

Diagnóstico de Anomalia no Tempo de Download em Sistema PCS7 Redundante

Felipe Alysso de Sá e Rodolpho V. A. Neves

Abstract — Sistemas de controle distribuído (DCS) com redundância de CPU são amplamente utilizados em processos industriais críticos que exigem alta disponibilidade. Este trabalho apresenta um estudo de caso de diagnóstico realizado em um sistema SIMATIC PCS7 (*Process Control System*) com par de CPUs 417-H redundantes de uma planta de mineração, no qual o processo de download de alterações de programa (*download changes*) apresentava duração anormal superior a 20 minutos. Por meio de uma metodologia baseada na eliminação de hipóteses, abrangendo sincronismo entre CPUs, infraestrutura de rede Ethernet e a estação de engenharia, identificou-se que a causa raiz estava na rede de campo Profibus DP: foi identificado um módulo de interface IM 153-2 pertencente a um Y-Link, sem função operacional ativa no processo, apresentando falhas intermitentes de redundância (aproximadamente 40 eventos por minuto), impedindo a estabilização do sistema durante a fase de download para as CPUs. O isolamento do equipamento normalizou o tempo de download para um patamar normal, menos de um minuto, sem necessidade de interromper a redundância do sistema. Discute-se o mecanismo com base na documentação técnica do fabricante, importância da manutenção preditiva da camada física em redes industriais, e os limites da documentação disponível para diagnóstico de sistemas proprietários.

Palavras Chaves — CPU redundante; diagnóstico de falhas industriais; PCS7; Profibus DP; redundância H-System; sistemas de controle distribuído.

I. INTRODUÇÃO

Sistemas de controle distribuído (DCS) com redundância de CPU são adotados em plantas industriais por assegurarem a continuidade operacional, tornando a confiabilidade dessa arquitetura um requisito crítico. Em operações com mineração subterrânea, por exemplo, a ventilação e o resfriamento da mina são funções vitais tanto para a segurança de pessoal quanto para a viabilidade da operação, exigindo automação robusta e de alta disponibilidade.

Apesar de os mecanismos de redundância reduzirem significativamente o risco de indisponibilidade decorrente de falhas de hardware, a necessidade de sincronização entre as CPUs em operações rotineiras de manutenção, como o download de alterações de programa (*download changes*),

pode ser afetada por instabilidades em camadas da arquitetura aparentemente não relacionadas ao sintoma observado, tornando o diagnóstico uma tarefa não trivial mesmo para equipes experientes. O Profibus DP, protocolo de campo amplamente utilizado na automação de processos [1], pode apresentar falhas intermitentes na camada física de diagnóstico complexo, como discutido neste trabalho.

Este trabalho apresenta um estudo de caso de diagnóstico realizado em um sistema SIMATIC PCS7 com par de CPUs 417-H redundantes, no qual o processo de download em modo *changes* apresentava duração anormal, superior a 20 minutos, sem indicação aparente de causa. O autor atuou como especialista contratado especificamente para diagnosticar e resolver o problema, sem envolvimento na concepção original da arquitetura da planta.

O objetivo deste trabalho é descrever a metodologia de diagnóstico empregada, baseada na eliminação de hipóteses - abordagem sistemática consolidada na literatura de diagnóstico de falhas [2] - abrangendo sincronismo entre CPUs, infraestrutura de rede Ethernet e a estação de engenharia, e apresentar a causa raiz identificada na rede de campo Profibus DP, discutindo seu mecanismo com base na documentação técnica do fabricante. Adicionalmente, discute-se a importância da manutenção preditiva da camada física em redes industriais e os limites da documentação disponível para o diagnóstico de sistemas de automação proprietários.

O restante deste artigo está organizado da seguinte forma: a Seção II apresenta a fundamentação teórica sobre redundância em sistemas H, redes Profibus DP e a arquitetura de rede recomendada para sistemas PCS7; a Seção III descreve o sistema estudado; a Seção IV detalha a metodologia de diagnóstico; a Seção V apresenta os resultados obtidos; e a Seção VI conclui o trabalho.

II. FUNDAMENTAÇÃO TEÓRICA

A. Sistemas DCS e redundância H-System

Sistemas DCS como o SIMATIC PCS7 são amplamente utilizados em processos industriais contínuos que demandam alta disponibilidade. Para aplicações críticas, o PCS7 oferece arquiteturas redundantes baseadas no conceito de H-System (do inglês *high availability*, alta disponibilidade), no qual duas CPUs (denominadas *master* e *standby*) operam em paralelo, executando a mesma lógica de forma sincronizada. A sincronização entre as CPUs ocorre através de um link duplo dedicado de fibra óptica, implementado por módulos de sincronismo específicos, exigindo quatro módulos idênticos por sistema H, dois por CPU [3]. Em caso de falha da CPU

master, a CPU *standby* assume o controle do processo sem interrupção perceptível.

B. Rede de campo Profibus DP redundante

Em arquiteturas H, a rede Profibus DP pode ser implementada de forma redundante, consistindo em duas redes eletricamente independentes, cada uma conectada a um dos mestres do sistema H [1]. Para viabilizar distâncias maiores ou aumentar a tolerância a falhas, o protocolo permite o uso de componentes ópticos, como o OLM (*Optical Link Module*), que convertem o sinal elétrico RS-485 em óptico e vice-versa [1].

Quando um segmento de dispositivos Profibus DP não redundantes precisa ser integrado a um sistema H, sem que esses dispositivos disponham de dupla conexão própria, a Siemens prevê o uso do acoplador Y-Link. O conjunto Y-Link é composto por dois módulos de interface IM 153-2, um conectado a cada mestre DP redundante do sistema H, e um Y-coupler, que une as duas linhas em um único segmento DP ou PA não redundante do lado de campo [5]. Dessa forma, os dispositivos do lado dos escravos de campo do Y-coupler operam como escravos DP convencionais, enquanto a redundância é mantida do lado dos mestres redundantes, entre os dois IM 153-2 e os respectivos mestres.

C. Download em sistemas redundantes

O processo de download de alterações em um *H-System* envolve a sincronização de configuração e blocos de programa entre as duas CPUs, o que dispara um ciclo de *link-up and update* [6]. O tempo necessário para essa transferência de parâmetros depende de fatores como taxa de transmissão, volume de dados e carga do barramento no momento da operação [6], sendo esse último fator especialmente relevante quando a rede de campo apresenta instabilidade, como discutido na Seção IV.

D. Mecanismo de sinalização de redundância de I/O (OB70)

O evento de perda de redundância de I/O em sistemas H é sinalizado pela OB70 (*Organization Block*), tratada pelo bloco de driver SUBNET, responsável por monitorar sistemas mestre DP redundantes específicos da CPU 417-H. A OB70 é executada a cada evento de perda ou retorno de redundância: quando uma rede DP falha, a perda é sinalizada, e o retorno é sinalizado assim que o escravo DP afetado restabelece a conexão [7], mecanismo diretamente observado no padrão de eventos analisado na Seção IV.

E. Manutenção de redes industriais

A confiabilidade da rede Profibus DP também depende da camada física: cabeamento, conectores e terminações degradam com o tempo e geram erros intermitentes de difícil diagnóstico, como neste caso. Ferramentas de análise de sinal, como o ProfiTrace, medem ruído, reflexões e qualidade de terminação, permitindo identificar esses pontos antes que causem falha de redundância [4], [9]. Equipamentos sem função ativa, como o Y-Link deste estudo, devem ser removidos ou isolados eletricamente, não só desconectados de

seu uso original, sob pena de se tornarem pontos que podem originar problemas futuros.

III. DESCRIÇÃO DO SISTEMA

Em uma planta de mineração de ouro de grande porte, com mina subterrânea, há um sistema de automação responsável pela ventilação e resfriamento da mina, uma operação com profundidade superior a 1.000 metros e extensa malha de galerias, da ordem de centenas de quilômetros. O sistema conta com ventiladores, exaustores, chillers e outros equipamentos. Sistemas como esse são de alta criticidade, exigindo automação robusta e de alta disponibilidade.

A planta foi projetada utilizando o DCS da Siemens denominado PCS7. O sistema conta com um par de CPUs 417-H redundantes, permitindo operação contínua mesmo durante expansões ou alterações que normalmente exigiriam parada, como downloads ou atualizações, além da disponibilidade mesmo com falhas em partes do sistema.

A rede de campo padrão utilizada é Profibus DP, segmentada em dois CPs (*Communications Processor*) distintos, conectados ao rack das CPUs: um dedicado à rede CCM (Centro de Controle de Motores) e outro à rede de I/O remotas e instrumentação Profibus PA. O cabo elétrico RS-485 sai dos CPs e forma um tronco até as IMs (*Interface Module*), com uma cabeça de rede para cada CPU. Em alguns trechos desse tronco, quando necessário por questões de distância, o sinal é convertido para fibra óptica por um OLM e reconvertido no outro extremo por um segundo OLM.

Além do par de CPUs redundantes, durante expansões da planta foram integradas CPUs S7-1200 convencionais, conectadas diretamente ao supervisório WinCC do PCS7. O sistema conta com dois servidores de supervisório, denominados OSs, garantindo maior disponibilidade da camada de supervisão, além de 4 clientes distribuídos em localizações estratégicas nas instalações industriais da planta.

A arquitetura de rede recomendada pela Siemens prevê segmentação em camadas distintas, *plant bus*, *terminal bus*, rede perimetral e rede corporativa, com firewalls entre essas camadas [8]. Essa segregação, no entanto, não era a realidade da planta em questão: as CPUs S7-1200 e sistemas corporativos/PIMS (*Plant Information Management System*) também estavam integrados à rede de terminal bus.

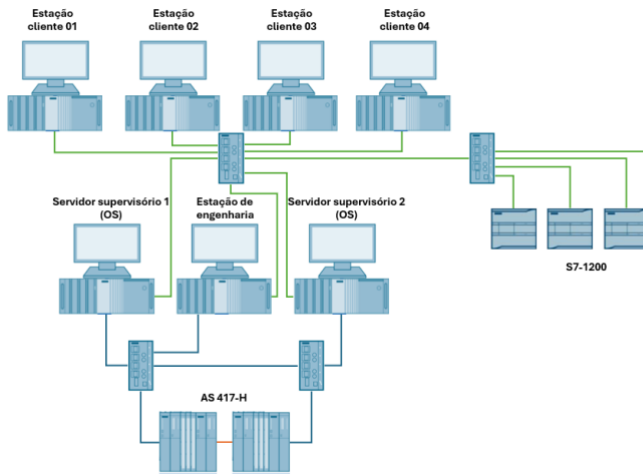


Fig. 1. Arquitetura do sistema de automação.

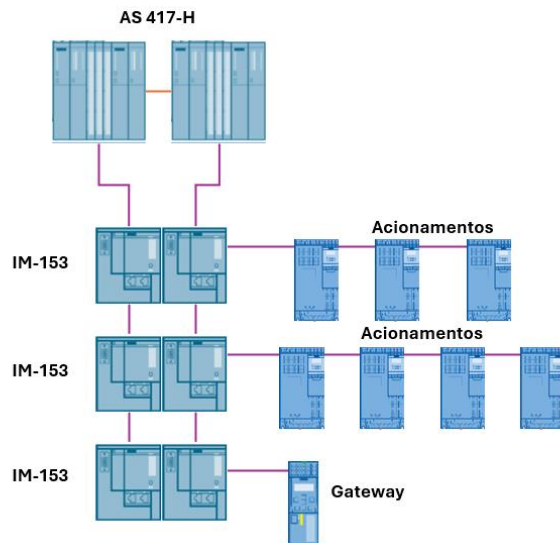


Fig. 2. Esboço arquitetura de rede Profibus DP.



Fig. 3. Par de CPUs redundantes.

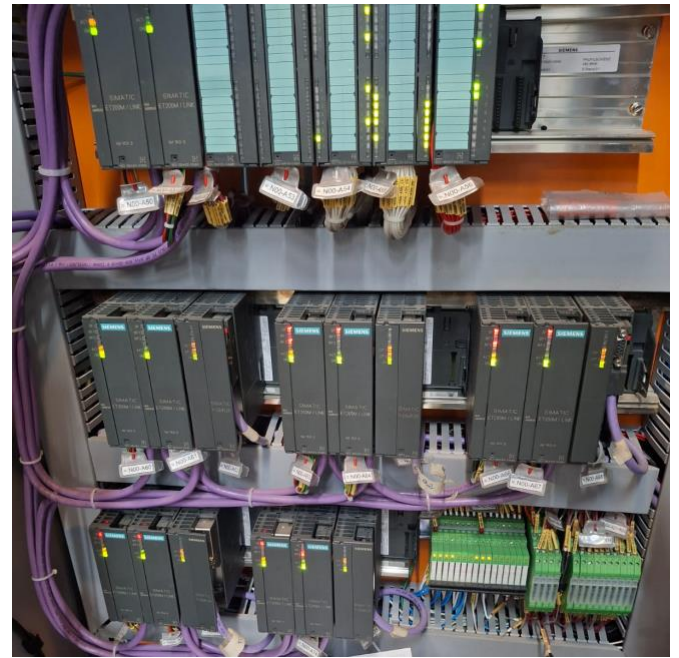


Fig. 4. Ims Profibus DP instaladas no painel do CLP.

IV. METODOLOGIA E DIAGNÓSTICO

O diagnóstico partiu de um levantamento inicial da arquitetura, seguido pela formulação e teste progressivo de hipóteses, conforme resumido na Tabela I.

TABELA I
CRONOLOGIA DO DIAGNÓSTICO

Etapa	Ação	Resultado
0	Levantamento de arquitetura (backup + campo) e verificações de sanidade (placas, ping, desempenho da engenharia)	Tudo normal; identificada segmentação de rede inadequada; sistema migrado (PCS7 8.2→10.0) poucos meses antes
1	Sincronismo entre CPUs: verificação de diagnóstico + substituição física de fibras e módulos	Sem melhora
2	Interconexão entre switches existentes	Sem melhora
3	Switch/cabeamento como causa física: switch novo (config. de fábrica) + cabos novos	Sem melhora
4	Conexão direta engenharia → CPU (sem switch)	Sem melhora
5	Engenharia como causa: máquina virtual (VM) nova, instalação limpa, backup restaurado	Sem melhora
6	Análise de logs	Causa raiz confirmada

A. Etapa 0

O levantamento inicial, realizado a partir do backup do sistema e de inspeção física, identificou: um servidor de engenharia PCS7, dois servidores OS, 4 clientes, o par de CPUs 417-H redundantes com rede Profibus DP/PA, e quatro CPUs S7-1200 operando como SCADA (*Supervisory Control and Data Acquisition*) clássico. O cliente relatou que o download de alterações de programa travava especificamente na fase '*Identifying Blocks*', e que o processo ocorria normalmente quando uma das CPUs era colocada em STOP, informação confirmada por teste direto antes do início da investigação do problema. Constatou-se também que as CPUs S7-1200 estavam conectadas ao mesmo switch dos servidores OS e da rede corporativa/PIMS, sem a segregação recomendada pelo fabricante [8]. O sistema havia sido migrado poucos meses antes (troca de servidores, engenharia e clientes, e atualização da aplicação do PCS7 da versão 8.2 para a versão 10.0), sem que fosse possível determinar se o sintoma já existia antes da migração.

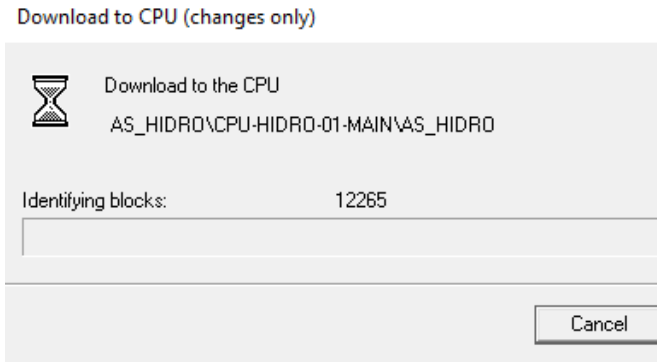


Fig. 5. Download travado na fase '*Identifying Blocks*'.

B. Etapa 1

A primeira hipótese investigada foi a de falha no sincronismo entre as CPUs. Verificação dos diagnósticos de sincronismo via HW Config (aba "*Sync module diagnostics*") não indicou nenhuma anomalia no link de sincronismo. Ainda assim, como medida de eliminação, foi realizada a substituição completa do par de fibras ópticas e dos quatro módulos de sincronismo, conforme exigência do fabricante de utilizar módulos idênticos em todo o sistema H [3]. O sintoma persistiu de forma idêntica, descartando o sincronismo entre CPUs como causa raiz.

C. Etapa 2 e 3

Com o sincronismo entre CPUs descartado, a hipótese seguinte foi a de que a infraestrutura de rede Ethernet, especificamente os switches e o cabeamento, fosse a causa da lentidão no download. Na arquitetura original, cada CPU do par redundante estava conectada a um switch próprio, com os dois switches interligados entre si e cada um recebendo também uma porta de um dos servidores OS, e um deles a estação de engenharia. Testou-se primeiro a conexão da engenharia e das duas CPUs em um único switch existente, eliminando a interligação entre switches como problema, sem melhora. Em seguida, montou-se uma rede isolada com switch

novo, com configuração de fábrica e cabeamento novo, conectando o mesmo conjunto (engenharia e as duas CPUs), eliminando tanto o switch quanto o cabeamento como possíveis causas, sem melhora observada.

D. Etapa 4

Como teste complementar, a estação de engenharia foi conectada diretamente a uma das CPUs, eliminando o switch da cadeia de comunicação. Ainda que o comportamento normal do sistema redundante já garanta o direcionamento do download à CPU parceira via link de sincronismo mesmo sem conexão direta da engenharia a ambas, o teste buscava eliminar qualquer efeito de gargalo decorrente da conexão simultânea dos três nós ao mesmo switch. O sintoma persistiu, descartando essa variável.

E. Etapa 5

Motivado pelo contexto de migração recente, testou-se a hipótese de a estação de engenharia ser a causa: uma máquina virtual foi criada com instalação limpa do PCS7 a partir dos instaladores oficiais do cliente, com o backup do projeto restaurado, conectada à mesma rede isolada da Etapa 3. O sintoma persistiu de forma idêntica, descartando engenharia, placa de rede, desempenho e firewall como causas.

F. Etapa 6

Com as hipóteses da camada Ethernet e da engenharia esgotadas, procedeu-se à análise detalhada dos logs de diagnóstico de hardware online das CPUs, coletados ao longo de todos os testes. Dado o alto volume (2.983 eventos na CPU master e 2.984 na standby, concentrados em uma janela de aproximadamente 16 minutos) e a presença de eventos não relacionados ao problema, foi realizada uma análise detalhada dos registros em busca de padrões recorrentes.

A análise identificou um padrão de comutação contínua de redundância Profibus DP no escravo DP de endereço 11, associada a um acoplador Y-Link, gerenciado pelo CP 443-5 responsável pela rede de instrumentação: 644 (CPU *master*) e 648 (CPU *standby*) pares de perda/retorno de redundância, com taxa média de ~40 ocorrências por minuto, além de 1.288/1.296 eventos de erro de I/O distribuído e 202/195 eventos de falha de parametrização do SDB (*System Data Blocks*) 2013. Cada evento de perda/retorno disparava a OB70 (I/O redundancy error) [7], levando o sistema a tentativas sucessivas de reparametrização da estação e aparentemente impedindo o SIMATIC PCS7 de obter um estado estável entre as CPUs durante a fase "*Identifying Blocks*" do download.

A hipótese foi confirmada operacionalmente: ao colocar a CPU standby em STOP, o sistema sai do modo redundante, a OB70 deixa de ser disparada, e o processo de download passa de mais de 20 minutos para menos de um minuto. A identificação física do equipamento correspondente ao escravo DP de endereço 11, posterior a essa análise, revelou tratar-se de um módulo IM 153-2, integrante do conjunto Y-Link responsável por conectar essa porção da rede a ambos os mestres DP redundantes, originalmente associado a um gateway já desativado e sem função ativa no sistema.

O isolamento do ramo do Y-Link associado ao módulo IM

153-2 em falha eliminou os eventos de comutação de redundância e restabeleceu o tempo normal de download. Embora a intervenção confirme a associação entre o comportamento anômalo e esse equipamento, não foi possível identificar qual componente interno do conjunto era responsável pela falha.

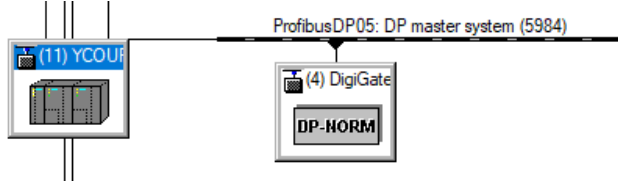


Fig. 6. Equipamento defeituoso na configuração de hardware.

V. RESULTADOS

A causa raiz foi confirmada em campo por meio do isolamento do ramo redundante do Y-Link associado ao escravo 11, o que normalizou o tempo de download sem necessidade de interromper a CPU standby, ao contrário do teste diagnóstico inicial (parada da CPU standby), que confirmava a causa, mas não constituía solução operacional viável, por sacrificar temporariamente a redundância do sistema. A remoção física definitiva do trecho de tronco Profibus DP associado permanece planejada para uma janela de manutenção subsequente.

O resultado foi replicado em três ocasiões subsequentes: duas execuções de download de lógica em modo *changes* e uma execução de download de hardware, todas apresentando o mesmo comportamento normalizado. Embora a maior parte dos testes de diagnóstico tenha sido conduzida em modo *changes*, a normalização observada também no download de hardware sugere que a causa raiz afetava o mecanismo de sincronização do H-System de forma geral, e não um modo de download específico.

Não foi realizada nova coleta e análise dos logs de diagnóstico da CPU após a intervenção para confirmar formalmente a ausência dos eventos de comutações no escravo 11. A validação baseou-se no comportamento observado (tempo de download), não em confirmação direta via log, uma limitação da validação que não compromete a robustez do diagnóstico, dado o padrão de causa-efeito já estabelecido, mas que representa uma verificação complementar não realizada.

O isolamento não gerou impacto operacional, uma vez que o escravo DP não possuía função ativa no sistema de controle.

VI. CONCLUSÃO

Este trabalho apresentou um estudo de caso de diagnóstico de falha em sistema PCS7 com CPUs redundantes 417-H, no qual um download em modo *changes* apresentava duração anômala superior a 20 minutos. Por meio de um processo baseado na eliminação de hipóteses, abrangendo sincronismo entre CPUs, infraestrutura de rede Ethernet e a estação de engenharia, identificou-se que a causa raiz residia na rede de

campo Profibus DP: um equipamento sem função ativa no sistema, mantido conectado por falha de manutenção, apresentava oscilações intermitentes de redundância que impedia o SIMATIC PCS7 de obter um estado estável do H-System durante o download. A remoção física do equipamento normalizou o processo, reduzindo o tempo de download para menos de um minuto.

O caso ilustra dois pontos relevantes para a prática de automação industrial. Primeiro, a importância da manutenção e do controle da topologia de rede: equipamentos obsoletos ou sem função ativa, mesmo quando fisicamente desconectados de seu propósito original, podem permanecer eletricamente presentes na rede, fora do escopo de manutenção rotineira, e causar instabilidades severas e de difícil diagnóstico. Segundo, o valor de uma metodologia baseada na eliminação de hipóteses diante de sintomas ambíguos, especialmente quando a primeira impressão da arquitetura direciona a investigação inicial para a camada equivocada.

Como limitação, a correção não foi validada por nova análise dos logs de diagnóstico, restringindo-se à observação do comportamento do sistema. A confirmação da causa física limitou-se à identificação e ao isolamento do ramo em falha, sem instrumentação específica de diagnóstico da camada física do barramento, como inspeção de conectores e terminação, e análise de níveis de sinal com ferramentas de análise Profibus, a exemplo do ProfiTrace, capazes de identificar ruído, quedas de tensão e problemas de terminação [8]. Tal verificação, somada à remoção física definitiva do Y-Link ainda pendente, é recomendada como continuidade deste diagnóstico, além de uma análise em toda rede, para que problemas similares não voltem a acontecer.

Além disso, o mecanismo interno exato do PCS7 durante a fase "*Identifying Blocks*" no download não é detalhado nas fontes oficiais consultadas, limitação comum em sistemas proprietários de automação industrial, que reforça o valor prático da experiência de campo e de metodologias estruturadas diante de sintomas cuja causa não é explicada pela documentação disponível.

REFERÊNCIAS

- [1] PROFIBUS Nutzerorganisation e.V. (PI). *PROFIBUS Design Guideline*, Order No. 8.012, V1.29, set. 2020.
- [2] ISERMANN, R. *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Berlin: Springer-Verlag, 2006.
- [3] SIEMENS AG. *Synchronization modules for S7-400H*, Equipment Manual, abr. 2020.
- [4] SIEMENS AG. *SIMATIC NET – PROFIBUS Network Manual*, System Manual, abr. 2009.
- [5] SIEMENS AG. *SIMATIC — DP/PA Coupler, DP/PA Link, Y-Link and Active Field Distributors — Operating Instructions*, dez. 2021.
- [6] SIEMENS AG. *CPU S7-400H (V6.0) System Manual*, nov. 2025.
- [7] SIEMENS AG. *SIMATIC Process Control System PCS 7 – Driver Blocks*, Reference Manual, out. 2001.
- [8] SIEMENS AG. *SIMATIC PCS 7 – Standard Architectures*, V9.1, dez. 2021.
- [9] PROCENTEC. *ProfiTrace 2 User Manual*, V5.0.1, mar. 2016.