EasyChair Preprint

№ 15156

Zero-Trust Security Implementation to Industrial Networks

Robson Santos Junior, Felipe Gomes Cabral and
Publio Macedo Monteiro Lima

September 28, 2024

Implementação de segurança zero-trust para redes industriais

Robson Santos Jr. * **Felipe G. Cabral** * **Publio M. M. Lima** *

* *Departamento de Engenharia de Automação e Sistemas (EAS), Universidade Federal de Santa Catarina (UFSC), Campus Trindade, Florianópolis, 88.040-900, SC, Brasil (robson.fsj@posgrad.ufsc.br, felipe.gomes.cabral@ufsc.br, publio.lima@ufsc.br).*

Abstract: Industrial processes have become more interconnected, which allows new production configurations, more efficiency, and operational safety. However, this increase in connectivity can make industrial systems vulnerable to cyberthreats that can compromise the confidentiality of the information transmitted in industrial networks. Several strategies have been proposed in the literature to defend industrial systems against external attacks, such as opacity and cryptography. However, only few works deal with the problem of industrial networks that are internally compromised. In this paper, a new defense approach is proposed considering that the industrial network has been compromised. To do so, an analysis of the efficiency of RSA cryptographic procedure is carried out to ensure the security of the communication between Programmable Logic Controllers (PLCs) and an SCADA application. In this context, the information is decrypted only after all network components validate it. Using this strategy, it is possible to guarantee a secure information traffic in the network even when one of the network agents is compromised by an attacker.

Resumo: Processos industriais têm se tornado cada vez mais conectados, permitindo novas configurações de produção, maior eficiência e segurança na operação. Entretanto, essa maior conectividade pode deixar sistemas industriais vulneráveis a ciberataques capazes de comprometer a confidencialidade da informação transmitida em redes industriais. Diversas estratégias têm sido propostas para defender sistemas industriais contra ataques externos, como opacidade ou criptografia. Porém, poucos trabalhos consideram que a rede industrial possa estar internamente comprometida. Neste artigo, uma nova abordagem de defesa é proposta considerando-se que a rede industrial foi comprometida, o que pode ocorrer quando um atacante tem acesso indevido a um elemento que faz parte da rede. Para tanto, uma análise da eficácia da criptografia RSA é feita para garantir que a comunicação entre Controladores Lógico Programáveis (CLPs) e uma aplicação SCADA seja segura. Nesse contexto, é considerado que nenhum CLP é confiável, de modo a implementar a chamada *zero-trust network*. Nessa rede, a informação é descriptografada apenas após ser validada por todos os componentes da rede. Com essa estratégia, é possível garantir o tráfego seguro de informações na rede mesmo que um de seus agentes seja comprometido por um atacante.

Keywords: Cybersecurity; SCADA; Zero Trust; Cryptography; RSA.
Palavras-chaves: Cybersegurança; SCADA; Zero Trust; Criptografia; RSA.

1. INTRODUÇÃO

Com o avanço da Indústria 4.0, o processo de digitalização permite que um gigantesco número de tecnologias e dispositivos sejam capazes de se comunicar uns com os outros a partir de qualquer lugar e a qualquer hora, como observado por Munirathinam (2020). Tais tecnologias estão presentes desde o controle dos semáforos nas cidades até grandes complexos tecnológicos como plantas petrolíferas, subestações de energia elétrica e usinas nucleares. Esses e outros exemplos fazem parte do cotidiano dos seres humanos, conforme apresentado por Ackerman (2017).

O avanço tecnológico, além de melhorar a qualidade da vida da população, abre precedentes para diversos ataques cibernéticos, a exemplo dos que vêm ocorrendo com gigantes da manufatura e automação como o ataque à *Renault*, apresentado em Habibzadeh et al. (2019), e o recente ataque por *ransomware* à *Siemens Energy*, avaliado por Alsabbagh and Langendoerfer (2022). Tais ataques são capazes de causar impactos financeiros na casa dos milhões de euros, como foi o caso da *Renault*, que teve seu parque de produção e diversos setores da empresa parados em consequência ao ataque sofrido. Tendo em vista o impacto que o comprometimento de uma planta industrial pode causar, os ambientes da rede operativa e os de infraestrutura crítica devem estar submetidos aos padrões mais elevados de segurança cibernética para

⋆ O presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Código de Financiamento 001.

que, de modo prioritário, possam estar protegidos contra as ameaças contínuas causadas por ataques e *malwares* (software malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável) cada vez mais sofisticados, como demonstrado em Mitsarakis (2023). Tendo em vista todo este cenário e sua relevância, o Governo Federal do Brasil publicou em Outubro de 2023 a Política Nacional de Cibersegurança (PNCiber), um decreto que tem por objetivo unificar ações regulatórias existentes no país, buscando diminuir o débito tecnológico nacional no setor e ampliar a participação brasileira na cooperação internacional sobre a temática - Federal (2023).

Ataques cibernéticos são classificados na literatura em dois tipos (Oliveira et al., 2023): ataques ativos, em que o atacante modifica os dados transmitidos para causar danos ao sistema (Lima et al., 2021), e ataques passivos, onde o objetivo do atacante é reconhecer algum padrão ou segredo do sistema (Lima et al., 2022, 2023). Neste trabalho, vamos considerar o problema de um ataque ativo em uma rede industrial. Mais especificamente, vamos considerar a vulnerabilidade do sistema contra ataques internos, ou seja, ataques em que o agente não autorizado é uma entidade na rede e assim transmite informações para confundir os outros integrantes da rede na tentativa de fazer o sistema evoluir para um estado indesejável. Nessa situação, é essencial que as mensagens transmitidas sejam validadas, caso contrário o atacante pode se comunicar com todos da rede e assim causar danos ao sistema. Considerando esse problema, o conceito de *zero-trust network* surgiu para que seja possível transmitir informações seguras em uma rede em que o atacante faz parte da rede.

2. TRABALHOS RELACIONADOS

Sistemas de controle industriais são formados por um conjunto de dispositivos, como CLPs, RTUs, IHMs, sensores e atuadores. Estes ativos costumavam estar localizados de forma isolada, lógica e fisicamente, do mundo externo e este perímetro era considerado confiável. Tal abordagem é conhecida como defesa por perímetro, como observado em Ackerman (2017). O *National Institute for Standards and Technology* (NIST), agência americana não reguladora com foco em inovação e estabelecimento de padrões, garante que com os avanços tecnológicos e a digitalização da indústria, os mecanismos legados de defesa por perímetro já não são mais efetivos no combate aos invasores, também conhecidos como hackers. Chegou-se a esta conclusão devido ao fato de que com a computação em nuvem fica cada vez mais difícil delimitar um perímetro e garantir que todos os ativos, sejam eles tecnológicos ou os próprios usuários, sejam confiáveis (Stafford, 2020). Estudos recentes indicam que uma nova abordagem, chamada *Zero Trust*, que será detalhada posteriormente neste artigo, possibilita implementar ações que tratam todo e qualquer usuário ou ativo tecnológico como uma ameaça em potencial. Esta premissa exige que haja, de forma constante, uma verificação e controle de acesso a qualquer recurso dentro de uma planta industrial. Qualquer tentativa de conexão não verificada e previamente autorizada deve ser bloqueada (Peterson, 2021). No entanto, alguns desafios para implementação de uma arquitetura Zero Trust estão relacionados com a dificuldade em se implementar uma única solução adequada, o que leva à integração de várias tecnologias, acarretando na dificuldade de gerenciamento. Outro ponto seria a exigência de substituição dos equipamentos legados, que não suportam tecnologias Zero Trust, e grandes investimentos financeiros, recursos e capacidade técnica (Stouffer et al., 2022).

Em contrapartida, do Nascimento (2020) propõe um mecanismo que busca aplicar os princípios Zero Trust em sistemas de controle industrial, preservando ativos preexistentes. Com a proposta de preservar os ativos legados, sua metodologia visa a implementação de controles de segurança granulares em pontos críticos da rede, como interfaces de comunicação com a nuvem e dispositivos de controle. No entanto, não aplica o conceito de Zero Trust no dado em si, conforme proposto neste artigo.

Outra abordagem proposta por Premnath et al. (2014) para proteger a comunicação entre ativos utiliza a aplicação de um algoritmo de criptografia para garantir a segurança das comunicações em um ambiente SCADA. No trabalho foi utilizado o algoritmo de criptografia NTRU, introduzido na próxima seção, para garantir a conformidade aos padrões de segurança dos protocolos SCADA e fornecer autenticação, integridade, confidencialidade e não-repúdio aos dados. Todos estes conceitos serão detalhados na seção 5 deste artigo. Esta abordagem garante a segurança da comunicação, no entanto, não aplica os conceitos de segurança com base na arquitetura Zero Trust.

3. CONCEITUAÇÃO

A era digital é uma realidade e, consequentemente, uma gama infinita de dados e informações estão sendo gerados a cada segundo. Independentemente do tipo de operação, seja ela bancária ou comunicação entre ativos pertencentes a uma planta de energia elétrica, garantir sua segurança é um desafio latente. Para auxiliar no processo de proteção de dados e informações, a criptografia é uma grande aliada. Existem inúmeros algoritmos de criptografia, entre eles DES (*Data Encryption Standard*), RSA (Rivest, Shamir & Adelman), NTRU (*Number Theory Research Unit*) e demais algoritmos utilizados para criptografia de dados (Patil et al., 2016). Os algoritmos são classificados em duas categorias: algoritmos de chave simétrica e assimétrica. Os algoritmos de chave simétrica compartilham a mesma chave pra criptografar e descriptografar os dados. Já os classificados como assimétricos, não utilizam a mesma chave para criptografia e descriptografia da informação original. Nas subseções a seguir, um breve resumo sobre cada uma dessas técnicas de criptografia é apresentado.

3.1 Data Encryption Standard (DES)

Data Encryption Standard (DES) é um mecanismo de criptografia que utiliza chave simétrica. O comprimento da chave é de 56 bits e o tamanho do bloco é de 64 bits. É vulnerável a ataques de chave quando uma chave fraca é usada. DES foi primeiramente publicado em 1972 pela IBM como método de criptografia de dados. Foi adotado pelo governo dos EUA como algoritmo de criptografia padrão. Começou com uma chave de 64 bits e então a NSA (*National Security Agency*) implantou uma restrição ao uso do DES com um comprimento de chave de 56 bits, portanto o DES descarta 8 bits da chave de 64 bits e então

usa a chave compactada de 56 bits derivada da chave de 64 bits para criptografar dados em tamanho de bloco de 64 bits (Jorstad and Landgrave, 1997).

3.2 RSA

RSA foi publicado em 1977 e é um sistema criptográfico de chave públicaque recebeu esse nome por conta de seus fundadores Rivest, Shamir e Adelman. São geradas duas chaves criptográficas: chave públicae chave privada. O algoritmo RSA consiste em três etapas, a primeira etapa é a geração de chave utilizada para criptografar e descriptografar dados, a segunda etapa é a criptografia, onde o processo real de conversão de texto simples em texto cifrado é realizado. Já a terceira etapa é a descriptografia, onde o texto criptografado é convertido em texto simples pelo destinatário da mensagem. O RSA é baseado no problema da fatoração para encontrar o produto de dois grandes números primos. O tamanho das chaves varia entre 1.024 a 4.096 bits. Chaves pequenas o torna vulnerável e podem possibilitar a quebra do algoritmo, concedendo acesso não autorizado às informações (Al Hasib and Haque, 2008).

Algoritmo Matemático RSA: Neste artigo, o algoritmo de chave assimétrica para fins de proteção da comunicação entre CLPs em uma rede de automação é utilizado. Para descrever o mecanismo matemático que rege o algoritmo RSA, serão apresentados os passos matemáticos em cada iteração a seguir.

Descrição do Algoritmo Matemático RSA:

(1) Seleciona dois números primos p e q;
(2) Calcula $n = p \times q$;
(3) Calcula $\phi(n) = (p - 1 \times q - 1)$;
(4) Calcula chave pública e = co-primo entre 1 e $mmc(p-1, q-1)$;
(5) Calcula chave privada d: $d \times e = 1 \times mod(\phi(n))$;
(6) Criptografa o dado M: $C = M^e \times mod(n)$;
(7) Decifra o dado C: $M = C^d \times mod(n)$;

3.3 NTRU

NTRU é um sistema criptográfico de chave pública (PKCS) e um padrão IEEE 1363.1 e X9.98. Foi publicado pela primeira vez em 1996 por J.Hoffstein, J.Pipher e Silverman. Ele usa criptografia baseada em rede para criptografar e descriptografar dados. NTRU é baseado em estruturas algébricas de certos anéis polinomiais (Premnath et al., 2014).

4. ESTADO ATUAL DA SEGURANÇA CIBERNÉTICA APLICADA A SISTEMAS DE CONTROLE INDUSTRIAIS

No ano de 2022, o Instituto Nacional de Padrões e Tecnologia (NIST) publicou um manual intitulado "Orientações para Garantia de Segurança em Sistemas de Controle Industrial" (Stouffer et al., 2022), com o intuito de oferecer instruções para assegurar a integridade dos Sistemas de Controle Industrial (ICS), abrangendo seus distintos componentes (SCADA, DCS, PLCs, entre outros). Esse documento fornece diretrizes para o desenvolvimento de uma estrutura de segurança sólida para os ICS. Embora o manual enfoque primariamente na salvaguarda convencional por meio da instalação de firewalls, também ressalta a ênfase em princípios essenciais de Zero Trust, tais como a segmentação e isolamento de redes, autenticação e autorização, em conjunto com práticas de monitoramento e auditoria.

Além das orientações gerais estabelecidas pelo Instituto Nacional de Padrões e Tecnologia (NIST), a literatura tem apresentado diversas propostas de arquiteturas para Sistemas de Controle Industriais (ICS). Um exemplo significativo é a arquitetura hierárquica proposta pelo Laboratório Nacional de Idaho, que estende o paradigma hierárquico do Modelo de Referência Purdue, integrando-o aos sistemas de controle em infraestruturas críticas inteligentes (Chiluvuri et al., 2015). É importante observar que a arquitetura proposta não aborda adequadamente a proteção horizontal entre unidades individuais na mesma camada de segurança. Como resultado, permanece vulnerável aos riscos de segurança que o modelo Zero Trust busca mitigar.

4.1 Modelo Purdue de Referência

O Modelo Purdue de Referência adota o princípio das zonas de segurança como mecanismo para segmentar, tanto a rede corporativa (TI) quanto a rede de Sistemas de Controle Industrial (OT/ICS), em unidades lógicas compostas por sistemas que desempenham funções semelhantes ou que apresentem requisitos de funcionalidade similares. Para este artigo, direciona-se o foco para o Nível 2 - Zona de Processo, uma vez que será o objeto de aplicação das soluções criptográficas. A Figura 1 apresenta a metodologia utilizada para agrupamento e classificação dos ativos em uma rede de automação.

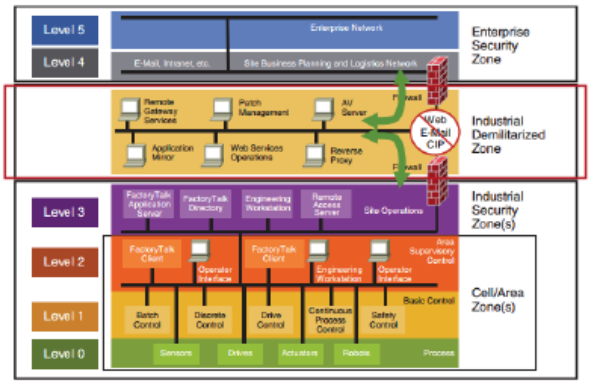

Figura 1. Modelo Purdue de Referência (Ackerman, 2017).

Uma infraestrutura de rede que utiliza o Modelo Purdue como metodologia de segurança cibernética adota uma abordagem baseada em perímetros para segmentar as zonas de segurança, conforme descrito anteriormente. Essa configuração é concebida sob a premissa de que as ameaças geralmente se originam do exterior, o que implica que, para comprometer a zona mais segura, seria necessário superar múltiplas camadas de defesa. Para o sucesso desejado na implementação do Modelo Purdue, são estabelecidas diretrizes rigorosas. Por exemplo, os dispositivos alocados em determinada zona são autorizados a se comunicar entre si e com servidores na Zona Desmilitarizada (DMZ), mas

são proibidos de estabelecer comunicação com dispositivos na rede corporativa ou na Internet. Quando ocorre a transferência de dados de uma zona de segurança para outra, esses dados são submetidos a filtragem com permissões explícitas. Esta abordagem dificulta certas atividades, mas não impede que um atacante que já esteja localizado na rede, execute movimentação lateral e se espalhe pelo ambiente. Por estas razões, um novo modelo surge para mitigar esta lacuna de segurança. O modelo proposto é chamado de Zero Trust e é apresentado na seção a seguir.

5. TRABALHO E ARQUITETURA PROPOSTA

O presente trabalho tem como objetivo propor a utilização de técnicas de criptografia para garantir a segurança e autenticidade das comunicações entre Controladores Lógicos Programáveis (CLPs) em um sistema de Automação e Controle de Supervisão de Processos (SCADA). Para que a integridade da comunicação seja alcançada, deve-se observar alguns pilares:

- Integridade dos Dados:
  Integridade de dados se refere à garantia de que os dados não foram alterados de forma não autorizada, mantendo sua precisão e consistência ao longo do tempo. O uso de algoritmos de criptografia assimétrica é muito útil para verificar a integridade dos dados.
- Autenticação: Autenticação é o processo de verificar a identidade de um usuário, garantindo que ele seja quem afirma ser. A criptografia assimétrica pode ser usada para confirmar a identidade de entidades na rede.
- Confidencialidade: Confidencialidade refere-se à proteção dos dados contra acesso não autorizado, garantindo que apenas pessoas autorizadas possam visualizar ou acessar as informações. Caso um canal de comunicação seja comprometido para garantir a confidencialidade algum tipo de criptografia deve ser utilizado.
- Não-repúdio: Não-repúdio é a garantia de que uma parte não pode negar a autenticidade de uma transação ou comunicação realizada.

Além disso, é importante adotar uma abordagem abrangente de segurança que inclua medidas como controle de acesso, monitoramento de rede e detecção de intrusões para proteger contra ataques cibernéticos mais avançados. Para este artigo, tais medidas complementares de segurança não serão abordadas.

5.1 Arquitetura Proposta

A comunicação entre CLPs em sistemas de automação industrial requer a adoção de medidas que garantam a segurança das informações transmitidas. A arquitetura proposta permite o envio de dados de duas maneiras: Comunicação direta e Comunicação Protegida.

Comunicação direta A comunicação direta é empregada para transmissão em tempo real, onde não há viabilidade de aplicação de técnicas adicionais de proteção. Esses dados são enviados ao destino sem passar por processos de criptografia e decodificação, geralmente consistindo em informações não críticas.

Comunicação Protegida Já a comunicação protegida é destinada aos dados críticos do sistema. Dados críticos e não críticos são classificados de acordo com a planta industrial ao qual os CLPs estão alocados. Estes dados passam por todo o processo de proteção descritos neste artigo. Para isso, um conjunto de técnicas de segurança são implementadas.

A seguir, será apresentado um passo a passo desse processo, com foco na comunicação entre o CLP 1 e o CLP 3, validada pelo CLP 2 e tendo como base a arquitetura proposta na Figura 2.

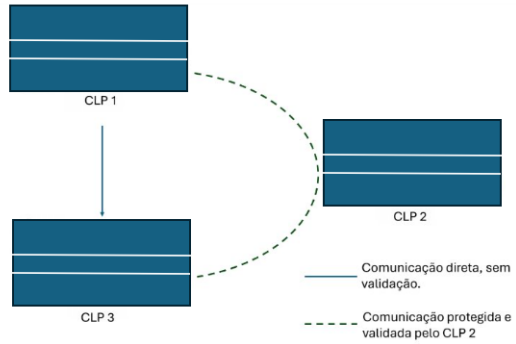

Figura 2. Arquitetura proposta – Comunicação segura entre CLPs.

(1) Preparação para a Comunicação: Antes de iniciar a troca de dados, o CLP 1 prepara-se identificando o tipo de informação a ser enviada e gerando um par de chaves (pública e privada) exclusivas para essa transmissão. Esta etapa utiliza a autenticação para reforçar a segurança da comunicação.
(2) Criptografia com a Chave Privada do CLP 1: O dado selecionado para envio é criptografado utilizando a chave privada do CLP 1. Esse passo assegura a autenticidade do dado, já que somente o CLP 1 possui acesso à sua chave privada. Nesta etapa, garante-se a integridade do dado.
(3) Criptografia Adicional com a Chave Pública do CLP 3: O texto cifrado resultante é então criptografado novamente, desta vez utilizando a chave pública do CLP 3. Essa medida garante que somente o destinatário pretendido, o CLP 3, possa decifrar e acessar o conteúdo da mensagem. Com o dado íntegro, esta etapa tem por objetivo garantir a confidencialidade da comunicação.
(4) Criptografia para validação pelo CLP 2: Para fortalecer ainda mais a segurança, o texto cifrado é criptografado mais uma vez, desta vez com a chave pública do CLP 2. Essa etapa é crucial, pois o CLP 3 só poderá decifrar e acessar a informação após validação realizada pelo CLP 2. Esta etapa, por sua vez, reforça novamente a autenticidade do dado.
(5) Decifragem pelo CLP 2: Ao receber o texto cifrado pelo CLP 1, o CLP 2 pode então decifrar a informação utilizando sua chave privada. Esta etapa garante que a mensagem está integra e autêntica.
(6) Decifragem pelo CLP 3: Em seguida, o CLP 3 ele utiliza sua chave privada para decifrar o dado do CLP 1, mas para chegar ao dado final utiliza a chave pública do CLP 1 para decifrar o texto original e, finalmente, acessar o dado enviado pelo CLP 1. Com

esta etapa o CLP 3 tem a certeza do dado que está recebendo. Portanto, o não-repúdio ao dado é garantido.

Esse processo garante a segurança e integridade das informações trocadas entre os CLPs, promovendo um ambiente confiável para as operações industriais. Ao seguir esses passos, os sistemas de automação podem proteger-se contra possíveis ameaças cibernéticas e manter a eficiência e precisão dos processos industriais.

5.2 Aplicação

Para demonstrar a aplicação da técnica proposta, será utilizada a arquitetura proposta na Figura 2, onde é apresentado um universo com três CLPs e um deles é utilizado como mecanismo de verificação da autenticidade e integridade do dado em trânsito. Os CLPs serão tratados como CLP 1, CLP 2 e CLP 3. O CLP 1 deseja se comunicar com o CLP 3. O CLP 2 validará a comunicação e a mensagem emitida pelo CLP 1 estará compreensível para o CLP 3 após esta etapa.

Os parâmetros para cada CLP podem ser observados na Tabela 1. É importante ressaltar que para o processo de criptografia, seguindo a sequência apresentada na seção 5, deve-se obedecer a seguinte regra: o tamanho da mensagem a ser criptografada deve ser menor que o valor de n. Caso haja a necessidade de criptografar um dado maior que n, deve ser adicionado na mensagem a ser criptografada o valor diferencial entre a mensagem e o n. Ao decifrar a mensagem, deverá ser somado a ela o valor que ultrapassou o tamanho de n. Desta forma, é possível compensar o dado que foi limitado pelo tamanho de n.

Tabela 1. Parâmetros para aplicação da metodologia.

CLP	p	q	n	$\phi(n)$	e	d
CLP1	3	11	33	20	7	3
CLP2	11	17	187	160	53	157
CLP3	7	17	119	96	29	53

Seguindo a metodologia proposta na seção 5.1, serão realizados os passos de criptografia para garantir a integridade, autenticidade, confidencialidade e não-repúdio dos dados. Os passos de 1 a 6 apresentados na seção 5.1 serão reproduzidos a seguir de modo a validar a metodologia proposta.

(1) Preparação para a Comunicação: Para esta etapa do processo, o CLP 1 estabelece o dado M a ser compartilhado. Para os fins de demonstração, será definido $M = 6$.

(2) Criptografia com a Chave Privada do CLP 1: Utilizando-se da chave privada d do CLP 1, é realizada a primeira criptografia. Esta etapa é crucial, pois garante que o dado foi de fato enviado pelo CLP 1, uma vez que somente ele conhece sua chave privada. A Equação (1) demonstra este processo.

$$C_1 = 6^3 \times mod(33) \tag{1}$$

Após calculado $C_1 = 18$, segue-se a lógica do passo 2, onde o dado criptografado com as informações privadas do CLP 1 será criptografado novamente com as informações públicas do CLP 2. Este passo tem por objetivo reforçar a segurança de que apenas o CLP 3 poderá ter acesso ao dado inicial.

(3) Criptografia Adicional com a Chave Pública do CLP 3:

Seguindo a mesma linha do passo 1, realiza-se a criptografia do dado $M_2 = C_1 = 18$. A Equação (2) descreve este passo.

$$C_2 = 18^{29} \times mod(119) \tag{2}$$

Como resultado da Equação (2) obtém-se $C_2 = 86$.

(4) Criptografia para validação pelo CLP 2:

De modo a aplicar uma camada extra de proteção à comunicação, o CLP 2 será utilizado como validador da comunicação entre os CLP's 1 e 3. Portanto, criptografa-se C_2 com as informações públicas do CLP 2, garantindo que o dado correto chegará ao CLP 3 apenas após a validação com as informações privadas que somente o CLP 2 conhece. A Equação (3) demonstra esta etapa do processo.

$$C_3 = 86^{53} \times mod(187) \tag{3}$$

Como resultado da Equação (3), é obtido $C_3 = 69$.

(5) Decifragem pelo CLP 2:

Tendo o CLP 2 recebido a solicitação para validar o dado enviado pelo CLP 1 ao CLP 3, inicia-se o processo de decifragem da mensagem. A (4) apresenta esta etapa.

$$M_2 = 69^{157} \times mod(187) \tag{4}$$

Como resultado da Equação (4), obtém-se $M_2 = 86$.

(6) Decifragem pelo CLP 3:

Nesta etapa o CLP 3 terá a possibilidade de decifrar o dado validado pelo CLP 2, uma vez que com as suas informações privadas e as informações públicas do CLP 1, poderá ter acesso ao dado inicial enviado pelo CLP 1. A Equação (5) apresenta este processo.

$$M_3 = 86^{53} \times mod(119) \tag{5}$$

A Equação(5) apresenta $M_3 = 18$. No entanto, este ainda não é o dado final. O dado final será alcançado através da Equação (6)

$$M_4 = 18^7 \times mod(33) \tag{6}$$

Com o retorno da Equação (6), é verificado que $M_4 = M = 6$, ou seja, a mensagem inicial enviada pelo CLP 1 foi, com sucesso, recebida pelo CLP 3 com todas as garantias de segurança validadas pelos processos de criptografia e validação.

6. RESULTADOS ESPERADOS

Espera-se com este estudo validar estratégias que possibilitem a implementação de conceitos de segurança Zero Trust na comunicação entre os ativos pertencentes à zona de operação do Modelo Purdue. Esta linha de pesquisa busca abrir caminhos no entendimento sobre a aplicabilidade e

eficácia da aplicação de conceitos de segurança Zero Trust em ambientes industriais em nível de processo.

Além disso, pretende-se avaliar outros algoritmos de criptografia para fins comparativos no que tange ao consumo recursos computacionais. Essa análise permitirá identificar as soluções mais adequadas em termos de custo computacional, garantindo que a implementação de uma camada de segurança cibernética não comprometa o funcionamento da planta.

Disclaimer: É sabido que o consumo de recursos computacionais para as validações de segurança propostas neste artigo é elevado quando utilizada a comunicação segura. Pelo fato de CLPs não possuírem alto poder de processamento, os próximos passos para esta pesquisa serão direcionados à aplicação de técnicas de criptografia com chaves simétricas. Tal solução requer menor poder de processamento e sua viabilidade poderá ser validada e comparada ao proposto neste artigo.

7. CONCLUSÃO

Neste artigo foram apresentadas as necessidades da industria quando se trata de digitalização. Entre as principais necessidades está a segurança dos ambientes industriais. Quando observado o mecanismo utilizado para proteção dos perímetros antes dos avanços tecnológicos e da digitalização, observa-se que as técnicas de segurança estão menos eficientes e podem permitir a presença de um atacante no ambiente sem a identificação pelas ferramentas de segurança. Com o objetivo de mitigar tais fragilidades, foi apresentado um modelo de segurança que busca sempre validar todas as comunicações dentro de uma planta. Para este artigo apresentou-se uma solução que objetiva levar conceitos de segurança Zero Trust ao nível de processo, ou seja, sempre validar as comunicações entre os ativos que estão no nível mais baixo do Modelo Purdue. Foram apresentadas técnicas de criptografia que possibilitam que tais comunicações alcancem sua autenticidade, integridade, confidencialidade e não-repúdio de dados. Uma sequência de ações foram apresentadas para que este objetivo seja alcançado. Observa-se, no entanto, que há limitações que precisam ser superadas para que as ações aqui apresentadas sejam factíveis. Por isso, trabalhos futuros serão conduzidos para comparar as principais técnicas de criptografia simétrica e assimétrica, de modo a apresentar quais delas possuem maior adaptabilidade ao cenário de CLPs em redes industriais.

REFERÊNCIAS

Ackerman, P. (2017). *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing.

Al Hasib, A. and Haque, A.A.M.M. (2008). A comparative study of the performance and security issues of aes and rsa cryptography. In *2008 third international conference on convergence and hybrid information technology*, volume 2, 505–510. IEEE.

Alsabbagh, W. and Langendoerfer, P. (2022). A remote attack tool against siemens s7-300 controllers: A practical report. In *Kommunikation und Bildverarbeitung in der Automation: Ausgewählte Beiträge der Jahreskolloquien KommA und BVAu 2020*, 3–21. Springer Berlin Heidelberg Berlin, Heidelberg.

Chiluvuri, N.T., Harshe, O.A., Patterson, C.D., and Baumann, W.T. (2015). Using heterogeneous computing to implement a trust isolated architecture for cyber-physical control systems. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 25–35.

do Nascimento, E.M. (2020). Applying zero trust principles to secure industrial control networks. In *Anais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 484–489. SBC.

Federal, G. (2023). Decreto nº 11.856. URL `https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289`. Acessado em: 15 Jan. 2024.

Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B., and Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50, 101660.

Jorstad, N.D. and Landgrave, T. (1997). Cryptographic algorithm metrics. In *20th National Information Systems Security Conference*, 1–38.

Lima, P.M., Alves, M.V., Carvalho, L.K., and Moreira, M.V. (2021). Security of cyber-physical systems: Design of a security supervisor to thwart attacks. *IEEE Transactions on Automation Science and Engineering*, 19(3), 2030–2041.

Lima, P.M., Carvalho, L.K., and Moreira, M.V. (2023). Ensuring confidentiality of cyber-physical systems using event-based cryptography. *Information Sciences*, 621, 119–135.

Lima, P.M., da Silva, C.K., de Farias, C.M., Carvalho, L.K., and Moreira, M.V. (2022). Event-based cryptography for automation networks of cyber-physical systems using the stream cipher ChaCha20. *IFAC-PapersOnLine*, 55(28), 58–65. 16th IFAC Workshop on Discrete Event Systems WODES 2022.

Mitsarakis, K. (2023). Contemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures.

Munirathinam, S. (2020). Industry 4.0: Industrial Internet of Things (IIOT). 117, 129–164.

Oliveira, S., B. Leal, A., Teixeira, M., and K. Lopes, Y. (2023). A classification of cybersecurity strategies in the context of discrete event systems. *Annual reviews in Control*.

Patil, P., Narayankar, P., Narayan, D., and Meena, S.M. (2016). A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish. *Procedia Computer Science*, 78, 617–624.

Peterson, E. (2021). Achieving visibility and control in ot systems: Remote maintenance, securing remote access, and the zero-trust approach.

Premnath, A.P., Jo, J.Y., and Kim, Y. (2014). Application of ntru cryptographic algorithm for scada security. In *2014 11th international conference on information technology: new generations*, 341–346. IEEE.

Stafford, V. (2020). Zero trust architecture. *NIST special publication*, 800, 207.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., and Lightman, S. (2022). Guide to operational technology (ot) security. *National Institute of Standards and Technology: Gaithersburg, MD, USA*.