Manual de Política de Segurança Cibernética

MU214004 Rev. A

28 de setembro de 2023

www.altus.com.br

Conforme o Código de Defesa do Consumidor vigente no Brasil, informamos, a seguir, aos clientes que utilizam nossos produtos, aspectos relacionados com a segurança de pessoas e instalações.

Os equipamentos de automação industrial fabricados pela Altus são robustos e confiáveis devido ao rígido controle de qualidade a que são submetidos. No entanto, equipamentos eletrônicos de controle industrial (controladores programáveis, comandos numéricos, etc.) podem causar danos às máquinas ou processos por eles controlados em caso de defeito em seus componentes e/ou de erros de programação ou instalação, podendo inclusive colocar em risco vidas humanas.

O usuário deve analisar as possíveis consequências destes defeitos e providenciar instalações adicionais externas de segurança que, em caso de necessidade, sirvam para preservar a segurança do sistema, principalmente nos casos da instalação inicial e de testes.

Os equipamentos fabricados pela Altus não trazem riscos ambientais diretos, não emitindo nenhum tipo de poluente durante sua utilização. No entanto, no que se refere ao descarte dos equipamentos, é importante salientar que quaisquer componentes eletrônicos incorporados em produtos contêm materiais nocivos à natureza quando descartados de forma inadequada. Recomenda-se, portanto, que quando da inutilização deste tipo de produto, o mesmo seja encaminhado para usinas de reciclagem que deem o devido tratamento para os resíduos.

É imprescindível a leitura completa dos manuais e/ou características técnicas do produto antes da instalação ou utilização do mesmo.

Os exemplos e figuras deste documento são apresentados apenas para fins ilustrativos. Devido às possíveis atualizações e melhorias que os produtos possam incorrer, a Altus não assume a responsabilidade pelo uso destes exemplos e figuras em aplicações reais. Os mesmos devem ser utilizados apenas para auxiliar na familiarização e treinamento do usuário com os produtos e suas características.

A Altus garante os seus equipamentos conforme descrito nas Condições Gerais de Fornecimento, anexada às propostas comerciais.

A Altus garante que seus equipamentos funcionam de acordo com as descrições contidas explicitamente em seus manuais e/ou características técnicas, não garantindo a satisfação de algum tipo particular de aplicação dos equipamentos.

A Altus desconsiderará qualquer outra garantia, direta ou implícita, principalmente quando se tratar de fornecimento de terceiros.

Os pedidos de informações adicionais sobre o fornecimento e/ou características dos equipamentos e serviços Altus devem ser feitos por escrito. A Altus não se responsabiliza por informações fornecidas sobre seus equipamentos sem registro formal.

Alguns produtos utilizam tecnologia EtherCAT (www.ethercat.org).

DIREITOS AUTORAIS

NOTIFICAÇÃO DE USO DE SOFTWARE ABERTO

Para obter o código fonte de componentes de software contidos neste produto que estejam sob licença GPL, LGPL, MPL, entre outras, favor entrar em contato através do e-mail opensource@altus.com.br. Adicionalmente ao código fonte, todos os termos da licença, condições de garantia e informações sobre direitos autorais podem ser disponibilizadas sob requisição.

Sumário

1. Introdução

A segurança cibernética desempenha um papel crucial no ambiente de automação industrial. Com o aumento alarmante de incidentes de segurança em fábricas, plantas e outras aplicações automatizadas, medidas efetivas para proteger esses sistemas tornaram-se imperativas. Este documento tem como propósito apresentar e justificar as medidas de cibersegurança implementadas nos produtos da Altus, notadamente o MasterTool, ambiente de desenvolvimento para controladores lógicos programáveis (CLPs), e as séries Nexto, Nexto Xpress e Hadron Xtorm.

Instituições governamentais, como a ICS-Cert e o Departamento Federal Alemão para Segurança da Informação (BSI), têm acompanhado de perto o aumento desses incidentes. Diante desse cenário, a elaboração de metodologias que assegurem a integridade e proteção dos sistemas tornou-se uma necessidade urgente. Um marco importante nesse sentido é a diretriz de padrão internacional IEC 62443, inicialmente publicada pelo comitê de segurança de sistemas de controle e automação industrial (ISA99) da Sociedade de Automação Industrial (ISA) e frequentemente referida como norma ISA/IEC 62443.

O escopo das medidas de cibersegurança abrange a proteção de vários aspectos, incluindo a disponibilidade das funcionalidades do controlador, a funcionalidade da aplicação, a confidencialidade do código fonte e da aplicação, a integridade das funções de aplicação, do sistema de desenvolvimento e dos componentes empregados, além da autenticidade do controlador e seus dados.

Neste contexto, este documento destaca as estratégias de cibersegurança adotadas pela Altus e seus produtos, visando proteger os clientes e suas operações industriais de ameaças cada vez mais sofisticadas e persistentes. O uso da norma ISA/IEC 62443 como referência sólida reflete o compromisso com a excelência na proteção do ambiente de automação industrial contra potenciais riscos cibernéticos.

2. Termos e Definições

2.1. Vulnerabilidades

Sistemas de automação podem sofrer ataques em diversos pontos de sua estrutura:

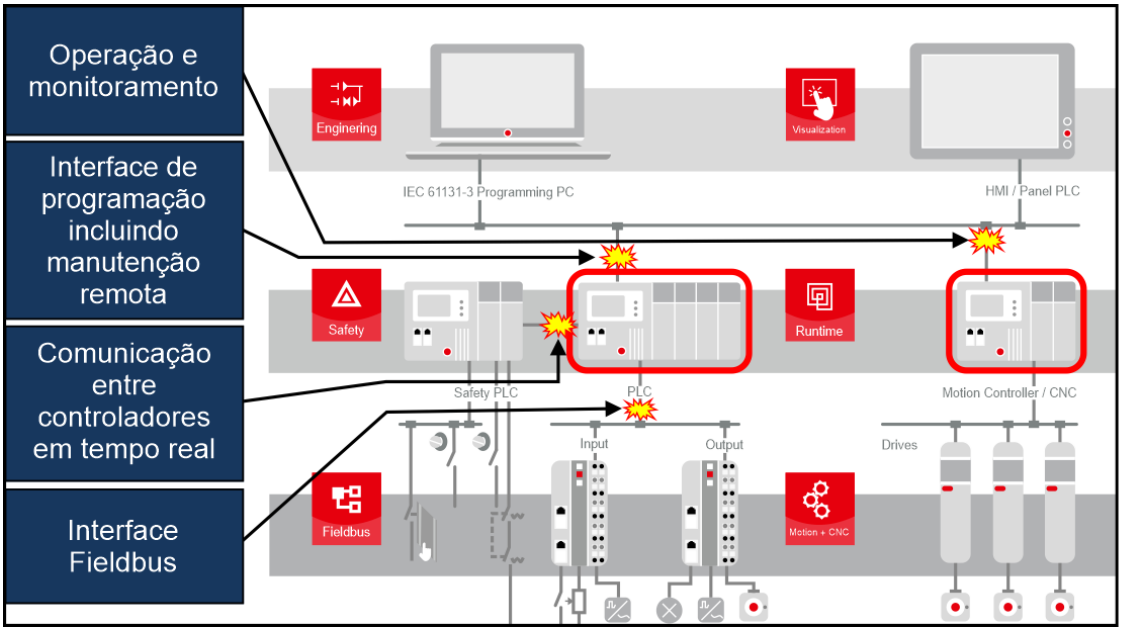

Figura 1: Possíveis vulnerabilidades de um típico sistema de automação.

2.2. Ameaça

Se refere a um conjunto de circunstâncias e sequência de eventos associados, com potencial para afetar negativamente as operações (incluindo missão, funções, imagem ou reputação), ativos, sistemas de controle ou indivíduos, através de acesso não autorizado, destruição, divulgação, modificação de dados e/ou negação de serviço. Em suma, é a possibilidade de ocorrência de eventos maliciosos ou indesejados que comprometam a integridade, confidencialidade ou disponibilidade dos recursos e informações em um ambiente de automação industrial.

2.3. Níveis de Proteção

Para atender a essa ampla abordagem, a norma ISA/IEC 62443 estabelece quatro principais níveis de proteção em escala crescente, cada um adaptado para enfrentar diferentes ameaças:

- Nível 1: Ameaças ocasionais e acidentais;
  Exemplos: Falha no disco rígido, erro operacional
- Nível 2: Ameaças intencionais por vias simples;
  Exemplo: Senha adivinhada com sucesso
- Nível 3: Ameaças intencionais por vias elaboradas;
  Exemplo: Uso de ferramental hacker
- Nível 4: Ameaças intencionais por vias elaboradas e recursos vastos.
  Exemplos: Desenvolvimento especializado, conhecimento da aplicação ou corrupção de funcionários

2.4. Controlador Programável

Um computador industrial usado na automação de sistema, que pode também ser chamado de CP ou apenas Controlador. Estes equipamentos podem ser alvos de ataques por suas características próprias e também dependem de uma programação projetada para a aplicação específica, que pode ser uma fonte de vulnerabilidades. Os controladores da Altus, tratados neste documento, são os pertencentes às linhas Nexto, Nexto Xpress ou Hadron Xtorm.

2.5. MasterTool

O MasterTool IEC XE é uma ferramenta completa para programação, depuração, configuração e simulação das aplicações do usuário. O software é baseado no conceito de ferramenta integrada, provendo flexibilidade e facilidade de uso permitindo aos usuários a programação em seis linguagens definidas pela norma IEC 61131-3: Texto Estruturado (ST), Sequenciamento Gráfico de Funções (SFC), Diagrama de Blocos Funcionais (FBD), Diagrama Ladder (LD) e Gráfico Contínuo de Funções (CFC).

2.6. Ambiente protegido

Todo sistema e equipamento precisa ser acessado durante sua instalação, operação e manutenção, porém o seu acesso não pode ser irrestrito para evitar falhas de operação e danos ao produto, intencional ou não. Para isso, é necessário que o sistema seja dividido em subsistemas para que cada subsistema tenha seu acesso controlado e apenas agentes autorizados os acessem, protegendo o ambiente.

3. Responsabilidades de diferentes agentes na segurança de sistemas industriais

Na configuração de aplicações de controle industrial, várias partes ativas e fornecedores estão envolvidos: os fornecedores de componentes de software e hardware, o integrador de sistemas ou construtor das aplicações de controle industrial e o operador. Como a segurança da tecnologia da informação é uma tarefa abrangente, todas as partes mencionadas devem realizar um esforço significativo para proteger a aplicação contra ataques.

- Fornecedor do Software:
  - analisar ativos e ameaças;
  - fornecer medidas de segurança aprovadas;
  - fornecer documentação técnica;
- Fornecedor de Componentes de Automação:
  - analisar ativos e ameaças;
  - implementar medidas de segurança de software e hardware;
  - fornecer documentação técnica;
- Integrador de Sistemas e Fabricante de Maquinário:
  - analisar ativos e ameaças;
  - implementar medidas de segurança de software e hardware;
  - implementar medidas de segurança de sistema;
  - fornecer documentação técnica;
- Operador/Gerente da Planta:
  - analisar ativos e ameaças;
  - implementar medidas de segurança de software, hardware e sistema;
  - testar, auditar e certificar sistema;
  - treinar funcionários;

4. Proteções gerais para Sistemas de Automação Industrial

Primeiramente, todas as medidas de segurança comumente conhecidas para computadores devem ser aplicadas em redes com equipamentos de automação industrial, tais como:

- Proteção contra vírus
- Senhas fortes que são regularmente alteradas
- Proteção de firewall
- Uso de túneis VPN para conexões entre redes
- Cautela ao lidar com dispositivos de armazenamento removíveis, como pen drives USB

Além disso, é obrigatório ter um gerenciamento de usuários e permissões bem definido para o acesso aos controladores e suas redes interconectadas.

4.1. Uso em um ambiente protegido

Localizar o controlador em um ambiente protegido é absolutamente necessário para evitar acessos acidentais ou intencionais ao controlador ou sua aplicação, que é executada para o funcionamento da máquina ou instalação.

Esse ambiente protegido pode ser, por exemplo, dentro de:

- Armários de controle elétrico trancados sem acesso de comunicação externa,
- Uma rede intranet com direitos de usuário bem definidos sem acesso externo, ou
- Uma rede com acesso à internet somente por meio de um firewall bem configurado via um túnel VPN.

Obviamente, o grau de proteção diminui ao longo desta lista.

Para criar um ambiente protegido como esse, várias regras devem ser seguidas:

- Manter a rede confiável o menor possível e independente de outras redes.
- Proteger a comunicação cruzada entre controladores e a comunicação entre controladores e dispositivos de campo por meio de protocolos de comunicação padrão (sistemas fieldbus) por medidas apropriadas.
- Bloquear essas redes e separá-las estritamente de acessos comuns.
- Usar sistemas de barramento de campo apenas em ambientes protegidos, pois eles não estão protegidos por medidas adicionais, como criptografia. O acesso físico ou de dados aberto aos sistemas de barramento de campo e seus componentes é um sério risco de segurança.

4.2. Usuários atentos à segurança

Usuários com conscientização sobre segurança desempenham um papel fundamental na proteção cibernética, visto que a maioria dos incidentes de segurança relatados ocorre sem intenção, devido a erros de manipulação ou de dispositivos. Portanto, tanto os fabricantes de máquinas e instalações quanto os operadores precisam estar cientes das possíveis ameaças e das medidas infraestruturais necessárias para evitá-las. Para alcançar esse objetivo, é recomendável aos usuários participar de treinamentos especiais ministrados por especialistas em segurança, seja dentro da empresa ou por profissionais externos. Esses treinamentos visam capacitar os usuários a adotarem práticas adequadas de segurança e a compreenderem como aplicar as medidas de proteção adequadas no desenvolvimento e operação dos controladores industriais.

5. Medidas de Segurança Presentes no MasterTool

Este capítulo informa sobre os recursos de segurança cibernética no programa MasterTool, informando sua importância e como encontrá-las nos manuais do produto. Abaixo dos títulos dos subcapítulos, é informado o requisito de componente (RC) da norma IEC 62443-4-2:2019-02 à qual ela diz respeito.

5.1. Usuário administrador nos níveis de projeto

RC 1.1 da norma IEC 62443-4-2

MasterTool oferece a capacidade de proteção de leitura/gravação de objetos individuais no projeto com uma administração de usuário. Essa proteção pode ser definida para comandos de menu, bem como para tipos de objeto específicos (por exemplo, criação de tarefas, POUs, métodos, GVLs etc.) ou objetos existentes no projeto (como configurações do projeto ou POUs ou tarefas dedicadas).

Através da administração de usuário, é possível limitar a gama de funcionalidades de uma forma mais profunda. Permitindo direito de acesso adaptados a necessidades de segurança específicas, protegendo assim a confidencialidade da propriedade intelectual, bem como a integridade do código do aplicativo.

O passo a passo para utilização destas funções do MasterTool se encontra no Capítulo “Gerenciamento de Usuários e Direitos de Acesso” do Manual do MasterTool.

5.2. Acesso ao Sistema de Runtime com gerenciamento de permissões/Autenticações

RC 1.4 da norma IEC 62443-4-2

Existem diferentes fases de uma aplicação industrial: desde o início do desenvolvimento do código-fonte para seu comissionamento até a produção com a máquina ou planta e sua manutenção. Essas fases são normalmente operadas por diferentes técnicos com níveis de qualificação adequados.

Ao considerar esses níveis de qualificação, bem como as ameaças de um possível uso além da tarefa ou competência, faz sentido limitar o uso para determinados grupos de usuários.

O MasterTool suporta autenticação e gerenciamento de permissão para um usuário ou grupo de usuários administradores. Dependendo da política de segurança do sistema de runtime, o gerenciamento de usuários pode ser aplicado por padrão ou não. Caso não seja, todos são membros do grupo de administradores e têm direitos ilimitados no controlador até que o gerenciamento de usuários seja ativado. Ao utilizá-lo é necessário que sua primeira ativação seja durante o primeiro login, especificando um usuário administrador.

Assim que pelo menos um novo usuário é adicionado, todos os usuários devem se autenticar com seus nomes de usuário e senhas para cada conexão online com o controlador. As senhas são transferidas criptografadas (por padrão, usando criptografia assimétrica) e armazenadas codificadas como hashes de criptografía no sistema de runtime.

Esta medida reduz a ameaça de acesso acidental ou pretendido ao controlador em execução, o que poderia afetar a disponibilidade ou a integridade da aplicação compilada executada em o controlador.

O Login Seguro no controlador programável provê uma maneira de proteger a aplicação do usuário de qualquer acesso não autorizado. Habilitando esta característica, a UCP da Série Nexto irá solicitar uma senha de usuário antes de executar quaisquer comandos entre MasterTool IEC XE e a UCP, como parar e programar a aplicação ou forçar pontos de saída em um módulo.

O passo a passo para utilização destas funções do MasterTool se encontra no Capítulo “Gerenciamento de Usuários e Direitos de Acesso” do Manual do MasterTool.

5.3. Configuração de conjuntos de símbolos via gerenciamento de usuários

RC 2.1 da norma IEC 62443-4-2

Dentro da SymbolConfiguration, pode-se criar subconjuntos de todos os símbolos definidos (symbolSets). Com um gerenciamento de usuário ativado, esses conjuntos de símbolos podem ser atribuídos a usuários dedicados para visibilidade e determinação dos direitos de acesso de escrita/leitura. Protegendo a confidencialidade dos dados que são trocados com os clientes conectados.

O passo a passo para utilização destas funções do Mastertool se encontra no Capítulo “Gerenciamento de Usuários e Direitos de Acesso” do Manual do Mastertool.

5.4. Gerenciamento de Usuários da Visualização Integrada

RC 2.1 da norma IEC 62443-4-2

A visualização integrada do MasterTool permite uma operação direta do controlador e da aplicação. Recomenda-se fortemente separar a operação em diferentes partes ou telas de acordo com seu nível de influência funcional e de segurança. O MasterTool fornece a capacidade de proteger elementos de visualização individuais, bem como telas de visualização inteiras do projeto por meio de um gerenciamento de usuário de visualização especial.

Este gerenciamento de usuários permite a limitação do alcance de funcionalidade para determinados operadores. Modos de operação de segurança crítica, como a exportação de dados de produção, o processo de inicialização e parada da planta, e o acesso a funções de serviço dedicadas, pode ser restrito a operadores com permissões explicitamente atribuídas, garantindo sigilo da propriedade intelectual, bem como a disponibilidade e confiabilidade da máquina ou processo da planta.

O passo a passo para utilização destas funções do MasterTool se encontra no Capítulo "Gerenciamento de Usuários e Direitos de Acesso" do Manual do MasterTool.

5.5. Encriptação da Comunicação com WebVisu

RC 3.1 da norma IEC 62443-4-2

Para prevenir a interceptação da comunicação entre o controlador e o navegador web no computador, é possível utilizar uma conexão com encriptação HTTPS. Esta pode ser configurada com certificado auto-assinado ou com um gerado por uma autoridade certificadora CA. Na tela de Device Security Settings, o uso de HTTPS pode ser configurado como obrigatório, ou permitir também conexões HTTP.

5.6. Servidor OPC UA Seguro

RC 3.1 da norma IEC 62443-4-2

OPC UA é um protocolo de comunicação industrial para interoperabilidade desenvolvido pela OPC Foundation. O MasterTool é equipado com uma funcionalidade de servidor OPC UA para fornecer acesso ao controlador e sua aplicação. Várias medidas de segurança são fornecidas como: um servidor OPC UA operante com uma comunicação criptografada baseada em certificados X.509 e atuando com acesso a um conjunto de símbolos específico ao usuário, garantindo uma maior confidencialidade aos dados que são trocados com os clientes conectados

5.6.1. Servidor OPC UA: Gerenciamento de usuários disponível

RC 2.1 da norma IEC 62443-4-2

Com um gerenciamento de usuários ativado para o OPC UA, o estabelecimento de uma sessão é restrito a usuários específicos. Essa medida reduz a ameaça de acesso acidental ou intencional ao Servidor OPC UA do MasterTool.

5.6.2. Servidor OPC UA: Suporte à comunicação baseada em certificados X.509

RC 3.1 da norma IEC 62443-4-2

Uma das funcionalidades do Servidor OPC UA é operar com uma comunicação criptografada baseada em certificados X.509. Os diferentes perfis de segurança são definidos pela Fundação OPC.

Dependendo do perfil, isso protege a integridade (apenas para perfis assinados) ou a integridade e confidencialidade (para perfis assinados e criptografados) dos dados trocados com os clientes conectados.

Essa medida protege a confidencialidade dos dados trocados com os clientes conectados.

5.7. Assinatura de bibliotecas IEC Compiladas

RC 4.1 da norma IEC 62443-4-2

Uma biblioteca IEC pode ser assinada com um certificado X.509 se for salva como uma biblioteca compilada. Enquanto as bibliotecas compiladas garantem a proteção do código-fonte, a assinatura permite uma verificação da autenticidade da mesma.

O status das assinaturas das bibliotecas pode ser observado pelos ícones no "Gerenciar de Biblioteca" ou pelos Detalhes no menu de "Adicionar a biblioteca".

5.8. Encriptação do código fonte da aplicação

RC 4.1 da norma IEC 62443-4-2

O código-fonte da aplicação contém as informações detalhadas sobre o sistema abordado e, portanto, a propriedade intelectual de seu fabricante. Dessa forma, a proteção do código-fonte da aplicação é prioritário na presença de informações confidenciais.

O MasterTool permite para todo o projeto a criptografia por senhas ou chaves de segurança físicas tipo USB Dongle. Descrito na norma IEC 62443-4-2 em "Requisito de componente 4.3", a criptografia de senha é baseada nos métodos AES (Advanced Encryption Standard), já as soluções embasadas em chaves de seguranças são fornecidas pela empresa WIBU Systems. A utilização de senhas tem como principal vantagem dispensar um hardware adicional, porém, a utilização das chaves tornam o nível de proteção muito maior, uma vez que uma senha pode ser hackeada ou publicada.

Possibilita-se também o vínculo de várias chaves diferentes ao mesmo tempo a um projeto, limitando o acesso do código-fonte ao número de chaves e minimizando o risco à privação de acesso ao código, caso alguma chave seja destruída ou perdida. Para esse fim, recomenda-se a associação de uma chave a mais do que o que seria necessário.

O código-fonte também pode ser protegido usando certificados X.509. Nesse cenário, o código-fonte será criptografado simetricamente (algoritmo AES). A chave simétrica será então criptografada assimétricamente (algoritmo RSA) usando a chave pública de cada usuário que compartilha o código-fonte. Opcionalmente, o código-fonte também pode ser assinado digitalmente usando a chave privada associada ao certificado X.509 do usuário atual. A assinatura será salva lado a lado com o código-fonte em um arquivo com o extensão ".p7s" seguindo o formato PKCS #7 para assinaturas digitais.

Caso não seja possível utilizar criptografia, é estabelecido que o arquivo do projeto é salvo em um formato proprietário e sua integridade será verificada cada vez que o projeto é carregado, protegendo o sigilo da propriedade intelectual.

6. Medidas de Segurança dos CLPs Altus

Os CLPs da Altus são equipados com diferentes dispositivos de segurança para evitar vulnerabilidades durante sua operação. Algumas medidas são presentes em apenas alguns modelos de controladores, então sempre cheque no manual específico do produto pelo recurso de segurança desejado. Abaixo dos títulos dos subcapítulos, é informado o requisito de componente (RC) ou o Requisito de dispositivo de rede (RDR) da norma IEC 62443-4-2:2019-02 à qual ela diz respeito.

6.1. Criptografia para a comunicação OPC UA

RC 3.1 da norma IEC 62443-4-2

Se desejado, o usuário pode configurar criptografia para a comunicação OPC UA usando o perfil Basic256 SHA256, para obter uma conexão segura.

Para configurar a criptografia num servidor OPC UA deve-se criar um certificado para o mesmo e o passo a passo pode ser encontrado no Capítulo “Configuração”, na seção “Configuração de Protocolos - OPC UA Servidor” do Manual de Utilização UCP Série Nexto.

6.2. Firewall

RDR 5.2 da norma IEC 62443-4-2

O Firewall foi desenvolvido para aumentar a segurança do dispositivo durante a sua utilização. A principal função do Firewall é realizar um filtro sobre os pacotes de dados que chegam e que saem do dispositivo. O filtro implementado utiliza informações de cada pacote de dados para decidir se aquele pacote é permitido ou não. Os principais parâmetros utilizados são as interfaces de entrada/saída, a porta, o protocolo da camada de transporte e os endereços de origem e destino.

O passo a passo para utilização desta função se encontra no Capítulo “Configuração”, na seção “Firewall” do Manual de Utilização UCP Série Nexto ou Nexto Xpress.

6.3. VPN

RDR 5.3 da norma IEC 62443-4-2

VPN (Virtual Private Network) é uma sigla para Rede Virtual Privada, utilizada para navegar em redes não seguras, trafegando dados importantes ou, simplesmente, realizando o acesso à internet com um nível elevado de privacidade. A rede virtual da VPN pode ser compreendida como um túnel no qual as informações trafegam de forma segura, protegidas por certificados e chaves de segurança. O OpenVPN é um serviço do tipo open source, ou seja, gratuito para ser utilizado e distribuído, e com o seu código fonte aberto para que sejam realizadas modificações, caso sejam necessárias. O principal objetivo da VPN é realizar uma comunicação de forma segura através de uma rede não segura. Para que isso seja possível, é utilizada a encriptação dos dados com base em certificados e chaves gerados utilizando o TLS, Transport Layer Security, um protocolo que realiza encriptações de 256 bits, uma das mais seguras.

O passo a passo para utilização desta função se encontra no Capítulo “Configuração”, na seção “OpenVPN” do Manual de Utilização UCP Série Nexto ou Nexto Xpress. No apêndice do mesmo documento, encontra-se a seção sobre “Gerenciamento de Certificados e Chaves TLS” que trata da geração e segurança dos certificados.

6.4. Proteção contra ataques tipo flood

RC 7.1 da norma IEC 62443-4-2

O módulo NX5000 (ethernet) é equipado com uma proteção contra ataques tipo flood. Esse recurso essencial de segurança é projetado para detectar e mitigar efetivamente ataques de inundação, nos quais uma grande quantidade de dados é enviada simultaneamente para sobrecarregar o sistema e causar indisponibilidade ou interrupção do serviço.

6.5. Possíveis fontes de riscos

Conectar o dispositivo à internet sem a configuração adequada de Firewall e VPN apresenta grandes riscos. A porta Host USB presente nos controladores de algumas séries permite ampliar as funcionalidades do controlador utilizando diversos tipos de dongles USB, incluindo modems com chip SIM e adaptadores WiFi. Para dispositivos em bridge ou roteadores com acesso externo ativado (encaminhamento de porta), uma vez conectado à Internet, qualquer pessoa que conheça o endereço IP do modem poderá acessar o controlador remotamente. Portanto, por motivos de segurança, é extremamente importante e recomendado configurar os Direitos do Usuário no controlador para restringir as operações online do MasterTool IEC XE com

login e senha. Por meio da página Web de gerenciamento, pode-se, inclusive, parar o controlador, o que é um risco para a segurança não apenas cibernética, mas também física dos funcionários e ativos.

6.6. Portas TCP/UDP Reservadas

As seguintes portas TCP/UDP das interfaces Ethernet, tanto locais quanto remotas, são tipicamente utilizadas por serviços da UCP (dependem da disponibilidade conforme manual do CP) e, portanto, são reservadas e não devem ser utilizadas pelo usuário.

Serviço	TCP	UDP
Página Web de Sistema	80	-
SNTP	-	123
SNMP	-	161
MODBUS TCP	502*	-
MasterTool MT8500	1217*	1740:1743
SQL Server	1433	-
MQTT	1883* / 8883*	-
EtherNet/IP	44818	2222
IEC 60870-5-104	2404*	-
OPC UA	4840	-
WEBVISU	8080	-
CODESYS ARTI	11740	-
PROFINET	-	34964

Tabela 1: Portas TCP/UDP reservadas

* Porta padrão, mas que pode ser alterada pelo usuário.

7. Conclusão

A segurança de sistemas de controle é um aspecto de extrema importância em um cenário onde a automação industrial está cada vez mais interconectada e digitalizada. Os incidentes de segurança têm aumentado significativamente, e isso exige que integradores e usuários estejam sempre vigilantes e proativos na observação e mitigação desses riscos.

Embora seja verdade que a segurança cibernética nunca pode ser garantida a 100%, é essencial compreender que a adoção de medidas de segurança e cuidados adequados pode elevar significativamente o nível de proteção para uma aplicação específica. A conscientização sobre as possíveis ameaças e a implementação de medidas preventivas podem criar uma barreira sólida contra ameaças potenciais.

Portanto, a colaboração entre fornecedores, integradores, operadores e usuários é fundamental para promover uma cultura de segurança robusta e eficiente. Ao investir em treinamento e capacitação, bem como na adoção de tecnologias de segurança adequadas, é possível mitigar riscos significativos e garantir a resiliência dos sistemas de controle em ambientes industriais.

Neste ambiente em constante evolução, é crucial reconhecer que a segurança é um esforço contínuo. Devemos permanecer atentos às últimas tendências e desenvolvimentos em segurança cibernética, atualizando e aprimorando regularmente nossas práticas e protocolos de segurança. Dessa forma, podemos enfrentar os desafios de segurança em um mundo cada vez mais digital, protegendo nossas operações e garantindo um ambiente de automação industrial mais seguro e confiável.