. Este método tem a vantagem de se permitir descrever sistemas com equações características de ordem maiores, ou que não podem ser modelados com equações diferenciais lineares invariáveis no tempo. Com

[23] No **Apêndice A** pode ser observado as principais propriedades das Transformadas de Laplace, bem como uma tabela com suas transformadas mais utilizadas.

[24] No **Apêndice B** pode ser observado as principais Funções de Transferência que descrevem componentes de sistemas mecânicos e elétricos.

[25] Equações no espaço de estados utiliza da representação matricial para modelar equações diferenciais de qualquer ordem, além de sistemas não-lineares, sistemas com múltiplas entradas e múltiplas saídas (Ogata, 2010).

isso, utiliza-se de matrizes e vetores, que podem ser mais facilmente empregado com o uso de processamento digital. Segundo Powell *et al.* (1998), a forma de estados permite que uma equação diferencial de qualquer ordem possa vir a ser representada por algumas equações de primeira ordem, conforme pode-se ver abaixo:

$$\dot{\boldsymbol{x}} = \boldsymbol{F}\boldsymbol{x} + \boldsymbol{G}\boldsymbol{u}\,, \tag{2.5}$$

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{J}\boldsymbol{u}\,. \tag{2.6}$$

Nas equações, o vetor **x** representa o vetor de estados do sistema e contém n elementos em sua coluna, que correspondem as n ordens do sistema de equações diferenciais e **u** é a entrada do sistema.

Para exemplificar, observa-se abaixo uma equação diferencial de segunda ordem, que pode ser descrita em variáveis de estado, conforme nas equações:

$$\ddot{y} + 2\zeta\omega_n\dot{y} + \omega_n^2 y = k_0 u\,. \tag{2.7}$$

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\end{bmatrix} = \begin{bmatrix}0 & 1\\ -\omega_n^2 & -2\zeta\omega_n\end{bmatrix}\begin{bmatrix}x_1\\ x_2\end{bmatrix} + \begin{bmatrix}0\\ k_0\end{bmatrix}u\,, \tag{2.8}$$

$$\boldsymbol{y} = [1 \quad 0]\begin{bmatrix}x_1\\ x_2\end{bmatrix}. \tag{2.9}$$

O estado, representado pelo vetor **x**, é um conjunto de variáveis capazes de descrever o comportamento futuro de um sistema.

$$\boldsymbol{x} = \begin{bmatrix}x_1\\ x_2\end{bmatrix} = \begin{bmatrix}y\\ \dot{y}\end{bmatrix}. \tag{2.10}$$

À medida que os sistemas de controle vêm se tornando cada vez mais complexos, saindo de sistemas com uma entrada e uma saída (SISO), para sistemas com múltiplas entradas e múltiplas saídas (MIMO)[26], as descrições de sistemas modernos vem requerendo um maior número de equações. Portanto, as soluções, como as variáveis de estado, que permitam uma melhor análise e síntese desses sistemas, vem se tornando cada vez mais utilizadas,

[26] Do inglês, *Single Input Single Output (SISO)* e *Multiple Input Multiple Output (MIMO).*

principalmente com a disponibilidade de computadores para facilitar o emprego desta ferramenta.

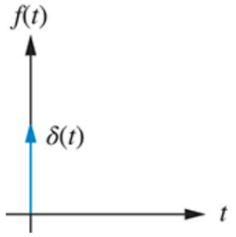
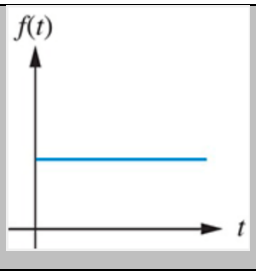
iv. **Simplificar o diagrama de blocos:** Em um sistema físico complexo, vários subsistemas são interconectados para representar seu comportamento, observa-se que vários processos ocorrem internamente a um sistema, entre sua entrada e sua saída, entretanto, para permitir que o sistema seja avaliado, faz-se necessário que ele seja simplificado a um único bloco, com apenas uma entrada e um saída.

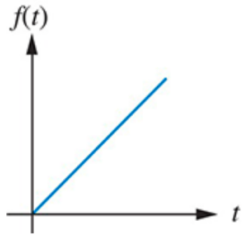
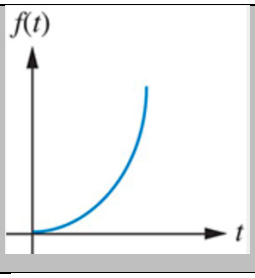
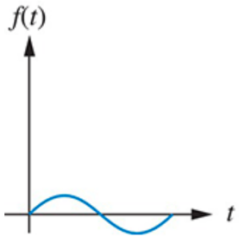
v. **Teste e análise das respostas do sistema:** Na última fase, serão realizados os testes e analises propriamente ditos, onde poderá se observar a performance do sistema como um todo, após ter sido reduzido a um único bloco de suas funções de transferência, ou identificar características de subsistemas. Caso as especificações requeridas inicialmente não possam vir a ser satisfatória, o *design* de controle do projeto pode ser alterado visando atender ao objetivo.

Segundo as principais literaturas, como Powell *et al.* (1998), Ogata (2010) e Nise (2020), os sinais de entrada de qualquer planta indústria, sobre ação de um sistema de controle, não são conhecidos, mas podem ser limitados. Com isso, os testes são realizados, em sua maioria, através de sinais de entrada que, sendo eles conhecidos, permitem a análise de maneira comparativa da resposta. Para tal, faz-se necessário a utilização de sinais padrões que não sejam de complexa avaliação, mas que possam oferecer observações relevantes do comportamento do sistema.

Na Tabela 2.1, pode-se observar alguns desses sinais que são utilizados e as observações que cada um deles permite que seja inferida.

TABELA 2.1 - Funções de entrada para avaliação de Sistemas de Controle

Entrada	Função	Descrição	Gráfico	Observação
Impulso	$\delta(t)$	$\delta(t) = \infty$ para $0^- < t < 0^+$. $\delta(t) = 0$ para os demais valores.		Resposta transitória; e Modelagem.
Degrau	u(t)	$u(t) = 1$ para $t > 0$. $u(t) = 0$ para $t < 0$.		Resposta transitória; e Erro em regime permanente.

Rampa	tu(t)	$tu(t) = t$ para t > 0. $tu(t) = 0$ para t < 0.		Erro em regime permanente.
Parábola	$\frac{1}{2}t^2u(t)$	$\frac{1}{2}t^2u(t) = \frac{1}{2}t^2$ para t > 0. $\frac{1}{2}t^2u(t) = 0$ para t < 0.		Erro em regime permanente.
Senoide	sin ωt			Resposta transitória; Modelagem; e Erro em regime permanente.

Fonte: Modificado de Nise (2019).

Pode-se dizer que existe uma relação direta entre o tipo de sinal de entrada e a informação que pode vir a ser adquirida na saída. Com isso, cada um dos sinais padrões permite uma interação com os diferentes tipos de sistema. Por exemplo, para a avaliação de um sistema de controle que varia gradualmente com o tempo, a função rampa pode vir a ser adequada. Enquanto para outros que variam bruscamente a qualquer sinal de entrada, a função degrau poderia ser mais eficiente como função de teste. Ou para sistemas que reagem a impactos, talvez a função impulso seja satisfatória (Ogata, 2010).

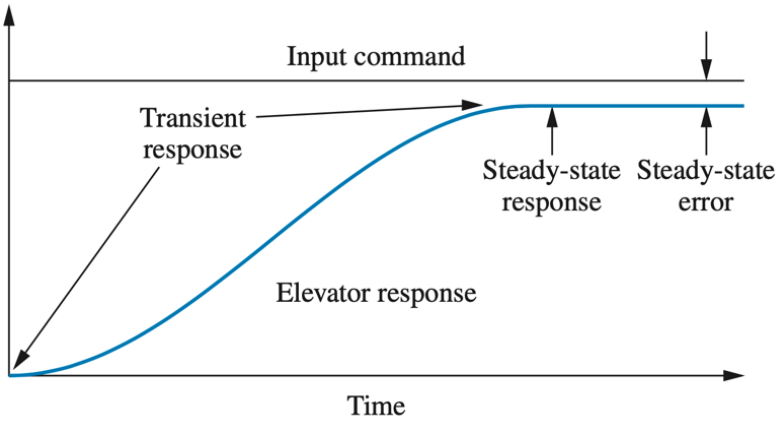
Desta forma, conclui-se que o processo de análise e *design* de um sistema de controle depende de uma observação minuciosa de toda a estrutura da planta a ser controlada, para que se possa atender as especificações e objetivos de respostas a serem alcançadas, permitindo que o sistema possa ser eficiente e seguro na sua operação. Além das observações que foram feitas acima, o sistema pode estar sujeito a flutuações de suas variáveis internas ou distúrbios que possam vir a alterar o seu comportamento. Com isso, as ações de controle devem atuar de forma a reduzir os erros gerados por essas oscilações, permitindo que sua performance permaneça dentro de limites aceitáveis. Na seção a seguir irá se discutir as principais considerações realizadas a partir das respostas dos Sistemas de Controle aos sinais padronizados.

2.1.3 Análise das respostas de um Sistema de Controle

Apesar de o projeto e *design* de um sistema de controle poder ser bem complexo, os passos introduzidos acima permitem que se possa realizar de maneira prática diversas simulações de comportamento, além de efetuar modificações e atualizações no sistema. Após uma minuciosa análise e modelagem da planta e seus requisitos, com a utilização de computadores e recursos como os *softwares* MATLAB ou SIMULINK[27], diversas técnicas de controle moderno, que serão abordadas superficialmente por não serem alvo deste trabalho, podem ser aplicadas, sempre buscando uma melhor performance.

Quando se trata de performance como um fator de avaliação da resposta de um sistema, introduz-se dois conceitos extremamente relevantes para uma análise: a resposta transitória (*Transient response*) e a resposta de regime estacionário (*Steady-state response*), como pode-se observar na Figura 2.4.

FIGURA 2.4 – Resposta transitória e de regime permanente.



Fonte: Nise, 2020.

Segundo Nise (2020), um sistema de controle é dinâmico, pois conforme observado, ao ser submetido a um sinal de entrada qualquer, seu comportamento passa por uma resposta transitória antes de atingir uma resposta de regime estacionário. Esta característica da resposta do sistema está relacionada com a descrição das soluções de equações diferenciais, que apresentam sua resposta como a soma de uma resposta forçada e uma resposta natural[28].

[27] São ferramentas que permitem que a partir da modelagem do sistema a ser analisado, seja através de funções de transferência ou variáveis de estados, possa-se realizar simulações, que possibilitem a identificação das principais características de resposta do sistema.

[28] Acordo as literaturas que dissertam sobre Cálculo, como Stewart (2014) e William (2015), resposta forçada pode ser conhecida como solução particular, enquanto a resposta natural como solução homogênea.

Portanto, os requisitos de operação de um sistema, como observado no primeiro passo da seção 2.1.2, passam por três objetivos principais: produzir uma resposta transitória conforme desejado, reduzir o erro de regime estacionário e alcançar a estabilidade.

As **respostas transitórias**[29] apresentam variadas características. Caso a resposta seja muito rápida pode acabar causando dano físico ao sistema, por outro lado se for muito lenta, pode não cumprir com os objetivos especificados. Por exemplo, um sistema controle de um elevador, caso seja muito rápido pode vir a oferecer risco para o passageiro, por outro lado, pode acabar se tornando menos eficaz do que se tivesse subido pelas escadas (Nise, 2020).

No caso de um motor de combustão ou turbina a gás, um ***overshooting***[30] pode vir a se tornar problema, causando dano ao material ou colocando em risco sua operação. Entretanto, para esses dois equipamentos, um bom tempo de resposta é fundamental para que atenda as demandas do seu utilizador. Desta forma, um sistema deve ser analisado pelas suas características de resposta existentes, comparando-as aos requisitos estabelecidos, com isso, caso necessário, pode ser realizado ajustes nos parâmetros de controle para se obter uma resposta mais eficaz (Nise, 2020).

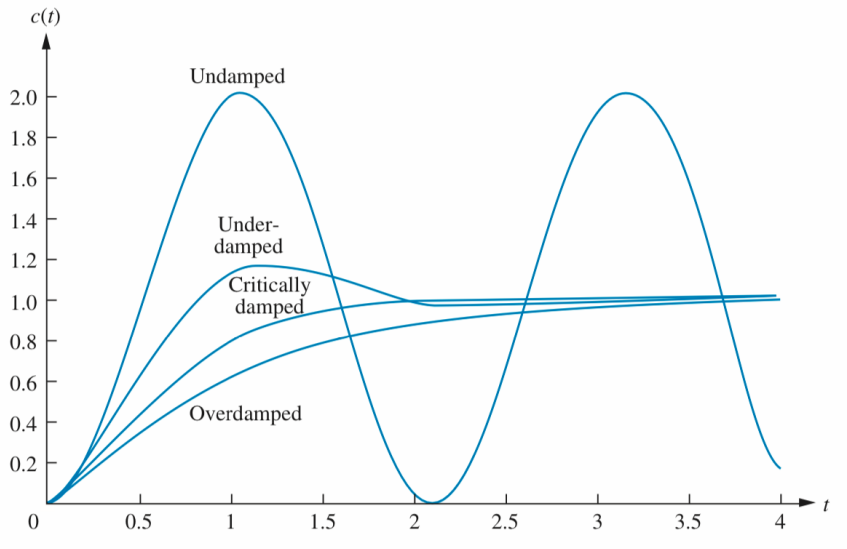
Outra análise pode ser realizada com foco na **resposta de regime estacionário**, neste caso, como pode-se observar na Figura 2.4, à medida que o tempo tende para infinito, prevalece o seu sinal de reposta em regime permanente, e o transitório tende para zero quando o sistema é estável. No caso do elevador, por exemplo, é crucial que esteja parado no andar correto de maneira que permita o passageiro efetuar o desembarque com segurança. Enquanto para o motor ou turbina a gás é importante que seja mantido um percentual erro satisfatório, em relação a sua rotação desejada, de forma que mais uma vez o seu utilizador possa cumprir com seus requisitos de operação (Nise, 2020).

Nesse contexto, na análise de um sistema de controle, é importante que sejam estudadas as respostas transitórias e de regime permanente, mas todos esses termos se tornam irrelevantes em caso de o sistema ser instável. Segundo Ogata (2010), um sistema possui estabilidade absoluta quando na ausência de qualquer distúrbio ou sinal de entrada, sua saída permanece inalterada, pode ser criticamente estável se possuir uma resposta puramente oscilatória e, por outro lado, instável quando a resposta diverge sem limites quando sujeito a uma entrada. Nenhuma das duas últimas situações seriam satisfatórias para um sistema de controle, uma vez

[29] No **Apêndice C** detalha-se mais as principais características de respostas em regime transiente.
[30] ***Overshooting****:* termo em inglês que define o pico de uma curva de resposta transitória.

que poderia vir a causar danos para sua estrutura física, como, por exemplo, o elevador oscilando permanentemente, ou o motor acelerando além de seu limite mecânico.

FIGURA 2.5 – Resposta ao degrau para sistemas de segunda ordem.[31]



Fonte: Nise, 2020.

As características, observadas na Figura 2.5, são alguns dos exemplos de dinâmicas que certos sistemas podem vir a ter no seu regime transitório, como vir a apresentar um certo grau de amortecimento ou comportamento puramente oscilatório. Muitas técnicas que não serão aprofundadas neste trabalho podem ser empregadas para se avaliar o comportamento das respostas, como a análise dos polos e zeros da transformada de Laplace[32], ou simulações com o auxílio gráfico de *softwares,* no caso de sistemas mais complexos.

Além disso, existem métodos de optimização para poder se obter melhoras de performance no regime transitório e no permanente, o primeiro deles através do ajuste do ganho, ou então uma modelagem do sistema de controle, com a adição de outros componentes e compensadores que tenham ações mais efetivas sobre a planta do sistema[33]. O desenvolvimento de projetos de compensadores pode ser feito de diversas maneiras, como pelo método de lugar das raízes, abordagens que permitam realizar uma sintonização de um PID, método de Ackerman (Ogata, 2010), entretanto essas abordagens não serão alvo de estudo deste trabalho.

---

[31] *Undamped, Underdamped, Critically damped* e *Overdamped:* termos em inglês que definem as respostas Oscilatórias, Sub amortecidas, Criticamente Amortecidas e Super Amortecidas, respectivamente.

[32] **Os polos e zeros** de uma função de transferência tem características similares aos de análises de equações diferenciais, enquanto os polos são as raízes da equação característica do denominador, os zeros, por sua vez, são as raízes do numerador. Juntos os polos e zeros podem trazer informações relevantes sobre o comportamento desta função de transferência no domínio do tempo.

[33] No **Apêndice D** encontra-se uma tabela com alguns dos principais compensadores industriais que atuam no controlador, em cascata com os atuadores e planta do sistema de controle.

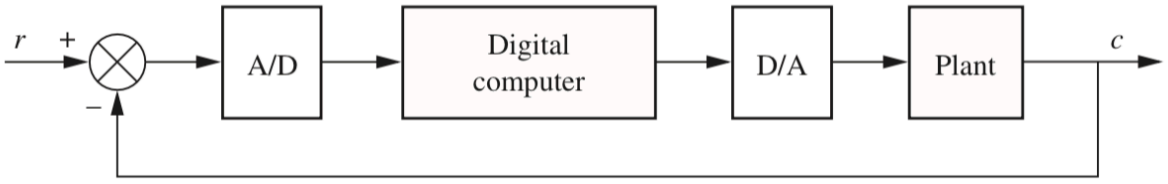
2.1.4 Sistemas de Controle Digitais

Os sistemas de controle modernos demandam, cada vez mais, uma grande quantidade de variáveis de entrada e saída. Uma mesma planta industrial pode vir a ter, simultaneamente, leitura de variáveis como pressão e temperatura, velocidade e posição, tensão e corrente. Além de processamento de comandos para atuadores em motores, bombas, compressores, válvulas, podendo estar sujeito a variações de parâmetros internos e distúrbios externos.

Com isso, os computadores digitais (DC)[34] podem oferecer diversas vantagens na operação de sistemas complexos. Inicialmente, através do aumento da capacidade de processamento, que permita a automação de plantas mais complexas, além de adição de novos recursos de análise e modelagem de malhas de controle com auxílio de recursos computacionais. No aspecto físico, permitem a redução de custos por meio da substituição de uma grande quantidade de cabos, relés e circuitos, por terminais de computadores com alta capacidade de processamento. Nesse contexto, os DC possuem uma maior flexibilidade, pois qualquer modificação que possa vir a ser realizada no projeto do sistema de controle, pode ser efetivada com uma simples reprogramação ou atualização do software (Nise, 2020).

A Figura 2.6 mostra o posicionamento de um computador dentro de um *loop* de controle. Os termos A/D e D/A[35] correspondem, simplificadamente, aos conversores de sinais digitais e analógicos, que se comunicam entre a planta e a malha de controle.

FIGURA 3.6 – Diagrama de blocos de um sistema de controle digital.



Fonte: Nise, 2020.

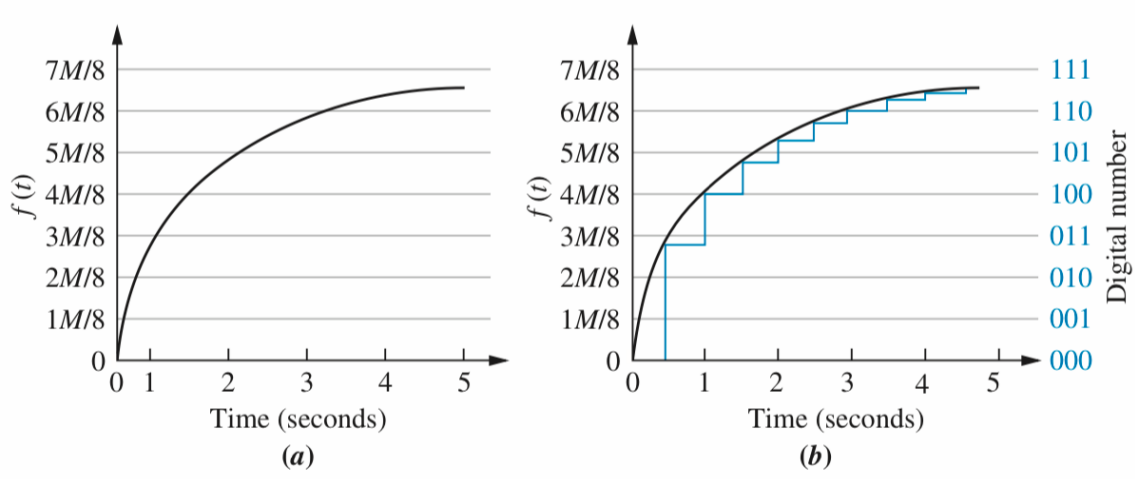
Analisando primeiramente o A/D, o conversor vai receber um sinal de voltagem, que pode ser contínuo (DC) ou variável (AC), que representa uma variável física do sistema, como por exemplo um sensor de temperatura ou pressão. Desta forma, seu papel é converter este sinal analógico em um número binário que normalmente consiste em 10 a 12 bits. Entretanto, em

[34] Do inglês, *Digital Computer*.
[35] Do inglês, *Analog-to-Digital converter e Digital-to-Analog converter.*

conversores A/D, o sinal analógico é convertido a uma certa taxa de amostragem, conhecidas como *sampled signal*[36], para depois ser transformado em uma sequência de números binários, que representam o valor médio de cada uma das amostras, que juntos formam o sinal digital (Powell *et al.*, 1998).

Segundo Nise (2020), a taxa de amostragem para se representar adequadamente um sinal contínuo deve ser pelo menos duas vezes maior que a frequência máxima presente no sinal, para garantir que não haverá distorções consideráveis na sua representação, esta regra é conhecida como Taxa de Amostragem de Nyquist.

FIGURA 2.7 (a) e (b)– Conversor analógico-digital.



Fonte: Nise, 2020.

Na Figura 2.7 (a), pode-se observar o sinal continuo a ser digitalizado, posteriormente, na Figura 2.7 (b) estão dispostas as amostras, em intervalos de tempo periódicos, através do *sampled signal,* que transformam o sinal analógico numa representação discreta.

O mecanismo responsável por interpolar o sinal é chamado de ***zero-order-hold*** *(z.o.h.)*[37], neste caso, o valor do sinal discreto é o mesmo do analógico no instante da amostragem, com isso, nivela um valor aproximado em forma de escada, que para intervalos de tempo cada vez menores, torna-o cada vez mais próximo do sinal original (Powell *et al.*, 1998).

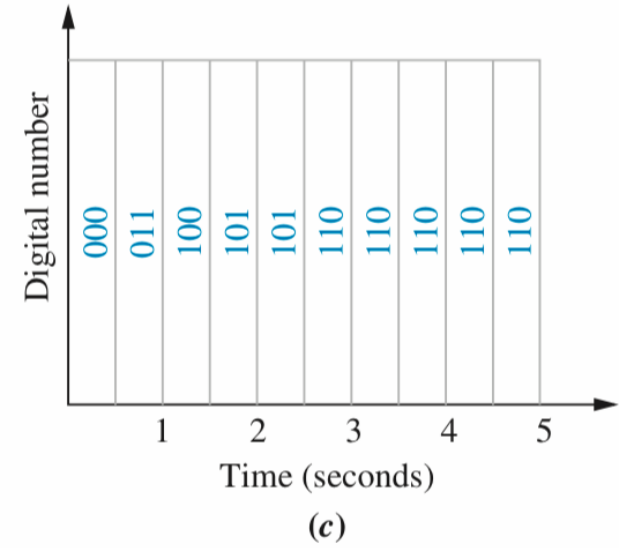
As amostragens são interpoladas e armazenadas antes de serem digitalizadas, pois o A/D irá converter esse valor fixado através de um contador digital, que demora um tempo para

[36] ***Sampled signal****:* termo em inglês, com tradução sinal amostrado ou discreto, sendo *sample* a amostragem (por segundos) e *sample rate* a taxa de amostragem (em Hz), é a representação de um sinal contínuo durante a sua conversão para sinal digital, através de amostras discretas que, quando somadas, o descrevem.

[37] ***Zero-order-hold*** é um tipo de interpolador que discretiza o sinal analógico em suas amostras, o valor de sinal discreto corresponde ao valor do sinal original no momento da amostragem, com isso tem a aparência de uma escada. Outros interpoladores de ordens maiores como o linear ou cúbico, podem apresentar uma representação mais precisas do sinal contínuo, entretanto sua representação pode ser um tanto quanto mais complexa.

alcançar o correto número digital (Nise, 2020). Após se tornar um sinal discreto, o conversor A/D transforma-o em um número digital ou binário, como na Figura 2.7 (c), ou seja, para cada um dos valores discretos, atribuídos ao sinal original, haverá um número digital de três bits correspondente.

FIGURA 2.7 (c)– Conversor analógico-digital.



Fonte: Nise, 2020.

Na Figura 2.7 (a) e (b), M corresponde ao maior valor de voltagem, portanto, como o conversor apresenta 3 bits, no sistema binário seria possível quantificar as amostragens em 8 níveis. Conclui-se que, para um sistema qualquer a diferença entre os níveis de amostragem corresponde a $\frac{M}{2^n}$, onde n é o número de bits de um sistema binário (Nise, 2020).

Sintetizando o que foi observado até agora, o DC estará localizado na malha de controle, onde antes amplificadores operacionais, compensadores analógicos e circuitos integrados agiam como malha de controle da planta industrial. O computador trabalhará, exclusivamente, com processamento de sinal digitalizado, através de amostras quantizadas do sinal contínuo presente na planta.

Vale destacar que, o fato de o sistema de controle digital estar trabalhando a uma taxa de amostragem, pode produzir um efeito de atraso na performance do sistema de controle de malha fechada, afetando a sua estabilidade e resposta transitória de acordo com o valor da taxa. Uma das soluções é utilizar frequências de amostragens maiores, de forma a aproximar o sinal discreto da sua representação continua (Nise, 2020). Segundo Powell *et al.* (1998), para sistemas controle modernos, que utilizem taxas de amostragens maiores que 30 vezes a maior

frequência do sinal contínuo, o controle do sistema irá funcionar de maneira aceitável, no que diz respeito a sua performance.

Para a análise do comportamento de um sinal discreto, como, por exemplo, seu atraso descrito anteriormente, faz-se necessário aplicar métodos matemáticos mais específicos para sistemas digitais. O recurso matemático da **transformada Z**[38], que substituirá a transformada de Laplace, permite uma melhor avaliação do sinal amostrado, até que ele seja convertido novamente em sinal contínuo, principalmente por permitir levar em consideração o atraso, atinente a taxa de amostragem.

A transformada Z pode ser definida da seguinte maneira:

$$Z\{f(kT)\} = F(z) = \sum_k^{\infty} f(kT)z^{-k}. \tag{2.9}$$

Onde: $f(kT)$ corresponde ao sinal discreto, T é o período de amostragem e k= 0,1,2,3...

Enquanto a transformada de Laplace resolve as equações diferenciais por meio da sua propriedade de derivação, presente na Tabela A.1 do Apêndice A, a transformada Z utiliza do método de Euler para transformar equações diferenciais em equações de diferenças. Com isso, posteriormente, a propriedade de translação permite que seja representado o atraso do sistema discreto, conforme abaixo:

$$\dot{x}(k) \approx \frac{x(k+1) - x(k)}{T}, \tag{2.10}$$

método de Euler.

$$Z\{f(t - kT\} = z^{-k}F(z), \tag{2.11}$$

propriedade de translação.

Como observado nas equações, a 2.10 permite reescrever as equações diferenciais de qualquer ordem, enquanto a 2.11 é a chave para passar os termos para o domínio de Z. Nesse contexto, a transformada Z, com suas propriedades matemáticas, está para os sistemas discretos, assim como a transformada de Laplace está para os sistemas lineares invariáveis no tempo (Powell *et al.*, 1998).

[38] No **Apêndice E** encontra-se algumas propriedades da transformada Z para melhor compreensão, além de uma tabela com algumas transformadas.

Com a Transformada Z, permite-se utilizar a representação por funções de transferência ou espaço de estados, para representar a malha de controle com sinal discreto. Desta forma, introduz-se ferramentas que serão necessárias para avaliar o comportamento de malhas de controle digitalizadas e suas plantas industriais, representá-las, realizar testes e análises de comportamento. Todos esses mecanismos, por meio do processamento digital, passam a ser extremamente facilitados, sendo essencial para sistemas complexos.

2.1.5 Sistemas de Controle Robustos e suas aplicações em Sistemas Navais

Como pôde-se observar até então, primordialmente, a teoria de controle clássico solucionou diversos problemas de controle, relevantes até os dias de hoje. Entretanto, com o aumento da complexidade dos sistemas de controle, a teoria de controle moderno passou a adotar métodos de análise mais abrangentes que, juntamente com os processos de digitalização dos sistemas e capacidade de processamento de dados, tornaram-se mais viáveis para descrever os sistemas reais.

Nesse contexto, a teoria de sistema de controles robustos tem como foco permitir que sejam controlados sistemas complexos, com uma certa tolerância a sua variação de parâmetros internos, sem comprometer os seus requisitos de desempenho. Outro fator relevante, é a capacidade de ser resiliente a distúrbios externos, como ruídos e perturbações que possam afetar a sua estabilidade. Dentro deste cenário, vale destacar que esta abordagem de sistemas de controle é relevante em diversas áreas da indústria que demandam alto nível de precisão, como aeroespacial, automotiva, petróleo e gás, geração de energia e, especialmente, em sistemas navais que se comportam como sistemas críticos (Ogata, 2010).

Um sistema embarcado precisa coordenar diversos sistema críticos, que operam de maneira integrada para desempenhar sua função. Adicionalmente, as condições em que as embarcações são expostas podem vir a ser extremamente desafiadoras para seus equipamentos e sistemas de controle. Dentre as características necessárias a esses sistemas, pode-se destacar: redundância e tolerância a falhas, adaptação a condições ambientais extremas, capacidade de se manter operando de maneira continuada. Com isso, vale destacar que muitas das soluções de controle, que foram introduzidas com as evoluções tecnológicas da indústria 4.0 e a teoria de controle moderno, são essenciais não só para a produtividade e eficiência da indústria naval, como para o aumento da sua disponibilidade e nível de segurança das operações.

2.2 Protocolos de Rede

O início do desenvolvimento dos protocolos de rede remonta a década de 1960, como consequência direta do processo de informatização. Nesta época um dos principais protocolos de rede, o NCP[39], funcionava como base para tecnologias como o ARPANET, de desenvolvimento para uso militar, que serviria futuramente como precursor para a internet. A partir dos anos 1980, o protocolo TCP/IP[40] prevaleceu como padrão de comunicação em boa parte das redes de informação, e tornou-se a base da internet como se conhece hoje, sendo a espinha dorsal para as comunicações WAN. Paralelamente, o protocolo *Ethernet,* mencionado no início deste trabalho, foi desenvolvido na década de 1970, definindo regras e convenções para comunicação e transmissão de dados entre dispositivos em uma rede LAN (Zurawski, 2015).

Um Protocolo de Rede é composto por regras que governam as comunicações em rede, em seus diferentes níveis de execução. Neste contexto, o modelo OSI[41] é um *framework* usado para definir como as redes de computadores funcionam, dividindo o processo de comunicação em sete camadas distintas, com suas respectivas funções, que permitem compreender melhor o funcionamento de sua estrutura. Em Zurawski (2015), define-se, brevemente, as seguintes camadas do modelo OSI:

i. **Camada de Aplicação:** Interação entre as aplicações dos usuários, é o limite entre o software e a unidade de comunicação da rede.

ii. **Camada apresentação:** Responsável por interpretar, compactar e criptografar dados para serem transmitidos pelas aplicações.

iii. **Camada de Sessão:** Estabelece, gerencia e encerra sessões de comunicação entre dispositivos, também envolve identificação e autenticação dos dados

iv. **Camada de transporte:** Garante a transferência confiável de dados e controla o fluxo de informação.

v. **Camada de rede:** Gerencia endereçamento e roteamento de pacotes de dados entre a sua origem e seu destino através da rede.

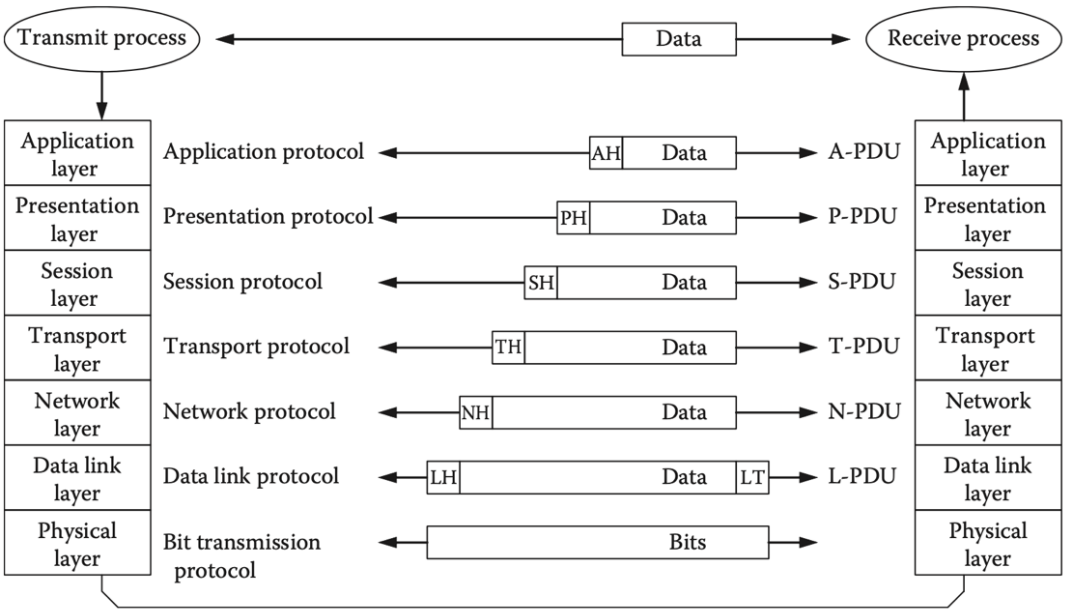
vi. **Camada de Enlace de Dados:** Coordena a transmissão de dados de dispositivos diretamente conectados à rede, além de detecção e correção de erros.

---

[39] Do inglês, *Network Control Protocol.*
[40] Do inglês, *Transmission Control Protocol/ Internet Protocol.*
[41] Do inglês, *Open Systems Interconnection*.

vii. **<u>Camada Física</u>:** Envolve o meio físico, presente nos conectores, cabos, *switches* e *hardwares*, e trata da transmissão de bits, que são os dados no estado bruto.

FIGURA 2.8 – Representação em camadas do Modelo OSI.



Fonte: Zurawski, 2015.

Nesse contexto, na Figura 2.8 observa-se como as camadas comunicam-se entre si verticalmente, dentro de sua estrutura, com os dados recebidos pelas camadas físicas, ainda em um estado bruto, e percorrem diversos estágios até a camada de aplicação, onde serão processados. Além de horizontalmente entre cada um dos níveis, através de dispositivos que compartilham de um mesmo link de dados, como os roteadores que conectam diferentes ambientes de rede, na camada de transporte. Seja no processo de transmitir ou de receber dados, cada nível irá executar a sua função prevista e preparar o conteúdo a ser transmitido para o próximo nível, segmentando em pacotes de dados individuais que sejam comportados pela respectiva camada que o sucede (Zurawski, 2015).

Com isso, nas seções a seguir, cada um desses conceitos será empregado para trazer características específicas atribuídas aos protocolos de rede de comunicação industrial, em diferentes momentos de sua evolução e consolidação como ferramenta de integração dos ICS.

2.2.1 Protocolos de Redes Industriais: A evolução dos *Fieldbuses*

Assim como diversas outras tecnologias ao longo da história da indústria, o desenvolvimento dos protocolos de rede permitiu um significativo aprimoramento no controle

e automação de sistemas. Hoje, seria inimaginável pensar nas mais diversas aplicações de sistemas de controle digitais, sem associá-las a um *background* robusto de *hardwares e softwares* capazes de entregar os recursos necessários para que ocorra comunicação entre sensores, atuadores e plantas industriais de maneira adequada.

No início da década de 1980, com o desenvolvimento da microeletrônica e aumento da capacidade de processamento distribuído, começaram a se estabelecer os primeiros protocolos ***fieldbuses***[42]. Com a finalidade de se atender aos novos requisitos de eficiência das plantas de controle, os protocolos de rede industriais substituíram as primitivas soluções de rede conhecidas até então, por uma topologia inovadora e voltado para as demandas que os desenvolvedores apresentavam na época (Lamb, 2015).

Nesse contexto, as antigas conexões estrela, que conectavam ponto a ponto os dispositivos a estruturas de controle central, deram lugar a um modelo de conexão descentralizada na qual todos estão conectados por uma linha compartilhada[43], que se mostrou mais adequado para operar com as demandas de transmissão de dados da época. Adicionalmente, com o pré-processamento de dados de dispositivos na própria planta industrial, possibilitou-se reduzir o número de cabos e aumentar a qualidade dos dados processados no campo, antes de serem encaminhados para monitoramento nos computadores centrais (Zurawski, 2015).

A primeira função de um *fieldbus* é conectar os dados brutos de sensores e atuadores, através das camadas físicas de seu protocolo, as suas respectivas unidades de controle e processamento de dados. Com isso, diferentemente dos protocolos de redes LAN desenvolvidos na época, estes sistemas foram projetados para serem eficientes sobre dois principais aspectos: transmissão de dados, para dispositivos com elevados requisitos de frequência de amostragem; e implementação de interfaces com aplicações simplificadas, capazes de lidar com dispositivos de campo com baixo recursos de processamento (Zurawski, 2015).

Nos protocolos de redes industriais são necessários uma programação de alto nível na sua camada de aplicação que permita ter flexibilidade para realizar a interface de diferentes sistemas complexos. Os dispositivos de controle, através da sua comunicação por rede, devem ser capazes de gerenciar o fluxo de informações e processos, malhas com realimentação,

---

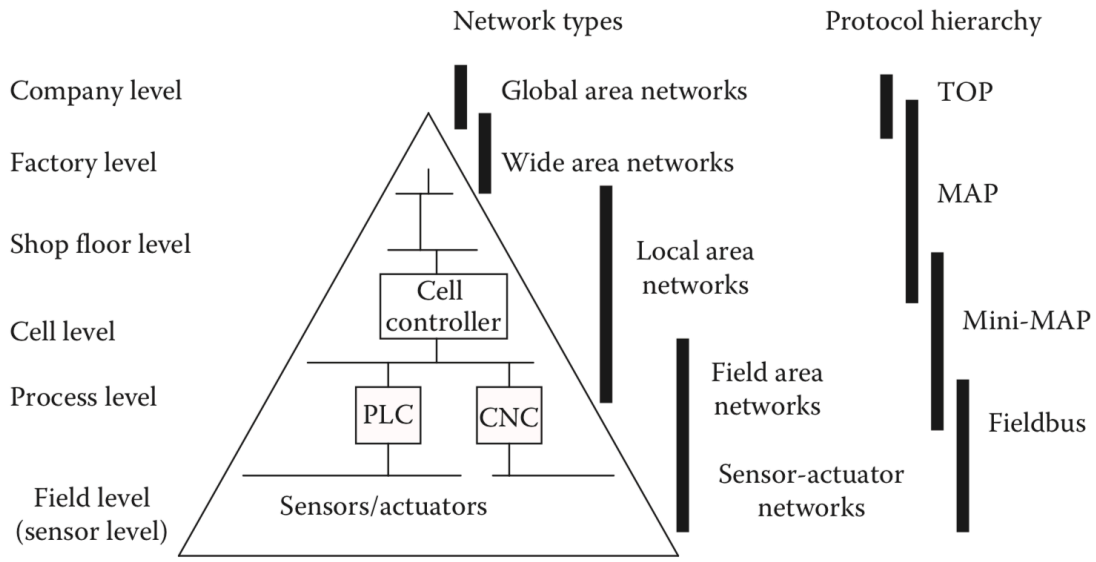
[42] **O *Fieldbus*** é um grupo de protocolos de comunicação para plantas industriais e dispositivos de instrumentação, que permite a conexão entre dispositivos atuadores e sensores aos sistemas de controle, funciona como uma LAN para processos de controle avançados, entradas e saídas remotas e aplicações de alta velocidade para automação industrial.

[43] Está topologia de rede, onde os dispositivos compartilham de uma linha comum de rede, ao invés de utilizar uma topologia estrela, é o que atribui o termo "*bus*", que em inglês refere-se a ônibus (transporte compartilhado), ao protocolo *fieldbus.*

controladores PID, comunicar-se com sinais discretizados, bem como suportar outros softwares e ferramentas de interação com os operadores. Portanto, os *fieldbuses* estabeleceram-se para os diversos níveis hierárquicos, com diferentes estruturas de rede que fossem mais convenientes para cada atividade, mas que por fim conversassem entre si de maneira a manter o fluxo de processamento (Zurawski, 2015).

No que diz respeito aos níveis hierárquicos de rede, pode-se definir uma distinção entre duas classes principais de atuação dos *fieldbuses*, como será observado na Figura 2.9. A primeira atua no **nível de campo** conectando os atuadores e sensores em rede aos sistemas de controle distribuídos. A segunda atua a **nível de processos**, conectando esses controladores e computadores a dispositivos mais inteligentes com capacidade de gerenciamento de dados, operando mais próximos de infraestruturas de rede superiores como as LAN (Zurawski, 2015).

FIGURA 2.9 – Níveis hierárquicos de rede.



Fonte: Zurawski, 2015.

Nestes níveis de comunicação de rede, trafegam dados com características intrinsicamente diferentes. Desta forma, faz-se necessário destacar algumas definições de fluxo de dados, que em grande parte se distinguem quanto aos seus requisitos de tempo de resposta e sua consistência. No que diz respeito ao tempo, pode-se dividir em duas classificações, a primeira que se baseia no *status* do processo, consiste nos dados que definem as variáveis internas de um sistema, que são continuamente amostrados e atualizados, sendo transmitido em ciclos constantes e formando a base do processo de monitoramento. E a segunda, baseia-se na mudança de *status,* onde os dados são transmitidos apenas quando se ultrapassa um limite pré-determinado de mudança do estado anterior (Zurawski, 2015).

Quanto a consistência, há por um lado dados que são transmitidos continuamente, como *looping* de controle em um sistema de malha fechada, onde os dados trafegam quase que ininterruptamente, durante o funcionamento da planta. Por outro lado, existem dados que são transmitidos quando sob demanda, que pode ser determinado por um processo estabelecido no seu código, que pede certo conteúdo quando se apresenta uma determinada condição, ou simplesmente uma informação solicitada pelo operador da planta (Zurawski, 2015).

As diferentes formas de fluxo de dados trazem consigo implicações diretas na forma de comunicação dos sistemas *fieldbuses,* desde a sua implementação até o seu protocolo. Por exemplo, as bases de dados que são atualizadas de maneira cíclica, como as presentes nos *loops* de controle, são geralmente enviadas em interfaces de camadas mais simples, sem grandes verificações e confirmações de autenticidade ou criptografia, de forma que sejam transmitidas rapidamente (Zurawski, 2015).

Na ocasião de um pacote de dados se perder, não há tempo hábil para enviá-lo novamente, pois até que chegasse ao seu destino, já estaria fora do seu tempo de resposta adequado e, certamente, um outro dado mais atualizado já estaria disponível para o processo. Esta característica do fluxo de dados em plantas industriais será utilizada posteriormente como mecanismo para se realizar ataques cibernéticos baseados na perda de pacote de dados (Zurawski, 2015).

No Quadro 2.1, observa-se o comparativo de algumas das características dos diferentes níveis hierárquicos de redes industriais. Além de se destacar alguns dos protocolos utilizados para os respectivos requisitos apresentados.

QUADRO 2.1 – Comparativo entre níveis hierárquicos de redes industriais.

Característica	**Informacional**	**Controle**	**Campo**	**Sensor**
Atuação	-Monitoramento de dados (Supervisory)	-Controle em tempo real -Interface	- Aquisição e atuação na planta industrial	- Aquisição direta de sensores para rede
Tamanho (Dados)	Mbytes	kbytes	bytes	Bits
Tempo de resposta	s	5 a 100 ms	ms	μs
Redundância	Sim	Sim	Sim	Não
Cobertura	Grande	Grande	Média	Pequena

Protocolos utilizados	-Profinet -Ethernet/IP -Fieldbus Foundation HSE	-Fieldbus Foundation HSE -Profibus PA -Modbus -Controlnet	-Profibus DP e PA -Fieldbus Foundation H1	-Sensorbus -Devicenet -CanOpen

Fonte: Elaborado pelo Autor (Lamb, 2015; Zurawski, 2015).

A comparação demonstra que, por apresentar diferentes requisitos, desde sistemas centralizados que monitoram toda a planta, até os mais diversos dispositivos controle distribuídos, o projeto de rede industrial irá se diferenciar de acordo com seu nível de atuação. Essas características podem ser devido aos níveis hierárquicos apresentados acima, ou podem ser particularidades do sistema a ser controlado. Por exemplo, em plantas de geração de energia, que possuem demandas muito especificas de ciclos de amostragem, pode ser necessária uma estrutura de rede específica para ser capaz de manter a rede elétrica estável.

A complexidade envolvida na modelagem de um sistema de controle e automação de uma planta industrial, somados aos diferentes níveis hierárquicos de rede, tornou um desafio a busca por uma maior unificação desses protocolos, como as que se apresentavam nas comunicações de IT. Ainda na década de 1980, foram realizadas algumas tentativas de padronização, mesmo que sem grande sucesso, pela Comissão Eletrotécnica Internacional (IEC)[44], para estabelecer especificações relacionadas aos protocolos *fieldbuses*. Com o tempo, ao longo deste processo, alguns desses parâmetros passaram a ser incorporados por sistemas notáveis, de protocolo aberto, tais como: ***PROFIBUS, DeviceNet e ModBus*** (Lamb, 2015).

O *PROFIBUS* é um protocolo de rede de comunicação industrial, encontrado com frequência na indústria por se tratar de um protocolo aberto, o que facilita sua integração em plantas que possuem dispositivos de diferentes fabricantes. Inicialmente, foi desenvolvido por um grupo de empresas da Alemanha, até se estabelecer nas versões mais recentes. Pode ser utilizado tanto no monitoramento de equipamentos de medição na automação de processos, através do *PROFIBUS PA (Process Automation*), quanto para comandar sensores e atuadores através de controladores descentralizados, com o *PROFIBUS DP (Decentralized Peripherals)* (Lamb, 2015).

Dentre outros protocolos, mas que atuam em níveis mais baixos da rede industrial, pode-se mencionar o *CANOpen*, comumente utilizado em sistemas embarcados. Este sistema, muito

[44] Do inglês, *International Electrotechnical Commission.*

comum em níveis mais baixos de processamento, é composto por uma camada de aplicação, de endereçamentos e alguns protocolos de comunicação para dados brutos. Outrossim, por também ser um protocolo aberto, pode suportar sensores e atuadores de vários fabricantes, sendo muito utilizado em servos e posicionadores (Lamb, 2015).

Adicionalmente, o *DeviceNet é* outro protocolo que conecta dispositivos no chão de fábrica com dispositivos de processamento distribuídos, como os PLC e DCS. Normalmente, a topologia de rede presente nesses protocolos de campo é utilizada para configurações de OT remotos, através do padrão físico de comunicação de rede de controle (CAN)[45], que são redes locais, de curtíssimo alcance, que trabalham com dados brutos (em bits) com tempo de resposta abaixo de $1ms$ (Lamb, 2015).

O gerenciamento de uma variada gama de atividades industriais complexas, em diferentes níveis de atuação das comunicações por rede, fez dos *fieldbuses*, por décadas, uma ferramenta extremamente conveniente para os seus usuários. Mas, apesar das tentativas de padronização, os sistemas industriais sempre exigiram serviços adicionais e personalizados, justificados pelos requisitos específicos de cada sistema e equipamento que os compõem. Esta característica, do ponto de vista dos utilizadores, pode vir a causar um aumento no custo de desenvolvimento dos sistemas, além da necessidade de suporte e manutenção geralmente disponibilizada exclusivamente pelos fabricantes.

Outro aspecto que tem se tornado evidente nos protocolos modernos, desde o início dos anos 2000, é o aumento da utilização combinada dos protocolos de comunicação e informação para aplicação em redes de automação industrial. Isso está relacionado a presença de dispositivos de controle cada vez mais inteligentes, necessidade de ciclos de amostragem mais curtos e tráfego de dados mais rápidos, além da possibilidade de conexão de sistemas de controle remotas com redes WAN, levando a integração vertical entre escritórios e o chão de fábrica (Hou *et al.*, 2010).

Os novos conceitos de protocolos de rede industriais, baseados em RTE, podem vir a permitir uma maior interconexão entre protocolos *fieldbuses* e os níveis hierárquicos superiores, anteriormente isolados. Portanto, os protocolos podem vir a integrar todo o gerenciamento nos níveis de campo e processo, aos níveis gerenciais e os escritórios, que atualmente são baseados em protocolos Ethernet e TCP/IP (Hou *et al.*, 2010).

[45] Do inglês, *Control Area Network.*

2.2.2 Industrial Ethernet: Protocolos RTE na indústria

Com o crescente aumento dos requisitos de sistemas de controle, a indústria passou a apresentar demandas cada vez mais especificas de taxa de dados, tempo de resposta, sincronismo e redundância. Isso levou a muitos protocolos rede industriais, baseado nos *fieldbuses*, como *PROFIBUS, DeviceNet* e *CANOpen*, mencionados anteriormente, a deixarem de ser totalmente compatível com algumas dessas novas exigências em seu formato original.

Por outro lado, com a evolução da capacidade de transmissão de dados dos protocolos de rede de comunicação, baseados em *Ethernet,* que passaram de 10 Mbps para mais de 10 Gbps, além das ferramentas já existente desses protocolos em diversas camadas, abriram-se novas possibilidades de integração destes sistemas. Nesse contexto, pode-se proporcionar uma solução para os novos requisitos apresentados pela indústria, com uma abordagem mais econômica para os desenvolvedores de plataformas, permitindo atender às crescentes demandas de desempenho e verticalização de sistemas de controle (Hou *et al.*, 2010).

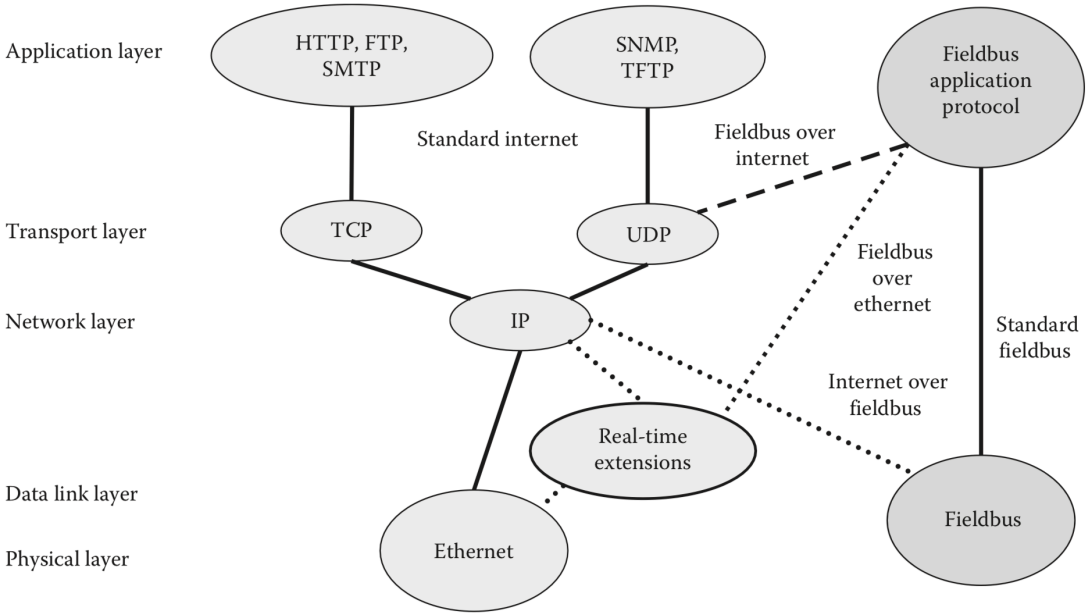
Desta forma, os protocolos antes voltados exclusivamente para IT, como *Ethernet* e TCP/IP, tornaram-se mais populares em redes de controle e automação. Apesar de, inicialmente, terem sido considerados inapropriados devido a sua lacuna de capacidade de transmissão de dados em tempo real. Com **a introdução de *switches***[46] e modificações em seus protocolos originais, o *Ethernet* ganhou característica que o permitiu tornar-se mais adequado aos requisitos da indústria. Outrossim, proporcionou argumentos favoráveis que o incentive a ser mais amplamente empregados nas fabricas, como a possibilidade de uma maior integração vertical com outros sistemas e redes, a nível de escritório, gerência e manutenção (Zurawski, 2015).

Na Figura 2.10 pode-se observar, segundo o modelo OSI, como os protocolos da família IT, principalmente Ethernet e TCP/IP, conseguem preencher os quatro níveis mais baixos das camadas de protocolos de rede industriais. Esta característica possibilita uma adequação dos protocolos, que antes eram utilizados apenas para comunicação e informação, combinados a camada de aplicação dos protocolos *fieldbuses,* para torná-los uma ferramenta integrada capaz de suprir os novos requisitos dos sistemas OT.

---

[46] Os ***switches*** são ferramentas de rede que atuam na camada de enlace de dados, são projetados para conectar vários dispositivos em uma LAN e encaminhar pacote de dados com base em seu endereçamento. Seu emprego permite um gerenciamento mais eficiente do tráfego de rede, com características como: segmentação de redes e aumento da largura de banda (Zurawski, 2015).

FIGURA 2.10 – Estrutura de combinação de fieldbus e Ethernet/IP.



Fonte: Zurawski, 2015.

Essas primeiras aproximações, como previstos no IEC 61158[47], trouxeram a combinação de uma camada de aplicação dos modelos *fieldbuses,* no topo dos protocolos baseados em mecanismos Ethernet/IP (neste caso IP refere-se a *Industrial Protocol*). Como nos seguintes exemplos: a variação da *Foundation Fieldbus*, com *Ethernet* de alta velocidade e as aplicações do *Foundation Fieldbus H1,* que até então era utilizado na indústria com o padrão *fieldbus*; e o uso do Protocolo de Controle e Informação (CIP)[48], conhecido dos sistemas *DeviceNet e ControlNet*, assistidos pelos protocolos de comunicação TCP/IP (Zurawski, 2015).

Como todas essas aproximações estavam fora do padrão estabelecido pela IEC, e diante de algumas dificuldades iniciais apresentadas pelas associações destes protocolos, como a perda de pacotes de dados em *switches,* quando sujeitos a altos níveis de demanda, foram estimulados o desenvolvimento de infraestruturas e alternativas que se mostrassem mais viáveis a indústria. Esse processo culminou em mais uma tentativa de padronização, com soluções técnicas previstas no IEC 61784-2[49], que esta presente no que hoje é chamado de ***Real-Time Ethernet*** (Zurawski, 2015).

[47] O termo IEC 61158 refere-se ao conjunto de normas e regulações que especificam as características para utilização de redes de comunicação digital amplamente utilizadas para aplicação industrial. Inclui protocolos combinados como *Fieldbus Foundation, PROFIBUS, DeviceNet* e outros (Zurawski, 2015).

[48] Do inglês, *Control and Information Protocol.*

[49] O IEC 61784-2 é parte da norma técnica que trata de sistema de comunicação industrial, especificamente voltado para a comunicação em tempo real para automação industrial, como é o caso do RTE.

Este grupo de estudos do RTE trouxe a classificação de três prováveis estruturas de aplicações em OT, baseadas em tempos de reação (Zurawski, 2015):

i. Classificação de baixa velocidade, tempo de reação por volta de 100 ms, típico para sistemas que envolvem observação humana, para engenharia e para processo de monitoramento.

ii. A segunda classificação, para tempos de reação menores do que 10 ms, requerido para processo de automação que envolva os PLC ou qualquer computador controlador.

iii. A classificação com maior demanda, voltada para sistemas mais críticos, com tempos de reação menores do que 1 ms, requisito de sincronização das amostras coletadas pela rede, empregado nos níveis mais baixos da planta industrial.

A partir dessas características, diversos protocolos de rede, baseados em RTE, foram desenvolvidos, como pode-se observar no Quadro 2.2, que compara alguns protocolos no que diz respeito a sua atuação nos níveis mais baixos da indústria, que como já mencionado, são os de maiores demandas de performance.

QUADRO 2.2 – Comparativo entre padronizações Real Time Ethernet.

Protocolos	**EherNet/IP**	**Modbus/TCP**	**Profinet-IRT**	**SERCOS III**	**EtherCAT**
Capacidade (na camada física)	100/1000 Mbps	100/1000 Mbps	100 Mbps	100 Mbps	100 Mbps
Performance Real Time	< 1ms	Não informado	1ms	8 axis em 31,35μs	8 axis em 31,35μs
Redundância	Resilient Ethernet Protocol[50]	Resilient Ethernet Protocol	Resilient Ethernet Protocol	Topologia anel (SERCOS)	Topologia anel (SERCOS)
Sincronismo	IEEE 1588[51]	Não suportado	IEEE 1588	SERCOS III system	IEEE 1588

Fonte: Modificado de Hou *et al.* (2010).

[50] O *Resilient Ethernet Protocol* é um protocolo de rede desenvolvido pela Cisco System para operar com sistemas que necessitam de elevada redundância e capacidade de ser resiliente a falhas, dentre outras características está a redundância de caminho, rápida detecção de falhas e compatibilidade de emprego com Ethernet padrão (Zurawski, 2015).

[51] IEEE 1588 é o padrão internacional que descreve um protocolo de precisão de tempo para redes de comunicação, este permite uma sincronização rede da ordem de μs ou ns. Implementado em redes Ethernet Industriais. (Zurawski, 2015)

Em Hou *et al.* (2010), observam-se algumas das características de sistemas de controle críticos, que demandam baixo tempo de reação, como, por exemplo, plantas de geração de energia para navios, que são sistemas robustos que necessitam de características de controle especificas. Dentre essas, e ainda não discutidas, pode-se mencionar a redundância, que é a capacidade de funcionar sem falhar, mesmo quando exposto a adversidades que podem se apresentar como danos por algum incidente, como incêndio ou alagamento, ou por fatores ambientais. Adicionalmente, a sincronização, com *loops* que funcionam com taxa de amostragem de alta frequência que podem chegar a períodos de até 1 μs.

Neste contexto, as comunicações por rede tornaram-se ponto focal de inúmeras discussões para as tecnologias da indústria 4.0. A necessidade de sistemas mais eficientes que atendam aos diversos requisitos de OT é cada vez mais premente. Com isso, a integração dos sistemas de tecnologia de informação com os protocolos de rede antes utilizados nas plantas industriais tornou-se inevitável, por já estarem disponíveis no mercado (Zurawski, 2015).

Diferentemente dos clássicos protocolos *fieldbuses,* os protocolos *Ethernet e TCP/IP* estão surgindo como uma base padronizada para a nova geração de sistemas de comunicação industrial. No entanto, essa base, apesar de ser vantajosa devido à sua disponibilidade no mercado, custo reduzido e à capacidade de oferecer uma variedade de ferramentas para atender aos sistemas de controle atuais, enfrenta o desafio cada vez mais significativo do surgimento de ameaças cibernéticas, que antes eram exclusivas das redes de IT. Isso ocorre, principalmente, devido à utilização de protocolos com autenticação e criptografia deficientes nas plantas industriais. Portanto, fica evidente a necessidade de se abordar o tema segurança cibernética em ambientes de OT, à medida que as fronteiras entre sistemas IT e OT são derrubadas.

2.2.3 Vulnerabilidades dos NCS e ataques baseados em RTE

Segundo as literaturas Peschke *et al.* (2006), De Sá *et al.* (2017) e Ferrari *et al.* (2020), as vulnerabilidades de segurança cibernética nunca se mostraram tão evidentes nos protocolos de rede industriais, quanto nos baseados em RTE. Os clássicos *fieldbuses* tinham por característica manter-se isolados, sendo dedicados das redes de controle e automação, técnica de segurança conhecida como *air gap.* Entretanto, com a introdução dos protocolos baseados em estruturas *Ethernet* e TCP/IP, bem como a possibilidade de integração vertical entre as plantas industriais e os escritórios, estes sistemas vem se tornando exponencialmente mais expostos as ameaças do domínio cibernético.

No Quadro 2.3 são apresentados alguns protocolos industriais baseados em *Ethernet* e suas respectivas, baixas ou nenhuma, especificações de segurança quando voltados para os requisitos de OT.

QUADRO 2.3 – Especificações de segurança dos protocolos industriais baseados em Ethernet e TCP/IP

IEC 61784 - Protocolo	**Medidas de segurança previstas**
Foundation Fieldbus	Proteção de acesso simples.
EtherNet/IP	Nenhuma medida de segurança especificada.
Profinet	Proteção entre switches para evitar sobre carga de segmentos de tráfego em tempo real.
EtherCAT	Nenhuma medida de segurança especificada
MODBUS-RTPS	Controle de acesso baseado em endereçamento IP.
SERCOS-III	Nenhuma medida de segurança especificada.

Fonte: Modificado de Peschke *et al.* (2006).

Como pode ser observado, os protocolos de rede industriais não foram projetados levando em consideração especificações básicas de segurança para emprego em OT. Um dos pontos críticos é a lacuna de autenticação entre os principais atores presentes em um sistema de controle e automação, abrindo as portas para que qualquer dispositivo malicioso possa se instalar entre os *loops* de controle, comportando-se como parte integrante do sistema.

Por um lado, apesar de protocolos RTE industriais utilizarem, em sua maioria, os recursos de segurança do TCP/IP, que possuem medidas consideradas razoáveis, a grande maioria desses recursos somente são aplicáveis a nível doméstico e empresarial. Por sua vez, quando esses recursos são implementados nas plantas industriais, dada a falta de capacidade de processamento dos computadores envolvidos, podem vir a causar sobrecarga do tráfego de dados nos seus processos de controle. Outrossim, vale destacar que esses mecanismos são desenvolvidos para atuar na integridade de dados e controle de acesso a informação, enquanto para o chão de fábrica, a confidencialidade de dados não é de fato uma prioridade (Peschke *et al.*, 2006).

Como consequência direta desta lacuna de segurança cibernética apresentada nos *Networked Control Systems*, pode-se observar uma série de ameaças que podem vir a se estabelecer, posicionadas exatamente entre esses atores de um sistema de controle e automação.

Em De Sá *et al.* (2017), são descritos alguns modelos de ataques aos NCS, estes podem ser classificados em três diferentes categorias, como pode-se observar a seguir:

i. **Negação do serviço (DoS)**[52]: Consiste em todos os tipos de ataques cibernéticos que tem por objetivo negar a execução de um processo físico, interrompendo a execução do serviço que aquela planta tem como objetivo realizar.

ii. **Degradação do serviço (SD)**[53]: Consiste em se realizar intervenções maliciosas que tem por objetivo reduzir a eficiência de determinado processo físico, podendo vir até mesmo a reduzir o **tempo entre falhas do equipamento (MTBF)**[54]. Geralmente essa medida tende a ser mais discreta, com objetivos prejudiciais de médio e longo prazo.

iii. **Inteligência Cyber-física (CPI)**[55]: As ações são concentradas nos *loops* de controle, com o objetivo de se coletar dados sobre o funcionamento da operação do sistema e sua modelagem, pode vir a ser utilizada com a finalidade de se planejar a execução de ataques mais eficazes ao sistema de controle da planta física.

No Quadro 2.4 pode-se identificar diferentes formas de se realizar as categorias de ataque mencionadas, por ordem de complexidade, de acordo com o nível de acesso ao sistema. Observa-se que os ataques podem ocorrer, primeiramente, de maneira **arbitrária (*arbitrary*)**, sem conhecimento prévio do sistema de controle, ou com um pouco mais de complexidade sendo **controlada (*controlled*)**. Nesse contexto, os ataques controlados dependem de uma ação preliminar de identificação do sistema através dos mecanismos de coleta de dados e espionagem que foram abordados no CPI (De Sá *et al.*, 2017).

Os ataques de SD só podem ocorrer de maneira controlada, pois precisam de um nível de precisão adequado para prejudicar o sistema, sem ultrapassar seus limites de operação ou virem a ser detectados como intrusos. Por fim, quanto ao método, os ataques podem ocorrer por meio das seguintes ações: **instabilidade no tempo (*jitter)*,** que tem por objetivo levar o sistema a falha, inserindo atrasos nos *loops* de controle; **perda de dados (*Data loss)*** desviando o fluxo de parte dos dados ao seu destino, o que pode causar a repetição de dados anteriores e modificar a resposta original; e **inserção de dados (*Data Injection)*,** que consiste em transmitir dados modificados com a intenção de alterar a resposta do sistema de controle (De Sá *et al.*, 2017).

[52] Do inglês, Denial-of-Service.
[53] Do inglês, Service Degradation.
[54] Do inglês, Mean Time Between Failure.
[55] Do inglês, Cyber-physical Intelligence.

QUADRO 2.4 – Comparativo entre ameaças cibernéticas a *loops* de controle de NCS.

		Acesso aos dados	
	Acesso ao *loop* de controle		
Negação do serviço (DoS)	- DoS-Arbitrary Jitter - DoS-Arbitrary Data Loss	-	- DoS-Controlled Jitter - DoS-Controlled Data loss - DoS-Arbitrary Data Injection
Degradação do serviço (SD)	-	-	- SD-Controlled Jitter - SD-Controlled Data loss - SD-Arbitrary Data Injection
Inteligência Cyber-física (CPI)	Espionagem	Identificação do Sistema	-
Complexidade	**Baixa**	**Média**	**Alta**

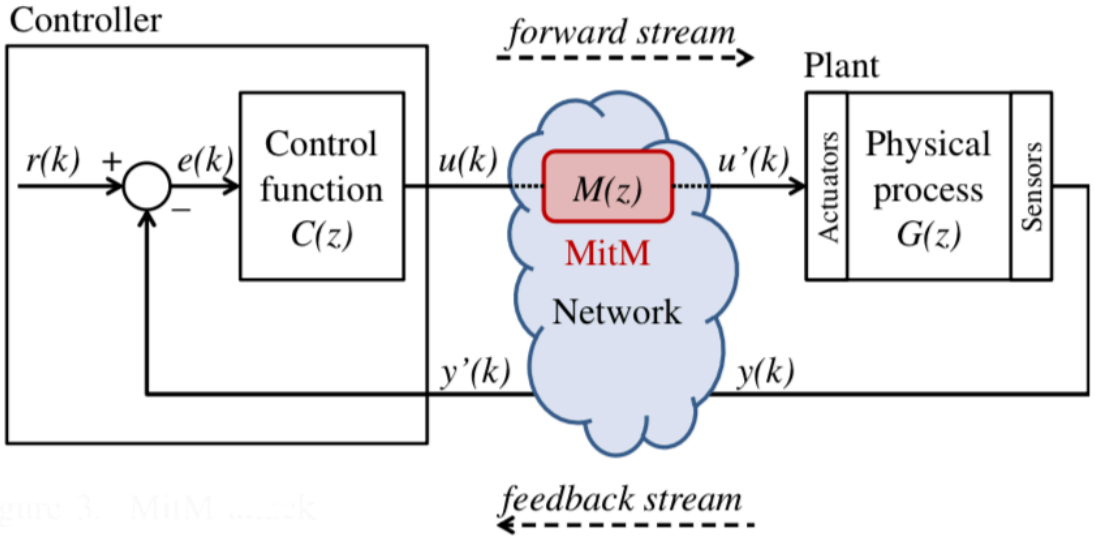
Fonte: Modificado de De Sá *et al.* (2017).

Os ataques cibernéticos aos NCS podem ser realizados ao se assumir uma posição entre os fluxos de dados que caminham dos computadores para os atuadores, o *forward,* e dos sensores de volta para os computadores, o *feedback.* **O *man-in-the-middle* (MitM)**[56], presente na Figura 2.10, posiciona-se, afetando o seu *loop* de controle e a resposta do sistema. O ataque a ser realizado vai ser definido com base nos objetivos do *hacker,* normalmente, com o intuito de permanecer oculto, utiliza-se de ataques controlados, que consigam identificar a planta e

[56] O termo ***man-in-the-middle,*** com tradução homem-no-meio, faz referência ao posicionamento da ameaça entre os demais atores do sistema de controle e automação.

lançar de medidas que desestabilizem o sistema apenas o suficiente para comprometê-lo (De Sá *et al.*, 2017).

FIGURA 2.11 – Man-in-the-middle (MitM) posicionado em um NCS.



Fonte: De Sá *et al.*, 2017.

Por fim, existem várias propostas que podem vir a mitigar as lacunas de segurança que existem nos protocolos industriais pautados em RTE. Mas em contrapartida, a adição de novas transações de segurança demandaria um elevado custo envolvido, na substituição ou *upgrade* de um elevado número de dispositivos (nas plantas industriais ao redor do mundo), para que estes dotassem da capacidade de processamento necessária a reduzir a exposição a ameaças cibernéticas. Enquanto isso não acontece, os antes isolados sistemas *fieldbuses,* vem dando lugar as redes RTE, que juntamente com a indústria 4.0, faz esse isolamento não mais existir, aumentando a quantidade de alvos disponíveis para as ameaças cibernéticas (Ferrari *et al.*, 2020).

3 METODOLOGIA

A presente pesquisa tem como objetivo aprofundar a compreensão das soluções de sistema de controle e automação, que desde a terceira revolução industrial, têm se tornado cada vez mais dependentes do processo de digitalização. Notavelmente, a indústria e sistemas navais, ao adotar protocolos RTE, associados a indústria 4.0, estão expondo as plantas industriais a crescentes vulnerabilidades do domínio cibernético. Diante deste cenário, o corrente trabalho sugere uma abordagem metodológica híbrida, que combina técnicas quantitativas e qualitativas para se analisar, por meio de estudos de caso e simulações, como a indústria 4.0 está se tornando cada vez mais suscetível a ataques cibernéticos.

3.1 Classificação da Pesquisa

Quanto às pesquisas realizadas, nas seções a seguir serão apresentadas as classificações que as norteiam. Primeiramente, serão abordadas as com base nos objetivos gerais do estudo. E posteriormente, aquelas que norteiam os procedimentos adotados para coleta de dados.

3.1.1 Quanto aos fins

Este trabalho pode ser classificado, quanto aos seus objetivos gerais, como uma pesquisa exploratória. Segundo Gil (2002), estas pesquisas têm por finalidade permitir maior familiaridade com o tema, proporcionando ampliar os horizontes de conhecimento sobre o objeto de estudo. Desta forma, inicialmente este trabalho assumirá forma de pesquisa bibliográfica, com foco nos principais periódicos (De Sá *et al.*, 2017; Ferrari *et al.*; 2020) e Livros (Ogata, 2010; Nise, 2020; Zurawski, 2015) que discursam sobre o tema abordado. Além de contribuir com Estudos de Caso sobre: SCADA System e o Ataque Cibernético “Stuxnet”.

3.1.2 Quanto aos meios

Neste ponto, conforme mencionado, o trabalho apresenta um caráter de metodologia híbrida. Primeiramente, com o forte caráter bibliográfico apresentado, além de estudos com vista a estimular a compreensão e a construção de hipóteses. Desta forma, busca-se construir

um arcabouço suficiente para desenvolver o objeto de estudo e, posteriormente, realizar uma pesquisa experimental.

Segundo Gil (2002), “o experimento representa o melhor exemplo de pesquisa científica”. Com base nessa premissa, foi desenvolvido uma pesquisa experimental em que o objeto de estudo, um sistema de controle de planta propulsiva, proposto por Whalley e Ebrahimi (2002), fará parte de um ataque cibernético, nos moldes propostos por De Sá *et al.* (2017) e Ferrari *et al.* (2020), a fim de se verificar a exequibilidade do algoritmo empregado pelos autores, sendo que neste caso em um sistema MIMO.

3.2 Coleta e Tratamento de Dados

O Sistema de controle e automação da planta propulsiva, descrito em Whalley e Ebrahimi (2002), será analisado e testado, para posterior simulação, através da plataforma SIMULINK[57]. Outrossim, a partir do *software* MATLAB[58], será possível realizar interações da planta de controle com o algoritmo proposto, armazenando as variáveis controladas para análise, a fim de se verificar o comportamento do ataque cibernético.

3.3 Limitações do Método

O projeto prevê a simulação de parte do comportamento necessário a uma ameaça cibernética ao ataque a um sistema de controle em rede, limitando-se a seleção de pacotes a serem desviados do sistema original. Determinadas variáveis serão excluídas, como a identificação passiva do sistema, processo de espionagem de dados e ganho de acesso.

Adicionalmente, as simulações ocorreram através da reprodução de modelos, não estando sujeitas aos distúrbios e variações que são características de uma planta de controle propulsiva em ambiente real. Neste estudo, não serão abordados as limitações físicas e mecânicas dos sistemas propulsivos empregados.

---

[57] SIMULINK é um ambiente de modelagem e simulação desenvolvido pela empresa *MathWorks*, amplamente utilizado para projetar sistemas de controle, a fim de realizar simulações e análises de comportamento das plantas (Nise, 2020).

[58] O MATLAB é uma ferramenta de computação numérica e ambiente de programação desenvolvido pela empresa *MathWorks*. Possui linguagem de programação de alto nível e permite realização de simulações integrado com o SIMULINK (Nise, 2020).

4 ANÁLISE DAS VULNERABILIDADES DOS SISTEMAS DE CONTROLE

Dando continuidade ao tema, neste capítulo serão apresentadas análises das vulnerabilidades cibernéticas dos Sistemas de Controle e Automação. Isso se baseia na evolução tecnológica atingida através de processos de digitalização, que transformou os Sistemas de controle em rede em ferramentas essenciais para plantas industriais e sistemas navais.

Nesse contexto, será dado enfoque no SCADA *System*, por se tratar de um sistema amplamente utilizado na indústria e infraestruturas navais. Além disso, será apresentado um estudo de caso de um ataque cibernético real conhecido como "*Stuxnet*". Esse caso é de particular importância, uma vez que representa um marco histórico em segurança cibernética para plataformas industriais.

4.1 Análise do Supervisory Control and Data Acquisition *systems*

O *Supervisory Control and Data Acquisition system* é utilizado na indústria desde a década de 1960, para o monitoramento e controle de plantas industriais e sistemas críticos, como em refinarias de petróleo, gasodutos, geração de energia, bem como, em sistemas navais. Ao longo do tempo, os protocolos do SCADA passaram de um sistema privado para aberto, o que possibilitou se tornar uma alternativa financeiramente mais viável, além de poder ser utilizado combinando equipamentos e sistemas de diversos fabricantes (NCS, 2004).

Outra evolução relevante, foi o fato de ter passado de uma infraestrutura monolítica, na primeira geração de SCADA, quando ainda não havia a disponibilidade protocolos de rede relevantes, para uma distribuída, na segunda, com a miniaturização dos sistemas através da microeletrônica e a evolução de tecnologias como LAN. Entretanto, ainda se tratava de um sistema limitado por operar apenas com hardwares e softwares selecionados e disponibilizados pelos fabricantes dos dispositivos e equipamentos da planta (NCS, 2004).

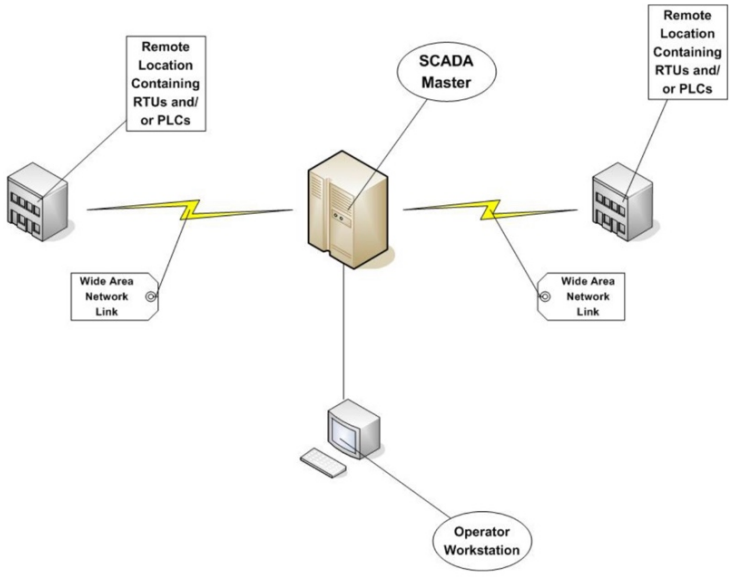
A terceira, e até então última geração de protocolos SCADA, o tornou um sistema com protocolo padrão aberto, através do IEC 61850. Com isso, além de integrar a estrutura de rede local presente no modelo anterior, possibilita que as funcionalidades e dados sejam distribuídos pela WAN. Assemelhando-se ao mencionado na seção 2.2.2, sobre protocolos industriais baseados em RTE, esta geração proporciona a possibilidade de conexão de diversos periféricos,

além de uma melhor integração IT/OT, onde basicamente, os protocolos de comunicação como Ethernet e TCP/IP são capazes de transmitir dados das unidades remotas nas plantas industriais, para uma unidade central que pode estar na fábrica ou em qualquer outro lugar com acesso a rede (NCS, 2004).

4.1.1 Descrição do SCADA *system*

O SCADA system tem em sua arquitetura uma estrutura semelhante a muitos dos sistemas de controle mencionados anteriormente. Apresenta diferentes níveis de processamento, começando pelos dispositivos de processamento distribuídos, como os DCS e os PLC. Estes dispositivos permitem transmitir e processar informação dentro do chão de fábrica. Posteriormente, através dos protocolos e conexões de rede, permite que esses fluxos de dados cheguem as unidades de processamento centralizadas, como os *mainframes*. Neste contexto, vale destacar que esses sistemas são monitorados e controlados através de uma vasta infraestrutura de comunicação LAN/WAN, com protocolos de rede que se adequam aos requisitos e demandas de diversas áreas da indústria (NCS, 2004).

FIGURA 4.1 – Modelo de SCADA System em rede.



Fonte: NCS, 2004.

Segundo a *National Communications Systems*[59] (2004), o SCADA system é composto pelos seguintes elementos:

[59] Do inglês, *National Communications Systems*, é uma organização federal dos EUA, responsável por emitir pareceres técnicos a cerca de infraestruturas de telecomunicações que sejam de interesse nacional.

i. Um computador central SCADA, conhecido como ***Master Terminal Unit (MTU)*** ou *Master Station*, que seria uma unidade central de processamento de dados, capaz de atuar como servidor de todo o sistema e de onde o operador pode ter acesso a todos os dados.

ii. As **Unidades de processamentos remotos (RTU)**[60] , bem como os DCS e PLC, são os dispositivos que atuam no chão de fábrica. Através dos quais se recebe as informações dos sensores para processamento e monitoramento, além de serem capazes de executar comandos, pré-programados ou de um operador, para interagir com os equipamentos através dos atuadores.

iii. Os **sistemas de comunicação** capazes de transmitir os dados de sensores e atuadores no chão de fábrica, até as unidades de processamento distribuídas, e entre estas e a unidade central de processamento do SCADA. Pode ser realizada através de uma rede local, por cabo ou *wireless; e* uma rede WAN, através da internet ou comunicação por satélite.

iv. Os ***softwares****,* que preenchem as camadas de comunicação, além de outros são utilizados como ferramentas para o sistema, como a interface gráfica para interagir com os utilizadores, conhecida como interface homem máquina (HMI)[61].

Uma grande vantagem adquirida através dos sistemas distribuídos em rede é a redundância de sua operação. O processamento distribuído, para diferentes computadores em localidades fisicamente separadas, permite retomar o controle por uma outra unidade que funcione como unidade de processamento secundária, o que para um sistema supercrítico, como um sistema naval, pode ser fundamental. (Parcharidis, 2018).

Como pode-se observar, com a atual geração do SCADA, os sistemas passaram de uma limitada utilização local com as RTU e PLC de operações muito especificas, para uma maior integração das redes com a introdução de protocolos de comunicação. Com isso, os fabricantes passaram a introduzir uma grande gama de dispositivos que operassem com o MTU e outros equipamentos de comunicação através de redes IT, com protocolos como o Ethernet e TCP/IP.

4.1.2 Protocolos de rede do SCADA system

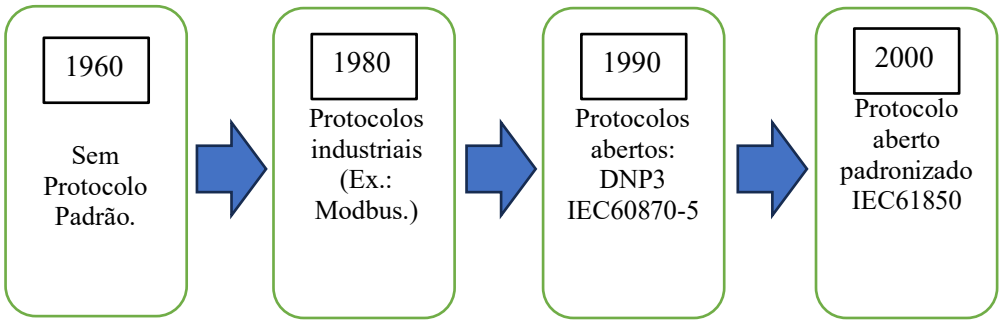
Como observado na arquitetura básica do SCADA system, um computador central que dispõe de um software HMI, associado a vários RTU e PLC distribuídos, irá coletar informações, além de receber e transmitir comandos de controle dos operadores. Os protocolos de comunicação do SCADA é o meio pelo qual esses dados irão transitar, sendo compostos por hardwares, softwares e uma infraestrutura de rede responsáveis por efetuar esta tarefa.

---

[60] Do inglês, *Remote Terminal Unit.*
[61] Do inglês, *Human Machine Interface.*

Segundo Parcharidis (2018), existem três protocolos de comunicação que são os mais comumente utilizados, a depender das características da planta industrial a ser controlada, sendo estes: o IEC 60870-5, normalmente utilizado na Europa; o ModBus e o DNP3, frequentemente utilizado no setor energético.

FIGURA 4.2 – Desenvolvimento dos protocolos de comunicação do SCADA *system*.



Fonte: Elaborado pelo Autor (Yang *et al.*, 2012).

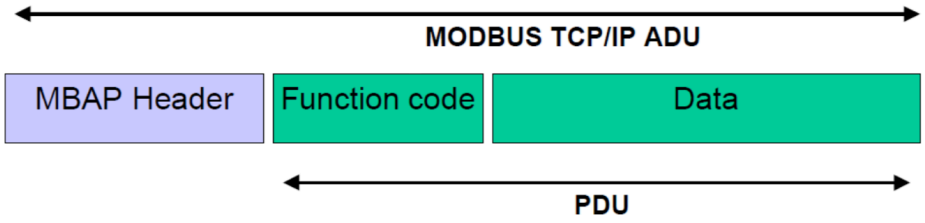
O **IEC 60870-5**, lançado primeiramente em 1995, define o protocolo através de um modelo de três camadas com arquitetura e desempenho aprimorado (EPA)[62], que busca uma implementação eficiente para operar com RTUs, PLC, sensores, relés e outros dispositivos eletrônicos inteligentes (IED)[63]. Adicionalmente, define uma camada de usuário, entre a camada de aplicação do modelo OSI e a execução do *software*, com o objetivo de implementar a interoperabilidade para funções como sincronização e transferência de dados. Entretanto, a transmissão de dados é realizada sem criptografia e sem nenhuma forma de autenticação, com uma arquitetura dependente do TCP/IP, que como dito anteriormente, possui certos problemas de segurança quando aplicado a sistemas OT (NCS, 2004).

O **ModBus**, protocolo desenvolvido pela empresa atualmente denominada *Schneider Electric*, foi criado em 1979, e até 2004 era utilizado em até 40% das aplicações industriais (Parcharidis, 2018). Seu protocolo original é um exemplo de *fieldbus,* que posteriormente sofreu uma extensão para operar com redes *Ethernet,* usando o mecanismo de transmissão de dados do TCP/IP, incluindo roteamento e controle de erros. Na Figura 4.3, pode-se observar a estrutura da unidade de dados de aplicação (ADU)[64] do ModBus TCP/IP, que reúne a camada

[62] Do inglês, *Enhanced Performance Architecture,* é um modelo com três camadas que simplificam a distribuição prevista no modelo OSI em camadas de: aplicação, distribuição e física, ou núcleo.
[63] Do inglês, *Intelligent Electronic Devices.*
[64] Do inglês, *Application Data Unit.*

de aplicação do ModBus (MBAP)[65], com o protocolo de unidade de dados (PDU)[66], que é o pacote de dados transmitido entre dispositivos em uma rede (Zurawski, 2015).

FIGURA 4.3 – ModBus TCP/IP



Fonte: Parcharidis, 2018.

Por fim, **o DNP3** é especificamente desenvolvido para comunicação serial de dispositivos, onde a transmissão de dados vai exclusivamente de um ponto A para um ponto B. Foi criado para permitir a comunicação entre MTU/RTU e RTU/IED, com base no modelo de eficiência do EAP presente no IEC 60870-5, com algumas alterações adicionais para cumprir requisitos voltados para Industria do setor energético. O protocolo foi desenvolvido para otimizar a transmissão de dados adquiridos e comandos de controle, dentro dos seus requisitos de tempo de respostas e sincronismo, de um unidade de processamento para outra, não suportando documentos grandes e processos elaborados, desta forma, sem espaço para sofisticadas implementações de segurança cibernética (NCS, 2004).

4.1.3 Vulnerabilidades dos ICS e SCADA *systems*

Observada a natureza dos principais NCS, tal como as gerações mais recentes do SCADA *system*, nesta seção serão analisadas as características que os tornam alvo de ameaças cibernéticas. Como padrão, a ISO27000[67] (2014) define para tecnologias de informação e comunicação, que ameaças são potenciais causas de incidentes não desejados, que podem vir a causar danos ao sistema ou a organização. Outrossim, as vulnerabilidades, segundo a ISO22399 (2007), são fraquezas de recursos ou controle da qual podem ser exploradas uma ou mais ameaças.

---

[65] Do inglês, *ModBus Application Protocol.*
[66] Do inglês, *Protocol Data Unit.*
[67] Do inglês, *International Organization for Standardization*, ISO refere-se à organização não governamental internacional que desenvolve e publica padrões técnicos de diversos setores, como normas de segurança do trabalho, gestão ambiental, segurança da informação.

Segundo Yang *et al.* (2014), o aumento da interconectividade e integração dos SCADA *systems*, com dispositivos inteligentes de controle e automação na indústria, vem causando uma maior exposição a ameaças, com uma ampla variedade de potenciais portas de entradas a ataques cibernéticos. Um exemplo que se tornou o mais famoso ataque malicioso a uma planta indústria, e será apresentado em um estudo de caso na seção a seguir, ocorreu em julho de 2010, e ficou conhecido como "*Stuxnet worm",* que foi um ataque ao Siemens SIMATIC WinCC SCADA *System*.

No Quadro 4.1 são apresentadas algumas limitações de sistemas de comunicação OT, devido a características presentes nos ambientes dos ICS, que podem vir a reduzir a sua capacidade de reagir contra ameaças no domínio cibernético.

QUADRO 4.1- Limitações de sistemas de comunicações de OT.

Categoria de controle:	**Limitação comuns de OT:**
Controle de Acesso	Fraco controle de acesso a usuários. Pouca, ou nenhuma, classificação de acesso ao usuário.
Dados auditáveis e contáveis	Não possui a habilidade de coletar e armazenar dados para posterior verificação de integridade ou detecção de violação de segurança.
Gerenciamento de configurações	Poucos mecanismos de controle de configurações que limitem o sistema ou sua utilização.
Identificação e autenticação	Não suporta técnicas fortes de autenticação de usuários.
Proteção de comunicação e do sistema	Limitados mecanismos de proteção de dados enquanto estão em comunicação. Pouco, ou nenhum, protocolo ou algoritmo de criptografia.
Integridade de informação e do sistema	Usualmente não oferece suporte que garanta a integridade do sistema. (mecanismos que identifique ações maliciosas que possam prejudicar o sistema).

Fonte: Modificado de Colbert e Kott (2016).

Dentre as limitações apresentadas, destacam-se as que são consequência da pouca memória e processamento reduzido dos ICS, que impossibilitam o suporte adequado a mecanismos eficientes de segurança, como detecção de invasores e *softwares* antivírus para realizar buscas com algoritmos eficientes através dos processos realizados em dispositivos OT. Adicionalmente, características inerentes aos requisitos dos NCS, como tempo de reação e sincronismo, tornam os procedimentos de segurança tarefas que comprometeriam o cumprimento dos seus requisitos de desempenho (Colbert e Kott, 2016).

Os SCADA systems são projetados para funcionar por anos sem serem reinicializados, com limitados recursos de conexão e processamento, além de ter características de não haver

atrasos que prejudiquem a operação do sistema. Outrossim, os sistemas não foram projetados com requisitos de mentalidade de segurança, pois foram desenvolvidos em ambientes que antes eram isolados de redes que oferecessem maiores vulnerabilidades. Consequentemente, com a maior interoperabilidade da terceira geração, observando-se uma maior integração entre seus dispositivos, com redes LAN e WAN, as plantas industriais passaram a estar mais expostas a vulnerabilidades que antes eram quase que exclusividade dos ambientes de IT (Colbert e Kott, 2016).

No Quadro 4.2 é possível observar uma comparação dos requisitos de segurança do SCADA *system* com as comunicações IT.

QUADRO 4.2 – Comparação entre requisitos de segurança do SCADA e IT.

Característica	**SCADA**	**IT**
Disponibilidade	Muito alta	Baixa a moderada
Integridade	Muito alta	Baixa a moderada
Confidencialidade	Baixa.	Alta.
Autenticação	Alta.	Moderada.
Antivírus	Incomum.	Frequente.
Ciclo de vida	15-20 anos.	3-5 anos.
Tempo de reação	Crítico.	Tolera atrasos.
Protocolos	IEC 61850, IEC 60870-5/6, DNP3, Modbus, etc.	TCP/IP, UDP, Ethernet.
Recursos de computação	Limitados.	Ilimitados.
Recursos de segurança	Poucos ou nenhum.	Disponível.
Danos	Impacto econômico. Danos a equipamentos. Danos de pessoal.	Impacto econômico.

Fonte: Modificado de Yang *et al.* (2012).

Os protocolos de comunicação observados anteriormente, como o IEC 60870-5 e DNP3 transmitem dados em texto sem nenhum tipo de criptografia ou mecanismos de autenticação. Seguem o padrão estabelecidos pela nova geração, funcionando com base no TCP/IP, que já possui muitas falhas de segurança em seu tráfego de dados em ambientes domésticos e escritórios. Os protocolos Modbus, que são muito utilizados em diversos setores por

desenvolvedores de NCS, sofrem com vulnerabilidades semelhantes, que criam um ambiente muito suscetível a incidentes de origem maliciosa (Parcharidis, 2018).

Por fim, no Quadro 4.3, segundo Yang *et al.* (2012), demonstra as possíveis consequências de diversos tipos de ataques maliciosos ao SCADA *systems*.

QUADRO 4.3 – Ataques cibernéticos e possíveis consequências ao SCADA system.

Tipo de ataque		**Consequência**
DoS	Interromper serviço.	Desativar o monitoramento ou controle de um sistema crítico; dano ao equipamento; dano de pessoal.
SD	Degradação do serviço.	Reduzir o tempo entre falhas e disponibilidade do equipamento, danos ao equipamento; danos de pessoal.
Invasão	- *Scanner* de IP; e - *Scanner* de porta.	Prejudicar os aspectos de comportamento do sistema. Perda da integridade e confidencialidade, e comprometimento de nós do sistema.
Software malicioso	*Virus, Worms, Trojan horses, Backdoors.*	Pode prejudicar a comunicação entre os equipamentos e seus controladores, reduzindo a eficiência do seu funcionamento.
Spoofing[68]	- *Man-in-the-middle*;[69] - Reenvio de mensagens; e - *Spoofing* de rede.	Pode causar problemas de segurança por introduzir um usuário malicioso. Perda de integridade e confidencialidade.
Furto de senha	Engenharia Social.	As consequências podem ser tão grandes quanto o nível de acesso da senha adquirida. Perda de confidencialidade e do controle de acesso ao sistema.

Fonte: Elaborado pelo autor (Yang *et al.*, 2012)

Desta forma, observa-se que as inúmeras vulnerabilidades apresentadas, devido a peculiaridade da implementação de protocolos de rede industriais baseados em RTE, colocam

[68] Termo, em inglês, utilizado para identificar indivíduos ou programas que falsifica informações para enganar o sistema, dispositivo ou usuário.

[69] Termo, em inglês, que se refere a ataques cibernéticos no qual o atacante se posiciona entre duas partes que estão se comunicando, interceptando ou manipulando os dados para fins maliciosos.

em risco crescente diversas infraestruturas de sistemas críticos que utilizam essas plataformas, inclusive sistemas embarcados. Estas ameaças foram colocadas de lado até o ataque cibernético que será estudado a seguir, o "stuxnet", a partir do qual muitos artigos e trabalhos científicos passaram a abordar, a lacuna de segurança cibernética que por ora se apresenta, em prol de um continuado aumento de produtividade da indústria.

4.2 Estudo de caso: Ataque cibernético "Stuxnet"

O ataque cibernético estudado nesta seção tem como objetivo, em continuidade ao raciocínio que vem se conduzindo, demonstrar em um caso real, as lacunas de segurança cibernética que vem sendo apresentadas em sistemas de controle e seus protocolos de rede. O *Stuxnet worm,* ocorrido em meados de 2010, evidencia o quanto os ICS colocam segurança em segundo plano, dependendo basicamente do isolamento das redes, os *air gaps,* e de controles de acessos, para separar o monitoramento e controle de sistemas críticos, das inúmeras ameaças presentes no domínio digital.

Diferentemente do que se observava até então, em segurança cibernética, o *Stuxnet* não era sobre espionagem de dados, não visou roubar, manipular ou apagar qualquer informação. O ataque tinha objetivo estratégico de destruir fisicamente uma planta de enriquecimento de urânio Iraniana, como um alvo militar. Apesar de seus autores não terem sido oficialmente identificados, o seu nível de sofisticação leva a crer que foi desenvolvido com apoio de nações que tinham interesse no ocorrido, assim como vazamento de informações oficiais dos Estados Unidos e Israel sugerem fortemente que ambos tiveram participação. Fato é que o surgimento deste vírus abriu precedente para que uma nova variedade de ameaças cibernéticas se tornasse relevante no cenário industrial, como o *Duqu*, em 2011, ou o *Flame*, em 2012 (Kushner, 2013).

4.2.1 Descrição do *"Stuxnet worm"*

O *Stuxnet worm* tinha como alvo principal atingir os sistemas de controle industrial, visando modificar o seu código operando nos PLC, para que estes se desviassem do seu comportamento habitual. Seus desenvolvedores introduziram diversos mecanismos para que esses desvios de comportamento passassem por despercebido por seus operadores, com alterações pequenas que só teriam consequências a longo prazo, além de recursos de programação que o fizesse se comportar como parte legitima do sistema, para que não fosse

identificado. A sofisticação do ataque consistia em se aproveitar das lacunas dos já conhecidos mecanismos de segurança dos computadores utilizados na época, para desenvolver um ataque bem planejado e customizado para um sistema de controle específico (Karnouskos, 2011).

O sistema de controle em questão é o *Siemens SCADA systems,* voltado para processos específicos que caracterizem o NCS alvo do ataque. O *Stuxnet* foi desenvolvido para infectar os dados do Siemens WinCC/PC S7 SCADA, um *software* de controle, além de interceptar as comunicações entre o WinCC, do sistema operacional Windows, e os PLC que se relacionam, posicionando-se como o anteriormente descrito no *man-in-the-middle.* Como os sistemas descritos são isolados da rede principal ou internet, o ganho de acesso aconteceu simplesmente de maneira física, através de uma porta USB interna a rede isolada, o que pode caracterizar um baixo nível de treinamento do pessoal, quanto a prevenção de ataques cibernéticos (Karnouskos, 2011).

Segundo Kushner (2013) e Parcharidis (2018), pode-se resumir em seis passos a forma como o *Stuxnet* trabalha:

i. **Infectar:** O *Stuxnet* entra no sistema através de portas físicas USB, além de mover-se por redes LAN disponíveis no interior da infraestrutura, e segue infectando os computadores que utilizam o sistema operacional Windows, por saber se comportar como um dado legitimo do sistema, passa ileso pelas detecções automáticas dos antivírus até atingir os controladores.

ii. **Buscar:** O *Stuxnet* baseia seu ataque em um processo específico controlado pelo sistema de controle Siemens SCADA, neste caso além de buscar pelo código de um sistema de referência, monitora os parâmetros do alvo como frequência, rotação e outras características que funcionam como uma **impressão digital**, atacando apenas o sistema que corresponda a suas especificações. Este método foi tão preciso que não foi reportado seu ataque em nenhuma outra instalação industrial.

iii. **Atualizar:** Caso o sistema não seja o alvo do ataque, nada irá acontecer. Entretanto, caso consiga identificar a planta correta, tentará realizar uma atualização automática, tão logo esteja conectado à internet, ou caso seja identificado uma versão mais atual do seu próprio código, presente em algum outro controlador, com o intuito de confirmar o seu alvo (LANGNER, 2011).

iv. **Comprometer:** Após identificar e confirmar o seu alvo, tem como objetivo comprometer a lógica operacional do sistema de controle, explorando lacunas de

vulnerabilidades como os ***zero day***[70]*,* além de outras deficiências por falta de atualizações, o que demonstra um conhecimento avançado do sistema de controle da planta industrial atacada.

v. **Controlar:** Inicialmente, posicionado como um ***man-in-the-middle***, o vírus espia o comportamento do sistema em questão. Posteriormente, utiliza as informações coletadas para tomar controle das centrífugas, alterando seu comportamento habitual, o que neste caso consistiria em alterar sua rotação, até levá-la a falha.

vi. **Enganar e destruir:** Por fim, com o objetivo de garantir a destruição da planta, pode produzir um *feedback* falso para o controlador, o que impossibilitaria a identificação pelo sistema ou por qualquer operador acompanhando os parâmetros de funcionamento, até que seja tarde demais para se tomar alguma providência.

Em suma, o *Stuxnet worm* foi um vírus de 500 kbytes, que tinha como alvo apenas um sistema de controle específico, o Siemens S7 PLC, e uma vez infectando qualquer computador operando em *Windows* funcionaria de forma a buscar as características deste ICS, até identificá-lo. Uma vez encontrado, carrega o sistema com seu código para monitorar e tomar o controle de maneira apropriada, para destruí-lo sem ser revelado. Caso não seja identificado, permaneceria inativo, que é o caso de mais de 100.000 copias deste que foram encontradas ao redor do mundo. Portanto, por conta do sofisticado código que garantia seu funcionamento preciso, com o objetivo de atingir as centrifugas de enriquecimento de urânio de Natanz, no Irã, leva a crer que tenha sido obra de um ataque estratégico e planejado, orquestrado por interesses de segurança nacional dos EUA, e possivelmente outras nações aliadas, como Israel (Langner, 2011).

4.2.2 Análise Técnica do "*Stuxnet worm"*

Como observado em Karnouskos (2011), apesar de o *Stuxnet worm* ter características extremamente sofisticadas e inovadoras, com estratégias muito especificas para cumprir com seu objetivo estratégico, algumas simples medidas poderiam ter mitigado sua proliferação e comprometimento do ICS. Dentre essas boas práticas, pode-se evidenciar uma infraestrutura projetada em módulos e constantes atualizações visando a incrementação da segurança do sistema. Algumas das vulnerabilidades, *zero days* do sistema, já haviam sido corrigidas em atualizações disponíveis a dois anos, e com base na premissa de "não se toca em um sistema

[70] *Zero Day* é um termo em inglês, que se refere a vulnerabilidades de softwares, estudadas com o objetivo de serem exploradas ou corrigidas, que ainda sejam desconhecidas por seus desenvolvedores (Langner, 2011).

em funcionamento", a segurança foi deixada em segundo plano, em prol da produtividade, o que se torna um fator de risco para qualquer ameaça que busque explorar essas fraquezas já conhecidas.

Para sistemas OT, com ciclos de vida longos que podem chegar a mais de 10 anos de operação ininterrupta, como observado na seção de protocolos de rede industrial, as atualizações são muitas vezes deixadas de lado, pois seus efeitos colaterais podem levar a produção a ter um *delay* indesejado. Outrossim, quando se analisa os PLC e DCS, por se tratar de sistemas com processamento completamente dedicado a suas tarefas operacionais, percebe-se que seus recursos deficientes de segurança e verificação do sistema, os tornam um elo fraco da infraestrutura de uma planta industrial. Apesar das vulnerabilidades apresentadas, o que claramente se mostrava a favor, da negligência da segurança, era a condição de sistema isolado de uma rede externa, além de medidas padrões de controle de acesso e antivírus capazes de detectar assinaturas conhecidas de alguma ameaça (Karnouskos, 2011).

Segundo Langner (2011), após discussão técnica das vulnerabilidades apresentadas por sistemas de controle industriais, como o SCADA System, uma possível solução seria monitorar as alterações dos controladores através de uma constante verificação dos seus códigos e integridade de suas configurações. Como as unidades de processamento dos controladores estão completamente comprometidas com sua atividade fim, seria necessário que algum outro computador fosse adicionado a infraestrutura com a tarefa dedicada de se analisar suas características essenciais, com um mecanismo semelhante ao do próprio *Stuxnet worm,* através de verificação da impressão digital do sistema, permitindo que fosse reportado ao operador ou desenvolvedor, qualquer alteração na impressão digital que venha a comprometer ICS. Entretanto, como pode-se imaginar, qualquer modificação da estrutura original de uma planta industrial seria extremamente dispendiosa, e mecanismos sofisticado de segurança possuem alto valor agregado, que geralmente não são vistos como prioridade.

5 SIMULAÇÃO DE ATAQUE CIBERNÉTICO A PLANTA PROPULSORA

Neste capítulo, será proposta a simulação de um ataque cibernético a um NCS, baseado em RTE. O ataque trata-se de uma adaptação do desenvolvido em De Sá *et al.* (2017) e Ferrari *et al.* (2020), que busca explorar as vulnerabilidades dos protocolos de rede industriais RTE, com técnicas furtivas, ou seja, que tenham a capacidade de ser realizada, sem ser identificada pelo operador ou mecanismos de segurança do sistema. Com o objetivo de trazer o experimento o mais próximo da realidade, foi utilizado um modelo de sistema de controle e propulsão de um navio militar, proposto por Whalley e Ebrahimi (2002), que se trata de um sistema MIMO. A seguir serão abordados uma descrição do ataque e seus componentes, modelagem do sistema e resultados da simulação de ataque.

5.1 DESCRIÇÃO DO ATAQUE

Conforme demonstrado nos capítulos anteriores, os protocolos *Real-Time Ehernet*, utilizados na indústria, não foram desenvolvidos levando a segurança com uma de suas prioridades. Um dos maiores problemas desses protocolos é a lacuna de autenticação entre seus principais elementos dos sistemas de controle e automação, bem como a falta de algum nível de criptografia no seu tráfego de dados. Com base nessa premissa, um ataque cibernético como o proposto deve ser dividido em certas fases, como as definidas a seguir: ganhar acesso a rede; aprender o comportamento do NCS através da coleta de dados; e elaborar um ataque discreto que cause a degradação do sistema (Ferrari *et al.*, 2020).

Dentro desta perspectiva, os objetivos desta simulação e análise de ataque cibernético podem ser descritos conforme a seguir:

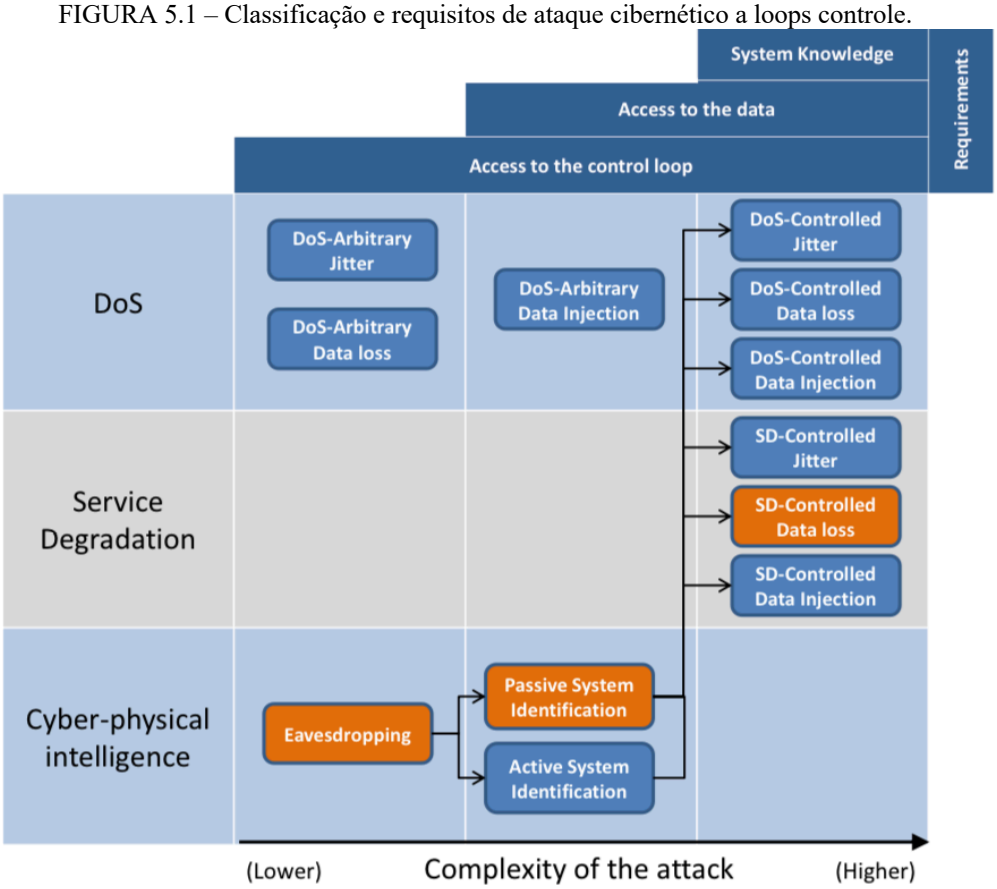
i. Apresentar um método de ataque capaz de realizar uma degradação de Serviço (SD) das respostas do sistema de controle, com o intuito de ser discreto, sem causar interrupção no mecanismo de comunicação do NCS ou qualquer extrapolação dos limites críticos da planta, que a levaria a uma parada forçada;

ii. Introduzir uma estratégia de ataque, de acordo com Ferrari *et al.* e De Sá *et al.* (2020), em que o código de ataque tenha a capacidade de aprender de maneira dinâmica a modelagem do NCS. Além de elaborar um ataque inteligente com base na perda de pacotes de dados de maneira limitada, causando uma interferência na resposta transitória e permanente do sistema.

Desta forma, caracteriza-se por um ataque Controlado de Degradação do Serviço. Conforme ilustrado anteriormente no Quadro 2.4.

iii. Demonstrar como é possível *hackear* um sistema de controle, com dados trafegando em tempo real, de forma a manipular o comportamento da planta, e podendo levá-la a uma redução do MTBF ou até mesmo a uma condição de perigo iminente.

FIGURA 5.1 – Classificação e requisitos de ataque cibernético a loops controle.



Fonte: Ferrari *et al.*, 2020.

Portanto, o principal objetivo do ataque é causar uma degradação no serviço performado pela planta. A simulação proposta irá utilizar um **SD-Controlled Data loss**, que conforme demonstrado na Figura 5.1, demanda uma ação preliminar de Espionagem e Identificação passiva do Sistema (PSI)[71]. Os estágios de PSI e SD usam um algoritmo meta-heurístico[72] bio-inspirado, o ***Backtracking Search Optimization Algorithm (BSA)***, que permite ao ataque aprender sobre o modelo do NCS, e decidir de maneira inteligente quais pacotes de dados deverá perder, para causar a interferência desejada (Ferrari *et al.*, 2020).

[71] Do inglês, *Passive System Identification.*
[72] Meta-heurística é um modelo para resolver problemas de otimização complexos, são estratégias para guiar a busca de soluções numéricas para problemas, independentemente de se conhece-lo .

5.1.1 Backtracking Search Optimization Algorithm

O *Backtracking Search Optimization Algorithm,* é um Algoritmo Evolucionário (EA)[73] para solução de problemas de otimização numérica, com valores reais. Os EAs são ferramentas amplamente conhecidas para a resolução de problemas matemáticos que envolvam equações não lineares, não diferenciáveis e numericamente complexas, característica intrínseca de sistemas de controle complexos e robustos (Xu e Gen, 2010). Segundo Civicioglu (2013), o desenvolvimento do BSA busca mitigar efeitos que são tipicamente encontrados em outros EAs, como não ser extremamente sensível aos seus parâmetros iniciais, estrutura simples que se adapta a diferentes otimizações numéricas e processamento lento.

O primeiro passo para se resolver um problema de otimização numérica, é determinar uma **função objetivo**, a partir da qual irá se estabelecer uma relação entre os parâmetros do sistema real e as limitações impostas pelo projeto do sistema. Em um sistema de controle robusto, por várias razões, o sistema real pode tomar formas não lineares, não diferenciáveis e complexas, podendo estar suscetível a ruídos e variações internas de seus parâmetros de projeto. Para resolução de problemas como este, os EAs procuram por um ótimo global, para otimização de um problema de ordem numérica, este processo é chamado de **otimização global** (Civicioglu, 2013).

Segundo Xu e Gen (2010), os algoritmos de otimização, possuem três características principais:

i. São baseados em **populações**, que são seu conjunto de soluções usados no processo de aprendizagem ou otimização;

ii. Dentro da população, cada solução é chamada de **indivíduo**, que por sua vez possui uma representação genética, que é seu código. Cada individuo tem sua aptidão testada, no seu desempenho para solução do problema, de forma a selecionar o mais apto. Essa convergência é a base da otimização do algoritmo; e

iii. A mutação é o processo de variação a que cada individuo é orientado, simulando as mudanças genéticas, e encontrando novas soluções.

O algoritmo proposto para esta simulação, o *Backtracking Search Optimization Algorithm*, possui um mecanismo único para geração de um individuo para teste, que possibilita a resolução do problema de otimização numérica de maneira mais eficiente e rápida, poupando

[73] Do inglês, ***Evolutionary Algorithm***, são algoritmos baseados na Teoria da Evolução de Darwin, com capacidade de realizar otimizações ou aprender tarefas. (Civicioglu, 2013)

recursos computacionais. O BSA usa três operadores genéticos - seleção, mutação e *crossover* - para com isso gerar o individuo de teste (Civicioglu, 2013).

FIGURA 5.2 – Estrutura geral do BSA.

```
1. Initialization
repeat
    2. Selection-I
    Generation of Trial-Population
        3. Mutation
        4. Crossover
    end
    5. Selection-II
until stopping conditions are met;
```

Fonte: Civicioglu, 2013.

Neste trabalho, o EA foi utilizado na simulação como parte do código da ameaça cibernética. O *SD-Controlled Data loss* demanda uma ação preliminar de identificação dos pacotes de dados a serem desviados, para que se obtenha uma degradação controlada do serviço. Com isso, o processo de otimização de busca do BSA é fundamental para analisar os dados entre o sistema de controle e a planta propulsiva, a fim de produzir o comportamento malicioso demandado.

Outra utilidade do algoritmo, que não será explorada neste trabalho, seria sua utilização como parte do código de identificação do sistema (PSI), conferindo grande portabilidade ao ataque ao passo que esse pode vir a se adaptar às características do alvo. Paralelamente, através da comparação do fluxo de dados espionado do sistema, com um modelo estimado de referência (a função objetivo), pode-se convergir a uma aproximação das variáveis internas do sistema de controle. Esses dois processos serão descritos na seção a seguir.

5.1.2 Identificação Passiva do Sistema (PSI)

Apesar de esta etapa do CPI não compor a simulação proposta, esta seção, para fins didáticos, demonstra brevemente como o BSA pode dar suporte ao Ataque de Identificação Passiva do Sistema de controle proposto. O objetivo principal do ataque PSI é estimar as funções de transferência do sistema de controle e da planta propulsiva ($\hat{y}(k)$), e o seu *delay* (d), correspondente a conversão A/D do sinal, através do fluxo de dados do seus *Feedback* e *Forward.* Para identificar o modelo da planta, o PSI utiliza os dados espionados da entrada ($u(k)$), do controlador ou da planta propulsiva, e os dados de saída ($y(k)$) (Ferrari *et al.*, 2020).

$$\hat{y}(k) = \mathcal{Z}^{-1}\left\{\frac{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0}{b_m z^m + b_{m-1} z^{m-1} + \cdots + b_1 z + b_0}\right\} * u(k-d)\,. \tag{5.1}$$

Na equação 5.1, pode-se observar o sinal de entrada sendo aplicado a equação estimada, com isso o PSI ajusta os valores dos coeficientes $(a_n, a_{n-1}, \ldots, a_1, a_0, b_m, b_{m-1}, \ldots, b_1, b_0)$ de forma a fazer o valor de $\hat{y}(k)$ convergir para $y(k)$. Desta forma, o BSA é utilizado para ajustar interativamente os parâmetros da equação, a fim de minimizar a função de aptidão ($f_{p,j}$), como pode ser observado abaixo:

$$f_{p,j} = \frac{\sum_{k=1}^{V}[y(k) - \hat{y}_j(k)]^2}{V}\,. \tag{5.2}$$

Na equação 5.2, cada indivíduo da população do BSA é identificado por um número de referência (j), a coordenada p_j $(d_j, a_{n,j}, a_{n-1,j}, \ldots, a_{1,j}, a_{0,j}, b_{m,j}, b_{m-1,j}, \ldots, b_{1,j}, b_{0,j})$ correspondem aos valores que cada indivíduo carrega como solução para o modelo estimado $(\hat{y}_j(k))$. Ao longo do processo, cada um deles tem sua aptidão avaliada na função, onde V é o total de amostras durante um período T de monitoramento. Este processo é realizado para as funções de transferência do sistema de controle e a da planta propulsiva, dando origem a duas funções de mínimo global, uma para cada malha, a fim de resultar nas equações que descrevem toda a malha do sistema (Ferrari *et al.*, 2020).

5.1.3 Ataque de Degradação do Sistema *(SD-Controlled Data Loss)*

O ataque *SD-Controlled Data Loss* proposto foi projetado para produzir uma interferência maliciosa no comportamento de uma planta propulsiva, a partir da perda controlada de pacotes de dados, por sua vez causada pela adição de pacotes mau formados no fluxo de controle e de *feedback*. Destaca-se que para um ataque SD, seja o processo do PSI ou a seleção inteligente dos dados a serem desviados, são ações preliminares fundamentais para se evitar a perda indiscriminada de amostras, que poderia vir a causar uma completa interrupção das comunicações do NCS.

Adicionalmente, existem diversas possíveis estratégias para se realizar uma degradação do serviço em uma planta de sistema de controle e automação, como pode-se observar a seguir:

i. Através de uma alteração na resposta transitória, como um aumento do *overshooting* do sistema. Desta forma, o sistema pode vir a alcançar índices acima dos previstos, gerando desgaste mecânico dos seus componentes (De Sá *et al.*, 2017);

ii. No regime permanente, introduzir um erro estacionário, com isso o sistema não atingiria o seu ponto ótimo de operação, reduzindo eficiência e aumentando o desgaste (De Sá *et al.*, 2017)

iii. Por fim, a estratégia selecionada como método deste trabalho, que é fazer com que o sistema alcance a sua estabilidade (regime permanente) em um tempo mais curto. Com esta alteração, a resposta transitória será modificada em alguns aspectos, como causar uma aceleração excessiva na planta, podendo causar danos semelhantes ao do *overshooting*.

A escolha por esse método será discutida na seção a seguir, quando forem apresentadas as características da planta propulsiva a ser atacada. Por ora, com relação a estratégia proposta, ressalta-se que a aceleração da planta propulsiva será causada pela perda de amostras especificas dos pacotes de dados que flui através dos *forwards* e *feedbacks* do NCS.

Conforme mencionado na seção 2.2.1, em protocolos de rede industriais de tempo real, durante o fluxo de dados dos *loops* de controle, a frequência de amostragem é tão elevada, que ao se perder um determinado dado, o sistema não tem tempo hábil para refazer essa amostragem e entregar ao processamento. Desta forma, será mantido o estado anterior da variável em questão, até que um outro dado mais atualizado seja entregue ao destino (Zurawski, 2015). Com isso, para encontrar as amostras que devem ser perdidas para se chegar à aceleração desejada para o sistema, o BSA pode ser mais uma vez utilizado, conforme anteriormente no ataque PSI.

Com a característica descrita, pode-se assumir que quando um pacote contendo a amostra $s(k)$ é desviado, o protocolo de rede utiliza a variável anterior, mais atualizada. Com isso, considerando uma sequência $S = \{s(k), s(k+1), \dots, s(k+h-1)\}$, com h amostras, a qual o algoritmo irá selecionar os que devem ser perdidos de forma a causar o comportamento malicioso desejado (Ferrari *et al.*, 2020).

Desta forma, utiliza-se um mecanismo de formar uma palavra ataque de h bits, conforme $W = \{b_0, b_1, \dots, b_{h-1}\}$, usada para indicar quais amostras da sequência S serão desviadas. Como os bits, só podem assumir valores binários de 0 e 1, por definição as amostras desviadas assumiram valor 0, enquanto as preservadas assumem valor 1. Considera-se que o ataque poderá ser realizado a ambos os fluxos de dados do *loop* de controle, *forwards* e *feedbacks,* devendo para solução haver as palavras W_{fw} e W_{fb}, respectivamente (Ferrari *et al.*, 2020).

Neste contexto, considerando que a função de controle, a função de transferência da planta e os *delays* de comunicação foram adquiridos pelo ataque PSI, quando se obtiver os parâmetros de $\hat{y}(k)$, será definida uma função de aptidão, ou objetivo, $(f_{p,j})$ para alcançar o comportamento malicioso desejado (Ferrari *et al.*, 2020).

A função de aptidão pode introduzir diversas condições para se avaliar se a reposta desejada é apta ou não para se obter o comportamento desejado. Neste trabalho, visando simular o comportamento do BSA na identificação dos pacotes a serem desviados para orientar o *SD-Controlled Data Loss*, a função $f_{p,j}$ será definida a partir do comportamento da reposta da função de transferência de malha fechada. Com isso, na próxima seção, a partir da modelagem do sistema de controle da planta propulsiva, proposto por Whalley e Ebrahimi (2002), será possível observar as principais características da resposta do sistema, e definir a parametrização do objetivo do ataque.

5.2 MODELAGEM DO SISTEMA DE CONTROLE ATACADO

Em Whalley e Ebrahimi (2002), o modelo de um sistema de propulsão com turbina a gás e hélice de passo controlado[74] voltado para um navio de guerra é proposto. O sistema forma uma configuração multivariável, em que qualquer entrada nos atuadores de fluxo de combustível e ângulo de passo do hélice, pode vir a alterar as saídas velocidade do eixo e torque no propulsor mutualmente. Para fins de modelagem, o sistema de controle, que tem características de MIMO, é assumido como linear, finito e invariante no tempo, de forma a poder ser analisado através de Laplace, conforme observado na seção 2.1.2.

Destaca-se que para a verificação das modelagens a seguir, serão utilizados os softwares MATLAB e sua extensão SIMULINK, de forma a permitir otimizar a representação e análise das repostas da planto do sistema de propulsão.

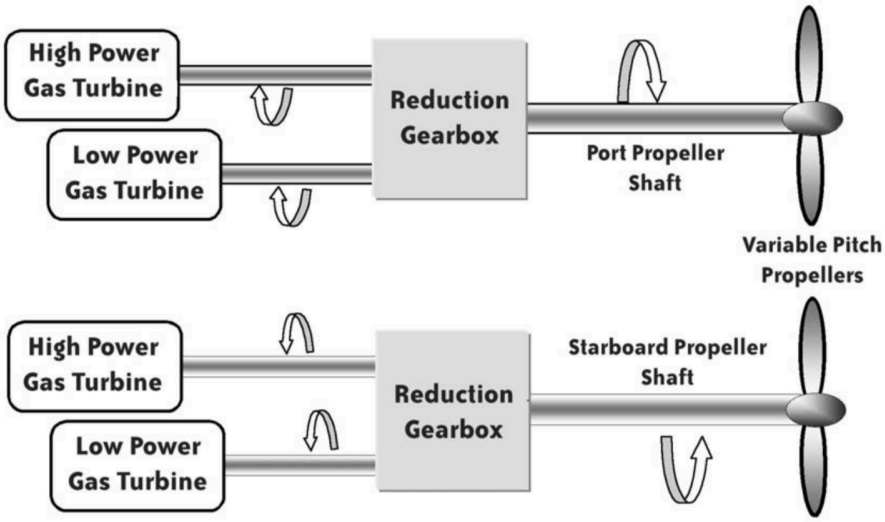
5.2.1 Representação esquemática do Sistema de Propulsão

Na seção 2.1.2 foram estabelecidos alguns critérios voltados para a modelagem e análise de um sistema de controle. Dentre os tópicos abordados estavam a descrição do sistema físico

[74] O modelo de sistema de propulsão proposto é amplamente utilizado por navios de guerra que demandem altas velocidades e grande flexibilidade. As turbinas a gás fornecem uma propulsão com alta entrega de potência ao eixo, enquanto o hélice de passo controlado, permite maior flexibilidade. Com a alteração do passo do hélice permitisse modificar o torque resultante, e com ele a velocidade do navio, sem precisar alterar a rotação do eixo.

e sua representação esquemática, na Figura 5.3 é ilustrado, inicialmente, a estrutura básica da planta de propulsão de um navio de guerra.

FIGURA 5.3 – Planta de propulsão de um navio de guerra.



Fonte: Whalley e Ebrahimi, 2002.

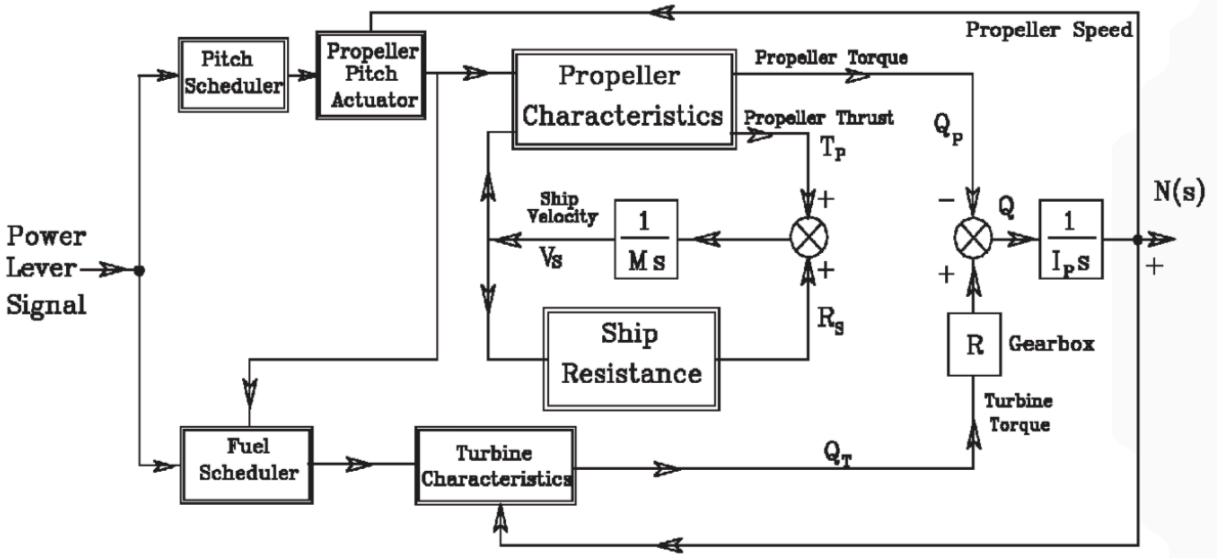
Segundo Whalley e Ebrahimi (2002), muitos navios de guerra utilizam sistemas de propulsão com dois eixos, ambos com um conjunto propulsor de Turbina a gás, eixo e hélice de passo controlado (HPC), um a bombordo e outro a boreste. Cada um dos eixos tem sua propulsão independente através da engrenagem redutora, que proporciona atender a requisitos velocidade e flexibilidade, além de essa configuração permitir um certo grau de redundância.

Na Figura 5.4, observa-se uma configuração do modelo do sistema de propulsão de um único eixo, através de um diagrama de blocos capaz de demonstrar as entradas e saídas dos principais blocos responsáveis pelo funcionamento do conjunto turbina e hélice de passo controlado (HPC). A configuração demonstra um sinal de controle único, que se distribui como um sinal do seletor do passo (*Pitch Scheduler*) e um sinal de seletor de fluxo de combustível (*Fuel Scheduler*).

O *Pitch Scheduler,* responsável por alterar o ângulo do passo do HPC, pode aumentar ou reduzir o ângulo de ataque da pá do hélice, o que produz uma alteração nas características do propulsor. Esta alteração causa um aumento ou redução no torque do eixo (*Propeller Torque*) e empuxo (*Propeller Thrust*). Paralelamente, o *Fuel Scheculer* altera a quantidade de combustível injetado na Turbina. Por característica as turbinas a gás produzem alta rotação e baixo torque, portanto em propulsões navais, são utilizadas engrenagens redutoras (*Reduction*

Gearbox) capazes de se reduzir a rotação e aumentar o torque entregue pelo propulsor através do eixo.

FIGURA 5.4 – Configuração do modelo do sistema de propulsão.



Fonte: Whalley e Ebrahimi, 2002.

Por um lado, o Torque do propulsor (Q_p) torna-se fruto de uma característica mecânica do posicionamento do ângulo de ataque das pás do HPC, que atua sobre o navio, enquanto o Torque da engrenagem (Q_G) é uma energia mecânica gerada pela turbina do navio, e atua sobre o eixo do propulsor. Portanto, no esquema apresentado ambos terão sinais opostos na variação de torque resultante no eixo (Q). A variação de velocidade de rotação do eixo ($N(s)$) é diretamente proporcional a variação de torque no eixo, que como visto anteriormente, pode ser causada pelo aumento do fluxo de combustível ou pela alteração do passo do hélice.

Um aumento no fluxo de combustível, ocasiona um aumento em Q_G, que por sua vez aumentará a rotação do eixo ($N(s)$), devido a um aumento na variação do torque resultante (Q). O aumento de $N(s)$ causa aumento na velocidade do navio (V_S), que é uma informação de entrada que altera a característica do eixo do propulsor, gerando um aumento no torque Q_p, até igualar o valor de Q_R, fazendo com que o resultante Q se estabilize e consequentemente a variação de $N(s)$ também.

De forma a descrever as dinâmicas da configuração apresentada na Figura 5.4. O modelo de sistema linearizado de Whalley e Ebrahimi (2002), descrito abaixo, permitirá uma melhor modelagem da planta propulsora. A matriz $\boldsymbol{G(s)}$ possui em seus elementos as funções de transferência que descrevem o funcionamento da planta. Sendo $\boldsymbol{u(s)}$ o vetor de entrada,

composto pelo ajuste do passo ($\phi(s)$) e variação do fluxo de combustível ($f(s)$)), e $\boldsymbol{y(s)}$ o vetor de saída**,** composto pela variação de rotação do eixo ($N(s)$)[75] e variação de torque no eixo ($Q(s)$)[76].

$$\boldsymbol{y(s) = G(s)u(s)} \tag{5.3}$$

Onde:

$$\boldsymbol{y(s)} = (N(s), Q(s)) \text{ e } \boldsymbol{u(s)} = \big(f(s), \phi(s)\big). \tag{5.4}$$

Dando prosseguimento aos passos para modelagem e análise de sistema de controle, da seção 2.1.2., será apresentado a seguir os parâmetros que definem $\boldsymbol{G(s)}$ e demonstrada as informações que podem ser inferidas a partir da Função de Transferência do sistema de propulsão. Outrossim, será possível esquematizar um arranjo referente a função de transferência de malha aberta, para uma análise das respostas do sistema, com base em entradas degrau unitário.

5.2.2 Função de transferência e diagrama de blocos da planta propulsiva

Como observado acima, o sistema de propulsão de um navio apresenta um certo grau de complexidade, com múltiplas entradas e múltiplas saídas, além de diversas variáveis internas que podem interferir na resposta da planta. Para reduzir a complexidade do sistema de equações que descrevem o funcionamento da planta, será descrito abaixo o modelo linearizado do sistema de propulsão, segundo Whalley e Ebrahimi (2002), já tendo sido realizada a sua simplificação e representação através do domínio de Laplace.

$$\boldsymbol{G(s)} = \\ \frac{\boldsymbol{\sigma^2 + \omega^2}}{\boldsymbol{\tau_1\left(s + \frac{1}{\tau_1}\right)((s-\sigma)^2 + \omega^2)}} \begin{bmatrix} \boldsymbol{k_{11}(1 + T_2 s)} & \cdots & \boldsymbol{k_{12}\dfrac{(1 + Ts)(1 + T_1 s)}{(1 + T_4 s)}} \\ \vdots & \ddots & \vdots \\ \boldsymbol{k_{21}(1 + T_3 s)(1 + T_4 s)} & \cdots & \boldsymbol{k_{22}\dfrac{(1 + T_1 s)}{(1 + T_4 s)}} \end{bmatrix} \tag{5.5}$$

[75] **A curva N(t)** descreve a variação da rotação no tempo, e é um valor adimensional por ser a razão da rotação do eixo pela rotação máxima do eixo a plena carga **($\frac{N}{N_{max}}$).**

[76] **A curva Q(t)** descreve a variação do torque no eixo no tempo, e é um valor adimensional por ser a razão do torque no eixo pelo torque máximo a plena carga **($\frac{Q}{Q_{max}}$).**

$$\boldsymbol{G(s)} = \begin{bmatrix} \boldsymbol{g_{11}(s)} & \cdots & \boldsymbol{g_{12}(s)} \\ \vdots & \ddots & \vdots \\ \boldsymbol{g_{21}(s)} & \cdots & \boldsymbol{g_{22}(s)} \end{bmatrix} \tag{5.6}$$

A equação 5.6 representa os termos da função de transferência de malha aberta. Como pode ser observado, por se tratar de um sistema MIMO, a representação se dá através da matriz $\boldsymbol{G(s)}$. A Tabela 5.1 apresenta os parâmetros estabelecidos para a máxima potência da planta propulsora.

TABELA 5.1 – Parâmetros da função de transferência malha aberta.

$\boldsymbol{\tau_1}$	$\boldsymbol{\sigma}$	$\boldsymbol{\omega}$	$\boldsymbol{\tau_4}$	$\mathbf{T_1}$	$\mathbf{T_2}$	$\mathbf{T_3}$	$\mathbf{T_4}$	$\boldsymbol{k_{11}}$	$\boldsymbol{k_{12}}$	$\boldsymbol{k_{21}}$	$\boldsymbol{k_{22}}$
10.9	-1.22	0.359	0.69	19.7	7.3	12.7	0.61	0.4013	-0.2472	0.9471	0.236

Fonte: Elaborado pelo autor (Whalley e Ebrahimi, 2002).

Primeiramente, a parametrização permite que seja observado os polos e zeros das funções de transferência da matriz. Percebe-se que para efeitos de estabilidade, todos os polos possuem parte real negativa, e há uma característica oscilatória representada pelos termos dos polos de uma equação característica de segunda ordem ($\boldsymbol{(s-\sigma)^2+\omega^2}$**).** Onde σ é a parte real negativa que irá atenuar o sinal e $\boldsymbol{\omega}$ é a frequência de oscilação amortecida, que posteriormente será utilizada para análise do sinal digitalizado.

Na Tabela 5.2 são apresentadas as funções de transferência referente aos elementos da matriz $G(s)$, com os valores estabelecidos como parâmetros anteriormente.

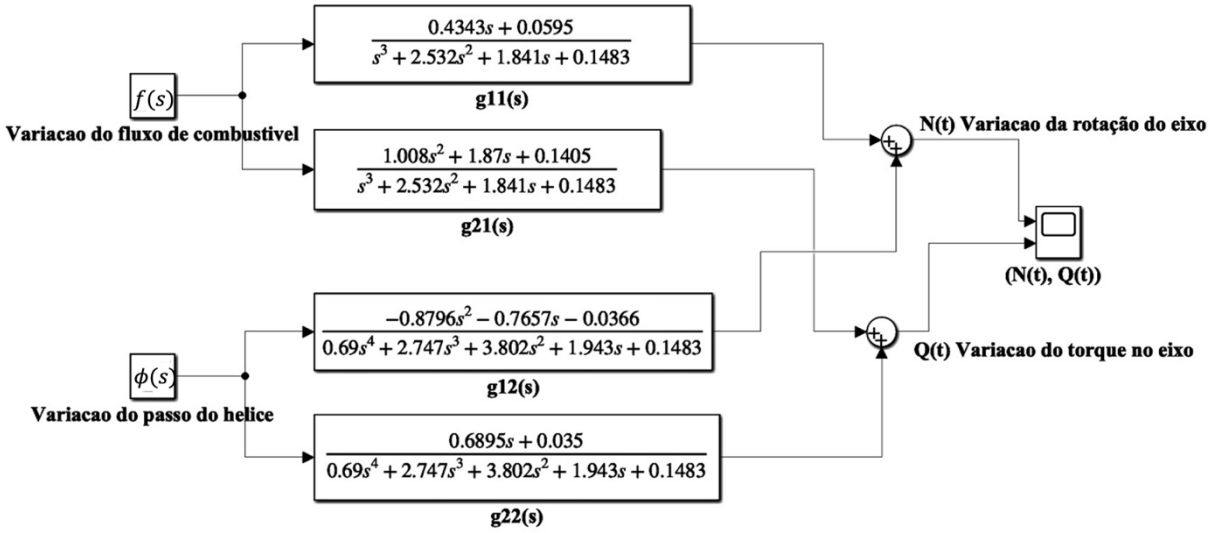
TABELA 5.2 – Elementos da matriz $G(s)$.

Elemento	**Função de Transferência**
$\boldsymbol{g_{11}(s)}$	$\dfrac{0.4343s + 0.0595}{s^3 + 2.532s^2 + 1.841s + 0.1483}$
$\boldsymbol{g_{12}(s)}$	$\dfrac{-0.8796s^2 - 0.7657s - 0.0366}{0.69s^4 + 2.747s^3 + 3.802s^2 + 1.943s + 0.1483}$
$\boldsymbol{g_{21}(s)}$	$\dfrac{1.008s^2 + 1.87s + 0.1405}{s^3 + 2.532s^2 + 1.841s + 0.1483}$
$\boldsymbol{g_{22}(s)}$	$\dfrac{0.6895s + 0.035}{0.69s^4 + 2.747s^3 + 3.802s^2 + 1.943s + 0.1483}$

Fonte: Elaborado pelo autor (Whalley e Ebrahimi, 2002).

Com isso, o arranjo estabelecido em Whalley e Ebrahimi (2002), ilustrado na Função de Transferência de Malha Aberta (FTMA) da Figura 5.5, foi implementado no MATLAB, com auxílio da ferramenta SIMULINK como pode-se observar abaixo:

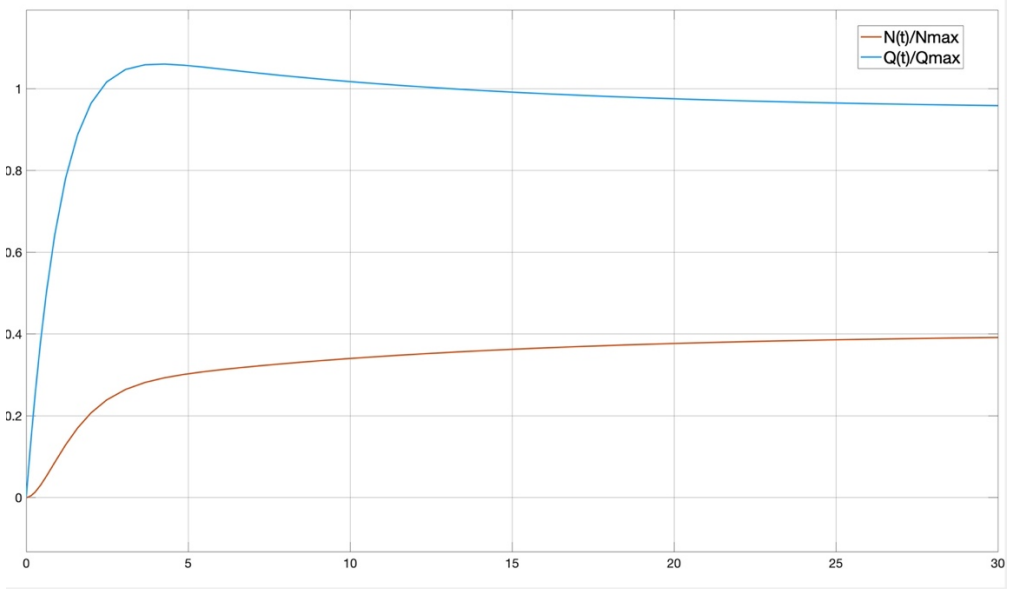
FIGURA 5.5 – Função de Transferência de Malha Aberta (FTMA) de $G(s)$.



Fonte: Elaborado pelo autor.

Com este modelo, permite-se que seja analisado os sinais de entrada individualmente, ou seja, os sinais de saída $(\boldsymbol{N(s)}, \boldsymbol{Q(s)})$ terão respostas a partir de uma entrada degrau em cada uma das entradas, primeiro $f(s)$ e posteriormente $\phi(s)$. Nas figuras 5.6 e 5.7, pode-se observar as respostas ao degrau unitário da FTMA, a primeira com a entrada na demanda de fluxo de combustível, enquanto a segunda no ângulo do passo.

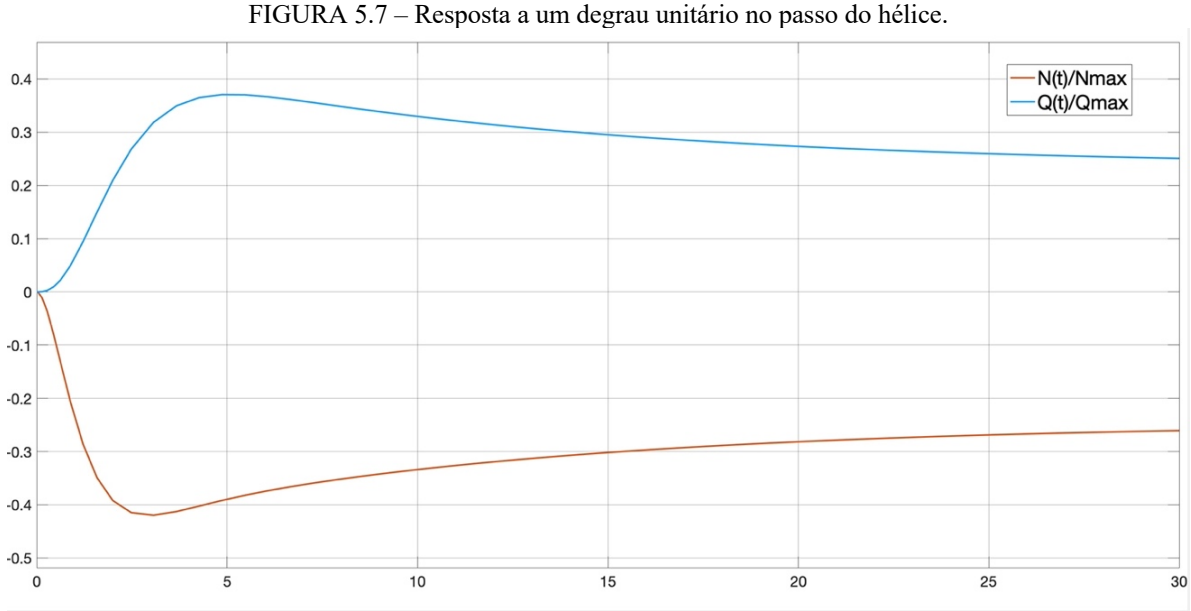
FIGURA 5.6 – Resposta a um degrau unitário no fluxo de combustível.



Fonte: Elaborado pelo autor.

Conforme analisado na representação esquemática, ao receber o aumento no fluxo de combustível a turbina acelera, o que ocasiona um aumento do torque da turbina, passando pela engrenagem redutora. O aumento do torque resultante gera um aumento na rotação, que por sua vez aumenta o torque no hélice, até que se equilibrem as forças resultantes.

FIGURA 5.7 – Resposta a um degrau unitário no passo do hélice.



Fonte: Elaborado pelo autor.

Comparando com a Figura 5.7, conforme esperado, observa-se que ao se incrementar o ângulo do passo, ocorre uma redução na rotação do eixo. Isto ocorre, pois, ao deslocar um maior volume de água, o eixo sofrera um aumento da carga, que será transmitida a turbina através da engrenagem redutora, com isso o torque da turbina irá aumentar, até que as forças entrem em equilíbrio novamente.

Conforme observado por Whalley e Ebrahimi (2002), as respostas ao degrau unitário apresentam um aumento considerável e rápido no valor do torque, para qualquer uma das entradas, o que demonstra que o sistema possui uma reposta sensível de $Q(t)$ em ambos os casos. Esta característica corrobora com o objetivo do ataque, apresentado na seção 5.1.3, pois ao tentar reduzir o tempo de estabilização do sistema da rotação do eixo, pode-se gerar um torque elevado, tendo em vista sua interação mútua.

Na seção a seguir será proposto uma malha de controle modelada para o sistema de propulsão de forma a otimizar o seu funcionamento. Com isso, será possível observar seu diagrama de blocos para um sistema de controle de malha fechada, proporcionando maiores análises da resposta da planta.

5.2.3 Modelagem do sistema de controle

O *design* do sistema de controle foi desenvolvido levando em consideração as interferências mútuas encontradas em um sistema MIMO, observadas anteriormente a partir da FTMA, com variação do fluxo de combustível e alteração do passo do hélice. Apesar de possuir uma resposta incialmente rápida de torque, faz-se necessário um controle que consiga oferecer um tempo de estabilização menor, bem como redução de oscilações no transitório para atingir a demanda de maneira mais eficiente. Para tal, sua otimização foi estabelecida com os seguintes requisitos como base (Whalley e Ebrahimi, 2002):

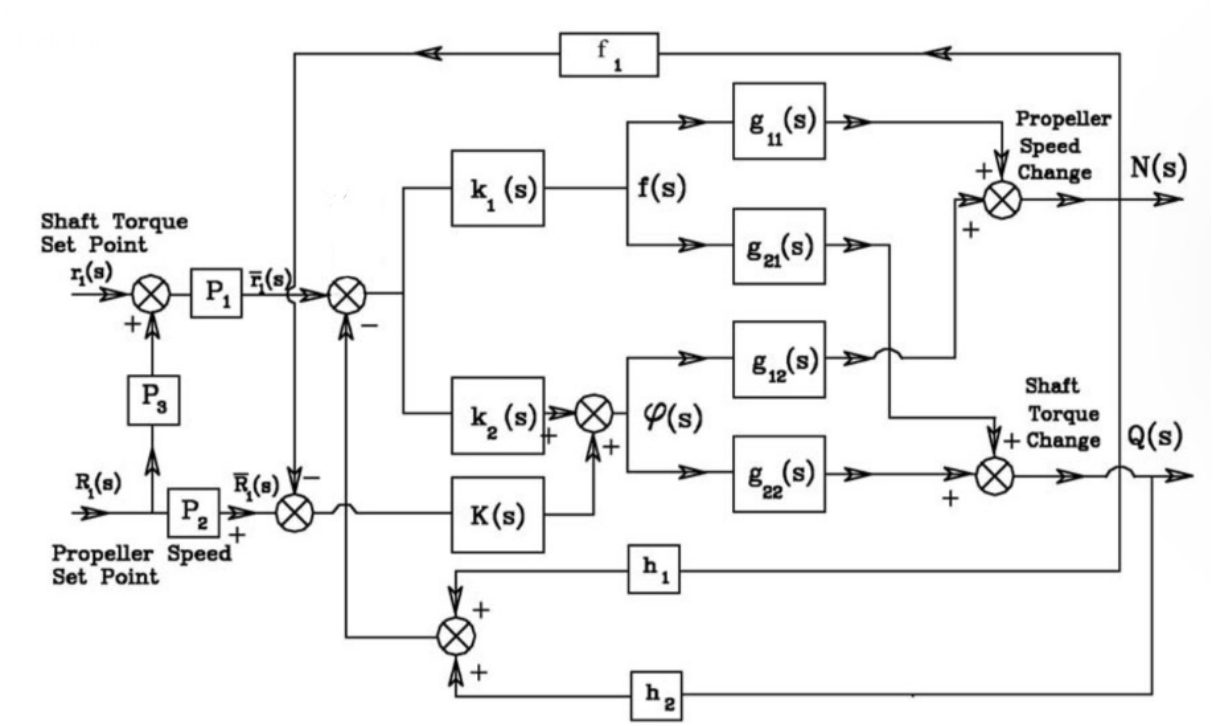
i. A rotação do eixo deverá atingir 90% do seu regime estacionário em aproximadamente 15 segundos;

ii. Redução dos efeitos transitórios apresentados nas respostas de FTMA, como a sensibilidade do torque do eixo as entradas e atenuação do efeito de pico do *overshooting*; e

iii. Utilização de um controle de mínimo esforço, de forma a reduzir o custo na confecção da malha de controle.

Como o foco deste trabalho não está no *design* de malha de controle, será omitido o processo de modelagem da malha desenvolvida por Whalley e Ebrahimi (2002).

FIGURA 5.8 – Diagrama de blocos do sistema de controle de malha fechada.



Fonte: Modificado de Whalley e Ebrahimi (2002).

Na Figura 5.8 apresenta-se o diagrama de blocos do sistema de controle da malha fechada, associando a malha de controle a função de transferência da planta propulsiva.

Segundo Whalley e Ebrahimi (2002), destaca-se que o set point de Torque ($r_1(s)$) foi incluído como entrada apenas por questão de completude. Na prática não haveria entrada para este sinal, e, portanto, para efeitos de testes e análises, a entrada $r_1(s)$ será considerada igual a zero. Em Navio de guerra, visando ter flexibilidade de suas configurações, esta entrada pode ser utilizada para obter variações de combinações de Torque (Diferentes ângulos de passo) e rotações do eixo.

No esquema de controle estabelecido como principal, o set point $r_1(s)$ permanecerá nulo, e as mudanças de velocidade do navio se darão a partir de entradas no *set point* de velocidade do eixo $R_1(s)$. Desta forma, de acordo com Whalley e Ebrahimi (2002), as mudanças do Torque no eixo $Q(t)$ estariam limitadas por projeto a aproximadamente 20%.

Na Tabela 5.3 estão listados os principais parâmetros que compõem o sistema de controle, seus ganhos de realimentação e pré-compensadores. Além disso, para conter o rápido pico de elevação do torque no eixo foi introduzido um *delay* no controlador $K(s)$. Com isso permitiu-se prevenir que pequenas mudanças de demanda de velocidade em $R(s)$, não atue diretamente no ângulo da pá do hélice, o que pode vir a aumentar o desgaste no eixo, devido a aumentos de torque repentinos e excessivos (Whalley e Ebrahimi, 2002).

TABELA 5.3 – Parâmetros do sistema de controle de malha fechada.

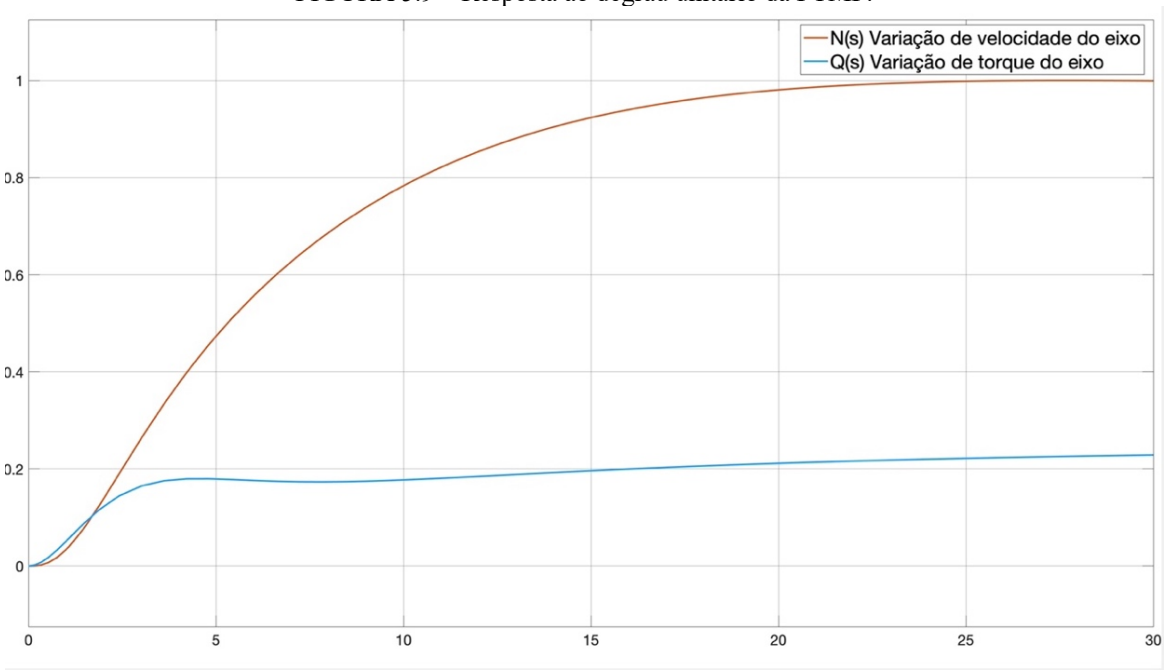
SÍMBOLO	DEFINIÇÃO	VALOR
$K(s)$	Controladores (Função no domínio da frequência)	$\frac{-3}{10s+1}$
$K_1(s)$		$\frac{1}{s+0.075}$
$K_2(s)$		$\frac{0.0072s+0.0104}{19{,}7s+1}$
P_1	Pré-compensadores (Escalar)	0.294
P_2		0.918
P_3		0.5
f_1	Ganho de *feedback* (Escalar)	0.1
h_1		0.0329
h_1		0.2059

Fonte: Modificado de Whalley e Ebrahimi (2002).

Interessante notar que, o esquema de controle detalhado, não inicia as mudanças de resposta do eixo, através de alterações diretas no fluxo de combustível na Turbina. Outrossim, as mudanças de velocidade são afetadas primeiramente por uma alteração na demanda de passo do HPC, para somente depois permitir que o controlador de mínimo esforço avance ou retarde o fluxo de combustível, de acordo com o sinal de feedback de mínimo esforço (Whalley e Ebrahimi, 2002).

Na figura 5.9, pode-se observar a resposta da Função de Transferência de Malha Fechada (FTMF)[77] a uma entrada degrau unitário no *set point* $R_1(s)$, mantendo-se a configuração principal do HPC, com entrada nula em $r_1(s)$. Com este teste será possível visualizar alguns dos comportamentos previstos para malha de controle, conforme mencionado acima.

FIGURA 5.9 – Resposta ao degrau unitário da FTMF.



Fonte: Elaborado pelo autor.

Desta forma, nota-se que foram alcançados os requisitos do designe da malha de controle. Primeiramente, fica evidente que o torque sofre um *delay* em relação as respostas da FTMA. Posteriormente, o transitório do torque reduziu seu *overshooting,* além de ter sido alcançado os cerca de 20% de torque máximo mencionados anteriormente, o que reduz o

[77] No **Apêndice F** encontra-se o modelo da FTMF com os parâmetros estabelecidos na Tabela 5.3. Esta representação foi criada através do software SIMULINK com o objetivo de se obter a resposta apresentada na Figura 5.9.

esforço sobre o eixo. Por fim, ocorre a otimização da acomodação da velocidade do eixo, alcançando o objetivo de 90% em aproximadamente 15 segundos.

A parametrização da função objetivo do ataque *SD-Controlled Data Loss* se dará sobre a curva de velocidade do eixo $N(s)$, com o requisito de reduzir seu tempo de acomodação, buscando uma maior aceleração do eixo, além de gerar um *overshooting* do torque $Q(s)$. Como a FTMF apresentada encontra-se com o sistema de controle no domínio da frequência, na seção a seguir, será realizada a conversão A/D, com uso do mecanismo *Zero-order-hold*. Desta forma, será estabelecido um sistema de controle digital para automação da planta propulsiva $G(s)$.

5.2.4 Sistema de controle digitalizado

Conforme observado na seção 2.1.4, a cerca de conversão A/D, quanto maior for a taxa de amostragem, melhor será a qualidade do sinal digital apresentado. Isto se deve pois no processo de conversão do sinal digital para contínuo, no fluxo de dados do controlador para planta, uma baixa taxa de amostragem pode gerar um atraso, ocasionando perda de performance e instabilidade no regime transitório.

Como altas taxas de amostragem demandam altos custos computacionais para o seu processamento, é de suma importância que se escolha a menor taxa de amostragem possível, que ainda assim garanta o desempenho do sistema. Diversas literaturas como Powell *et al.* (1998), Ogata (2010) e Nise (2020) divergem sobre a taxa de amostragem ideal para cada situação. Para este trabalho será adotado a taxa de amostragem ideal (f_s) como 20 vezes a maior frequência do sinal contínuo da função de transferência da planta de controle $G(s)$.

Por ocasião da parametrização da matriz $G(s)$, na equação 5.3, observa-se que os polos de uma equação característica de segunda ordem descrevem um comportamento oscilatório através de $\boldsymbol{\omega}$ que é a frequência de oscilação. Como a planta propulsiva é projetada para receber apenas entradas contínuas e não oscilatórias, como uma função impulso ou degrau, a frequência de oscilação da planta será considerada a maior frequência para efeitos de cálculo de frequência de amostragem. Com isso, a taxa de amostragem é definida conforme abaixo:

$$w = 0.359\ rad/s, \tag{5.7}$$

$$f_{max} = \frac{w}{2\pi} = 0.5714\ Hz, \tag{5.8}$$

$$f_s = 20 * f_{max} = 1.1427\ Hz, \tag{5.9}$$

$$T = \frac{1}{f_s} \cong 8ms. \tag{5.10}$$

(Aproximando para um valor menor, por ser mais eficiente.)

Definida a Taxa de amostragem, foram realizadas simulações com entrada degrau unitário para verificação de possíveis atrasos, por meio dessas pode-se observar que não houve atrasos significativos para performance da planta. Na Tabela 5.4 encontram-se os parâmetros dos controladores digitalizados, em termos da transformada Z.

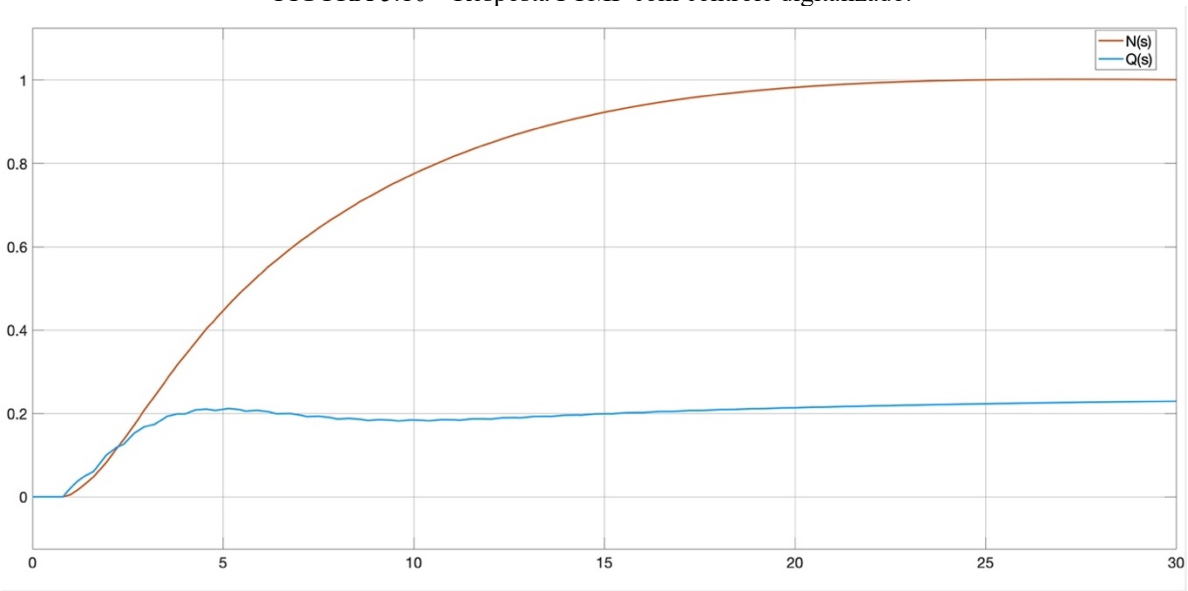
TABELA 5.4 – Parâmetros do sistema de controle digitalizado.

PARAMETROS	VALOR
$K(z)$	$-\frac{0.2307}{Z-0.9602}$
$K_1(z)$	$\frac{0.7765}{Z-0.9418}$
$K_2(z)$	$\frac{0.0003655z+0.00004839}{Z-0.9602}$

Fonte: Elaborado pelo autor.

Na Figura 5.10, pode-se observar a resposta da FTMF, em condições similares a da Figura 5.9, entretanto com os controladores digitalizados[78], conforme os parâmetros acima.

FIGURA 5.10 – Resposta FTMF com controle digitalizado.



Fonte: Elaborado pelo autor.

[78] No **Apêndice G** encontra-se o modelo da FTMF com controladores digitalizados, nos parâmetros estabelecidos na Tabela 5.4. Esta representação foi criada através do software SIMULINK com o objetivo de se obter a resposta apresentada na Figura 5.10. No modelo pode-se observar que, o bloco *zero-order-hold* foi utilizado no sentido da realimentação, para digitalizar o sinal, e no sentido de controle, para fazer a conversão D/A.

Desta forma, pode-se observar que a frequência de amostragem escolhida esta adequada, pois atende aos mesmos requisitos de performance do sistema de controle mencionados anteriormente.

5.3 CUSTOMIZAÇÃO DO ATAQUE

Nas seções a seguir será dada continuidade ao designe do ataque *SD-Controlled Data loss*. Como mencionado anteriormente, a simulação do ataque se limitará a explorar a capacidade de resolver problemas de otimização numérica do BSA, para selecionar os pacotes de dados a serem desviados, de forma a atender as demandas parametrizadas na função objetivo. Com isso, a modelagem do sistema de controle da planta propulsiva foi fundamental para se colher a informações necessárias a orientação do ataque, como a resposta da FTMF com o sistema de controle digitalizada, apresentada na Figura 2.10.

5.3.1 Parametrização da função objetivo

Conforme apresentado na seção 5.1.3, a função objetivo (f_{obj}), ou de aptidão, será empregada para se obter o comportamento malicioso desejado. A estratégia definida previamente, para uma planta propulsiva, busca que o sistema alcance a estabilidade em um tempo mais curto, podendo causar uma aceleração excessiva do eixo e, principalmente, o *overshooting* na variação do torque (Q).

A função f_{obj} pode estabelecer diversas condições para avaliar a aptidão da resposta desejada. Na equação abaixo pode-se observar o método de comparação que será utilizado neste trabalho, para definir a função objetivo:

$$f_{obj} = \sum_{k=1}^{V} [n(k) - \hat{n}(k)]^2 \ . \tag{5.11}$$

Onde $n(k)$ é a curva objetivo que se deseja obter na saída da planta para que ocorra o comportamento malicioso esperado, e $\hat{n}(k)$ corresponde a resposta da FTMF para uma palavra de ataque $W = \{b_0, b_1, \dots, b_{h-1}\}$, usada para indicar quais amostras da sequência serão desviadas. Com isso, ao se achar o mínimo global de f_{obj}, o BSA buscará pela solução de ataque mais próxima da curva $n(k)$.

A $n(k)$ será parametrizada a partir da curva resposta da rotação do eixo (N(t)), apresentada na Figura 5.10. Pode-se observar que esta curva descreve um comportamento gráfico similar a seguinte função:

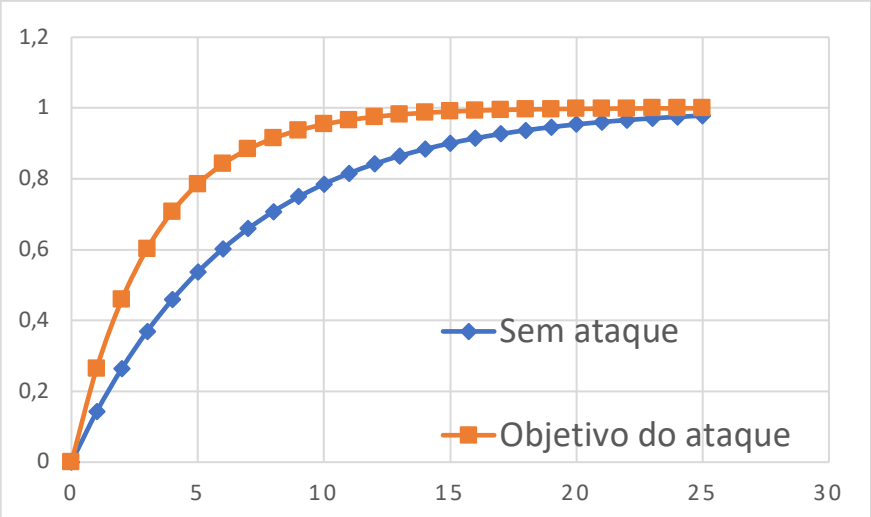
$$N(t) \cong 1 - e^{-\frac{t}{\tau}} \tag{5.12}$$

Onde τ é a constante de tempo da resposta do sistema.

Considerando-se os requisitos estabelecidos por Whalley e Ebrahimi (2002), em que a curva se estabiliza a aproximadamente 90% em 15 segundos, pode-se definir a constante de tempo da Equação 5.12, sendo $\tau \cong 6.5$ segundos.

Definindo a curva $n(k)$, para uma constante de tempo com metade da reposta original ($\tau_n = 50\% * \tau$), a curva objetivo irá se estabilizar a aproximadamente metade do valor original, como pode-se observar na figura comparativa abaixo.

FIGURA 5.11- Comparativo entra curva sem ataque e objetivo do ataque.



Fonte: Elaborado pelo autor.

Foram realizadas simulações com diversas reduções de constante de tempo (40%, 50%, 60%, 70%) e como em todas o BSA conseguiu obter um desempenho satisfatório na aceleração da curva $N(t)$ e overshooting do torque $Q(t)$, para este trabalho será utilizado a constante de tempo da Figura 5.11 ($\tau_n = 3.25\, segundos$), como parâmetro da curva objetivo $n(k)$. Portanto, fica definido que:

$$n(k) = 1 - e^{-\frac{k}{3.25}} \tag{5.11}$$

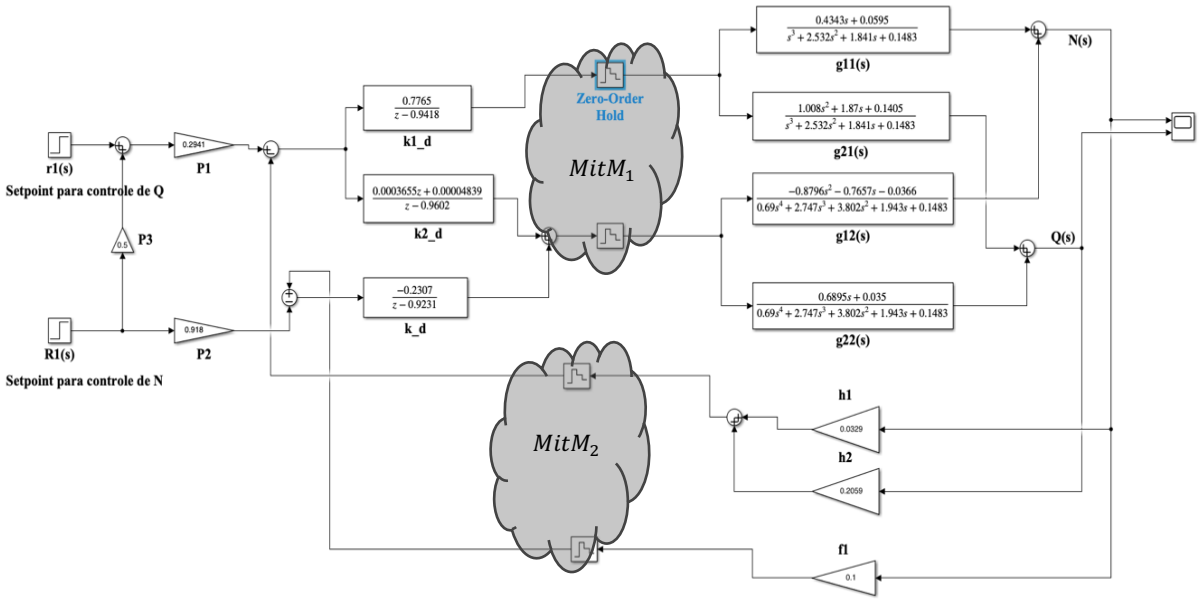
5.3.2 Posicionamento do *Man-in-the-middle*

Na seção 2.1.3, ao se falar sobre as vulnerabilidades dos NCS, o *Man-in-the-middle* foi posicionado, na Figura 2.10, entre o sistema de controle digital e a planta industrial, em um sistema SISO, semelhante ao proposto em Ferrari *et al.* (2020) e De Sá *et al.* (2017). No entanto, neste trabalho, por se tratar de um sistema MIMO, são utilizados três controladores ($k_1(z), k_2(z) e\ k(z)$) e quatro funções de transferência que descrevem o funcionamento da planta ($g_{11}(s), g_{12}(s), g_{21}(s)\ e\ g_{22}(s)$), que possuem *loop* de controle com interações mais complexas que os exemplos anteriores.

A função de transferência de malha fechada, na Figura 5.8, permite avaliar que seriam necessários ao menos quatro seguimentos de rede para posicionamento do MitM, com o objetivo de se obter um ataque mais eficiente. São eles dois seguimentos de rede que seguem o fluxo de controle (*foward*) e duas realimentações que vão das respostas de torque (Q) e rotação (N) do eixo de volta para os controladores (*feedback*).

A figura abaixo ilustra o posicionamento do ataque no NCS em questão, para que consiga compreender todos os seguimentos do *loop* de controle.

FIGURA 5.12- Posicionamento do MitM na malha de controle.



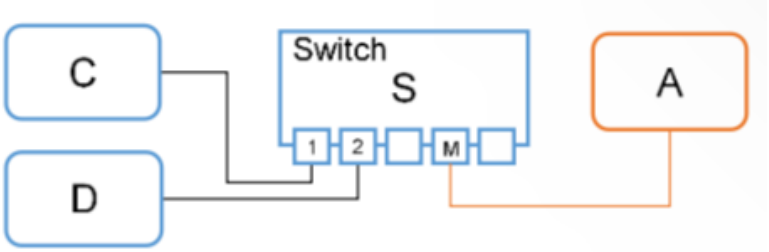
Fonte: Elaborado pelo autor.

Segundo De Sá *et al.* (2017) e Ferrari *et al.* (2020), comparativamente, apesar do maior número de segmentos de rede, para o *SD-Controlled Data loss* conseguir agir e coordenar todas

as interações necessárias, bastaria que o *host* malicioso fosse infiltrado em um *switch.* Desta forma o MitM passaria a ter acesso a todos os trechos de *fowards* e *feedbacks* mencionados. Neste caso o $MitM_1$ e o $MitM_2$ estariam atuando no mesmo dispositivo de comunicação da rede, apesar de desviarem dados de seguimentos distintos do *loop* de controle.

Na simulação realizada em Ferrari *et al.* (2020), o ataque proposto utiliza um switch industrial *Siemens Scalance XB28*, onde os controladores (C) estão conectados a porta 1 e os dispositivos da planta (D) na porta 2, na porta M um microcomputador infectado funciona como *host* malicioso, infectando a rede, conforme ilustrado abaixo. Esta distribuição pode ser considerada adequada

FIGURA 5.13 – Diagrama com esquema de ligação em switch.



Fonte: Ferrari *et al.*, 2020.

Neste trabalho, os segmentos de rede e toda a planta de controle do NCS terão suas iterações simuladas através do software SIMULINK, o modelo do sistema de controle da planta propulsiva utilizado na simulação encontram-se no **Apêndice I**.

5.4 RESULTADOS DAS SIMULAÇÕES

Após uma ampla análise da planta de controle propulsiva e extensa pesquisa realizada, nesta seção serão apresentados e analisados os dados das simulações, com base nos critérios estabelecidos ao longo deste trabalho. Os resultados serão apresentados de maneira objetiva, de forma a permitir uma análise quantitativa e qualitativa para subsequente discussão.

Na Tabela 5.5 são apresentados os parâmetros utilizados no experimento:

TABELA 5.5 – Parâmetros de simulação do BSA.

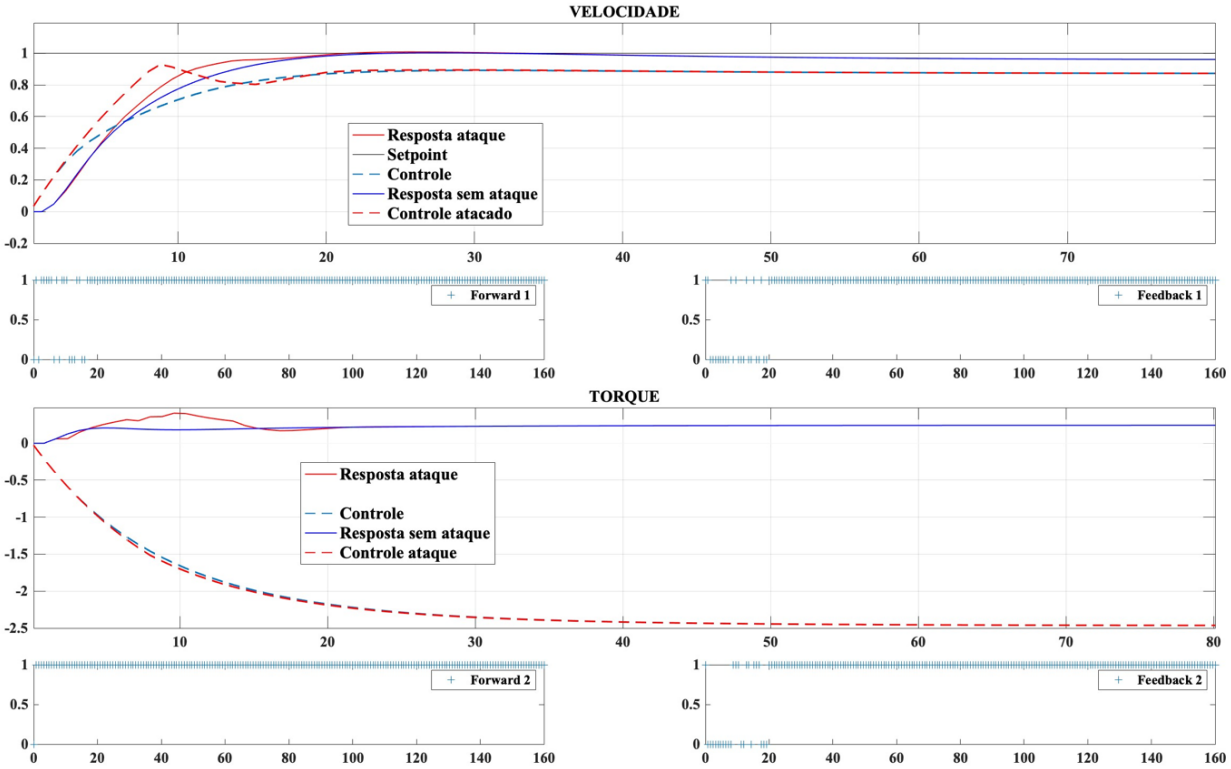
Parâmetro	Valor
Número de Simulações	10
Número de iterações	800
Amostras por iteração	200

Amostras manipuladas	25
Tempo de amostragem	0.8 segundos
População	100
Função aptidão (ou objetivo)	$f_{obj} = \sum_{k=1}^{25} [n(k) - \hat{n}(k)]^2,$ Onde: $\boldsymbol{n(k) = 1 - e^{-\frac{k}{3.25}}}.$

Fonte: Elaborado pelo autor.

O código fonte da simulação pode ser encontrado no **Apêndice J**, onde por meio de um *QR-Code* dará acesso a um repositório com os principais códigos utilizados no experimento.

FIGURA 5.14 - Resultado individual da 7ª simulação.



Fonte: Elaborado pelo autor.

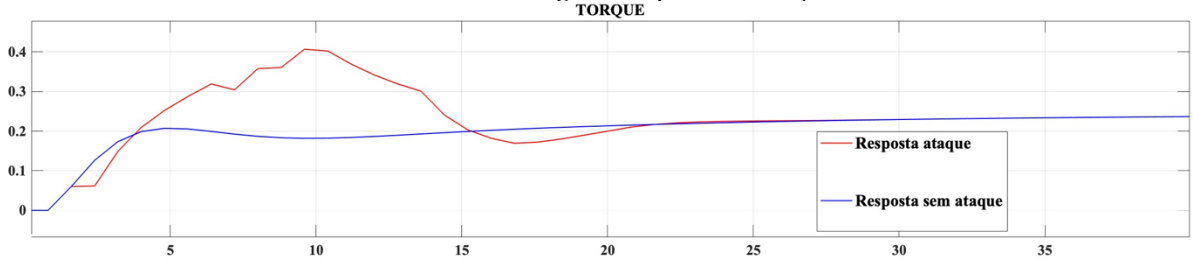
A Figura 5.14 apresenta o resultado da sétima simulação de um total de dez simulações realizadas em condições similares. Nesta encontram-se as respostas mais próximas da função aptidão apresentada, ou seja, a solução que apresentou o menor mínimo global dentre os experimentos realizados. No gráfico "Velocidade", a resposta original (linha contínua azul)

alcança os 90% do seu regime estacionário em aproximadamente 16 s, enquanto na resposta com ataque (linha contínua vermelha) ocorre em cerca de 10,2 s, uma redução de 36,25%.

Os quadros *Feedback* e *Fooward* representam as palavras de ataque para cada um dos quatros segmentos de rede onde atuam os MitM, conforme mencionado, esse código binário ($W = \{b_0, b_1, \dots, b_{h-1}\}$) identifica os pacotes a serem desviados pelo código malicioso. Pode-se observar que, como a função objetivo é relacionada a curva de rotação do eixo, apresentou-se mais pacotes desviados no *Feedback 1* e *Fooward 1*. Entretanto, como se trata de um sistema MIMO, as alterações no torque também podem vir a influenciar na resposta da velocidade[79], o que justifica terem sido desviados pacotes no *Feedback 2*.

Relembra-se que, os pacotes de dados desviados fazem com que as amostras anteriores, que são as mais atualizadas disponíveis, sejam repetidas para efeito de controle. Com isso o atraso gerado na reposta do torque através de sua realimentação, faz com que ocorra uma elevação da curva do torque original, a fim de acelerar a resposta de rotação no eixo. Este fato evidencia que o BSA consegue identificar as interações na planta, e atuar internamente tanto na demanda de combustível quanto no *set point* do passo, de forma a alcançar repostas mais próximas a função aptidão.

FIGURA 5.15 – *Overshooting* no Torque da simulação individual.



Fonte: Elaborado pelo autor.

Na Figura 5.15, pode-se observar o comportamento do torque aplicado sobre o eixo, que apesar de não ser alvo direto da função aptidão do BSA, por se tratar de um sistema MIMO, sofre uma ação indireta com o objetivo de acelerar a curva de rotação do eixo. Este dado comprova a exequibilidade da estratégia de ataque, apresentada na seção 5.1.3, em que o *SD-Controlled Data Loss* tem por objetivo gerar um sobretorque no eixo, além da aceleração causada pela curva objetivo com constante de tempo menor.

No *overshooting* ocorre um aumento de aproximadamente 102% do torque em relação a curva original, que na configuração utilizada prevê que o torque chegue até aproximadamente

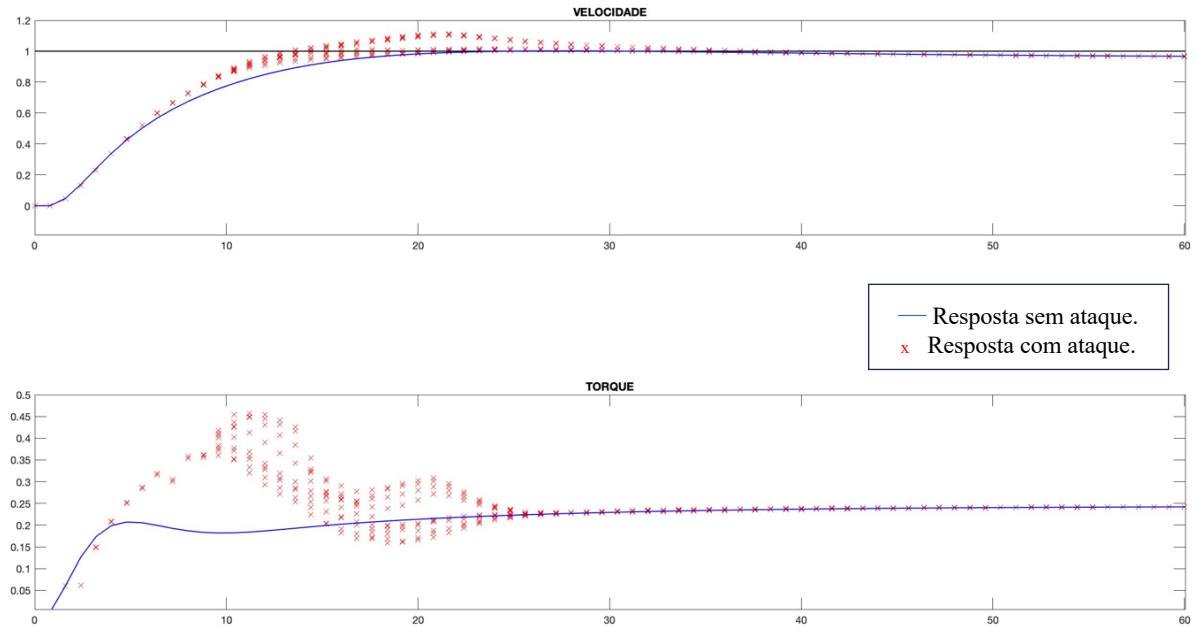
[79] Esta relação entre entradas e saídas da planta propulsiva foi destacada na seção 5.2.2, por ocasião das análises das repostas ao degrau da FTMA.

20% do torque máximo. Não foi objetivo deste trabalho apresentar os limites de falha do eixo para um determinado valor de sobretorque. Entretanto, vale destacar que ao operar acima de valores para o qual foi projetado, o eixo e demais componentes que fazem parte da transmissão de potência, como engrenagens redutoras e mancais, podem vir a se desgastar e reduzir o MTBF, que é o objetivo de degradação de serviço (SD) deste ataque.

Nas demais simulações, apresentadas na Figura 5.16, pode-se observar que apesar de o valor do global mínimo verificado para cada uma das iterações não ter variado de forma significativa, o torque mostrou consideravelmente sensível as variações de aceleração do eixo correspondentes. Os *overshooting* tiveram um aumento de 75 a 125% da curva sem ataque, enquanto as rotações do eixo não apresentaram grande alteração na sua aceleração até os 90%.

Entretanto, para as curvas de rotação que passaram a ter um valor acima do set point (linha contínua preta), os sobretorques foram maiores. Como o objetivo não é obter um valor maior de torque, mas sim próximo do desejado, uma solução para aprimorar o ataque poderia ser uma função aptidão combinada, que descarta as soluções que apresentassem um torque acima do valor de pico desejado.

FIGURA 5.16 – Resultado das 10 simulações de ataque.



Fonte: Elaborado pelo autor.

Por fim, os resultados indicam que a planta se comportou adequadamente em relação ao que era planejado para o ataque, sem oferecer efeitos colaterais que pudessem aparentemente levar a uma interrupção de seu funcionamento, o que faria o ataque ser inefetivo quanto a sua estratégia. É relevante enfatizar que poderiam ter sido utilizadas mais de uma função aptidão

que englobassem outros comportamentos da curva de rotação do eixo, ou até mesmo objetivos combinados com rotação e torque. Segundo Ferrari *et al.* (2017), esta característica possibilita a ameaça mudar entre uma estratégia e outra de forma a não criar um padrão claro de ataque e reduzir as possibilidades de ser detectado.

6 CONCLUSÃO

Considerando os objetivos propostos no início deste trabalho, a presente pesquisa contribui significativamente para ampliar o conhecimento no que diz respeito a soluções de sistemas de controle e automação. Abrangendo a evolução dessas soluções desde suas raízes tecnológicas até culminar nos sistemas digitais, presentes na indústria 4.0.

As evoluções tecnológicas destacadas, nos campos de engenharia computacional e telecomunicações, desempenharam um papel fundamental na criação da infraestrutura necessária ao avanço da indústria. Nesse contexto, essas inovações permitiram atender a demandas crescentes por maior produtividade e eficiência nos processos industriais. Com isso, representam uma parte essencial da história da automação e controle, que esta pesquisa busca contribuir para uma compreensão mais profunda desse progresso tecnológico e seus impactos na segurança das instalações.

Não obstante disso, com a miniaturização dos componentes eletrônicos, os sistemas embarcados passaram a integrar este conjunto de sistemas complexos, que utilizam dos sistemas de controle digitais e protocolos de rede, no desempenho de suas principais funcionalidades. Entretanto, a evolução dos sistemas navais na digitalização, apesar de contribuir para efetividade e otimização de seus processos, expõe o setor marítimo as crescentes ameaças cibernéticas, com dados do triênio 2018 a 2021 mostrando um crescimento de 900% no registro de ataques a plataformas marítimas (Freire *et al.*, 2021).

Os sistemas de controle industriais (ICS) e sistemas de controle em rede (NCS) baseados nos protocolos Real-Time Ethernet, conforme mencionado, apresentam diversas lacunas de mecanismos de segurança, como autenticação forte e criptografia. Desta forma, este trabalho apresentou estudos e experimentos que pudessem demonstrar esse contexto, de forma a apontar as vulnerabilidades, e permitir uma reflexão sobre a necessidade de se aprimorar os requisitos de segurança cibernética.

A análise do SCADA *system* permite observar que as vulnerabilidades apresentadas não estão distantes da realidade da indústria, por se tratar de um sistema de protocolo aberto e amplamente utilizado em sistemas críticos na atualidade. Isso inclui sistemas embarcados, geração de energia elétrica e até mesmo instalações de enriquecimento de uranio, como a abordada no estudo de caso.

O estudo de caso do *"Stuxnet worm"* ilustra o quão significativo pode ser o tópico da segurança cibernética, tanto do ponto de vista estratégico quanto em termos de ameaças

potenciais. Isso coloca o domínio cibernético como um ambiente onde interesses não apenas de empresas, mas também de nações, estão em jogo. Portanto, a partir deste caso, a proteção contra ameaças cibernéticas tem se tornado uma prioridade não apenas para o setor privado, mas também para governos e organizações internacionais.

Desenvolvido objeto de estudo, a partir da simulação do modelo de ataque cibernético apresentado, o *SD-Controlled Data Loss,* pôde-se demonstrar a exequibilidade de um ataque furtivo e controlado a uma planta propulsiva de navio de guerra, dentro das limitações estabelecidas. O algoritmo do BSA, assim como nos artigos De Sá *et al.* (2017) e Ferrari *et al.* (2020), foi eficiente na seleção dos pacotes de dados a serem desviados, provocando uma redução da constante de tempo na resposta de rotação eixo de aproximadamente 40%, além de um sobretorque no eixo de mais de 100% do valor nominal projetado.

Nesse contexto, os temas abordados demonstram o quanto os mesmos recursos tecnológicos utilizados para desenvolver a capacidade da indústria, também podem ser empregados por softwares maliciosos com o intuito de infringir danos as plantas industriais. O ponto positivo é que as novas tecnologias permitem a evolução e crescimento de diversos setores que são essenciais para a sociedade. Por outro lado, as falhas de segurança podem colocar em risco não só as plantas industriais e sistemas embarcados envolvidos, mas também todos os elementos internos e externos que se relacionam com eles.

6.1 Considerações Finais

Os sistemas embarcados sofrem mudanças tecnológicas relativamente mais lentas do que a da indústria. Isso ocorre, pois, navios mercantes e de guerra são construídos para funcionar por mais de 20 anos, em um ambiente limitado, com sistemas críticos expostos a inúmeras intempéries. Todavia, na última década os sistemas navais vêm recebendo crescente investimento em sistemas de controle e automação modernos, em alguns casos que possam vir a permitir a comunicação e manutenção em qualquer lugar e a qualquer hora. Nesse contexto, é essencial que a indústria naval intensifique as discussões e empregue recursos para poder enfrentar as ameaças cibernéticas, que já são realidade na indústria em geral desde a implementação dos NCS.

Como contramedidas, é imperativo adotar uma mudança de postura expressiva, com a implementação de ações voltadas para aumentar a conscientização e desenvolver ferramentas que auxiliem na segurança cibernética. Isso começa com treinamentos dos operadores,

prevenindo comportamentos inadequados que possam colocar os sistemas em risco. Além disso, é fundamental investir no desenvolvimento de protocolos de segurança adequados e sistemas que sejam capazes de detectar intrusão.

Por fim, a colaboração desempenha um papel crucial na melhoria das medidas de segurança contra as possíveis ameaças, o que inclui o compartilhamento de dados e informações que possam contribuir para o aprimoramento da segurança. A Organização Marítima Internacional (IMO) é um dos principais atores que vem estimulando essas contramedidas, especialmente através da adoção de *frameworks* de segurança cibernética, como o *Guidelines on Cyber Security on board Ships* (BIMCO, 2020) e o *Framework for improving critical infrastructure cybersecurity* (Barrett, 2018). Essas diretrizes fornecem orientações importantes para proteger as operações marítimas contra ameaças cibernéticas em constante evolução.

6.2 Sugestões para Futuros Trabalhos

Sugere-se que, para continuidade desse trabalho, sejam considerados estudos de casos envolvendo navios mercantes ou de guerra que nos últimos anos possam ter reportado ataques cibernéticos. Estes estudos podem oferecer insights valiosos sobre as vulnerabilidades e os desafios enfrentados na indústria naval e de defesa.

Além disso, do ponto de vista de pesquisa experimental, existem inúmeras possibilidades para expandir os estudos realizados. Por exemplo, é possível modelar funções objetivos que compreendam um maior número de variáveis de resposta do sistema, complementar o algoritmo para simular a identificação passiva (PSI) de um sistema de controle MIMO e até mesmo variar as estratégias de ataque utilizadas. Essas abordagens podem aprimorar a pesquisa e enriquecer a compreensão das questões de segurança cibernética em sistemas de controle e automação.

REFERÊNCIAS

BARRETT, M. **Framework for improving critical infrastructure cybersecurity.** Proceedings of the Annual ISA Analysis Division Symposium. Gaithersburg: National Institute of Standards and Technology, 2018. Disponível em: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Acesso em: 07 de agosto de 2023.

BIMCO. **The Guidelines on Cyber Security Onboard Ships**. 4. ed. Copenhaga: Baltic and International Maritime Council, 2020.

CIVICIOGLU, P. Backtracking Search Optimization Algorithm for numerical optimization problems. **Applied Mathematics and Computation**, v. 219, n. 15, p. 8121–8144, abr. 2013.

COLBERT, E.; KOTT, A. **Cyber-security of SCADA and Other Industrial Control Systems**. 63. ed. Cham: Springer International Publishing, 2016.

DE SÁ, A. O.; CARMO, L. F. R. D. C.; MACHADO, R. C. S. Covert Attacks in Cyber-Physical Control Systems. **IEEE Transactions on Industrial Informatics**, v. 13, n. 4, p. 1641–1651, ago. 2017.

DIAS, A. L. et al. **Panorama, challenges and opportunities in PROFINET protocol research**. 2018 13th IEEE International Conference on Industry Applications, INDUSCON 2018 - Proceedings. **Anais**...IEEE, nov. 2019. Disponível em: https://ieeexplore.ieee.org/document/8627173/. Acesso em: 12 de agosto de 2023.

EUA. **National Maritime Cybersecurity Plan**. Washington, 2020.

FERRARI, P. et al. Model-Based Stealth Attack to Networked Control System Based on Real-Time Ethernet. **IEEE Transactions on Industrial Electronics**, v. 68, n. 8, p. 7672–7683, ago. 2021.

FRANCHI, C. M.; CAMARGO, V. L. A. **Controladores Lógicos Programáveis - Sistemas Discretos**. 1. ed. São Paulo: Editora Érica Ltda., 2008.

FRANCIA, G. A. I.; FRANCIA, X. P.; PRUITT, A. M. Towards an In-depth Understanding of Deep Packet Inspection Using a Suite of Industrial Control Systems Protocol Packets. **Journal of Cybersecurity Education, Research and Practice**, v. 2016 No. 2, p. 5–13, 2016.

FREIRE, W. P. et al. Blockchain-based Maritime Monitoring System. **2021 IEEE International Workshop on Metrology for the Sea: Learning to Measure Sea Health Parameters, MetroSea 2021 - Proceedings**, p. 394–399, 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas S.A., 2002.

HOU, C. et al. **Research on Implementing Real Time Ethernet for Ship Power System**. 2nd International Workshop on Intelligent Systems and Applications. **Anais**...Wuhan: IEEE, 2010. Disponível em: https://ieeexplore.ieee.org/document/5473577/. Acesso em: 18 de agosto de 2023.

IBRAHIN, E. O encalhe do Ever Given. **Revista do Clube Naval**, v. 1, n. 397, p. 58–61, 2021.

IEC. **Standard IEC 60870-5-104 data types - Beckhoff Information System**. Disponível em:https://infosys.beckhoff.com/english.php?content=../content/1033/tf6500_tc3_iec60870_5_10x/984447883.html&id=. Acesso em: 18 de agosto de 2023.

IMO. **Guidelines on Maritime Cyber Risk Management**. London: International Maritime Organization, 2017.

KARNOUSKOS, S. **Stuxnet worm impact on industrial cyber-physical system security**. IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society. **Anais**...IEEE, 2011. Disponível em: http://ieeexplore.ieee.org/document/6120048/. Acesso em: 18 de agosto de 2023.

KESSLER, C. G.; SHEPARD, D. S. **Maritime Cybersecurity: A Guide for Leaders and Managers**. 2. ed. [s.l.] Gary Kessler Associates, 2022.

KUSHNER, D. The real story of stuxnet. **IEEE Spectrum**, v. 50, n. 3, p. 48–53, 2013.

LAGOUVARDOU, S. **Maritime Cyber Security: concepts, problems and models.** Master's thesis - Technical University of Denmark, Lyngby, 2018.

LAMB, F. **Automação Industrial na Prática**. Porto Alegre: AMGH, 2015.

LANGNER, R. Stuxnet: Dissecting a Cyberwarfare Weapon. **IEEE Security & Privacy Magazine**, v. 9, n. 3, p. 49–51, 2011.

NCS. **TECHNICAL INFORMATION BULLETIN 04-1 Supervisory Control and Data Acquisition (SCADA) Systems**. Arlington: National Communications System, 2004.

NISE, N. S. **Control Systems Engineering**. 8. ed. Pomona: Wiley, 2020.

Modbus.org. **Modbus Messaging Implementation Guide V1_0b**. Disponível em: https://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf. Acesso em: 20 de agosto de 2023.

OGATA, K. **Engenharia de Controle Moderno**. 5. ed. São Paulo: Person Education do Brasil, 2011.

PARCHARIDIS, M. D. **Simulation of Cyber Attacks Against SCADA Systems**. Master's thesis - International Hellenic University, Tessaloniki, 2018.

PESCHKE, J. et al. Security in Industrial Ethernet. **ETFA 2006 IEEE Int. Conference on Emerging Technologies and Factory Automation**, v. 10, n. Section 2, p. 2–5, 2006.

POWELL, D.; FRANKLIN, G.; WORKMAN, M. **Digital control of dynamic systems**. 3. ed. Menlo Park: Addison-Wesley, 1998.

REINO UNIDO**. Code of Practice: Cyber Security for Ships**. Londres, 2017.

ROSA, L. et al. Intrusion and anomaly detection for the next generation of industrial automation and control systems. **Future Generation Computer Systems**, v. 119, p. 50–67, jun. 2021.

SAPIR, M. et al. **Evil plc attack: Weaponizing plcs**. Disponível em: <https://web-assets.claroty.com/resource-downloads/team82-evil-plc-attack-research-paper-1661285586.pdf>. Acesso em: 26 de julho de 2023.

WHALLEY, R.; EBRAHIMI, M. Gas Turbine Propulsion Plant Control. **Naval Engineers Journal**, v. 114, n. 4, p. 77–94, out. 2002.

WOLLSCHLAEGER, M.; SAUTER, T.; JASPERNEITE, J. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. **IEEE Industrial Electronics Magazine**, v. 11, n. 1, p. 17–27, mar. 2017.

YANG, Y. et al. **Man-in-the-middle attack testbed investigating cyber-security vulnerabilities in smart grid SCADA systems**. IET Conference Publications. **Anais**...Institution of Engineering and Technology, 2012. Disponível em: https://digital-library.theiet.org/content/conferences/10.1049/cp.2012.1831. Acesso em: 27 de agosto de 2023.

YANG, Y. et al. **Stateful intrusion detection for IEC 60870-5-104 SCADA security**. IEEE Power and Energy Society General Meeting. **Anais**...IEEE, jul. 2014. Disponível em: http://ieeexplore.ieee.org/document/6939218/. Acesso em: 27 de agosto de 2023.

YU, X.; GEN, M. **Introduction to Evolutionary Algorithms.** Londres: Springer, 2010.

ZURAWSKI, R. **The Industrial Communication Technology Handbook**. 2. ed. San Franciso: CRC Press, 2015.

APÊNDICE A – TRANFORMADAS DE LAPLACE

TABELA A.1 - Teoremas da transformada de Laplace

Item	Teorema	Nome
1	$\mathcal{L}[\,f(t)\,] = F(s) = \int_{0-}^{\infty} f(t)e^{-st}dt$	Definição
2	$\mathcal{L}[\,kf(t)\,] = kF(s)$	Teorema da Linearidade
3	$\mathcal{L}[\,f_1(t) + f_2(t)\,] = F_1(s) + F_2(s)$	Teorema da Linearidade
4	$\mathcal{L}[\,e^{-at}f(t)\,] = F(s+a)$	Teorema da translação
5	$\mathcal{L}[\,f(t-T)\,] = e^{-sT}F(s)$	Teorema da translação
6	$\mathcal{L}[\,f(at)\,] = \frac{1}{a}F\left(\frac{s}{a}\right)$	Teorema escalar
7	$\mathcal{L}\left[\frac{d^n f}{dt^n}\right] = s^n F(s) - \sum_{k=1}^{n} s^{n-k} f^{k-1}(0)$	Teorema da diferenciação
8	$\mathcal{L}\left[\int_{0-}^{t} f(t)d\tau\right] = \frac{F(s)}{s}$	Teorema da Integração
9	$f(\infty) = \lim_{s\to 0} sF(s)$	Teorema do valor final
10	$f(0) = \lim_{s\to \infty} sF(s)$	Teorema do valor inicial

Fonte: Nise, 2020.

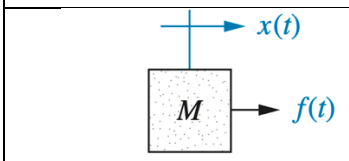
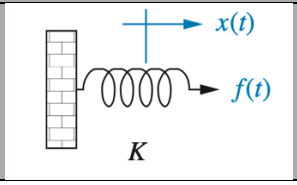
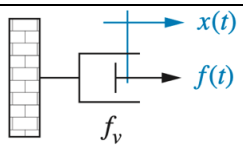
TABELA A.2 - Transformadas de Laplace

Item	$f(t)$	$F(s)$
1	$\delta(t)$	1
2	$u(t)$	$\frac{1}{s}$
3	$tu(t)$	$\frac{1}{s^2}$
4	e^{-at}	$\frac{1}{s+a}$
5	$sin\,\omega t$	$\frac{\omega}{s^2+\omega^2}$
6	$cos\,\omega t$	$\frac{s}{s^2+\omega^2}$

Fonte: Elaborado pelo Autor.

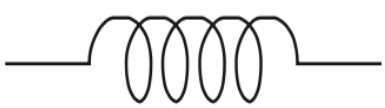
APÊNDICE B – PRINCIPAIS EQUAÇÕES DIFERENCIAIS PARA SISTEMAS MECÂNICOS E ELÉTRICOS.

TABELA B.1 – Componentes mecânicos de um sistema.

Sistema	Força-Deslocamento (Domínio do tempo)	Função de Transferência (Domínio da frequência)
Massa 	$f(t) = M\frac{d^2x(t)}{dt^2}$	Ms^2
Mola 	$f(t) = Kx(t)$	K
Atrito viscoso 	$f(t) = f_v\frac{dx(t)}{dt}$	$f_v s$

Fonte: Nise, 2020.

TABELA B.2 – Componentes de circuitos elétricos de um sistema.

Sistema	Voltagem-Corrente (Domínio do tempo)	Função de Transferência (Domínio da frequência)
Resistor (R) 	$v(t) = Ri(t)$	R
Capacitor (C) 	$v(t) = \frac{1}{C}\int_0^t i(\tau)\,d\tau$	$\frac{1}{Cs}$
Indutor (L) 	$v(t) = L\frac{di(t)}{dt}$	$f_v s$

Fonte: Nise, 2020.

APÊNDICE C – CARACTERÍSTICAS DE RESPOSTA TRANSITÓRIA

Segundo Ogata (2010), antes de se atingir o regime permanente, a resposta transitória apresentada por um sistema, quando sujeita a uma entrada de degrau unitário, apresenta as seguintes características:

1.Tempo de atraso t_d, tempo para que alcance a metade do seu valor final, pela primeira vez.

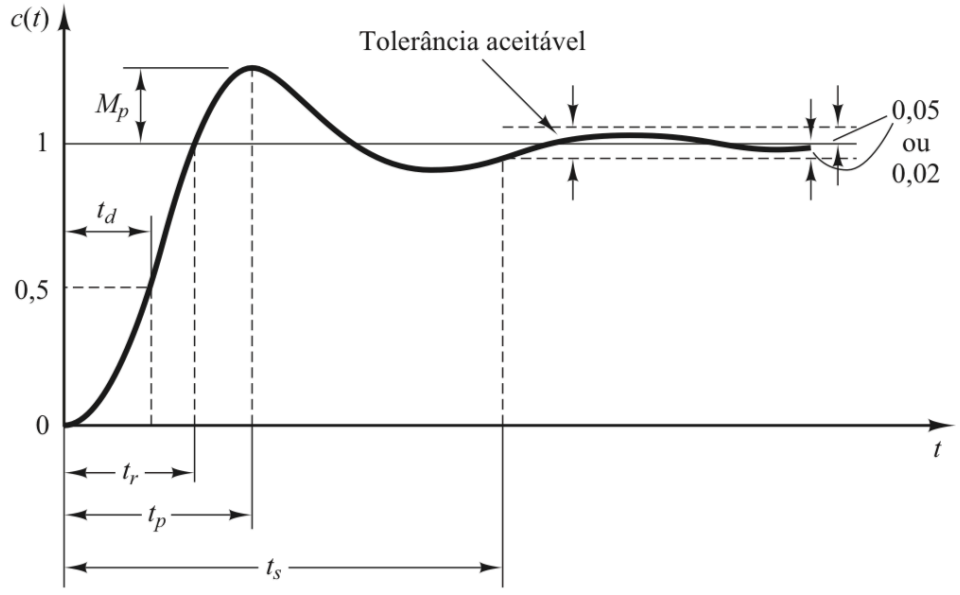
2.Tempo de subida t_r, tempo necessário para que a curva passe de um ponto do valor inicial a outro do valor final, as circunstâncias variam com o sistema.

3.Tempo de pico t_p, tempo para que e atinja o primeiro pico de sobressinal.

4.Máximo sobressinal (*Overshooting)* M_p, é o valor máximo do pico da curva.

5.Tempo de acomodação t_s, tempo necessário para que a curva oscilante alcance valores estabilizados, com cerca de 2 a 5% do valor final.

FIGURA B – Características da curva de resposta transitória.



Fonte: Ogata, 2010

APÊNDICE D – EXEMPLOS DE COMPENSADORES INDUSTRIAIS

TABELA D.1 – Tipos de compensadores em cascata.

Compensador	Função de transferência	Característica
Compensador Proporcional (P)	K_p	Melhora da resposta em regime estacionário; e Pode levar a instabilidade.
Compensador Proporcional Integrativo (PI)	$K_p\left(1+\frac{1}{T_i s}\right)$	Melhora no erro em regime permanente
Compensador Proporcional Derivativo (PD)	$K_p(1+T_d s)$	Melhora na resposta transitória
Controlador Proporcional Integrativo e Derivativo (PID)	$K_p\left(1+\frac{1}{T_i s}+T_d s\right)$	Melhora no erro em regime permanente; e Melhora na resposta transitória.

Fonte: Nise, 2020.

Onde: K_p é o ganho proporcional, $K_i = K_p/T_i$ que é o ganho integrativo, $K_d = K_p T_d$ que é o ganho derivativo.

Como pode-se observar, os compensadores acabam por adicionar polos e zeros ao sistema, com exceção do Proporcional que só adiciona um ganho, desta forma, permitem que sejam realizados controles mais eficazes a depender das características que o sistema apresente. Os métodos para regulagem de compensadores são diversos, mas não serão foco do desenvolvimento deste trabalho.

APÊNDICE E – PROPRIEDADES DA TRANSFORMADA Z

TABELA E.1 – Propriedades da transformada Z

Item	Teorema	Nome
1	$Z\{f(kT)\} = F(z) = \sum_{k}^{\infty} f(kT)z^{-k}$	Definição
2	$\boldsymbol{Z[\,af(t)\,] = aF(z)}$	Teorema da Linearidade
3	$\boldsymbol{Z[\,f_1(t) + f_2(t)\,] = F_1(z) + F_2(z)}$	Teorema da Linearidade
4	$\boldsymbol{\mathcal{L}[f(t-nT)\,] = e^{-n}F\,(z)}$	Teorema da translação
5	$\boldsymbol{f(\infty) = \lim_{z\to 1}(1 - z^{-1})F(z)}$	Teorema do valor final
6	$\boldsymbol{f(0) = \lim_{z\to\infty} F(z)}$	Teorema do valor inicial

Fonte: Nise, 2020.

TABELA E.2 - Transformadas de Laplace e Z

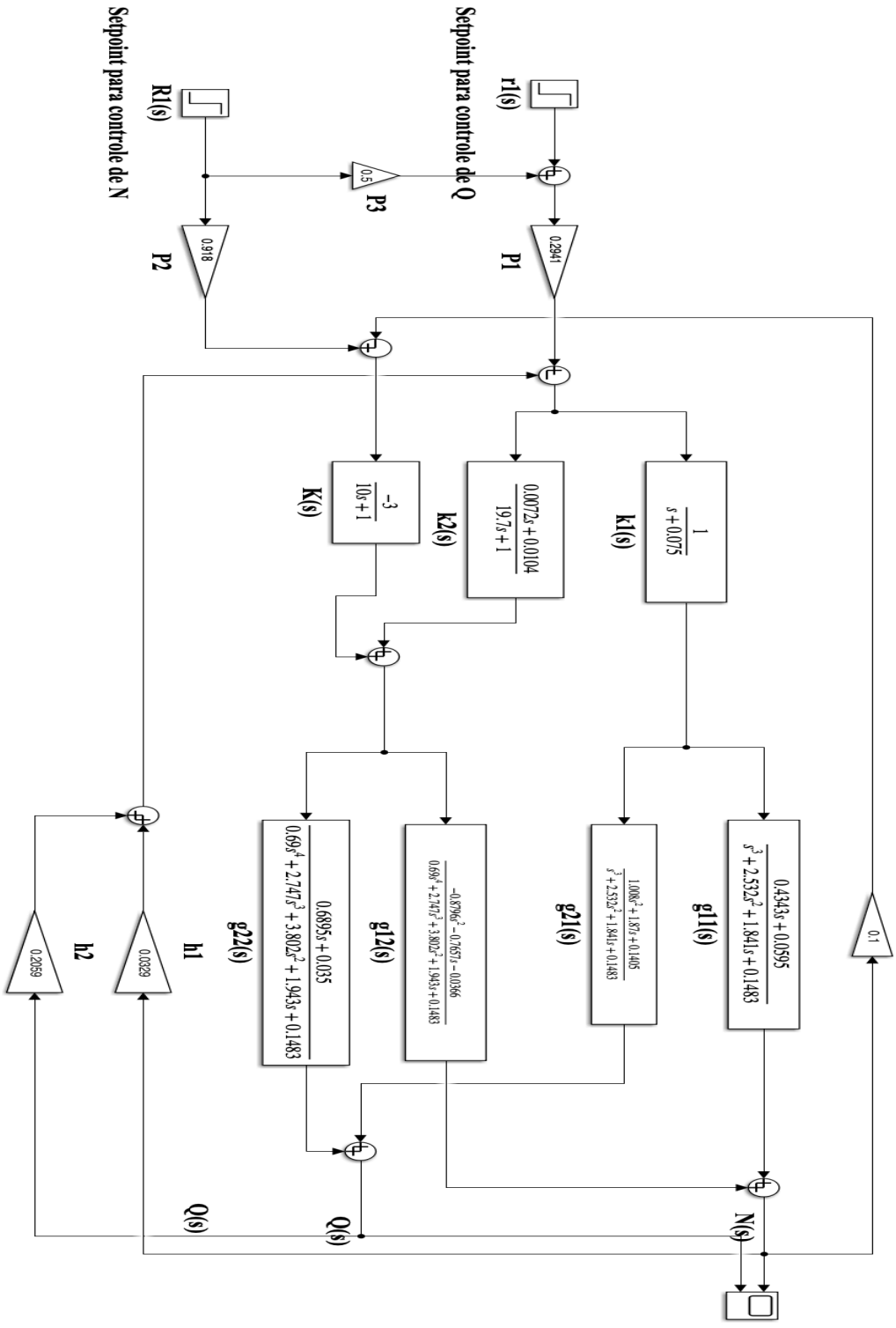
Item	$\boldsymbol{f(t)}$	$\boldsymbol{F(s)}$	F(z)	$\boldsymbol{f(kT)}$
1	$\boldsymbol{u(t)}$	$\boldsymbol{\frac{1}{s}}$	$\boldsymbol{\frac{z}{z-1}}$	$\boldsymbol{u(kT)}$
2	$\boldsymbol{t}$	$\boldsymbol{\frac{1}{s^2}}$	$\boldsymbol{\frac{Tz}{(z-1)^2}}$	$\boldsymbol{kT}$
3	$\boldsymbol{e^{-at}}$	$\boldsymbol{\frac{1}{s+a}}$	$\boldsymbol{\frac{z}{z-e^{-aT}}}$	$\boldsymbol{e^{-akT}}$

Fonte: Elaborado pelo Autor.

Onde: $f(kT)$ corresponde ao sinal discreto, T é o período de amostragem e k= 0,1,2,3...

APÊNDICE F – MODELO DE FTMF PARA SINAL CONTÍNUO

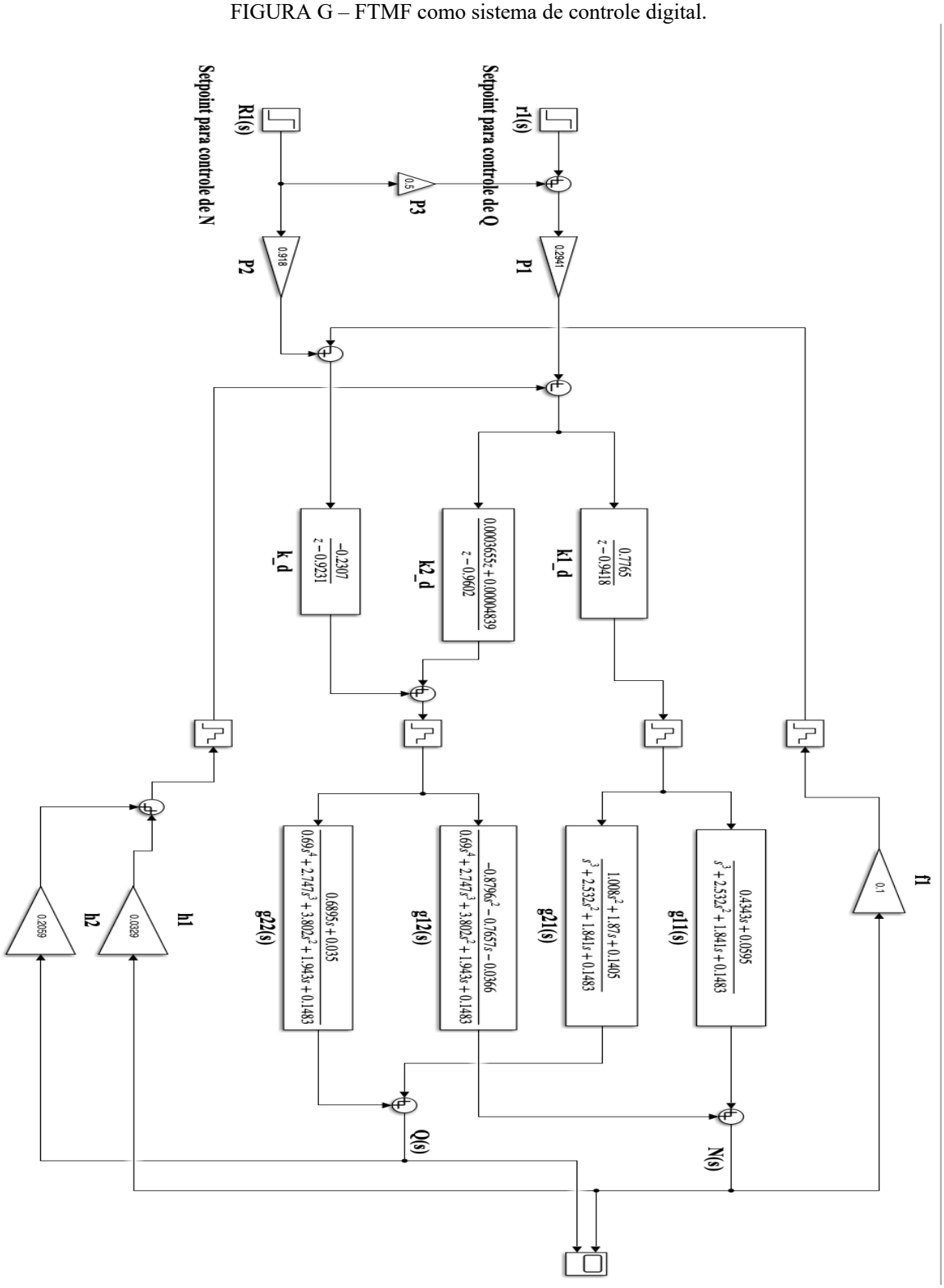
FIGURA F – FTMF com sinal contínuo.



Fonte: Elaborado pelo Autor.

APÊNDICE G – MODELO DE FTMF COM CONTROLADOR DIGITALIZADO

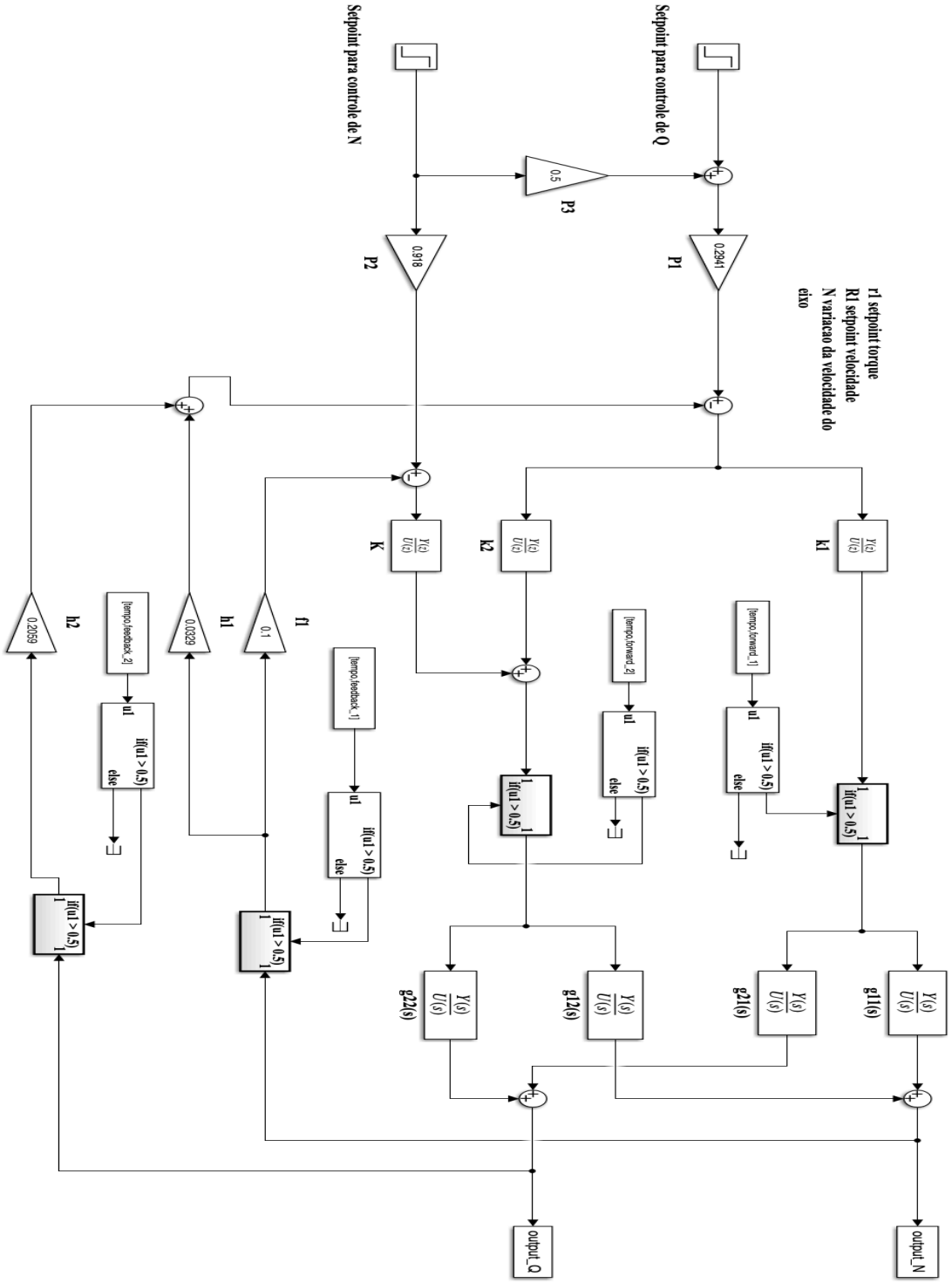
FIGURA G – FTMF como sistema de controle digital.



Fonte: Elaborado pelo Autor.

APÊNDICE I – MODELO DE SIMULAÇÃO DA PLANTA PROPULSIVA

FIGURA H – Modelo de simulação da planta propulsiva em SIMULINK.



Fonte: Elaborado pelo Prof. Alan de Oliveira de Sá.

APÊNDICE J – QR CODE PARA ACESSO AO CODIGO DA SIMULAÇÃO

Na Figura abaixo encontra-se o *QR Code* para acesso a um repositório no GitHub, onde foram armazenados os códigos da simulação de ataque do *SD-Controlled Data Loss.*

FIGURA I – QR Code para acesso ao repositório.

Fonte: Elaborado pelo Autor.