Universidade Federal do ABC
Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas
Engenharia de Informação

Segurança em redes de barramento de campo utilizando protocolo S7comm

Filipe Calado Gomes

Santo André - SP, 2023

Filipe Calado Gomes

Segurança em redes de barramento de campo utilizando protocolo S7comm

Trabalho de Graduação apresentado à Engenharia de Informação, como parte dos requisitos necessários para a obtenção do Título de Bacharel em Engenharia de Informação.

Universidade Federal do ABC – UFABC

Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas – CECS

Engenharia de Informação – EINFO

Orientador: Prof. Dr. João Henrique Kleinschmidt

Santo André - SP

2023

Filipe Calado Gomes
Segurança em redes de barramento de campo utilizando protocolo S7comm/ Filipe Calado Gomes. – Santo André - SP, 2023-
63 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. João Henrique Kleinschmidt

Trabalho de Graduação – Universidade Federal do ABC – UFABC
Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas – CECS
Engenharia de Informação – EINFO, 2023.

1. Sistema OT. 2. Cibersegurança. 3. Rede de Barramento de Campo. 4. S7comm.

Filipe Calado Gomes

Segurança em redes de barramento de campo utilizando protocolo S7comm

Trabalho de Graduação apresentado à Engenharia de Informação, como parte dos requisitos necessários para a obtenção do Título de Bacharel em Engenharia de Informação.

Trabalho de Graduação III.
Santo André - SP, Dezembro de 2023

Prof. Dr. João Henrique Kleinschmidt
Orientador

Santo André - SP
2023

Resumo

As redes de tecnologia operacional (ou de barramento de campo) se aplicam à comunicação entre máquinas e possuem como principais características sua robustez ao lidar com interferências de sinal em ambiente industrial e determinismo na troca de dados. Apesar desta robustez às intempéries do ambiente industrial as tornarem funcionalmente seguras estas redes não são boas referências no que se refere à segurança de dados e boa parte da evolução em segurança observada em redes TCP/IP não é facilmente transferível para as redes industriais. A pesquisa a seguir possui como tema segurança em redes de tecnologia operacional baseadas em PROFIBUS. A pergunta de pesquisa abordada foi "quais são os riscos mais importantes em redes de tecnologia operacional do ponto de vista de cibersegurança e como inibí-los". Com esta pergunta , foi possível definir os objetivos de pesquisa. Limitando a pesquisa às redes de Barramento de Campo baseados em PROFIBUS, os objetivos são (a) definir redes de tecnologia operacional e diferenciá-las de redes de tecnologia de informação, (b) conhecer os principais protocolos utilizados em redes de barramento de campo baseados em PROFIBUS, (c) avaliar nestes protocolos o interesse em atingir segurança, integridade, autenticidade e confidencialidade, (d) avaliar incidentes relevantes neste tipo de rede e em redes de tecnologia de informação que possam ser extrapolados para este tipo de rede e (e) definir segurança de redes de tecnologia operacional com base em normas já existentes. Para atingir estes objetivos entendeu-se que a pesquisa de referencial teórico é a metodologia mais apropriada, associada à análise de amostra de pacotes de rede coletados para alguns protocolos. Esta pesquisa é de relevância para a área de engenharia pois avalia itens voltados ao projeto de sistemas industriais de controle e supervisão com dispositivos distribuídos conectados em rede.

Palavras-chave:Sistema OT, Cibersegurança, Rede de barramento de campo, S7comm.

Abstract

The Operational tecnology networks (Fieldbuses) are applied in industrial machine-to-machine comunication and their main caracteristics are robustness against noise in industrial environments and deterministic behaviour in data exchange. Despite they being functionaly safe, their data security is an issue and the developments observed on data security on TCP/IP based networks can not be easily transferred to those Operational tecnology networks. The following research has the theme safety on operational tecnology networks based on PROFIBUS. The research question was "which are the most important risk agents in operational tecnology networks regading cybersecurity and how to inhibit their action". After the proposition of the research, it was possible to define its research objectives. Limiting the research to fieldbuses based on PROFIBUS, the objectives are to define operational tecnology networks and point out the differences between them and information tecnology networks, to know the most used protocols in fieldbuses based on PROFIBUS, evaluate in those protocols concerns to achieve safety, integrity, authenticity and confidenciality, evaluate relevant incidents in operational tecnology networks and on information tecnology networks that could be extrapolated to operational tecnology networks, define network security on operational tecnology networks based on existing norms. In order to fulfill those objectives, the research on theoretical references and the study of some real samples of network packages was adopted. This research has its greater relevance to the field of engineering because it evaluates elements related to the project of industrial control and supervisory systems with distributed devices conected by networks based on concepts of telecomunications project.

Keywords: OT system, Cybersecurity, Fieldbus, S7comm.

Lista de ilustrações

Lista de abreviaturas e siglas

ISO	Organização internacional de padronização
KPI	Indicador chave de desempenho
CLP	Controlador lógico programável
IHM	Interface homem-máquina
ICS	Sistema de controle industrial
SCADA	Sistema de supervisão e aquisição de dados
CAD	Desenho assistido por computador
CAM	Manufatura assistida por computador
CAE	Engenharia assistida por computador
CAPP	Planejamento de processo assistido por computador
ERP	Planejamento de recursos empresariais
MES	Sistema de execução da manufatura
IEC	Comissão internacional de eletrotécnica
TSAP	*Transport Service Access Point*
CSV	Valores separados por vírgula
NMAP	*Software* de varredura de rede

Sumário

1 INTRODUÇÃO

Este projeto de pesquisa se propõe a buscar compreender os principais riscos existentes em redes de tecnologia operacional baseados em PROFIBUS. A conectividade horizontal e vertical na Indústria vem ganhando força com o advento da Indústria 4.0, e é um dos pilares da etapa de digitalização do processo (BECKER et al., 2022). Esta forte conectividade insere riscos no que se refere à segurança de dados, de forma que há necessidade de que se protejam os dados e o *know-how* referente aos produtos e processos das empresas, para que não haja mau uso (KAGERMANN et al., 2013). Para Kagermann, os riscos cibernéticos devem ser considerados em conjunto com os riscos de operação, e cita como fatores determinantes para possibilitar a implementação da indústria 4.0 a segurança ser prevista por design em sistemas ciberfísicos e o desenvolvimento e implementação de padrões, arquiteturas e estratégias de TI. O maquinário industrial tem por característica uma longa vida útil e ciclos de inovação curtos associados a equipamentos velhos e heterogêneos do ponto de vista de redes, o que dificulta a adoção de medidas de segurança e a própria atualização de dispositivos OT (KAGERMANN et al., 2013). Devido à grande diversidade dos dispositivos OT aplicados ao chão de fábrica e dos seus protocolos de rede, este projeto teve por foco os CLPs, que são são os dispositivos centrais do controle das máquinas industriais, sendo assim mais críticos do ponto de vista de segurança. A preocupação com cibersegurança de CLPs ganhou visibilidade após o ataque Stuxnet, que teve como alvo uma usina de enriquecimento de Urânio no Irã causando danos desastrosos. A usina utilizava CLPs Siemens da família S7-300 e S7-400 , os mesmos que serão estudados nesta pesquisa (ALSABBAGH; LANGENDOERFER, 2022a).O método adotado foi a pesquisa de material bibliográfico associado a experimentos pontuais por auxílio de simuladores.

1.1 Problema

O problema que se apresenta é a difícil definição de ações para inibir a atuação de agentes de risco em redes de sistemas de tecnologia operacional. As redes de tecnologia operacional surgiram por conta de necessidade de descentralizar o processamento e a aquisição de sinais provenientes de sensores e atuadores numa planta industrial, uma vez que sensores e atuadores são distribuídos numa planta numa área grande, e o cabeamento individual dos dispositivos torna o sistema mais complexo e suscetível à falha. O projeto das diversas redes de barramento de campo empregadas hoje tem por fim garantir a aquisição de sinal com precisão e em tempo real, mas elementos como suscetibilidade à intrusão e armazenamento de dados para uso posterior não eram prioritários. No cenário da Indústria

4.0, onde a integração vertical pode incluir exposição à internet, as redes de barramento de campo passaram por uma grande transformação, saindo de modelos baseados em mestre-escravo e comunicação serial e caminhando para uma estrutura TCP/IP. Este grau de integração é algo comum para redes de computadores e os riscos envolvidos nisso são objetos de estudo há décadas. No que se refere às redes de barramento de campo, os seus dispositivos diferem muito dos computadores, tanto na sua aplicação como na sua estrutura, e os riscos ao qual estas redes estão submetidas diferem muito aos das redes de tecnologia de informação. Desta forma, por mais que muitos dos problemas referentes à segurança de dados em redes de tecnologia operacional e de informação sejam compartilhados, há agentes de risco específicos das redes de tecnologia operacional, que não podem ser descartados por terem sua ação potencializada pelo risco envolvido específico da operação de sensores e atuadores presentes nos sistemas de automação industrial.

1.2 Hipótese

Para definir uma estratégia de defesa cibernética que atenda às necessidades específicas de redes de tecnologia operacional, é necessário um estudo de suas fragilidades. Devido à grande diversidade de redes de tecnologia operacional, foi selecionada a rede Ethernet Industrial utilizando protocolos da família PROFIBUS, e foi analisado em específico o protocolo S7comm, utilizado na interação entre CLPs das família S7-300/400 e demais dispositivos de campo. Com base neste estudo de fragilidades é proposta como hipótese de ação de contenção de riscos o uso de hardware e software assistentes, que reduzam a ação dos agentes de risco identificados em comunicações utilizando protocolo S7comm, trazendo visibilidade para eventos de modificação do código executável em CLPs da família S7-300/400.

1.3 Objetivos

Esta pesquisa tem por objetivo conhecer quais os principais agentes de risco que devem ser levados em conta no projeto de redes de tecnologia operacional visando uma maior segurança de operação e buscar por soluções que atendam às especificidades de redes de barramento de campo.

1.3.1 Objetivos gerais

Esta pesquisa tem por objetivo principal abordar o tema Segurança em redes de tecnologia operacional baseados em PROFIBUS de CLPs Siemens da família S7-300 e S7-400. Esta temática é relevante pois os ambientes industriais estão cada vez mais integrados à internet. Ataques a redes de computadores de grandes indústrias e orgãos

públicos ganharam notoriedade nos últimos anos com o relato de ataques por parte de grupos *hackers*. A intrusão desta natureza às redes de barramento de campo, que são compostas por tecnologia operacional podem trazer um prejuízo ainda maior que ataques a redes de computadores, por serem capazes de destruir um parque industrial e causar dano físico àqueles próximos ao ambiente industrial alvo. Os objetivos gerais desta pesquisa são conhecer melhor a diferença entre sistemas de tecnologia de informação e tecnologia operacional e definir quais são estes agentes de risco presentes nas redes de tecnologia operacional.

1.3.2 Objetivos Específicos

Uma vez que boa parte dos conceitos a serem discutidos demandará conhecimento de redes de tecnologia operacional, um material introdutório resumido terá por objetivo expor conceitos relacionados a redes desta natureza, com enfoque em redes da família PROFIBUS. Uma vez abordados os temas introdutórios relacionados a redes de barramento de campo, outros temas surgem com objetivos mais diretamente relacionados aos objetivos gerais. Com base em tudo isso, os objetivos específicos definidos são os seguintes:

a)- Definir redes de tecnologia operacional e diferenciá-las de redes de tecnologia de informação.

b)- Conhecer os principais protocolos empregados em redes de barramento de campo baseado em PROFIBUS em CLPs Siemens das famílias S7-300 e S7-400.

c)- Conhecer e analisar meios de ataques relacionados à segurança cibernética de redes de tecnologia operacional.

d)- Propor ações de contenção com base nas tecnologias e normas técnicas disponíveis para tal e tendo em vista demandas específicas das redes de barramento de campo.

1.4 Justificativa

Uma das justificativas para esta pesquisa é viabilizar um desenvolvimento mais seguro da Indústria 4.0 no ambiente fabril. A integração de dispositivos inteligentes a redes externas à indústria traz consigo riscos que incomodam não apenas as grandes corporações mas também aqueles que estão geograficamente inseridos próximos a estas indústrias. Ataques cibernéticos têm sido utilizados também como instrumento de guerra, e redes de tecnologia operacional possuem dispositivos que podem atuar como armamentos bélicos. O caso STUXNET, ocorrido em Junho de 2010, trouxe luz à importância de tratar dispositivos de tecnologia operacional de uma maneira diferente dos dispositivos de tecnologia de informação e exemplificou o potencial de exploração com fins bélicos que estes

dispositivos de campo possuem. A planta de geração de energia nuclear Iraniana que sofreu o ataque STUXNET utilizava tecnologias de controle industrial aplicadas em indústrias dos mais diversos ramos, com um ataque direcionado a CLPs Siemens da Família S7-300 e S7-400, que são dispositivos empregados até hoje. Conforme divulgado pelo fabricante destas famílias de CLP, a família S7-300 iniciou o processo de *phase-out* em outubro de 2023 e poderão ser descontinuados apenas após outubro de 2035, sendo a família S7-400 indicada como uma das substitutas funcionais, sinalizando uma previsão ainda mais futura de descontinuação desta família de dispositivos de automação. (SIEMENS, 2022). Por ainda serem dispositivos em produção pelo fabricante e com forte adoção em diversas áreas da indústria, as famílias S7-300 e S7-400 de CLPs da Siemens continuam sendo um assunto relevante e são objeto de estudo neste trabalho de pesquisa.

1.5 Estrutura do trabalho

Este trabalho segue com um material elaborado no Capitulo 2 que é uma revisão bibliográfica sobre características de redes OT com ênfase em redes PROFIBUS, PROFInet e Ethernet Industrial; Indústria 4.0 e seu papel na demanda por integração IT-OT e conceitos básicos de Segurança de redes. O Capítulo 3 é uma revisão bibliográfica sobre as justificativas para integração IT-OT e desafios esperados. O Capítulo 4 é uma demonstração prática das vulnerabilidades reportadas do protocolo S7comm e o Capítulo 5 apresenta estratégias para mitigar os riscos envolvidos na integração IT-OT envolvendo CLPs que utilizam o protocolo S7comm e conclui propondo e descrevendo um monitor de código fonte baseado em ferramentas de código aberto.

2 CONCEITOS BÁSICOS

Antes de discutir a segurança em redes de tecnologia operacional, um material introdutório tem por finalidade definir conceitos importantes relacionados a redes desta natureza.

2.1 Sistemas de tecnologia operacional e de informação

2.1.1 Definição

Em ambiente industrial é comum distinguir as redes de comunicação em duas classes: redes de escritório, que é composta por tecnologias de informação, e redes de controle de processo, que é composta por tecnologias operacionais. As redes tecnologias de informação (IT) processam e armazenam dados voltados a gestão de negócio enquanto as redes de tecnologias operacionais (OT) são projetadas para controlar processos de fabricação (CRAIG; BROOKS, 2022).

A norma técnica ISA-95 propõe uma divisão de redes de comunicação em cinco níveis, que define o tipo de dados que são úteis em cada nível e assim determinam o tipo de rede a ser utilizado, conforme a Figura 1 (CRAIG; BROOKS, 2022).

Um processo de nível 0 é denominado processo físico, e este nível é onde o processo de manufatura em si ocorre.

Um processo em nível 1 é composto por dispositivos de controle. Estes dispositivos de controle podem ser tanto dispositivos de controle centralizados como também sensores e atuadores inteligentes. Neste nível de processo há trocas de dados que ocorrem em um intervalo de tempo inferior a um segundo. As redes aplicadas nestas circunstâncias devem possuir uma latência muito baixa e não podem permitir perda de dados. Neste contexto se aplicam as redes de barramento de campo.

Um processo nível 2 é composto por sistemas SCADA. Neste nível ocorre a transformação de dados discretos em informações úteis para a intervenção humana. As interfaces homem-máquina são aplicadas neste contexto, conectadas a sistemas de controle numa troca de dados que deve possuir, dentre outras características, baixíssima latência e alta confiabilidade na transmissão de dados. A comunicação entre dispositivos de controle e sistemas de supervisão costuma ocorrer por redes de barramento de campo.

Um processo nível 3 é composto por sistemas voltados à gestão de operações de manufatura. Os sistemas MES, que se encarregam de adquirir dados do processo provenientes dos sistemas de controle e transformar em informação útil para a gestão do

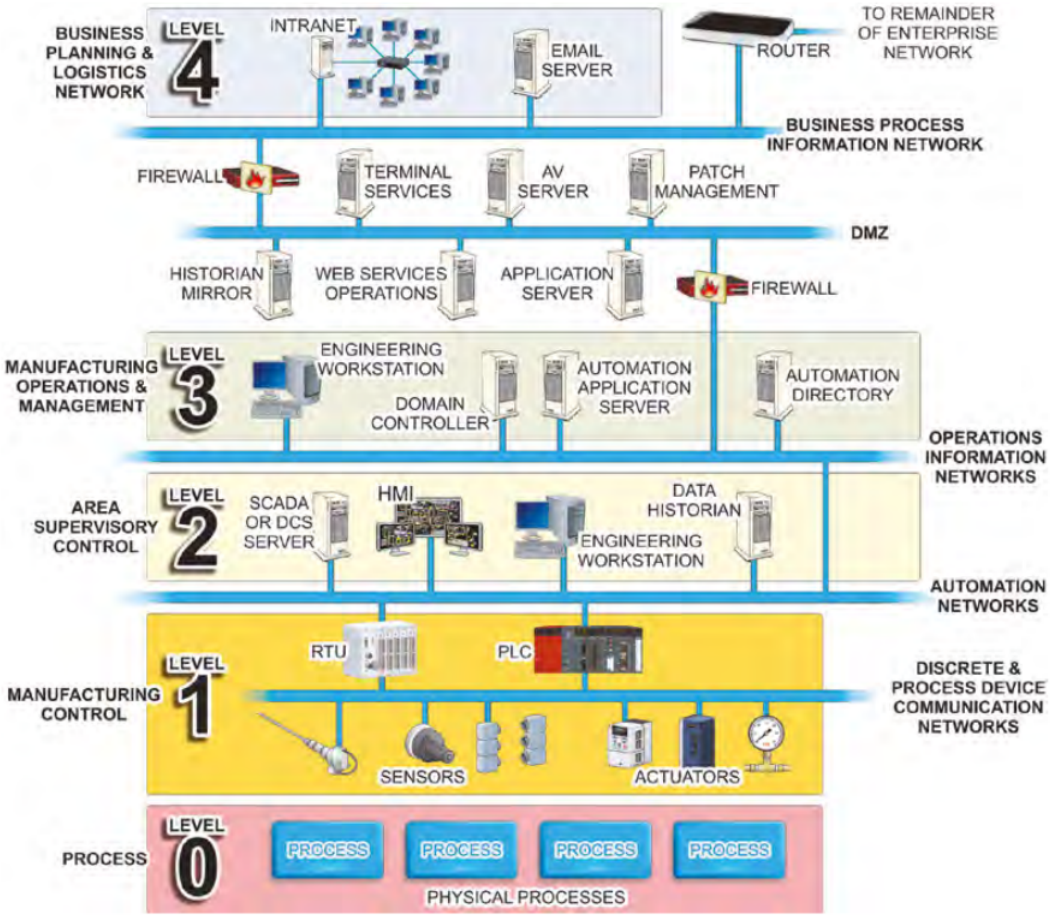

Figura 1 – Estrutura de Integração OT-IT
(CRAIG; BROOKS, 2022)

processo se encaixam neste nível. A comunicação entre sistemas de controle e sistemas MES não exigem a mesma baixa latência que a comunicação com sistemas SCADA e não exigem uma comunicação por protocolos e meios físicos específicos, o que abre margem para aplicação de estruturas de rede semelhantes àquelas vistas em redes de tecnologia de informação. Os dados adquiridos por estes sistemas costumam fazer sentido quando correlacionados com dados colhidos por horas, dias e até semanas, diferindo muito dos processos nível 2 onde os dados colhidos pelo sistema de controle são para uso imediato. Processos de nível 3 costumam ser definidos como responsáveis pela interface entre sistemas de tecnologia de informação e sistemas de tecnologia operacional.

Um processo nível 4 é composto por sistemas voltados ao planejamento de negócio e de logística. Este nível ocorre a uma distância grande dos dispositivos de controle. Se inserem neste nível sistemas ERP, que são aplicados para gerenciamento geral de um processo de manufatura, assim como gestão de empregados, fluxo logístico e demais atividades voltadas à manutenção do processo de manufatura enquanto negócio. Informações colhidas neste nível costumam ser úteis num intervalo de dias, semanas e até meses. É comum que haja correlação entre os dados colhidos em diversos processos de manufatura diferentes

neste nível. Redes projetadas neste nível podem fazer uso da internet. Neste nível, há o emprego de sistemas de tecnologia de informação e o modelo das redes se dá com base em redes de computadores.

Os processos de níveis 1 e 2 são compostos por sistemas de tecnologia operacional, e são objeto principal deste trabalho de pesquisa. Em suma, tecnologia operacional é composta por sistemas de controle industrial (ICS) e sistemas supervisórios e de aquisição de dados (SCADA), e a comunicação entre eles se dá por redes de barramento de campo (*Fieldbus*).

2.1.2 Sistemas de controle industrial

Um sistema de controle é aquele encarregado por executar instruções conforme um programa para que algum processo de manufatura ocorra. Dispositivos comumente empregados para este fim são os CNCs, Robôs industriais, CLPs, DCSs e PCs industriais. Este controle pode se dar em malha aberta ou malha fechada (GROOVER; JAYAPRAKASH, 2015).

Um sistema em malha fechada é composto por um parâmetro de entrada, um controlador, um atuador, um sensor de realimentação que atua como monitor do processo, o processo e a variável de saída. O parâmetro de entrada representa um parâmetro desejado na saída, e é definido de acordo com o processo desejado. O sistema de controle em malha fechada utiliza o controlador para executar comparação entre o valor obtido pelo sensor de realimentação e o parâmetro de entrada e, com base nesta comparação, utilizar atuadores de maneira adequada, de forma que se obtenha o parâmetro de saída desejado e assim o processo ocorra da maneira desejada (GROOVER; JAYAPRAKASH, 2015).

Um sistema em malha aberta difere de um sistema em malha fechada por dispensar o uso de um sensor de realimentação. O elemento controlador atua de acordo com o modelo real que possui e aciona os atuadores sem a possibilidade de comparar a variável de saída com a desejada. Este tipo de aplicação em um sistema de manufatura costuma depender de um elemento humano como monitor do processo, e diminui o grau de automação do processo em questão (GROOVER; JAYAPRAKASH, 2015).

Dentro da responsabilidade de um sistema de ICS em executar instruções, sistemas mais modernos são capazes de executar monitoramento de elementos relacionados à segurança do processo de manufatura em questão, diagnóstico de confiabilidade dos componentes do processo incluindo coleta de informações úteis para manutenção preditiva e detecção precisa de erros (GROOVER; JAYAPRAKASH, 2015).

Para definir um dispositivo de controle como ICS ele deve ser capaz de responder em tempo real, ou seja, num intervalo de tempo que não traga prejuízos ao processo. As intervenções no processo por parte de um ICS se dão utilizando eventos ou tempo

como gatilhos. A execução das instruções solicitadas deve ocorrer com o mínimo de atraso, exigindo assim que ele seja multitarefas. Dentre as suas instruções, ele deve ser capaz de fazer intertravamentos no processo, deve adquirir amostra de dados num ciclo pré-estabelecido, deve ser capaz de realizar interrupções para priorizar tarefas mais críticas e de lidar com exceções de acordo com instruções previstas para este fim (GROOVER; JAYAPRAKASH, 2015).

2.1.3 Sistemas de supervisão e aquisição de dados

Do ponto de vista de software, o sistema SCADA é uma aplicação executada em uma plataforma computacional que está conectada a um ICS por uma rede de barramento de campo.Ele possui um banco de dados local que armazena um histórico para análise de tendência do processo. Normalmente, estes dados obtidos do processo são advindos do monitoramento de algum parâmetro pré-definido do processo associado a um *timestamp* (CRAIG; BROOKS, 2022).

Este tipo de sistema se comunica com dispositivos ICS por redes de barramento de campo e costumam possuir uma interface de rede adicional compatível com sistemas IT, uma vez que se trata de uma plataforma computacional executando uma aplicação sobre um sistema operacional.

2.2 Redes de barramento de campo

Uma rede de barramento de campo é uma comunicação bilateral entre dispositivos inteligentes de campo. Ela surge com vários fabricantes individuais, cada um com seus protocolos proprietários, com o intuito de conectar dispositivos distribuídos em campo num modelo de periferia descentralizada. Desde meados da década de 1980 há um esforço em estabelecer um padrão de rede de barramento de campo, mas ainda hoje existem diferentes padrões que não são interoperáveis. As famílias mais dominantes hoje são a *Foundation Fieldbus* e PROFIBUS (SEN, 2017).

2.3 Modelo OSI/ISO

Um conceito muito importante no estudo de qualquer tipo de rede é o empilhamento de protocolos. As redes PROFIBUS seguem o modelo OSI/ISO, também empregado na internet, baseada nos protocolos Ethernet e TCP/IP (SEN, 2017). O modelo OSI propõe uma divisão em sete camadas de comunicação (conforme Figura 2), sendo elas:

1.Camada Física: Responsável pelos mecanismos de transporte de dados pelo meio físico.

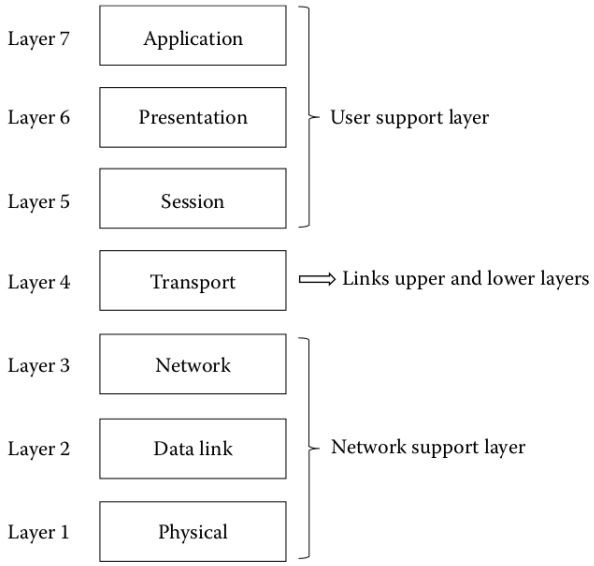

Figura 2 – OSI-ISO
(SEN, 2017)

2.Camada de Enlace: Responsável pela comunicação entre nós adjacentes da rede.

3.Camada de Rede: Responsável pela definição do percurso entre origem e destino do pacote transmitido.

4. Camada de Transporte: Responsável pela entrega do pacote ao serviço que aguarda o pacote no destino.

5. Camada de Sessão: Responsável por controlar o diálogo entre origem e destino.

6. Camada de Apresentação: Responsável pela descompressão e interpretação da mensagem contida no pacote.

7. Camada de Aplicação: Responsável por processar a mensagem recebida.

Estas 7 (sete) camadas podem ser agrupadas em 3 (três) subgrupos. As camadas 1,2 e 3 se referem ao suporte à rede, as camadas 5,6 e 7 se referem ao suporte ao usuário e a camada 4 é a interface entre rede e usuário. Na internet, as camadas de suporte ao usuário não costumam existir e os pacotes são entregues diretamente à aplicação desejada. Em redes de barramento de campo é comum que haja protocolos de camada de sessão e apresentação, que inclusive servem de auxílio para manutenção do tempo de resposta e confiabilidade de dados transmitidos. Uma abordagem contrária à essa também ocorreu no passado no que se refere às redes de barramento de campo que estão em uso há mais tempo, como as PROFIBUS-FMS, PROFIBUS-DP e PROFIBUS-PA, onde o modelo de 7 camadas é resumido em camada física, enlace e aplicação, e o objetivo é otimizar a capacidade de processamento dos dispositivos para viabilizar a aplicação destas redes com as restrições de processamento impostas na época (SEN, 2017).

2.4 PROFIBUS e PROFINET

O nome PROFIBUS vem da junção das palavras *Process Fieldbus* e foi desenvolvida, inicialmente pela Siemens. Sua principal característica é a aplicabilidade onde o tempo de resposta é um fator crítico, característica muito desejada em redes de barramento de campo. Este padrão hoje não é vinculado à uma empresa e segue o modelo OSI/ISO para comunicação. As normas alemã DIN 19 245 e europeia EN 50170 servem de base para este padrão. Existem três versões em uso, sendo a PROFIBUS-FMS voltada para comunicação multimestre e ponto-a-ponto, a PROFIBUS-PA voltada a aplicações onde segurança é um fator especialmente interessante e PROFIBUS-DP com uma estrutura de mestre e escravo. As comunicações pelas redes da família PROFIBUS utilizam como meio físico RS-485, RS-485-IS, MBP e fibra óptica. O PROFINET foi incluído posteriormente e faz uso de uma estrutura baseada em ethernet e o PROFIsafe possui versões com diversos meios físicos, que incluem o ethernet.(SEN, 2017)A Figura 3 descreve o empilhamento dos protocolos comuns ao Profibus em meio físico RS485, fibra óptica e MBP.

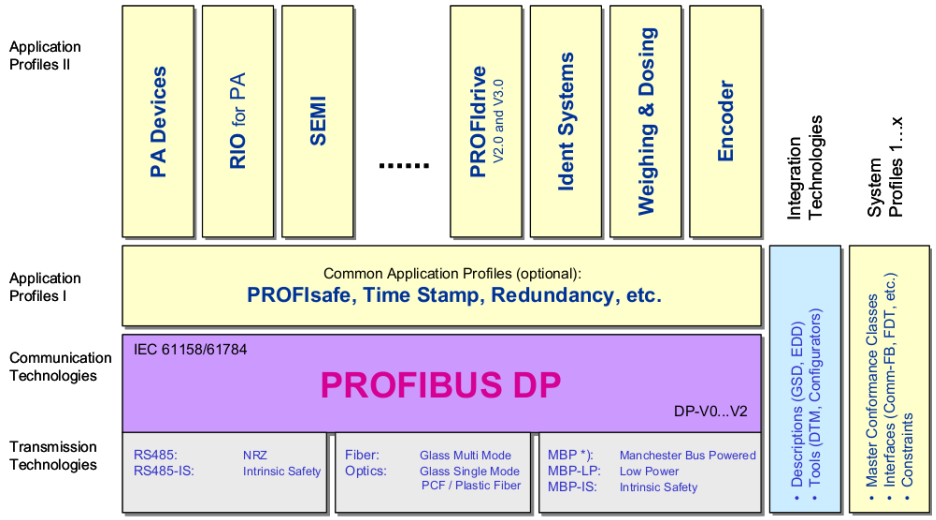

Figura 3 – Emplilhamento típico para PROFIBUS (PROFIBUS. . . , 2002)

2.4.1 RS485

O meio físico RS485 emprega um par trançado de fios de cobre e atinge taxas de transmissão entre 9,6 Kbit/s e 12 Mbit/s com até 32 estações conectadas num único segmento. O início e o fim da rede possuem terminadores de rede (descrito na Figura 4) e há a possibilidade de emprego de repetidores para expansão da rede. Para aplicações intrinsecamente perigosas (por exemplo, aplicações relevantes à segurança) que fazem uso do meio físico RS485, há um caso especial denominado RS485-IS onde há a exigência de atendimento a níveis de tensão e corrente específicos para a transmissão de dados e dispositivos que atendam a estes requisitos.

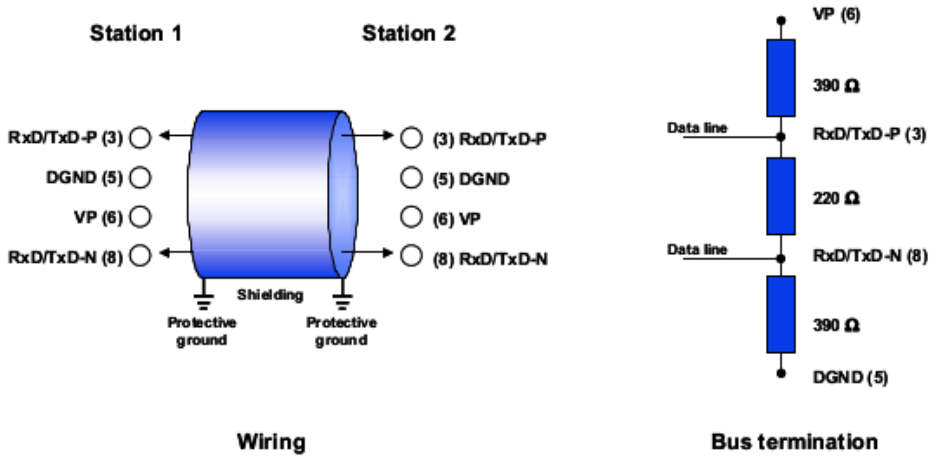

Figura 4 – Cabeamento e terminação RS485
(PROFIBUS. . . , 2002)

2.4.2 MBP

O meio físico MBP aplica em conjunto dois atributos: a codificação de *Manchester* e Barramento ativo. Neste meio físico, a taxa de transmissão de dados é de 31,25Kbit/s utilizando cabos e terminação iguais ao RS485 com capacidade restrita a 32 dispositivos por segmento (desde que atenda aos níveis de tensão e corrente especificados). Sua principal aplicação é em aplicações intrinsecamente perigosas, como em ambientes com atmosfera explosiva. É comum que se use este meio físico apenas em um trecho do segmento de rede, em áreas de alto risco, e que este trecho seja acoplado a outros segmentos em meio físico RS485, por acopladores transparentes para o restante da rede.(PROFIBUS. . . , 2002)

2.4.3 Fibra óptica

Em aplicações em que há uma interferência eletromagnética muito alta ou em que há de se percorrer longas distâncias, o emprego de fibra óptica é mais adequado. Sistemas utilizando opto-acopladores fazem o acoplamento entre meio físico RS485 (ou MBP) e fibra óptica, conectando os segmentos de rede de maneira transparente. A Figura 5 lista as caracerísticas de fibra óptica aplicáveis para este fim.(PROFIBUS. . . , 2002)

2.4.4 Protocolo de enlace PROFIBUS DP

O protocolo DP (periferia descentralizada) atua na camada de enlace e tem por finalidade troca rápida de dados entre CLPs e dispositivos de campo. Ele se divide em três modos, de acordo com a demanda requerida pela aplicação (conforme descrito na Figura 6).

O DP-V0 trata em geral da leitura cíclica dos estados dos I/Os e diagnóstico de

Fiber type	Core diameter [µm]	Range
Multimode glass fiber	62.5/125	2-3 km
Singlemode glass fiber	9/125	> 15 km
Plastic fiber	980/1000	< 80 m
HCS® fiber	200/230	approx. 500 m

Figura 5 – Fibra Óptica em PROFIBUS
(PROFIBUS..., 2002)

falhas funcionais dos dispositivos e do canal de comunicação. O DP-V1 trata de comunicação assíncrona, com prioridade inferior ao DP-V0 trocando dados como confirmação de alarmes. O DP-V2 tem função de *broadcast*, para comunicação direta entre módulos escravos, sincronização de *clock* (operação isócrona), controle centralizado do *Time-stamp* e operações de download e upload. (PROFIBUS..., 2002)

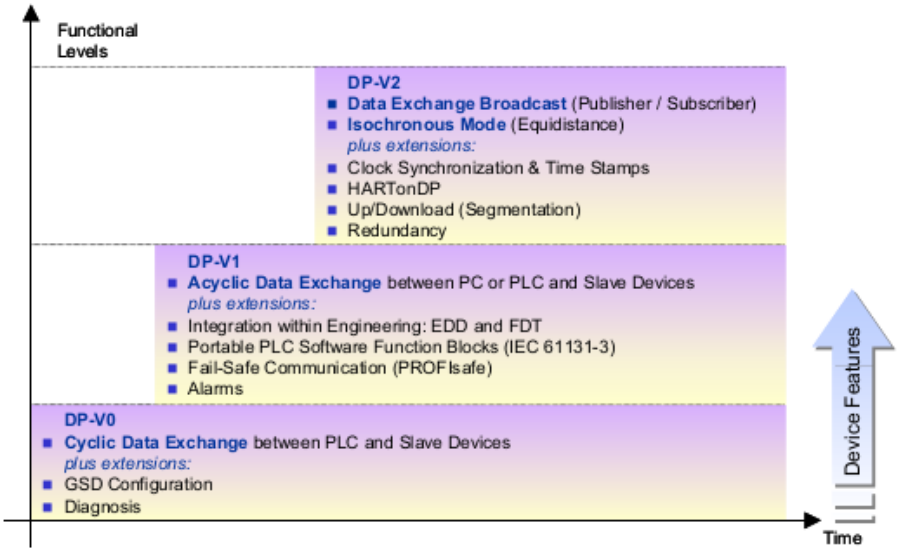

Figura 6 – Características PROFIBUS DP
(PROFIBUS..., 2002)

2.4.5 Protocolos de aplicação em PROFIBUS

Os protocolos de aplicação em PROFIBUS são diversos e podem ser caracterizados em de aplicação geral ou específica. A diferença essencial destes protocolos é em relação à forma que interagem com os dispositivos de campo, possibilitando compatibilidade com dispositivos que empregam modelo de comunicação proprietário ou que, devido à sua aplicação, devem atender a padrões específicos de comunicação (sistemas pneumáticos, inversores de frequência e sistemas relevantes para segurança, por exemplo).

Dentre os protocolos de aplicação geral destacam-se o PROFIsafe, HART, *Time-stamp* e *Slave redundancy*. O protocolo PROFIsafe se usa em aplicações relevantes para segurança (como barreiras de luz, botões de emergência e chaves de intertravamento, por exemplo) e atinge a categoria SIL3, utilizando recursos como envio de telegramas consecutivos, monitoramento de tempo excedido para confirmações nos envios de dados, identificador único entre emissor e receptor e CRC. Devido ao PROFIsafe implementar estas medidas de segurança em nível de aplicação, é possível utilizar um mesmo segmento com mesmo meio físico para todos os dispositivos, facilitando integração e barateando custos. O HART em camada de aplicação permite compatibilidade com dispositivos HART em rede PROFIBUS de maneira simplificada. O *Time-stamp* provisiona data e horas precisas para gestão de alarmes e avisos programados para controle da planta. O *Slave-redundancy* permite que pacotes sejam enviados em redundância, por interfaces primárias e secundárias, e que o mestre execute um diagnóstico da qualidade do envio de dados (PROFIBUS. . . , 2002).

Dentre os protocolos de aplicação específica estão o *PROFIdrive*, PA, *Fluid Power*, *SEMI*, *Ident Systems* e *Remote I/O for PA*. O *PROFIdrive* é aplicado a *Drives* de sistemas elétricos, desde inversores de frequência até servo-controles complexos. O PA é aplicado a dispositivos inteligentes, que enviam sinais pré-processados. O *Fluid Power* se aplica a atuadores aplicados a fluídos, como bombas e válvulas proporcionais, tratando de calibração, linearização de valores em escala, monitoramento para falhas funcionais e modo de operação. O *SEMI* se aplica a dispositivos que utilizam o padrão especificado pela organização *"Semiconductor Equipment and Materials International"*. O *Ident Systems* é aplicado a *transponders* e leitores de código. Por fim, o *Remote I/O for PA* é dedicado para comunicação com estações remotas.(PROFIBUS. . . , 2002)

2.4.6 PROFInet

O padrão PROFInet é uma evolução dos padrões inicialmente adotados pelo PROFIBUS e possui características chave para facilitar automação e digitalização sendo elas:

- Integrável verticalmente com redes de gerenciamento corporativo por utilizar Ethernet.
- Integrável horizontalmente por ser independente de fabricante e por manter compatibilidade com padrões Profibus.
- Implementado com base em padrões de redes de tecnologia de Informação.

2.4.7 Comunicação Ethernet nas famílias S7-300 e S7-400

A capacidade de dispositivos de campo de se comunicar em redes Ethernet baseadas em TCP/IP é um salto muito importante para permitir a digitalização de plantas industriais. Os CLPs Siemens das famílias S7-300 e S7-400 possuem este recurso e se comunicam em redes Ethernet Industrial e PROFInet, seja de maneira nativa ou por utilizar processadores de comunicação (CPs). A Figura 7 mostra a relação entre as redes PROFInet (PN), Ethernet Industrial (IE) e o Ethernet. Por facilitar a integração vertical destes dispositivos, o emprego dos protocolos TCP/IP tornam também estes dispositivos mais expostos, uma vez que se tornam acessíveis também por computadores e suas redes, antes dedicadas à comunicação maquina-à-máquina, podem ser roteadas para redes externas, incluindo a própria internet (SUPORT, 2023).

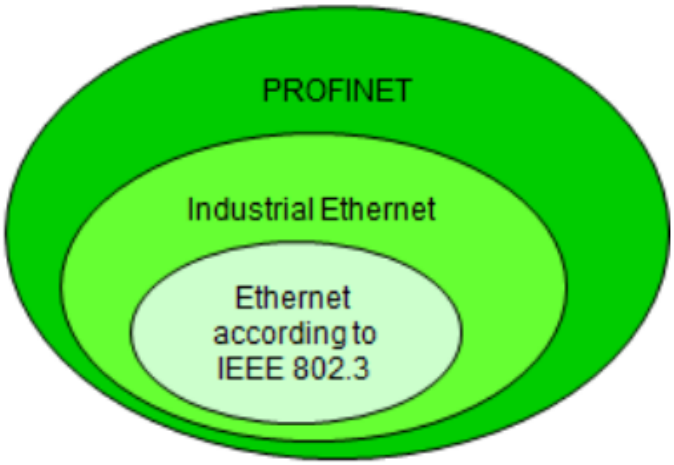

Figura 7 – Relação entre PN, IE e Ethernet
(SUPORT, 2023)

O protocolo Ethernet Industrial utiliza nas camadas física e de enlace o protocolo Ethernet. As implementações que utilizam o protocolo S7 podem fazê-lo saltando da camada de enlace diretamente para a camada de transporte, utilizando o protocolo ISO, ou utilizando o protocolo IP na camada de rede e utilizando o protocolo TCP associado ao protocolo *ISO-on-TCP* (ilustrados na Figura 8).

O protocolo S7 se divide em dois tipos: *S7 basic communication* e o *S7 communication*. O *S7 basic communication* serve para comunicar dois dispositivos apenas utilizando interface de rede integrada da CPU, enquanto o *S7 communication* utiliza também processadores de comunicação e permite comunicação com dispositivos terceiros.(SUPORT, 2023). Utilizando o protocolo *S7 communication* (s7comm) é possivel estabelecer conexão com CLPs Siemens S7-300 e S7-400 e executar ações como leitura e escrita de dados, dentre outros recursos.

O protocolo S7 define o formato de comunicação mais adequado entre dispositivos, principalmente num modo cliente-servidor, como em comunicações entre IHM e CLP. A

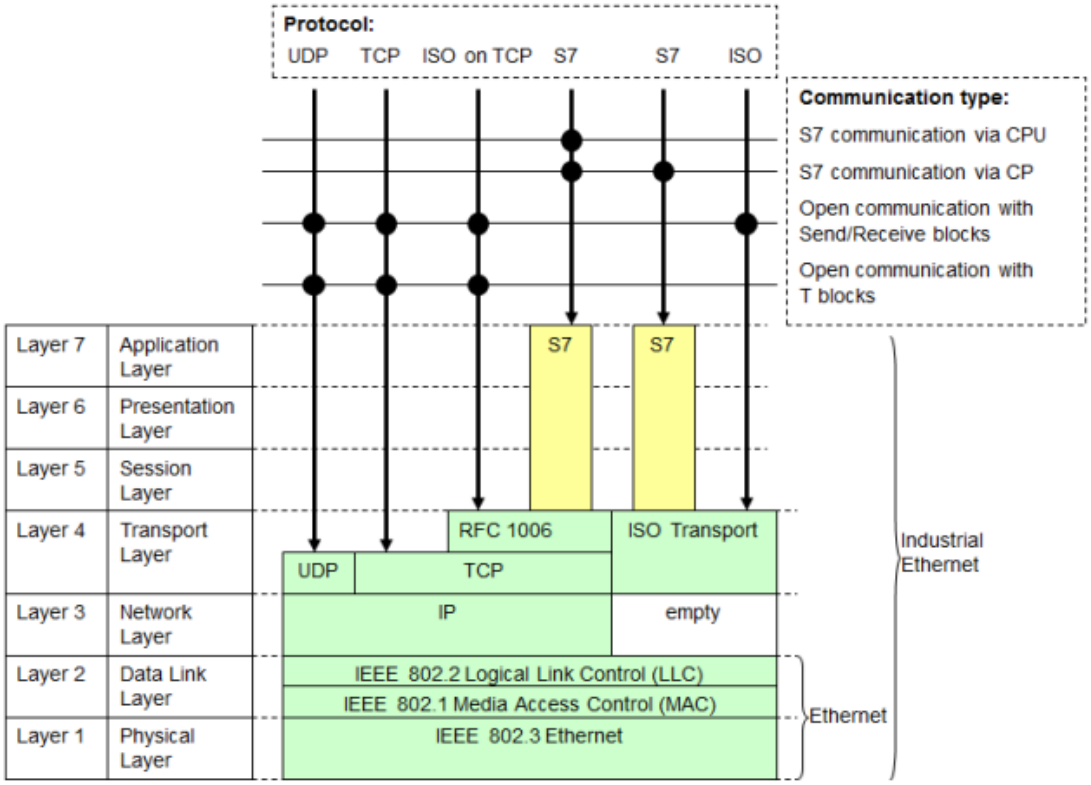

Figura 8 – Protocolos compatíveis com o Ethernet Industrial (SUPORT, 2023)

Siemens utiliza duas versões do protocolo *S7 communication*: o protocolo 0x32, conhecido como S7comm nas famílias mais antigas (incluindo S7-300 e S7-400) e o protocolo 0x72, conhecido como S7commPlus. O protocolo S7commPlus possui 3 versões. O S7commPlusV3, implementação mais nova do *S7 communication*, é a versão utilizada na família S7-1500 e possibilita o uso de recursos como alteração de modo de operação (*RUN/STOP*), *Download/Upload* do código fonte e ler/escrever valor de uma variável de controle. Apesar de este protocolo possuir recursos que demonstram preocupação com segurança de dados, Alsabbagh e Langendoerfer relatam ter conseguido realizar um ataque de injeção de código malicioso utilizando este protocolo. (ALSABBAGH; LANGENDOERFER, 2022a) O protocolo S7comm, como primeira implementação do protocolo *S7 communication*, utilizado em CLPs S7-300 e S7-400 apresenta ainda mais brechas exploráveis para acesso malicioso, algumas dessas brechas serão exemplificadas nesta pesquisa.

O Ethernet Industrial é um padrão projetado para integração com sistemas corporativos e, nesta pesquisa, os experimentos serão realizados em rede Ethernet Industrial, utilizando o protocolo S7comm para interagir com o CLP, em um ambiente simulado, compatível com um cenário real.

2.5 Indústria 4.0

Conforme relatado por Hermann, Pentek e Otto, uma definição clara, concreta e aceita de forma geral da indústria 4.0 ainda não foi publicada. Eles complementam que ela costuma ser descrita em termos de cenários, visão e tecnologias habilitadoras (HERMANN; PENTEK; OTTO, 2015).

A indústria 4.0 tem grande contribuição para a demanda por convergência entre IT e OT observada hoje. Serão descritas as tecnologias habilitadoras para definir as demandas básicas da indústria 4.0 e o seu plano de implementação com base em graus de maturidade que mostra a agregação de valor potencial da implantação da indústria 4.0.

2.5.1 Grau de maturidade de implantação da Industria 4.0

O índice de maturidade da implantação da Indústria 4.0 está descrito na Figura 9 e define etapas de maturidade da implantação da indústria 4.0 (BECKER et al., 2022).

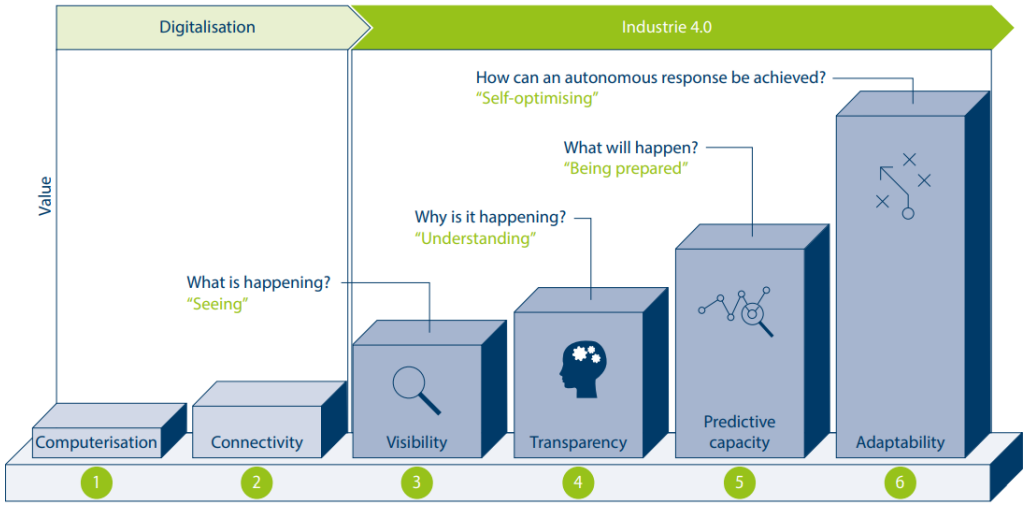

Figura 9 – Estágios da implantação da Industria 4.0
(BECKER et al., 2022)

2.5.1.1 Fase de digitalização

A fase de digitalização corresponde aos estágios de Informatização e Conectividade e serve de sustentação para a implantação dos estágios referentes à Industria 4.0. No estágio de Informatização há a aplicação de sistemas computacionais adquirindo dados para processamento interno e ainda sem interação com sistemas adjacentes. Na etapa de Conectividade parte dos sistemas de tecnologia Operacional empregados na indústria se comunicam com sistema de tecnologia de Informação e a adoção de dispositivos OT com capacidade de comunicar em rede com protocolo IP na camada de rede é crescente.(BECKER et al., 2022)

2.5.1.2 Etapas de Visibilidade e Transparência

Na etapa de visibilidade, sensores são empregados para captura de dados de processo em tempo real criando assim uma sombra digital do processo e possibilitando a obtenção de KPIs atualizados. Na etapa de transparência, os dados coletados em tempo real pela sombra digital são armazenados gerando assim uma base de *big data* que é analisada para justificar comportamentos indesejados e identificar causa raiz de problemas.(BECKER et al., 2022)

2.5.1.3 Etapas de Capacidade Preditiva e Adaptabilidade

Na etapa de Capacidade Preditiva, os dados coletados e processados são utilizados para simulação e assim é possível projetar a sombra digital no futuro e simular cenários futuros e que podem ocorrer, avaliar qual a probabilidade de cada um e recomendar ações para cada cenário. Na etapa de Adaptabilidade, a tomada de decisão no caso de um cenário previsto se concretizar é tomada de maneira autônoma.(BECKER et al., 2022)

2.5.2 Tecnologias Habilitadoras da Industria 4.0

Conforme proposto por Russmann, a Indústria 4.0 tem por base tecnológica nove tendências, que estão ilustradas na Figura 10 e definidas como segue:(RÜSSMANN et al., 2015)

Figura 10 – Tecnologias habilitadoras da Indústria 4.0 (RÜSSMANN et al., 2015)

- *Big Data* e *Analytics*: É a aquisição de grandes bases de dados de diversas fontes para análise e tomada de decisão.

- Robôs autônomos: Robôs autônomos têm por característica interagir com demais robôs e com humanos de maneira segura, empregando sistemas de visão e outras tecnologias que dêem melhor capacidade de decisão aos robôs.
- Simulação: A simulação tem por finalidade gerar um modelo virtual que seja um espelho do que existe fisicamente para teste e otimização de configuração e *setup* de máquinas.
- Integração: A integração tem por finalidade facilitar a interação entre diferentes sistemas de IT, trocando dados de produto e processo entre diversos departamentos. Essa integração é horizontal quando ocorre num mesmo nível, geralmente no nível de processo em interação máquina-à-máquina (M2M). Este integração é vertical quando ocorre entre os diferentes níveis das redes industriais.
- IIoT: Se baseia em empregar dispositivos inteligentes de forma que o processamento da informação seja mais descentralizado e que seja possível interação entre diferentes dispositivos em rede.
- Cibersegurança: Comunicação segura, confiável com gestão de acesso e identidade dos usuários.
- A Nuvem: Armazenamento e processamento de dados de processo em um servidor remoto.
- Manufatura Aditiva: Utilizar técnicas como a impressão 3D para facilitar customização de produtos e reduzir necessidade de estocagem e distância de transporte.
- Realidade Aumentada: Dispor de modelos virtuais para descrição de processos.

2.6 Princípios de segurança em redes

A segurança de sistemas computacionais é definida como:

"A proteção conferida a um sistema de informação automatizado para atingir os objetivos aplicáveis de preservação da integridade, disponibilidade e confidencialidade de recursos de sistemas de informação."(STALLINGS, 2015)

Esta definição destaca três princípios básicos da segurança de sistemas computacionais: Confidencialidade, integridade e disponibilidade, conhecida como tríade da segurança. A confidencialidade se refere a garantir que informações privadas e confidenciais não sejam disponibilizadas para indivíduos não autorizados (confidencialidade de dados) e que haja mecanismos para permitir ou recusar coleta e armazenamento de dados por terceiros (privacidade). A integridade se refere a garantir que os dados sejam modificados apenas de

modo especificado e sob autorização (integridade de dados) e que o sistema que manipula os dados não seja modificado inadvertidamente (integridade de sistema). A disponibilidade se refere a manter o sistema em funcionamento, sem negar serviços a usuários autorizados.Além desta tríade, o conceito de autenticidade, que defende a existência de meios para verificar a validade da transmissão e o conceito de irretratabilidade, que defende a rastreabilidade de origem da informação costumam também ser incluídos como princípios de segurança de sistemas computacionais.(STALLINGS, 2015)

Uma comunicação segura pode ser pautada em quatro características principais, sendo elas a segurança operacional, Integridade da mensagem, autenticação de ponto final e confidencialidade (S-I-A-C).(KUROSE; ROSS, 2013)

A segurança operacional trata de buscar garantir que não haja danos físicos nem aos componentes do sistema de tecnologia operacional como às pessoas ao seu redor. A confidencialidade trata de medidas para que a mensagem transmitida seja de conhecimento exclusivo dos dispositivos de origem e destino. A integridade trata de garantir que o conteúdo da mensagem não seja alterado no meio do processo de transmissão. A autenticação envolve conhecer a identidade do remetente e do destinatário da mensagem.(KUROSE; ROSS, 2013)

Nas redes de barramento de campo, o conceito de segurança toma uma forma diferente por se aplicar em sistemas ciberfísicos. A segurança operacional é o princípio mais importante e isso se dá por conta do potencial perigo associado ao uso inadvertido de tecnologias operacionais. A depender da natureza do sistema de tecnologia operacional em questão, os danos que podem ser causados vão além do comprometimento da estrutura física do sistema em questão e pode por em risco a saúde e segurança de pessoas ao redor deste sistema. Logo em seguida, a integridade de dados também ganha importância. Em aplicações onde há a necessidade de um tempo de resposta muito baixo, é comum que não haja tempo para solicitar uma retransmissão de dados e perda de um dado referente a um sistema de segurança poderia ocasionar um grave problema. A autenticação e a confidencialidade são princípios muito relevantes em redes de barramento de campo e também trazem um risco de operação ao sistema OT, e seu estudo se mantém justificado, principalmente em redes integradas à internet, que inclusive são uma tendência devido à forte integração que é um dos pilares da Industria 4.0.

3 Vantagens e desafios na Convergência entre redes IT e OT

A internet industrial das coisas, uma das tecnologias habilitadoras da Indústria 4.0, prevê obtenção de dados em redes de nível de campo e o fluxo destes dados para redes de nível gerencial e a internet, como meio de provisionar novos serviços e modelos de negócio. Este grau de integração insere a internet num ambiente em que há diversos sistemas ciberfísicos, o que traz uma série de desafios do ponto de vista de segurança de dados (KAGERMANN et al., 2013).

Um destes desafios são as limitações técnicas de dispositivos de campo. O longo tempo de vida útil destes dispositivos associado a ciclos de inovação curtos ocasiona uma grande diversidade de sistemas muitas vezes antigos e que não atendem a requisitos básicos de segurança de informação. A adoção de um sistema único padronizado para implementar maior segurança é dificultada pela diversidade dos sistemas e protocolos adotados, normalmente específicos a depender do fabricante ou da versão do dispositivo (KAGERMANN et al., 2013).

A indústria tem percebido o impacto que a adoção de software traz valor agregado ao seu produto e processo, e cada vez mais há a adoção de componentes de software na indústria. Esta percepção, porém, não vem acompanhada da percepção das ameaças do ponto de segurança da informação. Inclusive a preocupação com ameaças em OT se tornou evidente apenas após o aparecimento dos *malwares* STUXNET, Duqu e Flame. Em muitos casos, é necessário o desenvolvimento de soluções para estes problemas e, em casos em que estas soluções existem, a implementação é pendente.(KAGERMANN et al., 2013)

Utilizando como exemplo comunicações pelo protocolo S7comm, meio principal de interação com CLPS das famílias S7-300/400 da Siemens por Ethernet Industrial, muito do que é implementável em computadores modernos, como criptografia ponta a ponta e armazenamento extensivo de *logs* de acesso remoto, não é presente. A substituição de um CLP num processo industrial por um mais moderno que tenha melhor adequação aos pilares de segurança de dados causa um efeito cascata que pode ser difícil de justificar do ponto de vista financeiro. Mesmo o protocolo S7commplusV3, utilizado pela família S7-1500, indicada como sucessora das famílias S7-300 e S7-400 (SIEMENS, 2022), tem algumas vulnerabilidades publicadas, como o ataque de injeção realizado por Albbasagh (ALSABBAGH; LANGENDOERFER, 2022a) e o *cert-report* publicado no início deste ano pela Siemens relata uma fragilidade relacionada ao *firmware* de dispositivos da familia S7-1500 descoberta por Yuanzhe Wu e Ang Cui da empresa *Red Balloon Security* (WU; CUI, 2023).

A atualização de hardware torna disponível recursos úteis do ponto de vista de cibersegurança, mas por si só não é medida suficiente para mitigar os riscos envolvidos na integração vertical destas tecnologias sensíveis. Alsabbagh e Langendoerfer sugerem como meios de mitigar o impacto de ataques a CLPs S7-300 o uso de monitores ativos com capacidade de monitorar desde interações suspeitas via rede com o CLP até o seu próprio *firmware* (ALSABBAGH; LANGENDOERFER, 2022b). Um monitoramento ativo da rede associado a um monitoramento do código fonte do CLP pode ser útil para detectar acessos maliciosos a dispositivos OT e determinar a origem do ataque, por serem capazes de, em conjunto, detectar um evento de modificação do código-fonte do CLP e rastrear a origem dos pacotes de rede referentes a estas modificações.

3.1 Aplicações que demandam integração vertical

A integração de CLPs a redes IT é uma tendência que ganhou força com a evolução dos dispositivos inteligentes de campo. Ao mesmo tempo em que diante de um cenário de transição gradual de tecnologias mais vulneráveis do ponto de vista de segurança de informação para tecnologias menos vulneráveis, convergir redes IT e OT pode ser arriscado, dispositivos OT, como os CLPs, são empregados majoritariamente em ambientes de manufatura, e sistemas de manufatura possuem demandas específicas que são melhor atendidas por intermédio de tecnologias que necessitam de um certo grau de integração entre dispositivos IT e OT, como será descrito ainda neste capítulo.

3.1.1 Sistemas de Manufatura

Um sistema de manufatura é uma coleção de equipamentos integrados e recursos humanos, que em conjunto transformam matéria-prima num produto final através de processamento e montagem. A Figura 11 exemplifica o funcionamento de um sistema de manufatura e define seus componentes (GROOVER; JAYAPRAKASH, 2015).

Os dispositivos OT são aplicados nas tecnologias de controle e automação. Estas tecnologias inteligentes possuem informações referentes ao processo em tempo real que são relevantes para a realimentação dos sistemas de controle de qualidade e para os sistemas de suporte de manufatura.

3.1.2 Sistemas de controle de qualidade

Um sistema de qualidade tem por principais finalidades avaliar se o produto final possui as características definidas por projeto do ponto de vista funcional e estético e avaliar se o produto está livre de deficiências que tenham sido definidas em projeto como não toleráveis. Controlar o processo com a finalidade de minimizar problemas de qualidade tem influência forte e direta com o custo do produto. Desde os anos 1980 há um interesse

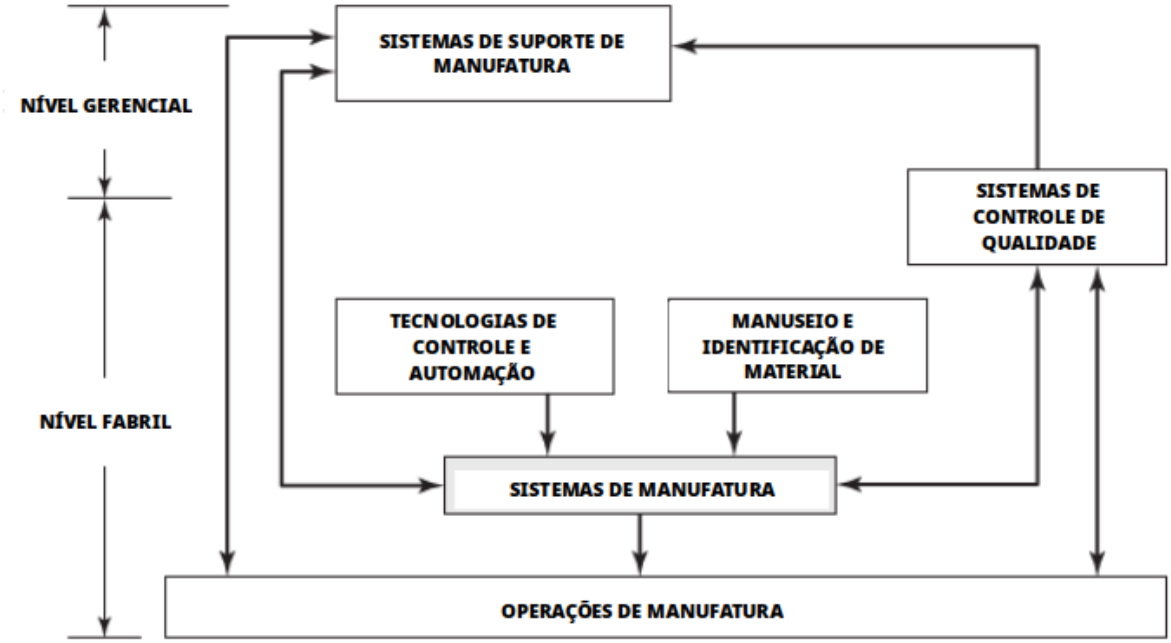

Figura 11 – Sistema de manufatura
(GROOVER; JAYAPRAKASH, 2015)

especial em desenvolver técnicas para detectar rapidamente desvios de processo e agir para minimizar seus impactos, como Controle estatístico de Processo e Seis Sigma (GROOVER; JAYAPRAKASH, 2015).

Técnicas de controle de qualidade é um assunto que foge do escopo deste trabalho de graduação, mas têm uma característica em comum: sua eficiência baseada na aquisição de dados de processo. Quanto mais próximo do tempo real for a detecção e mais flexível for o processo para aplicar soluções para desvios de processo mais prontamente, melhor a efetividade destes sistemas. Os dados, tão importantes para estes sistemas de qualidade são aqueles processados e armazenados nos dispositivos inteligentes das redes OT, onde a principal fonte destes dados são os CLPs. A flexibilidade do processo tem dependência direta na proporção do controle implementado por software em relação ao implementado por hardware, onde maior controle via software facilita implementação rápida de modificações. Quando se fala em controle via software em sistemas automatizados de manufatura, o principal dispositivo inteligente responsável por isso é, novamente, o CLP. A aquisição de dados armazenados em CLPs por parte de sistemas informacionais de qualidade possuem um grande impacto na redução do custo de fabricação do produto mas demanda integrar sistemas OT com sistemas IT.

Além do interesse na redução de custo, o controle de certos parâmetros do processo relevantes para a segurança do cliente no uso do produto e gestão ambiental são pré requisitos para atendimento a normas como a ISO 9000 e ISO 14000 e, para atender estes requisitos legais, é comum se empregar sistemas TI de rastreabilidade, que monitoram

estes parâmetros e os armazenam como documentação por períodos estabelecidos por lei. Aplicar rastreabilidade sem a aquisição de dados do processo por meio informatizado pode dificultar muito a implementação de um sistema de rastreabilidade e esta aquisição por meio informatizado demanda alguma convergência de sistemas OT e IT.

3.1.3 Sistemas de suporte de Manufatura

Os sistemas de suporte de manufatura são aqueles aplicados para solução do problemas técnicos e logísticos. Eles são empregados desde a etapa de concepção do processo e de modificações do processo, com o emprego dos sistemas CAD, CAM e CAE, e também são presentes no planejamento do processo de manufatura para manter o seu fluxo. É comum o emprego de sistemas automatizados para manter este fluxo de processo (GROOVER; JAYAPRAKASH, 2015).

O desenvolvimento de protótipos assistido por computador, com o uso de softwares CAD, CAM e CAE se baseiam em modelos prontos que simulam o processo e permitem reduzir o tempo de implantação de novos processos e modificação de processos já existentes. Os modelos empregados se baseiam no processo real que se deseja implantar. A aquisição de dados do processo para análise e modelagem é fundamental para que o modelo do processo seja fiel com a realidade, e a aquisição destes dados passa pela extração de dados armazenados e processados em CLPs. Esta extração demanda alguma integração entre redes OT e IT.

Do ponto de vista de planejamento de processo, o planejamento manual dependendo da experiência pessoal de quem o planeja pode tornar o processo dependente desta pessoa e a troca deste planejador pode ocasionar uma mudança drástica no processo que não necessariamente trará algum benefício, mais provavelmente trará variações e inconsistências ao processo. Por conta disso, há um interesse no Planejamento de processo assistido por computador (CAPP). Um CAPP é fortemente dependente de dados do processo e se baseia em padrões de processo preconcebidos e monitoramento do processo enquanto flui para manter o seu fluxo. Outra tecnologia voltada para o planejamento de recursos generalizado em nível empresaria são os sistemas ERP. Um sistema de Planejamento de recursos em nível empresarial (ERP) organiza e integra funções de gerenciamento de negócio associando todos os dados obtidos a partir de um banco de dados centralizado, onda cada função é dividida em módulos orientados por função e otimizados para o melhor desempenho destas funções.A integração de um software ERP pode exceder a jurisdição de uma planta industrial local e abranger todas as plantas da manufatura, com gestão de ponta a ponta (GROOVER; JAYAPRAKASH, 2015).

Na fronteira entre as tecnologias de controle e automação os sistemas computacionais em nível gerencial, há os sistemas de execução de manufatura MES. Os sistemas MES são fortemente integrados às tecnologias de controle e automação e obtém dados relevantes

para a manutenção do fluxo do processo mas também para a supervisão de processo em um nível mais generalizado. Dentre os dados obtidos por sistemas MES estão aqueles relevantes para a análise de confiabilidade dos equipamentos empregados em nível fabril, ou seja, os dispositivos OT. Os sistemas MES são implementados parte em redes OT para a extração dos dados dos dispositivos OT, em geral dos CLPs e estão presentes na rede OT. Ao mesmo tempo, o sistema MES precisa ser acessível em nível gerencial e, assim, se situa também em rede IT, utilizando módulos para estatísticas obtidas a partir dos dados adquiridos em nível fabril. Por definição, um sistema MES é a integração de redes OT com redes IT, e se situa na sua fronteira, o ponto mais crítico do ponto de vista de segurança de informação.

Todos estes sistemas de suporte de Manufatura necessitam estar em redes IT para que sejam acessíveis em nível gerencial, em alguns casos até pela Internet e, ao mesmo tempo, precisam adquirir dados de dispositivos OT, e demandam assim algum grau de convergência IT/OT.

3.2 Riscos envolvidos em utilizar Hardware Vulnerável sem monitoramento Ativo

Na seção anterior foram abordados argumentos que justificam a integração de sistemas IT/OT. Esta integração, porém, tem um risco associado, do ponto de vista de segurança de informação, e que se agrava quando os dispositivos OT empregados possuem vulnerabilidades facilmente exploráveis num ambiente de alta exposição, como o das redes IT. No que se refere aos CLPs S7-300/400, alguns ataques foram inclusive documentados, e são abordados nesta seção.

Antes de abordar os ataques, é necessário entender fundamentos básicos da estrutura de programação empregada em CLPs Siemens S7-300/400.

Os CLPs Siemens em geral possuem o seu programa dividido em diferentes tipos de blocos, sendo estes os Blocos Organizacionais (OBs), Funções (FCs), Blocos Funcionais (FBs) e Blocos de Dados (DBs). Esta distribuição dos programas tem uma base sólida no paradigma de Programação Estruturada. Os OBs são os ciclos principais que chamam para execução os blocos FC e FB. Os DBs são blocos que atuam como banco de dados interno do CLP e armazenam dados que são utilizados durante o processo e podem ser do tipo global (acessíveis por qualquer bloco de programação) e *instance* (associados a um único FB). Uma outra forma de armazenamento de dados num CLP S7-300/400 é utilizando um *Merker*, que é um espaço de memória compartilhado. Os FBs são blocos de função que possuem um banco de dados próprio para armazenar os dados de suas variáveis, sendo este bancos de dados um bloco DB do tipo *instance*. Os FCs não possuem um banco de dados associado e armazenam os dados de suas variáveis ou de maneira

temporária (apenas durante o tempo de execução do bloco) ou em espaços compartilhados da memória do CLP. O CLP é programado em linguagens de programação estabelecidas na norma IEC 61131-3, e instruções programadas nestas linguagens são encontradas nos blocos FC e FB que são executados nos momentos em que são chamados pelos OBs, que concentram a chamada destes blocos e não costumam conter lógicas associadas ao controle dos I/Os do CLP (ALSABBAGH; LANGENDÖRFER, 2021). A Figura 12 é um resumo desta descrição dos blocos de programação de CLP.

TIPOS	DESCRIÇÃO	FUNÇÃO TÍPICA
OB	Bloco Organizacional	Definir sequência em que o programa do usuário deve ser executado
FC	Função	Programar instruções a serem executadas com frequência mas que não demandam memória de dados
FB	Bloco Funcional	Programar instruções a serem executadas com frequência mas que demandam memória de dados
DB	Bloco de dados	Áreas de memória para armazenamento de dados durante execução do programa.

Figura 12 – Blocos de programação de CLP

O bloco OB1 é aquele que contém o ciclo principal para a execução da máquina. Outros OBs possuem chamadas de lógicas para execução como interrupção, seja por agendamento temporizado, seja como uma lógica para lidar com exceções decorrentes de erros específicos de execução das instruções do OB1 ou para execução de lógicas importantes para segurança e que exigem baixa latência de execução para atender normas de segurança. Os blocos OBs possuem preferência de execução preestabelecida na configuração do CLP. O bloco OB1 possui um tempo de execução monitorado e limitado a um valor máximo pré-configurado para garantir a baixa latência na execução do código (o tempo padrão é de 150 milisegundos, mas pode ser modificado de acordo com necessidade).(ALSABBAGH; LANGENDÖRFER, 2021)

O programa que será executado pelo CLP é desenvolvido e compilado em um software de engenharia Siemens, de acordo com o modelo do CLP. Os CLPs S7-300/400 podem ser programados por versões mais antigas do *Simatic Manager* ou por versões mais novas integradas ao software TIA Portal, a depender do seu modelo e do modelo dos *hardwares* adicionais empregados, como IHMs, controladores de motor e demais dispositivos. O programa desenvolvido num software de engenharia é traduzido em instruções numa linguagem em baixo nível chamada pelo fabricante de STL, que é uma linguagem de máquina muito semelhante ao Assembly. O código fonte em STL é compilado num executável em formato MC7, que converte as instruções STL em código Hexadecimal que é interpretado pelo CLP.(ALSABBAGH; LANGENDÖRFER, 2021)

3.2.1 Ataque de Negação de serviços

Baseado no ataque realizado e reportado por Alsabbagh e Langendörfer, é possível injetar código malicioso no CLP e temporizar a sua execução, de forma a dificultar a sua detecção. Neste ataque fez-se uso de interrupções programáveis num CLP S7-300 para que uma instrução de parada de execução do código fosse executada num momento arbitrário, causando a parada da máquina controlada pelo CLP.(ALSABBAGH; LANGENDÖRFER, 2021)

Para causar uma negação de serviços, os autores utilizaram a instrução "*STOP*"que interrompe a execução cíclica do CLP. Num processo de manufatura, uma parada não planejada pode gerar um grande prejuízo. Isso porque a retomada de operação vai depender do tempo necessário para que os atuadores em uso possam ser iniciados e de uma maneira segura. Uma paralisação abrupta de execução do CLP pode causar danos irreversíveis ao produto e também pode danificar os atuadores controlados pelo CLP.

Para realizar o ataque, os autores utilizaram ferramentas *Opensource*, como a biblioteca SNAP7 e a ferramenta desenvolvida em linguagem C desenvolvida pelos próprios autores denominada por eles como *PLCinject*. Para elaborar os blocos de programação a serem injetados no programa do CLP, os autores utilizaram o software de engenharia Siemens *TIA Portal*. O programa do CLP foi modificado para executar uma interrupção programada em tempo que executa as instruções contidas no OB10, criado pelos autores, que possui a instrução *STOP*. Os autores modificaram o bloco OB1 para que chamassem os FCs SFC28 e SFC30, responsáveis pela interrupção, parametrizaram esta interrupção via software, armazenando os parâmetros no DB1 e desenvolveram o OB10 que é chamado apenas quando as condições para interrupção forem satisfeitas para executar a instrução contida nele, que é a instrução de parada do ciclo de execução. Utilizaram o *TIA Portal* para gerar o código e a biblioteca SNAP 7 para armazenar o MC7 correspondente ao código gerado. Utilizando a ferramenta *PLCinject*, o MC7 armazenado foi enviado ao CLP, injetando assim o código malicioso. Segundo análise dos próprios autores, a interrupção cíclica para avaliação das condições para execução do OB10 causou um acréscimo inferior a 1 milissegundo na execução do código do CLP, tornando pouco plausível que este acréscimo fosse detectado pelo monitor de tempo de execução do CLP. Esta modificação no código fonte seria detectável apenas numa comparação intencional entre o código fonte que deveria ser executado e o código que está sendo executado no CLP. A Figura 13 mostra as modificações implementadas no ataque(ALSABBAGH; LANGENDÖRFER, 2021)

Este ataque tem algumas características relevantes. O ataque é genérico, o que significa que não importa se o CLP controla o volume de água de um aquário (a aplicação utilizada pelo autor do ataque), uma usina nuclear ou um elevador industrial, paralisar a execução cíclica do CLP trará algum prejuízo em qualquer um destes cenários. O ataque não exige acesso ao CLP durante a execução do código malicioso, após a injeção do

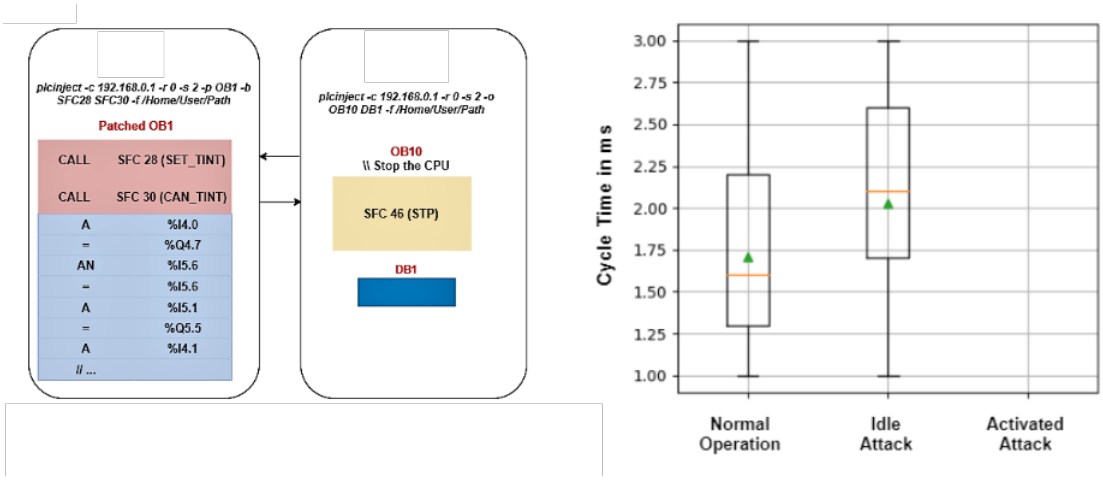

Figura 13 – Modificações implementadas
(ALSABBAGH; LANGENDÖRFER, 2021)

código fonte, o ataque ocorrerá mesmo que o CLP seja desconectado de qualquer rede IT ou OT. Supondo que haja um monitoramento na rede OT em que ocorreu o ataque, a detecção de que este acesso ao CLP foi malicioso pode ser constatada num momento posterior tão distante do ataque que talvez não seja possível utilizar os *logs* de acesso à rede para identificar o autor do ataque, e a execução temporizada deste ataque dificulta inclusive a detecção de uma anomalia no código do CLP. A menos do atraso na execução do ciclo de varredura do CLP, o código malicioso não interfere no funcionamento da planta até que seja executado. No caso de um ataque direcionado, as instruções executadas no OB10 podem ser projetadas com o fim de maximizar os danos do ataque, o que traria consequências ainda mais desastrosas. Por fim, o ataque exige software proprietário apenas para gerar o código MC7, ou seja, em posse do código MC7 do código malicioso, a injeção do código pode ser realizada por qualquer dispositivo capaz de executar programas em C ou Python, sem a necessidade também de investimento financeiro na compra de um software de engenharia Siemens.

3.2.2 Ataques por *Replay Attack* e *Man in the middle*

Levando em consideração uma comunicação sem criptografia, ataques do tipo *replay* e *man in the middle* se tornam mais facilmente implementáveis

Ataques do tipo *Man in the middle* são aqueles em que um terceiro recebe os pacotes trocados entre dispositivos que estabeleceram uma comunicação legítima. Quando este terceiro mal intencionado armazena estes pacotes, ele pode executar um ataque do tipo *replay*, em que ele envia os pacotes capturados se passando por um dos dispositivos com comunicação legítima estabelecida. No caso de um CLP, um ataque desta natureza pode ser utilizado para alterar o valor de variáveis ou enviar comandos de sistema, como a execução do *upload* do código fonte ou envio de comando para parada de execução do

ciclo principal do programa.

Um exemplo de ataque desta natureza bem sucedido é o publicado por Sandaruwan, Oleshchuk e Ranaweera (SANDARUWAN; RANAWEERA; OLESHCHUK, 2013). O ataque tem por finalidade parar a execução do ciclo principal do CLP. Para isso, os autores utilizaram um software de engenharia Siemens e enviaram um comando legítimo para parada de execução do ciclo principal do CLP, e capturaram o pacote que possui este comando utilizando o software Wireshark. Com base neste pacote (Figura 14) é possível observar não só um método para solicitar parada de execução do código, mas também é possível ver outras informações como modelo do CLP e outros parâmetros. A escolha de um ataque em que os danos sejam maximizados é muito difícil quando se trata de CLP, pois isso depende muito da aplicação da máquina. Num ataque *Man in the middle*, o atacante tem a possibilidade de estudar a troca de dados do CLP enquanto em uso e utilizar isso como base para projetar um ataque direcionado para a máquina em questão, causando assim um dano ainda maior do que um ataque generalizado (SANDARUWAN; RANAWEERA; OLESHCHUK, 2013).

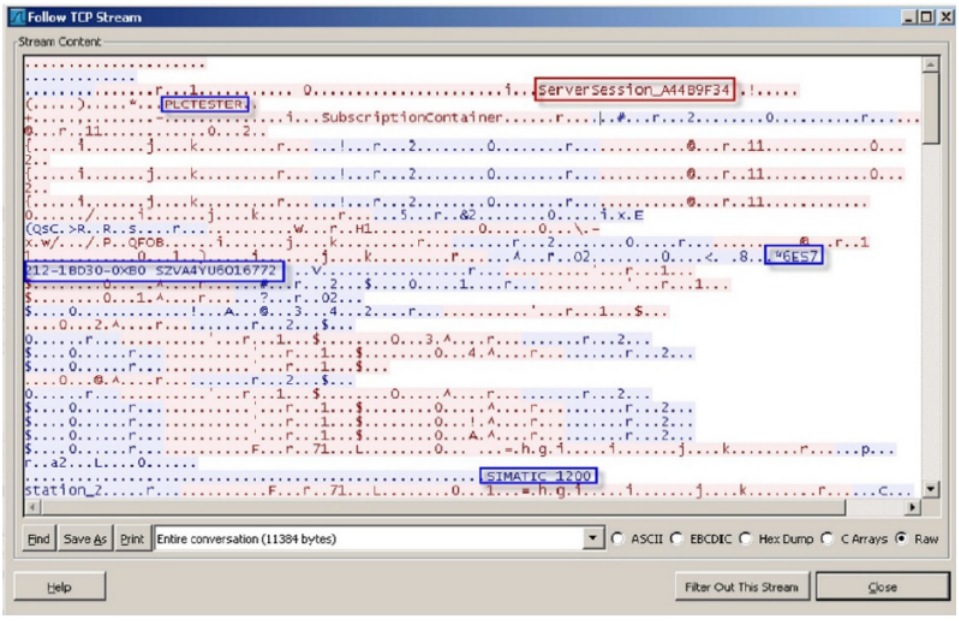

Figura 14 – Pacote capturado com comando de *STOP* CPU (SANDARUWAN; RANAWEERA; OLESHCHUK, 2013)

Este tipo de ataque abre margem para ataques direcionados de difícil detecção. Quando o código fonte é alterado, a comparação do código em execução com o código que deveria estar em execução serve para detecção do ataque. Em ataques em que parâmetros de processo, armazenados em DBs são alterados, a detecção se torna muito difícil. Isso se dá porque CLPs são aplicados para controle em malha fechada e isso implica que os valores obtidos na saída da planta sejam realimentados e processados para que a planta opere de acordo com o *setpoint* estabelecido. Estes valores realimentados variam de acordo

com o estado de operação da planta e, assim, é muito difícil implementar um monitor de DBs que tolere esta variação natural sem gerar alarmes falsos.

4 Experimentos computacionais de vulnerabilidades em CLPs S7-300/400

Conforme demonstrado por Alsabbagh e Langendoerfer, no seu ataque de negação de serviços, o protocolo S7comm apresenta fragilidades que podem ser exploradas para violação de segurança dos CLPs que utilizam este protocolo (ALSABBAGH; LANGENDÖRFER, 2021). Estes mesmos autores, em sua publicação intitulada *"A remote attack tool against Siemens S7-300 controllers: A practical report"* reportaram e simularam ataques utilizando uma ferramenta denominada *"IHP-attack tool"* (ALSABBAGH; LANGENDOERFER, 2022b). Neste capítulo, serão demonstrados alguns ataques que exploram fragilidades do protocolo S7comm, semelhantes aos reportados mas utilizando programas desenvolvidos em python e a biblioteca SNAP7, e outros utilizando o próprio software de engenharia desenvolvido pelo fabricante.

A biblioteca Python-SNAP7, desenvolvida por Molenaar e Preeker utiliza os protocolos *Iso-on-TCP* e S7comm para realizar conexão com CLPs Siemens que utilizem S7. Nesta biblioteca foram implementados métodos para conectar com CLP, ler e escrever dados e utilizar comandos de interação, como mudança do modo de execução, informações de fabricante e outras possíveis com o protocolo S7comm.(MOLENAAR; PREEKER, 2023)

Para simular um CLP foi a utilizada a combinação entre os softwares PLCSIM e NetToPLCSIM. O PLCSIM é um recurso desenvolvido pela própria Siemens para simular um CLP para fins de análise e depuração de falhas antes de realizar o *download* do código-fonte para um CLP real. Este CLP simulado, porém não é acessível via rede e, para fins de análise dos protocolos S7comm e Iso-on-TCP, uma ferramenta adicional chamada NetToPLCSIM foi utilizada. Sua função é redirecionar a troca de dados utilizando os protocolos Iso-on-TCP e S7comm do *localhost* para uma interface de rede acessível externamente, de forma que um computador executando o PLCSIM e o NetToPLCSIM juntos atue na rede local como um CLP simulado.

A Figura 15 ilustra a topologia do ambiente montado para as simulações. Uma máquina virtual com o sistema operacional Windows 7 executando os softwares PLCSIM e NetToPLCSIM atua como um CLP simulado. A placa de rede desta máquina virtual está configurada de modo que atue como se estivesse em rede com o *host*. O *host* é um PC com o sistema operacional Ubuntu 22.04 executando programas em Python utilizando a biblioteca Python-SNAP7 para se comunicar através dos protocolos Iso-on-TCP e S7comm com o CLP simulado.

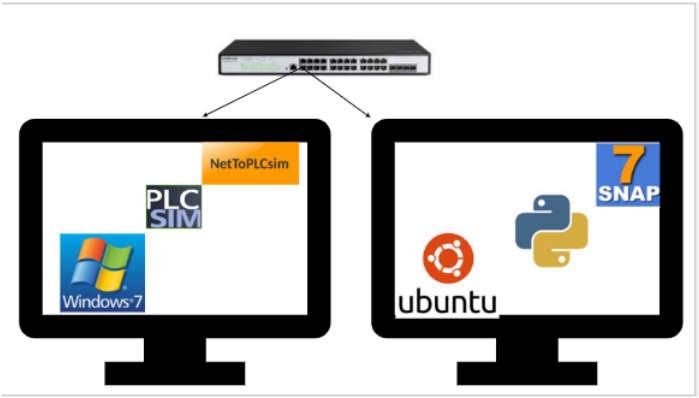

Figura 15 – Topologia do ambiente de simulação

4.1 Ataque para Obtenção de credenciais de autenticação

Os CLPs S7-300/400 possuem a opção de exigir credenciais de autenticação para estabelecer conexão com o CLP. Esta autenticação exige uma senha de até oito dígitos para que a comunicação seja estabelecida. Apesar de ser uma medida de segurança presente no CLP, ela é burlável, e a dificuldade no processo de quebra de senha vai depender de quão forte é a senha proposta. Numa comunicação legítima com o CLP, o dispositivo que deseja a conexão envia um *hash* correspondente à senha de acesso ao CLP. Utilizando um ataque *replay*, um atacante pode obter este *hash* legítimo e utilizá-lo para ganhar acesso ao CLP.Outra forma sugerida pelo autor foi o emprego de força bruta, que demanda um maior esforço computacional.(SANDARUWAN; RANAWEERA; OLESHCHUK, 2013)

Para exemplificar uma obtenção por força bruta de uma senha de acesso ao CLP, foi criado um ambiente de simulação utilizando o software *PLCSim* desenvolvido pela Siemens e a ferramenta *NETtoPLCSIM*, disponível online, para simular um CLP real bloqueado por senha. Para simplificar o experimento, foi suposto que a senha seja fraca e simplesmente numérica. Para descobrir a senha por força bruta, foi criado um programa em Python utilizando o método *"set session password"* da biblioteca SNAP7. Este método tenta realizar conexão com um CLP protegido por senha. Quando a senha enviada está errada, a autenticação falha. O programa tenta sucessivamente senhas numéricas diferentes até que obtenha a senha desejada. Nas Figuras 16 e 17 é possível observar o resultado deste experimento.

Neste exemplo, o CLP foi bloqueado com a senha "123"que foi obtida pelo programa. Quanto mais forte for a senha, mais tempo será necessário para obtê-la por força bruta e, se tratando de um dispositivo OT, é uma boa prática temporizar a requisição de conexão de forma que o envio sucessivo de pacotes de conexão não gerem uma sobrecarga muito grande à placa de rede. Se tratando de CLPs, atrasos na comunicação via rede podem causar uma parada de execução do programa por se tratar de uma situação perigosa do ponto de vista de segurança funcional.Ainda assim, numa rede OT, onde a troca de dados muitas vezes é

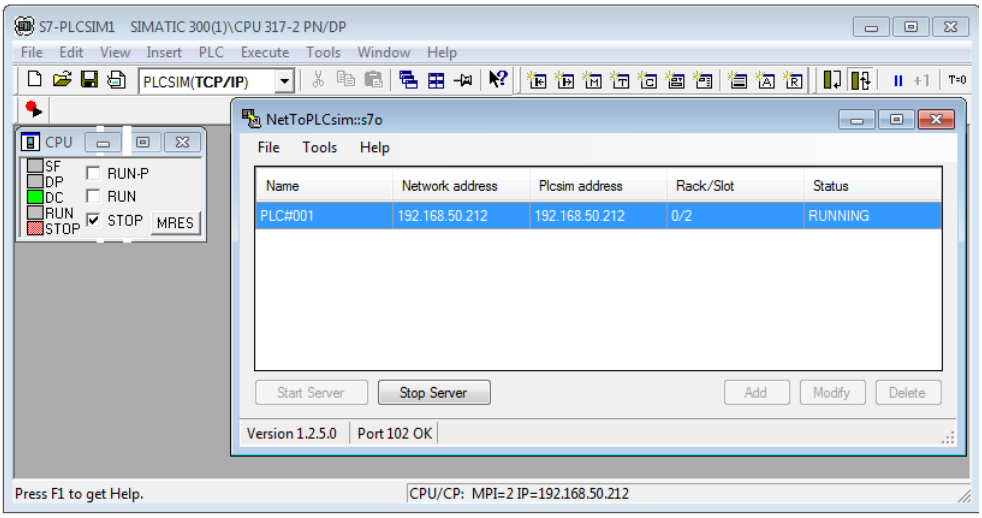

Figura 16 – Configuração de CLP Simulado

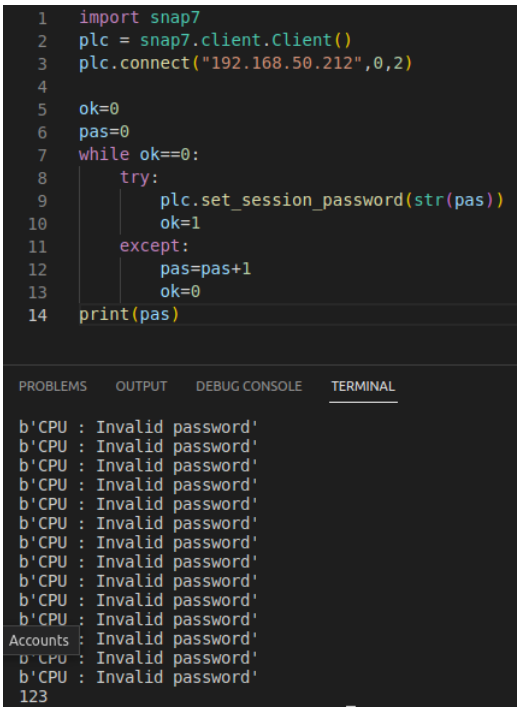

Figura 17 – Programa para *Bruteforce*

cíclica e ininterrupta, é possível crer que esta atividade maliciosa de tentativa sucessiva de acesso ao CLP passe despercebida, mesmo que dure por algumas horas, a não ser que exista um monitor de rede ativo projetado para detectar este tipo de atividade maliciosa. Este tempo necessário para a descoberta da senha por força bruta pode ser reduzido por utilizar algoritmos de quebra de senha mais otimizados, privilegiando senhas mais comuns, e utilizando uma linguagem de mais baixo nível que o Python, como o C.

4.2 Ataque de Apagamento de Código fonte

Se tratando de ataques genéricos a CLP, um outro ataque que pode causar um grande transtorno e ocasionar negação de serviço é o apagamento do código fonte do CLP.

O programa exibido na Figura 18 executa um ataque combinado em que a senha de acesso é obtida e em seguida o programa do CLP é completamente apagado e o CLP é enviado para STOP. Após a aquisição da senha de acesso o programa utiliza o método *"list blocks of type"* para saber quais blocos estão presentes no CLP, o método *"delete"* para solicitar apagamento de todos os blocos listados e o método *"plc stop"* para mandar o CLP para *Stop*. Na Figura 19 é possível notar que restaram no CLP apenas os blocos de sistema (SFC, SFB) que vêm de fábrica e que ele está em modo *STOP*.

```
1  import snap7
2  plc = snap7.client.Client()
3  plc.connect("192.168.50.212",0,2)
4
5  ok=0
6  pas=0
7  while ok==0:
8      try:
9          plc.set_session_password(str(pas))
10         ok=1
11     except:
12         pas=pas+1
13         ok=0
14 tipos = ['OB','FB','FC','DB']
15 for tipo in tipos:
16     indices_do_tipo = plc.list_blocks_of_type(str(tipo),1000)
17     for item in indices_do_tipo:
18         plc.delete(tipo,item)
19 plc.plc_stop()
20 plc.clear_session_password()
```

Figura 18 – Programa com ataque combinado

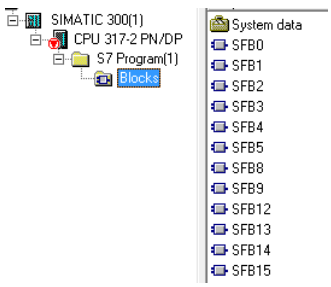

Figura 19 – CLP após ataque combinado

Um ataque desta natureza traz à luz também a importância de armazenar *backups* de CLP atualizados, já que neste cenário o código fonte do CLP foi perdido. Manter um *backup* de programa de CLP atualizado é viabilizado com o emprego de monitores ativos de código fonte. Por monitorar o código fonte, é possível detectar modificações e agir prontamente, seja para desfazer modificações maliciosas, seja para atualizar o *backup* existente diante de uma modificação sob projeto. O armazenamento destes *backups* também é um assunto importante do ponto de vista de segurança de informação, uma vez que um atacante que ganhe acesso a estes *backups* terá total liberdade para projetar um ataque direcionado ao CLP e, uma vez que ganhe acesso a este dispositivo, poderá efetuar um ataque com danos maximizados.

4.3 Ataques Utilizando Software de Engenharia para ação maliciosa

Até o momento, foram avaliadas formas de acesso ao CLP utilizando ferramentas *Opensource* simulando o ataque de um dispositivo IT presente indevidamente numa rede OT. Uma outra possibilidade existente é a de que o atacante que conseguiu acesso à rede OT possua o software de engenharia apropriado para o ataque ou assuma controle de algum computador com estes recursos numa rede IT com acesso à rede OT. A situação se agravaria caso o atacante conseguisse acesso remoto a um PC de Engenharia (Computador que substitui os antigos programadores de CLP e que é utilizado para programar CLPs) dentro da rede OT.

PCs de Engenharia hoje são computadores comuns, que possuem placas de rede especiais para estabelecerem comunicação com CLPs por meio de redes baseadas em Ethernet ou outras que sejam comuns para o CLP. O grande problema na atualização destes dispositivos não está no grau de avanço tecnológico, mas sim na obsolescência dos softwares de engenharia. A atualização do Sistema Operacional de um PC de Engenharia pode causar incompatibilidade com determinados hardwares que são programados com softwares incompatíveis com versões mais novas de sistemas operacionais. Além disso, a configuração indevida de meios de acesso remoto a estes PCs de Engenharia pode torná-los ainda mais vulneráveis. Supondo um atacante que tenha acesso ao PC de Engenharia que possua um *backup* do programa do CLP em uso e algum conhecimento em programação de CLP, o ataque é trivial.

Supondo que o atacante ganhe acesso à rede OT, possua software de Engenharia apropriado para modificar o programa de CLPs S7-300/400 mas não possua um *backup* do código fonte do CLP, existem meios para realizar um ataque utilizando os próprios recursos do software. Utilizando o mesmo CLP simulado utilizado no exemplo de quebra de senha e um PC com *Simatic Manager*, é possível demonstrar um ataque.Utilizando um computador na mesma rede do CLP, é possível utilizar o recurso de *Upload* do CLP

para o Computador. As Figuras 20 e 21 ilustram este cenário. O grande obstáculo para o atacante nesta situação é que o programa obtido não possui descrição alguma, seja da lógica implementada, seja das variáveis e, assim, é difícil decifrar a finalidade do programa. Em contrapartida, é muito mais fácil entender a lógica de execução do programa tendo ele em mãos do que capturando pacotes de troca de dados por interceptação. Todas as ações de interação com o CLP, como *download* de programa, modificação de variáveis e outras ações demais podem ser realizadas através do próprio software de engenharia, facilitando muito a definição de uma estratégia de ataque efetiva. Por fim, como mostrado na Figura 22, o software de Engenharia também dispõe de meios para mandar o CLP para *Stop*.

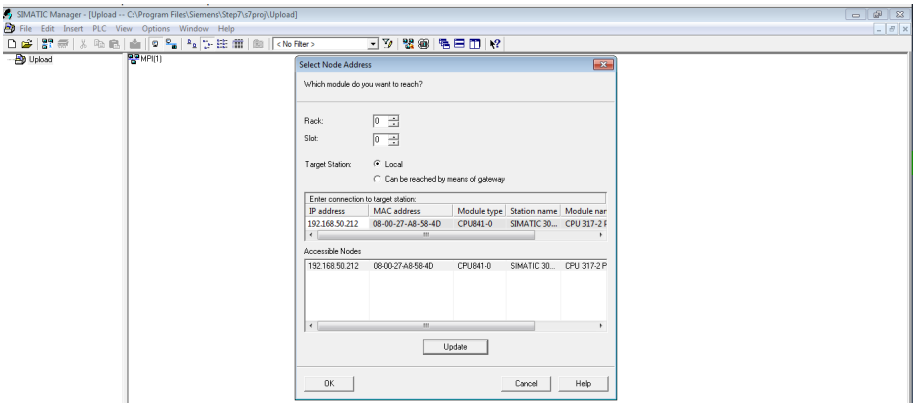

Figura 20 – *Upload* do Código fonte do CLP

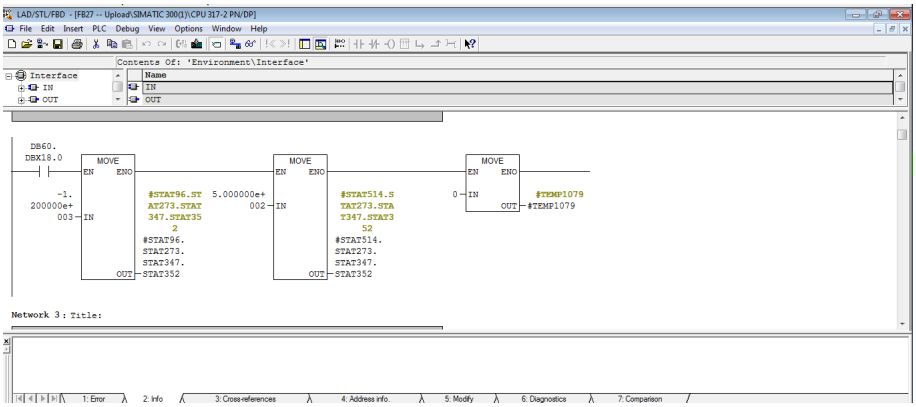

Figura 21 – Programa obtido por *Upload*

Numa condição em que o atacante utiliza o software de engenharia para executar ataques ele faz uso de meios legítimos para modificar o código fonte e interagir com o CLP, com os mesmos recursos de um usuário legítimo e, assim, o ataque fica muito direcionado e difícil de conter. Para que um cenário como este ocorra, o atacante se utilizaria de fragilidades que vão muito além daquelas em dispositivos S7-300/400 mas da própria infraestrutura da rede, e faz mais sentido num cenário em que a rede OT esteja extremamente exposta, como em casos em que ela esteja conectada diretamente à internet.

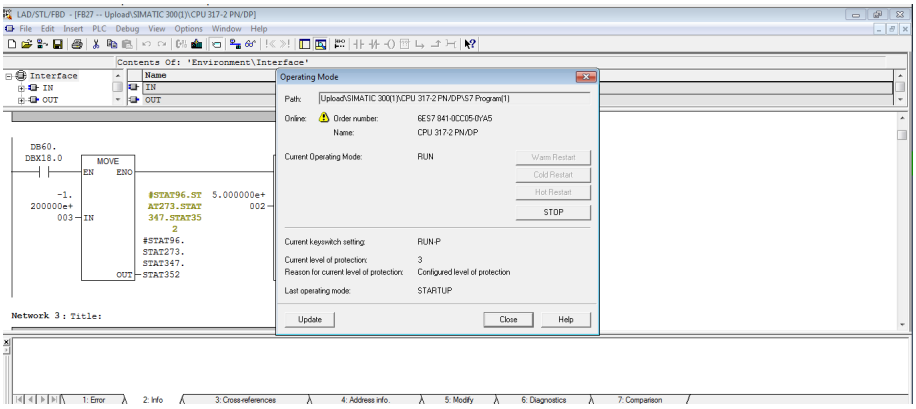

Figura 22 – Recurso para mandar para *Stop*

4.4 Ataque para detecção de dispositivos vulneráveis em redes locais

Um assunto referente aos riscos de expor um CLP S7-300/400 a uma rede OT é a facilidade em se detectar estes dispositivos por parte de um atacante.

No exemplo anterior foi demonstrado um meio de identificar um CLP Siemens na rede utilizando o próprio software de Engenharia do fabricante. Existem, porém outros meios para identificar alvos vulneráveis na rede. Utilizando novamente a biblioteca SNAP7, um destes meios é através do método *"connect"* variando os parâmetros de comunicação. Em adição, é possível adquirir dados do CLP utilizando o método *"Get CPU info"* e assim saber a família e o modelo do dispositivo, possibilitando assim o projeto de um ataque e inclusive a consulta em fragilidades reportadas referentes ao CLP específico ao qual se estabeleceu conexão. A Figura 23 traz um exemplo nestas condições. No exemplo, os parâmetros de *slot* e *rack* (parâmetros utilizados no protocolo Iso-on-TCP para definir TSAP) foram fixados nos valores mais comuns para CLPs S7-300 e apenas o último octeto foi variado para varrer a rede 192.168.50.0/24. Por se tratar apenas de uma prova de conceito o valor do último octeto foi inicializado em 200, mas este programa pode ser aplicado numa forma mais genérica variando outros parâmetros, como o próprio *rack* e *slot* e os octetos do IP de acordo com a classe da rede a ser monitorada.

Uma informação interessante de ser levada em conta é que CLPs S7-300/400 são acessados para parametrização e modificação do código fonte pela porta TCP 102. Com esta informação, é possível utilizar ferramentas mais populares em tecnologias de informação, como o NMAP, por exemplo, para buscar na rede dispositivos que aceitem conexão na porta TCP 102 e, em seguida, tentar conexão utilizando o protocolo S7comm, por meio da biblioteca SNAP7. Algo semelhante foi implementado no programa descrito na Figura 24, onde a rede é varrida em busca de uma conexão na porta TCP 102 e, em seguida, é executada uma conexão S7. Desta forma, ocorre uma conexão com troca de dados sem carga útil, apenas de *flags* de controle de comunicação do protocolo TCP (descrito na Figura 25) e outra utilizando o protocolo Iso-on-TCP (COTP) e S7comm (ilustrado na

```python
import snap7
plc = snap7.client.Client()


ok=0
oct=200
while ok==0:
    try:
        ip="192.168.50."+str(oct)
        plc.connect(ip,0,2)
        ok=1
    except:
        plc.disconnect
        oct=oct+1
        ok=0
print(ip)
print(plc.get_cpu_info())
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL                                  Python

b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
b' TCP : Unreachable peer'
192.168.50.212
<S7CpuInfo ModuleTypeName: b'' SerialNumber: b'' ASName: b'SIMATIC 300(1)' Copyright: b'Original Siemens Equipment' ModuleName: b'CPU 317-2 PN/DP'>
```

Figura 23 – Detectar CLPs na rede local

Figura 26).

```python
import snap7
import socket

plc = snap7.client.Client()

result=1
oct=200
ip=""
while result!=0:
    ip="192.168.50."+str(oct)
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    socket.setdefaulttimeout(1)

    # returns an error indicator
    result = s.connect_ex((ip,102))
    if result ==0:
        plc.connect(ip,0,2)
    s.close()
    oct=oct+1
print(ip)
print(plc.get_cpu_info())
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL                                  Python

RuntimeError: b' ISO : An error occurred during send TCP : Connection timed out'
filipe@filipe-Inspiron-15-3567:~$ /bin/python3 /home/filipe/Documents/VScode_projects/attack_plc/attack_v0.2.py
Target 192.168.50.212 is plc
192.168.50.212
<S7CpuInfo ModuleTypeName: b'' SerialNumber: b'' ASName: b'SIMATIC 300(1)' Copyright: b'Original Siemens Equipment' ModuleName: b'CPU 317-2 PN/DP'>
filipe@filipe-Inspiron-15-3567:~$ /bin/python3 /home/filipe/Documents/VScode_projects/attack_plc/attack_v0.2.py
192.168.50.212
<S7CpuInfo ModuleTypeName: b'' SerialNumber: b'' ASName: b'SIMATIC 300(1)' Copyright: b'Original Siemens Equipment' ModuleName: b'CPU 317-2 PN/DP'>
```

Figura 24 – Detecção de CLP monitorando porta TCP 102

No.	Time	Source	Destination	Protocol	Length	Info
235	22.792520	192.168.50.92	192.168.50.212	TCP	74	38968 → 102 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1073578896 TSecr=0 WS=128
238	22.792802	192.168.50.212	192.168.50.92	TCP	74	102 → 38968 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=2426008 TSecr=10735
239	22.792942	192.168.50.92	192.168.50.212	TCP	66	38968 → 102 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1073578896 TSecr=2426008
248	22.800694	192.168.50.92	192.168.50.212	TCP	66	38968 → 102 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1073578904 TSecr=2426008
249	22.800722	192.168.50.212	192.168.50.92	TCP	66	102 → 38968 [ACK] Seq=1 Ack=2 Win=66560 Len=0 TSval=2426009 TSecr=1073578904
251	22.800842	192.168.50.212	192.168.50.92	TCP	66	102 → 38968 [FIN, ACK] Seq=1 Ack=2 Win=66560 Len=0 TSval=2426009 TSecr=1073578904
252	22.801379	192.168.50.92	192.168.50.212	TCP	66	38968 → 102 [ACK] Seq=2 Ack=2 Win=64256 Len=0 TSval=1073578904 TSecr=2426009

Figura 25 – Conexão TCP para detecção do CLP

4.5 Ataque para detecção de dispositivos vulneráveis na internet

Quando se trata de CLPs expostos à internet, existem ferramentas implementadas projetadas para a sua detecção. Uma ferramenta web muito popular é o SHODAN.

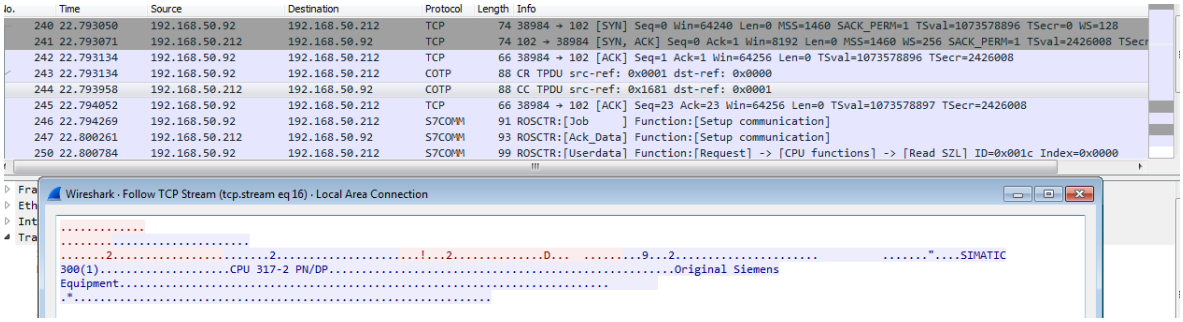

Figura 26 – Conexão por Iso on TCP e S7comm

Realizando uma busca rápida no SHODAN pelo termo S7-300, é possível constatar que centenas de CLPs desta família estão expostos à internet, conforme Figura 27. É possível saber o IP externo destes dispositivos e sua localização geográfica.

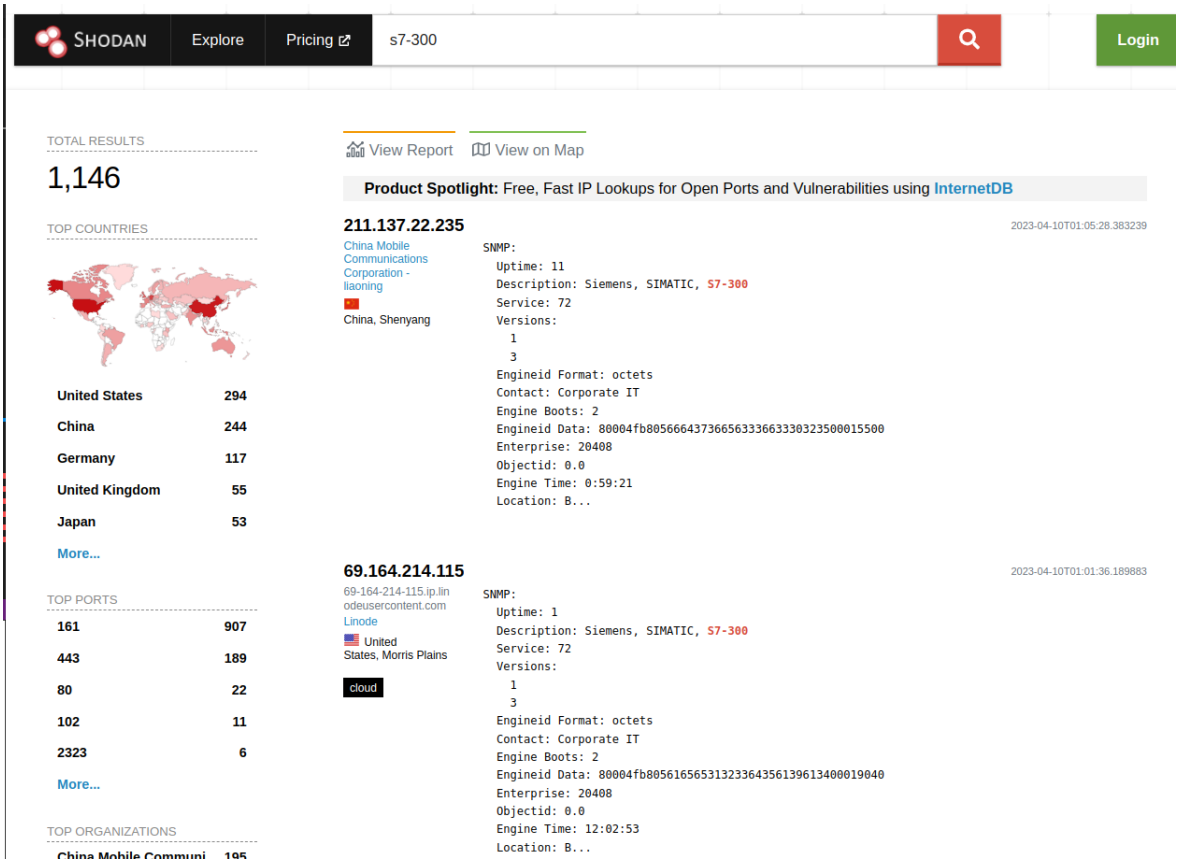

Figura 27 – Resultado da busca utilizando SHODAN

Estes exemplos servem de alerta para mostrar que dispositivos OT expostos a redes IT não passam despercebidos devido ao emprego de técnicas de detecção facilmente implementáveis e, no caso de CLPs expostos à internet, devido ao emprego de ferramentas de monitoramento ativo já existentes.

5 Monitoramento ativo

Neste capítulo, serão abordados o monitoramento ativo de rede e de código fonte e será descrita uma proposta de monitoramento ativo de código fonte baseado em ferramentas *opensource* e aplicável em ambiente industrial.

5.1 Monitoramento ativo de rede

O monitoramento ativo de redes OT é uma técnica com a finalidade de possibilitar defesa em níveis para os dispositivos de campo. Devido à arquitetura empregada em dispositivos OT, é difícil aplicar técnicas de forense digital, o que dificulta a prevenção e a análise de ataques contra estes dispositivos. Um exemplo de monitor desta natureza é o proposto por Ken Yau, Ka-Pui Chow e Siu-Ming Yiu.(CHAN et al., 2018)

Os autores propuseram um *proxy* transparente entre a rede IT e a rede OT. Quando um dispositivo estabelece conexão com um CLP S7-300/400 o monitor captura dados como endereço IP, comandos enviados e *timestamps* e os armazena num *log* que pode ser utilizado posteriormente para fins de análise forense (ilustrado na Figura 28). O monitor pode ser executado num computador conectado à rede OT e, com base no *log* gerado, é possível definir os comandos enviados ao CLP, a duração do ataque e o endereço IP utilizado pelo atacante.(CHAN et al., 2018)

Date/Time	Source IP Address	Protocol	PLC Command	PLC Memory Value Change
01 Jan 2017 10:05pm	192.168.0.10	TCP	Establish connection	N/A
01 Jan 2017 10:10pm	192.168.0.10	S7comm	WRITE	Set Output Q0.7 to TRUE from FALSE
01 Jan 2017 11:00pm	192.168.0.10	S7comm	CPU STOP	N/A
01 Jan 2017 11:30pm	192.168.0.10	TCP	Close connection	N/A

Figura 28 – Exemplo de *log* gerado pelo monitor ativo de rede

Por natureza, CLPs não são dispositivos projetados para o armazenamento de dados e gerar logs de acesso consumiria mais recursos do que eles dispõem. Assim, utilizar um monitor ativo de rede numa rede OT transfere essa responsabilidade para um dispositivo que tenha recursos para isso, e permite a detecção de intrusões à rede à qual o CLP está conectado.

5.2 Monitoramento ativo de código fonte

Uma forma de tentar diminuir o impacto de modificações indevidas de código fonte é rastreando estas modificações os mais rapidamente o possível, e isso é possível com o emprego de Monitoramento ativo de código fonte. Diferindo do monitoramento ativo de rede, o objetivo do monitoramento ativo de código fonte é detectar modificações no código fonte que está em uso no CLP. Um programa desta natureza se conecta ao CLP e analisa o código fonte em uso. Uma forma de realizar esta comparação é avaliando os CRCs (*cyclic redundancy check*) do código-fonte. Os CLPs das famílias S7-300 e S7-400 possuem uma estrutura de código fonte baseada em OBs, FBs e FCs, como já descrito no capítulo 4, e cada um destes componentes de programa possui um CRC próprio. O monitor de código fonte que será descrito a seguir utiliza estes os valores dos CRCs para detectar modificações no programa. Ele está descrito no fluxograma da Figura 29.

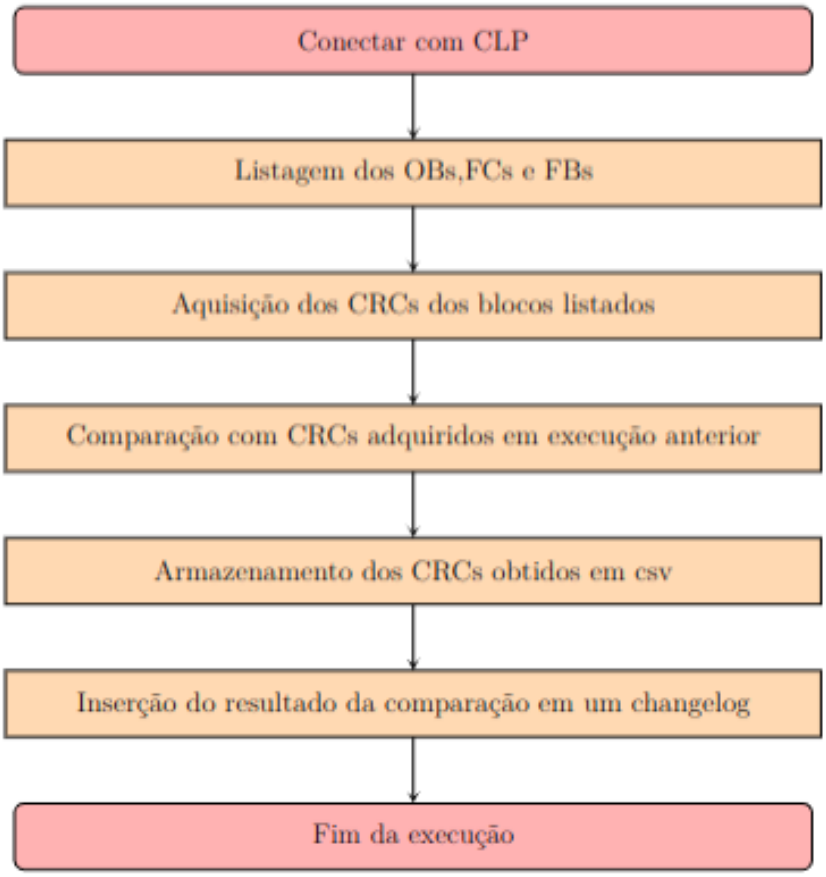

Figura 29 – Descrição de funcionamento do monitor proposto

5.3 Monitor de código fonte *Opensource*

O monitor de código fonte proposto foi programado em linguagem Python (versão 3.10.12), utilizando a biblioteca SNAP7 para interação com o CLP e alguns recursos de

geração de base de dados para armazenamento dos dados obtidos para comparação.

Descrevendo o funcionamento de maneira geral, na primeira execução o monitor desenvolvido se conecta ao CLP por uma conexão Ethernet, solicita uma lista de quais OBs, FCs e FBs estão em uso e em seguida solicita o CRC de cada um deles e os armazena num arquivo no formato CSV. Nas próximas execuções do monitor, os CRCs obtidos são comparados aos armazenados anteriormente e, caso haja a adição de um bloco novo no CLP ou modificação de lógica em algum deles, o monitor detecta esta modificação e armazena num arquivo de texto um *changelog* informando o horário em que a modificação foi detectada e qual bloco foi modificado. Para determinar qual modificação foi realizada dentro do bloco, há a necessidade de se conectar ao CLP com o software de engenharia e o *backup* do último código fonte em uso e comparar o bloco modificado com o do backup. Com base nesta comparação é possível para o usuário avaliar se a modificação detectada deve ser mantida ou se trata de uma modificação maliciosa, que deve ser desfeita. Se a modificação for mantida, é necessário que seja incorporada ao *backup* do projeto. A efetividade do monitoramento do código fonte passa por uma boa gestão de modificações do código fonte do CLP e do armazenamento de *backups* com versões estáveis que possam ser utilizadas para comparação e para reversão de modificações maliciosas. O código será explicado em etapas a seguir e o seu funcionamento será exemplificado na prática.

5.3.1 Conexão com o CLP

Seguindo as etapas ilustradas na Figura 29, a primeira etapa realizada pelo monitor de código fonte é a conexão com o CLP. Esta conexão se estabelece utilizando o método *"connect"* da biblioteca Snap7. Este método estabelece uma conexão utilizando o protocolo Ethernet na camada de enlace, protocolo IP na camada de rede e protocolos TCP e Iso-on-TCP na camada de transporte. Para que a conexão ocorra, é necessário que sejam descritos previamente o endereço IP, a porta TCP e os parâmetros *Iso-on-TCP* necessários para a conexão. Estes parâmetros ficam descritos em um arquivo chamado "dados.csv", onde há uma lista com a denominação do CLP e os seus parâmetros de conexão para que os dados referentes a estes CLPs sejam agrupados adequadamente. Na Figura 30 há um exemplo do monitor nesta etapa de execução e o pacote capturado pelo *Wireshark* no momento da conexão com os parâmetros que estão descritos no arquivo dados.csv, também exposto na Figura 30.

Para que o monitor se conecte ao CLP, é necessário que este seja capaz de receber conexões Ethernet. Como o objetivo de monitorar o código fonte do CLP é para integrá-lo a uma rede IT, pode-se assumir que o CLP que será monitorado tem esta capacidade, seja por possuir uma placa de rede Profinet *"onboard"* (S7-300/400-PN) ou um processador de comunicação Ethernet/Profinet adicional (CP 343/443).

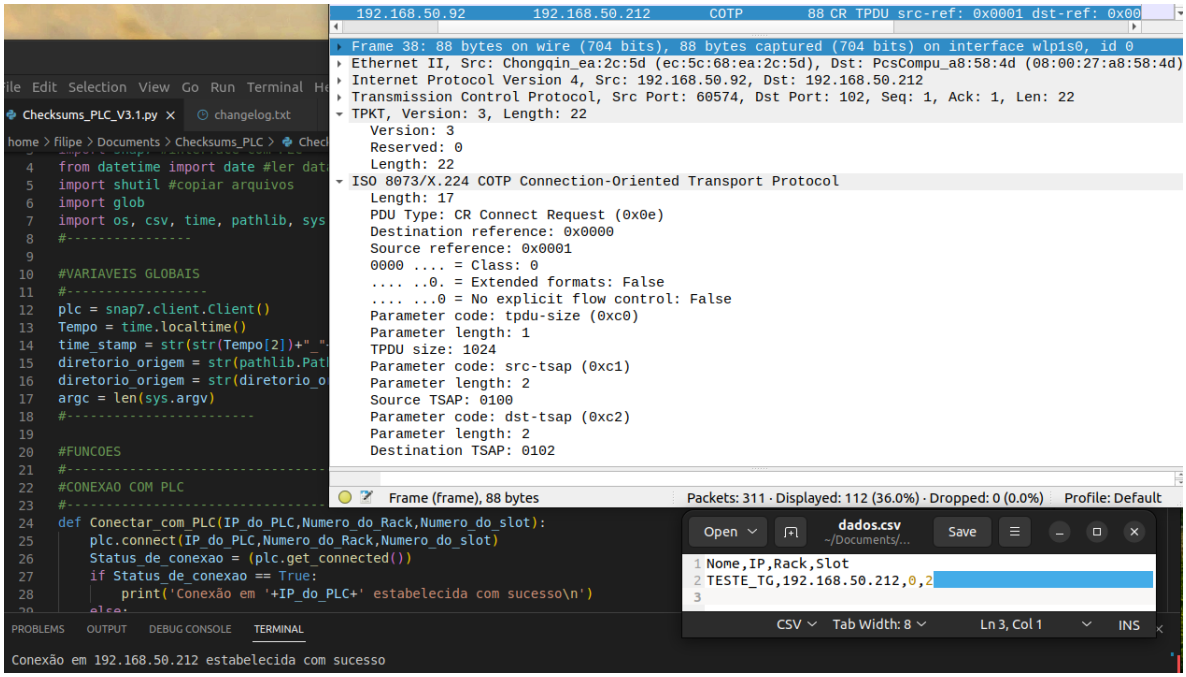

Figura 30 – Conexão do monitor ao CLP

5.3.2 Aquisição dos CRCs

Após estabelecida a conexão com o CLP, o programa solicita uma listagem de todos blocos de programação (OBs,FBs,FCs) utilizando o método *"list blocks of type"* da biblioteca Snap7 e para cada bloco é feita a consulta do CRC associado a ele calculado pelo CLP, através do método *"get block info"* da biblioteca Snap7. Estes dados são armazenados em um arquivo CSV que possui a data no seu nome e que é estruturado com uma coluna para o tipo de bloco, uma para o índice e outra para o CRC calculado. Nas Figuras 31 e 32 há um exemplo desta etapa de execução. Na primeira imagem é possível ver o arquivo csv com os CRCs obtidos e as funções implementadas no programa para realizar esta etapa. Na segunda imagem é possível ver a captura do pacote recebido pelo monitor com o valor do CRC do FB1 em hexadecimal no campo *"Block Checksum"*.

Utilizando esse método é possível realizar o monitoramento do código fonte sem a necessidade realizar *upload* do programa existente no CLP e sem a necessidade de processar uma versão do código fonte localmente onde o monitor é executado, reduzindo assim o esforço computacional envolvido no monitoramento e o tráfego de dados na rede que conecta o CLP ao PC onde o monitor de código fonte é executado.

5.3.3 Comparação de CRCs

Uma vez que haja uma base para comparação, a próxima etapa realizada pelo monitor é a comparação dos CRCs obtidos com os anteriores. Para isso, o arquivo csv com os CRCs atuais é comparado com o arquivo csv com os CRCs obtidos na última varredura executada pelo monitor. As entradas no *changelog* se iniciam com uma *timestamp* para que

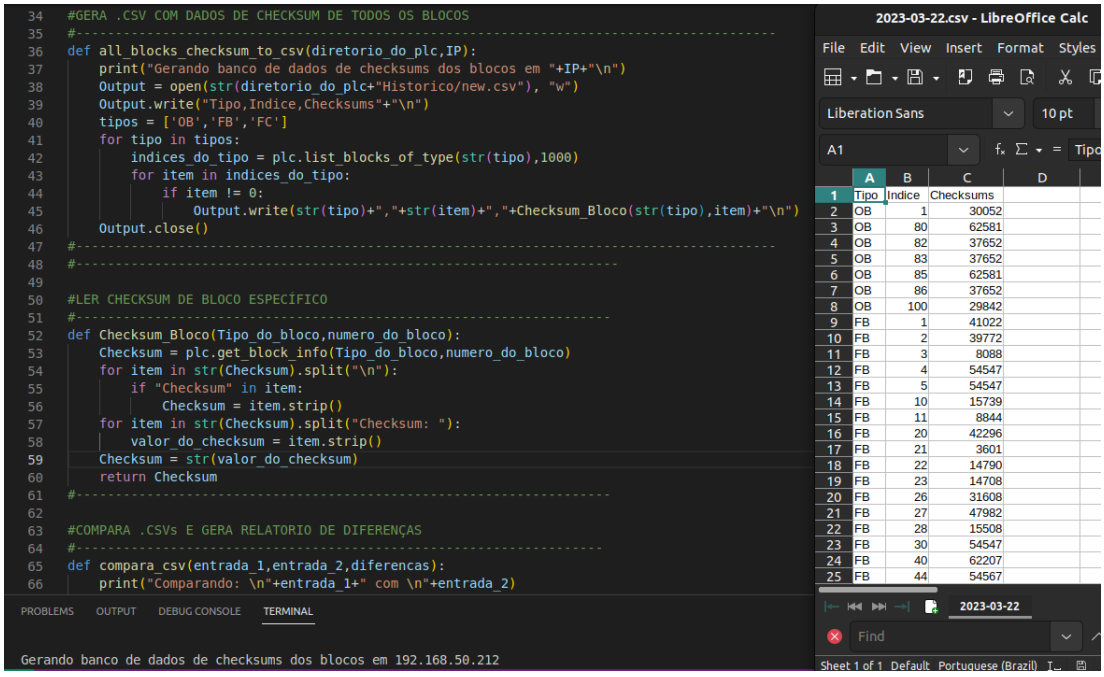

Figura 31 – Código para obter os CRCs e arquivo em formato CSV

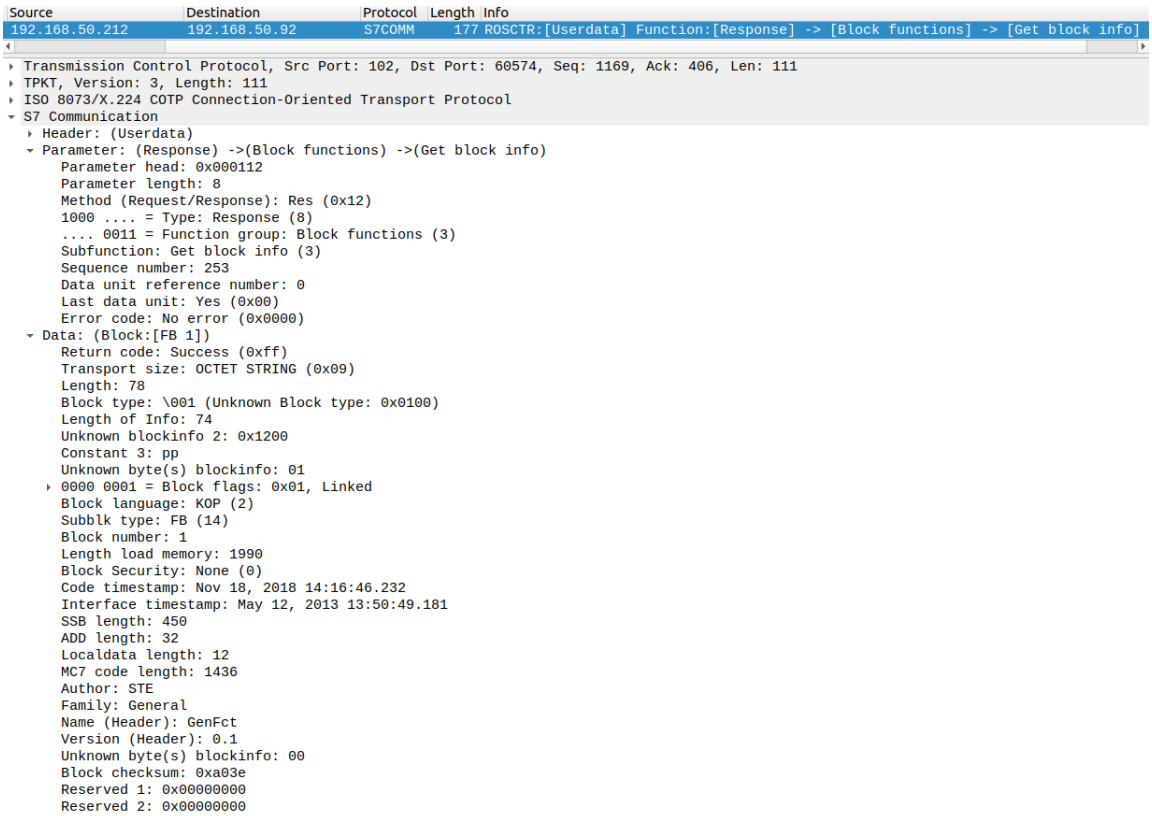

Figura 32 – Pacote capturado pelo *Wireshark* contendo CRC do FB1

seja possível saber o intervalo em que ocorreram as modificações detectadas pelo monitor. Para cada CRC diferente é gerada uma entrada num arquivo de *changelog*, que é único para cada CLP e armazena um resumo do resultado das comparações e a *timestamp* de cada comparação executada.

Na Figura 33 há um exemplo de *changelog* após a execução da varredura e a função implementada em Python responsável por esta etapa da execução. No início do *changelog* todos os blocos do CLP são listados pois trata-se de uma inicialização e não há parceiro de comparação. Nas execuções seguintes há a especificação apenas dos blocos que sofreram alteração. Caso nenhuma modificação seja detectada, a entrada no *changelog* contém apenas a *timestamp* e a linha onde estariam os blocos modificados fica em branco.

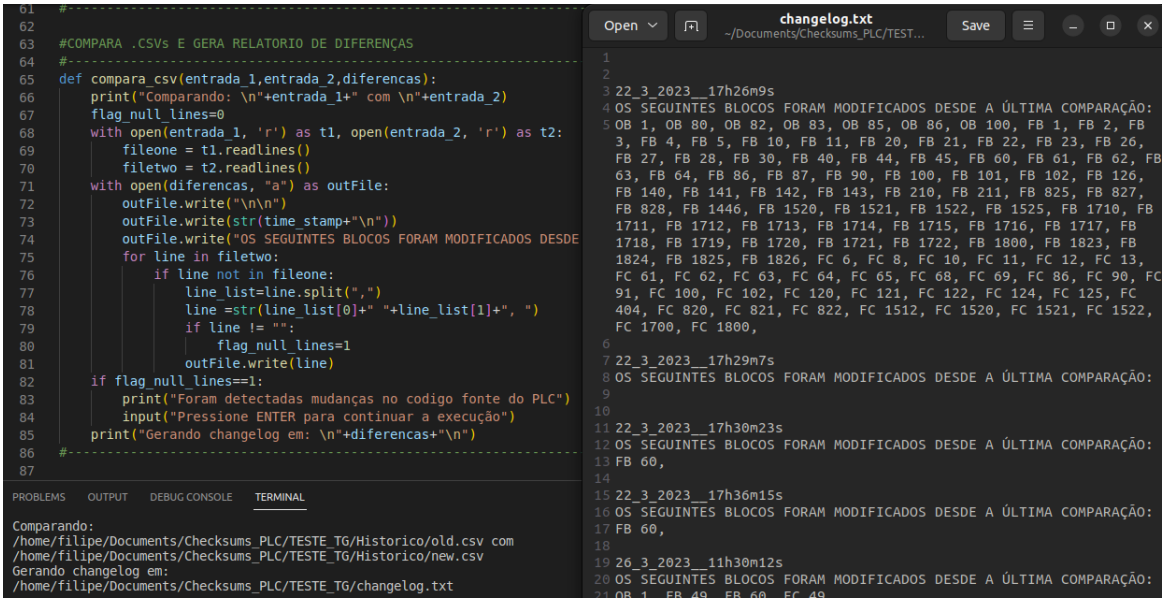

Figura 33 – Exemplo de *changelog* após varreduras

Com base no *changelog* gerado é possível rastrear o período em que estas modificações foram implementadas. Quanto menor for o intervalo entre as varreduras, maior será a precisão da detecção do momento da modificação. As modificações são detectadas com precisão de bloco de programação. Para determinar a modificação exata que ocorreu, é necessário possuir um *backup* do código fonte do CLP fiel com a última verificação, uma estação de engenharia com os softwares do fabricante para acesso ao CLP e uma boa gestão de modificação de código fonte do CLP para determinar se a modificação é ou não maliciosa.

5.3.4 Monitoramento de dados

Este monitor foi projetado para verificar modificações no código fonte, ou seja, nas OBs, FBs e FCs. O espaço de memória do CLP dedicado ao armazenamento de dados foi propositalmente ignorado. Isto se deu pois, em CLPs, é comum armazenar

neste espaço memória valores obtidos por sensores ou parâmetros dinâmicos e, por conta disso, monitorar modificação de dados pode levar à ocorrência de muitos falsos positivos. Existem situações onde é importante garantir que determinada variável se mantenha entre um valor mínimo e máximo. Nestas circunstâncias, é importante que este limite seja estabelecido explicitamente no código fonte do CLP e, a partir deste momento, caso algum valor indesejado seja atribuído a uma variável nestas condições, o próprio código fonte se encarregaria de desfazer a modificação e até sinalizar por meio de alarmes que houve a tentativa de atribuir um valor proibido a esta variável. Uma tentativa de desfazer este controle por parte de um atacante demandaria modificação no código fonte e, neste caso, a modificação maliciosa seria detectada pelo monitor de código fonte.

5.3.5 Desempenho do monitor ativo de código fonte diante de ataques

Para testar o desempenho do monitor ativo de código fonte, ele foi empregado em situações simuladas em que ataques como aqueles descritos no capítulo anterior foram realizados contra o CLP simulado.

5.3.5.1 Negação de serviços

No capitulo anterior foi descrito um ataque de injeção maliciosa de código fonte para programar a execução de um ataque agendado. Para este ataque, foram utilizados os blocos SFC28, SFC30, SFC46, OB1, OB10 e DB1. Os blocos SFC são de sistema e vêm de fábrica no CLP, não sendo assim enviados ao CLP e, desta forma, não há como detectá-los com um monitor de código fonte. O DB1 também não será detectado pois blocos de banco de dados não são monitorados por este monitor. Já o OB10 não passa despercebido e é detectado pelo monitor de código fonte. O OB1, que foi modificado também tem sua modificação detectada. A Figura 34 mostra o resultado da comparação.

```
17_4_2023__21h53m18s
OS SEGUINTES BLOCOS FORAM MODIFICADOS DESDE A ÚLTIMA COMPARAÇÃO:
OB 1,

17_4_2023__21h54m24s
OS SEGUINTES BLOCOS FORAM MODIFICADOS DESDE A ÚLTIMA COMPARAÇÃO:
OB 1, OB 10,
```

Figura 34 – Detecção de Injeção de código malicioso

Sabendo que houve uma modificação e quais são os blocos envolvidos, a próxima etapa é comparar a versão que está no CLP destes blocos com a versão no *backup offline*. A comparação detectaria o que está exposto na Figura 35 para o OB1 e na Figura 36 para o OB10. Analisando a modificação, é possível perceber que foi feito uso do SFC28 e SFC30 no OB1 e que os parâmetros do SFC28 estão armazenados no DB1, associando este bloco à modificação. Analisando o OB10, seria possível perceber o uso do SFC46. Utilizando a própria biblioteca de "ajuda"do software de engenharia, é possível saber para que servem os SFC 28 e 30, que são utilizados para agendar a chamada de um OB e, com base no código

que está no OB1, é possível perceber que este OB é o OB10. Analisando o código no OB10 e consultando na "ajuda"do software a função do bloco SFC46, fica claro que o OB10 tem a função de parar a execução do código fonte do CLP. Há circunstâncias em que utilizar uma interrupção para executar uma instrução de parada de execução do código fonte pode ser uma boa prática, por exemplo, para preservar a integridade da máquina em uma circunstância prevista. Assim, o simples uso do SFC46 não implica em ação maliciosa, mas com análise e com um bom controle de modificações do código fonte é possível detectar que a modificação é maliciosa e reverter para uma versão anterior estável. Dependendo do intervalo entre monitoramentos, neste caso, a detecção do código malicioso pode prevenir o ataque, já que ele é agendado.

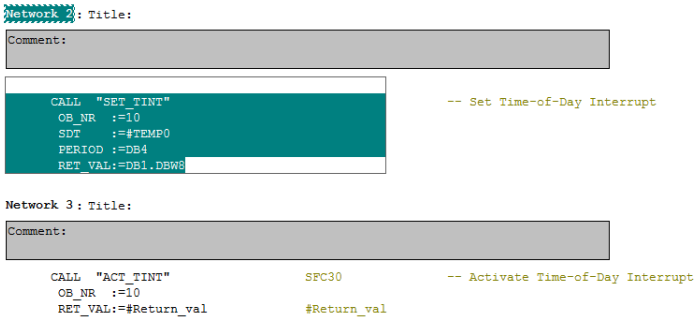

Figura 35 – Modificação do OB1

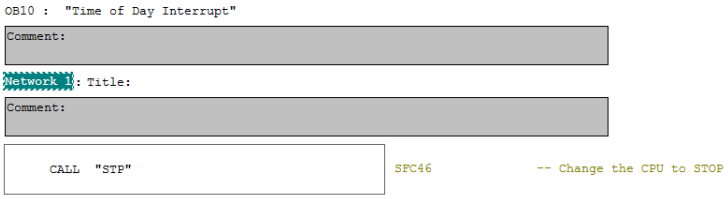

Figura 36 – Modificação do OB10

5.3.5.2 *Replay attack*, *Man in the middle* e Quebra de senha de acesso

Ataques *replay*, *Man in the middle* e Quebra de senha de acesso exploram fragilidades relacionadas a criptografia e à possibilidade de se conectar ao CLP sem estabelecer sessão. Este tipo de ataque foge do escopo de um monitor de código fonte e se aplica melhor a um monitor de rede. Por conta disso, o monitoramento ativo de código fonte tem seu resultado potencializado quando empregado em conjunto com o monitoramento ativo de rede.

5.3.5.3 Ataques direcionados

Quando se trata de ataques onde todo o código fonte se perde ou que o CLP imediatamente vai para condição de *Stop*, o monitoramento de código fonte não é a melhor

linha de defesa pois, mesmo que a detecção do monitor seja eficaz, o ataque já é bastante explícito e, no caso do apagamento do código fonte, o impacto sobre o funcionamento da máquina muito provavelmente será perceptível. Em casos onde o ataque é direcionado, o monitoramento de código fonte tem sua eficácia melhor aproveitada.

Em ataques direcionados, é comum que o atacante tenha conhecimento sobre o funcionamento da máquina, seja porque obteve acesso ao PC de engenharia e conhece o programa da máquina a ponto de projetar um ataque ou porque quebrou a senha de acesso ao CLP (supondo que esteja protegido desta forma) e estudou os pacotes de troca de dados do CLP num ataque *Man-in-the-middle*. Nestes casos, os ataques costumam ser mais sutis, modificando parte específica do código fonte onde o prejuízo causado seja maximizado, e de uma forma que seja difícil detectar inclusive que houve o ataque. Para estas circunstâncias, o monitoramento ativo de código fonte é útil, pois detecta a modificação e sinaliza a ocorrência de um ataque, comprovando a necessidade de ações adicionais para proteger a rede de acesso indevido.

A detecção de ataques por monitorar o código fonte pode desencadear ações que modifiquem a política de acesso às redes OT numa indústria, por exemplo, isolando-a de outras redes por onde um ataque possa ocorrer. Quando a rede em questão é a internet, não há como limitar o acesso de dispositivos do mundo inteiro e projetar uma estratégia de defesa com base apenas em monitores ativos. Assim, o monitoramento ativo de rede e de código fonte são ações de contenção apenas em redes isoladas em que o acesso de dispositivos IT possa ser controlado e a política de acesso possa ser modificada de acordo com a necessidade, e não são suficientes para justificar a exposição de dispositivos vulneráveis à internet.

Comentários finais

Analisando o cenário atual da indústria, percebe-se um grande potencial de se agregar valor a produto e processo através da digitalização e da Indústria 4.0. Para que uma indústria atinja um grau de maturidade elevado de indústria 4.0, utilizando recursos como gêmeos digitais e adoção de resposta autônoma, é necessária uma forte integração entre as redes industriais, e isso tem impacto sobre os dispositivos de campo, em especial os CLPs, que controlam processos específicos da planta e adquirem dados relevantes para as mais diversas aplicações. Apesar de esta integração ser inevitável e trazer vantagens competitivas à empresa, os dispositivos de campo, ou tecnologias operacionais, possuem necessidades especiais em relação às tecnologias de informação e, por atuarem um sistemas ciberfísicos, negligenciar estas necessidades pode ter resultados catastróficos. A inclusão da segurança cibernética como uma tecnologia habilitadora da Indústria 4.0, junto à integração vertical e horizontal e à internet das coisas mostra que estas tendências devem ser tratados com mesma importância.

Avaliando o protocolo S7comm, utilizado nos CLPs Siemens das famílias S7-300 e S7-400, é possível concluir que há fragilidades que abrem margem para a execução de ataques utilizando ferramentas de código aberto, como a biblioteca SNAP7, e que a sua exposição direta à internet deve ser fortemente desencorajada. O protocolo S7commPlus, evolução do protocolo S7comm utilizado em CLPs Siemens da família S7-1500, apesar de possuir melhorias em relação ao seu predecessor, ainda é suscetível a ataques cibernéticos e a sua integração vertical deve-se dar com a adoção de medidas de segurança adicionais.

Uma das propostas de medida adicional é a adoção de monitores de código fonte. Neste trabalho de graduação, foi proposto um software aberto programado em Python justamente com esta função, utilizando a biblioteca SNAP7 para integragir com o CLP utilizando o protocolo S7comm. Associar esta ferramenta a monitores de rede torna possível não só detectar uma modificação de código fonte no CLP mas também rastrear a origem do ataque.

Por fim, mesmo que haja uma preocupação com cibersegurança em dispositivos OT desde a etapa de projeto, e que se utilize os dispositivos mais atuais e técnicas de monitoramento de rede e código fonte, continua sendo importante que haja um cuidado especial com estes dispositivos, especialmente os CLPs que controlam a planta industrial de maneira centralizada. A integração vertical e a internet industrial das coisas viabilizam um avanço tecnológico muito grande à indústria, abrindo margem inclusive para novos modelos de negócio, mas continua sendo especialmente importante proteger os dispositivos de campo de acessos maliciosos adotando boas práticas de rede como restringindo o seu acesso

direto a sistemas que realmente necessitem desta interação, e utilizando computadores de borda ou estratégias semelhantes onde esta interação possa ser indireta.

Referências

ALSABBAGH, W.; LANGENDOERFER, P. A new injection threat on s7-1500 plcs - disrupting the physical process offline. *IEEE Open Journal of the Industrial Electronics Society*, v. 3, p. 1–1, 01 2022. Citado 3 vezes nas páginas 13, 27 e 32.

ALSABBAGH, W.; LANGENDOERFER, P. A remote attack tool against siemens s7-300 controllers: A practical report. In: JASPERNEITE, J.; LOHWEG, V. (Ed.). *Kommunikation und Bildverarbeitung in der Automation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2022. p. 3–21. ISBN 978-3-662-64283-2. Citado 2 vezes nas páginas 33 e 42.

ALSABBAGH, W.; LANGENDÖRFER, P. Patch now and attack later-exploiting s7 plcs by time-of-day block. In: IEEE. *2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*. [S.l.], 2021. p. 144–151. Citado 5 vezes nas páginas 6, 37, 38, 39 e 42.

BECKER, T. et al. *Industrie 4.0 Maturity Index [eng.]*. [s.n.], 2022. (Managing the Digital Transformation of Companies). ISBN 978-3-8316-7314-8. Disponível em: <https://www.acatech.de/publikation/industrie-4-0-maturity-index-update-2020/download-pdf?lang=en>. Citado 4 vezes nas páginas 6, 13, 28 e 29.

CHAN, C.-F. et al. Enhancing the security and forensic capabilities of programmable logic controllers. In: SPRINGER. *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14*. [S.l.], 2018. p. 351–367. Citado na página 51.

CRAIG, P.; BROOKS, C. *Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT*. Wiley, 2022. ISBN 9781119883043. Disponível em: <https://books.google.com.br/books?id=nTtvEAAAQBAJ>. Citado 4 vezes nas páginas 6, 17, 18 e 20.

GROOVER, M.; JAYAPRAKASH, G. *Automation, Production Systems, and Computer-integrated Manufacturing*. Pearson Education Limited, 2015. (Always learning). ISBN 9781292076119. Disponível em: <https://books.google.com.br/books?id=t2fXoAEACAAJ>. Citado 6 vezes nas páginas 6, 19, 20, 33, 34 e 35.

HERMANN, M.; PENTEK, T.; OTTO, B. Design principles for industrie 4.0 scenarios: A literature review. 01 2015. Citado na página 28.

KAGERMANN, H. et al. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group*. [S.l.]: Forschungsunion, 2013. Citado 2 vezes nas páginas 13 e 32.

KUROSE, J.; ROSS, K. *Redes de computadores e a internet: uma abordagem top-down*. Pearson, 2013. ISBN 9788581436777. Disponível em: <https://books.google.com.br/books?id=g-cCkAEACAAJ>. Citado na página 31.

MOLENAAR, G.; PREEKER, S. *Snap7 documentation*. [S.l.], 2023. Disponível em: <https://python-snap7.readthedocs.io/en/latest/>. Acesso em: 16 nov. 2023. Citado na página 42.

PROFIBUS Tecnology and Application. 2002. Citado 5 vezes nas páginas 6, 22, 23, 24 e 25.

RÜSSMANN, M. et al. Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston consulting group*, Boston, MA, USA:, v. 9, n. 1, p. 54–89, 2015. Citado 2 vezes nas páginas 6 e 29.

SANDARUWAN, G.; RANAWEERA, P.; OLESHCHUK, V. A. Plc security and critical infrastructure protection. In: IEEE. *2013 IEEE 8th international conference on industrial and information systems*. [S.l.], 2013. p. 81–85. Citado 3 vezes nas páginas 6, 40 e 43.

SEN, S. *Fieldbus and Networking in Process Automation*. CRC Press, 2017. ISBN 9781351831680. Disponível em: <https://books.google.com.br/books?id=nAhEDwAAQBAJ>. Citado 4 vezes nas páginas 6, 20, 21 e 22.

SIEMENS. *Information about the product phase-out of S7-300 / ET 200M components*. [S.l.], 2022. Citado 2 vezes nas páginas 16 e 32.

STALLINGS, W. *Computer security principles and practice*. [S.l.: s.n.], 2015. Citado 2 vezes nas páginas 30 e 31.

SUPORT, S. *CPU-CPU Communication with SIMATIC Controlllers*. [S.l.], 2023. Disponível em: <https://cache.industry.siemens.com/dl/files/908/78028908/att_1134019/v1/78028908_SIMATIC_Comm_DOKU_v23_e.pdf>. Acesso em: 13 nov. 2023. Citado 3 vezes nas páginas 6, 26 e 27.

WU, Y.; CUI, A. *Missing Immutable Root of Trust in Hardware*. [S.l.], 2023. Citado na página 32.