SISTEMAS DE CONTROLE INDUSTRIAL

Índice

Lista de figuras

1.0 ESCOPO

Esta norma técnica contém recomendações de prevenção de perdas para sistemas de controle industrial (SCIs) e utiliza a abordagem sistêmica para avaliar SCIs em toda a operação, inclusive suas redes de comunicação e riscos cibernéticos. O objetivo deste documento é fornecer soluções de redução de risco do ponto de vista de proteção patrimonial e continuidade do negócio.

Para as finalidades deste documento, SCI é definido como a combinação de hardware e software que fornece controle, proteção e monitoramento de processos, produção, fabricação e atividades relacionadas em instalações industriais e não industriais. A lista a seguir, que não inclui todas as possibilidades, oferece exemplos de ativos de hardware que podem ser conectados à rede do SCI:

- Sistema de supervisão e aquisição de dados (SCADA)
- Sistema digital de controle distribuído (SDCD), inclusive historiador
- Controlador lógico programável (CLP)
- Controlador de automação programável (CAP)
- Gateway de dispositivo externo
- Unidade terminal remota (UTR)
- Dispositivos de rede, inclusive comutadores, firewalls, roteadores etc.
- Dispositivos de campo inteligentes (ex., medidores, válvulas, relés e transmissores de processos inteligentes)
- Barramento de instrumentos
- Interface homem-máquina (IHM)
- Estação de trabalho de engenharia
- Painéis de controle industrial, incluindo gabinetes de equipamentos e instrumentação, gabinetes de entrada/saída (I/O) etc.
- Sistema de automação/gestão predial
- Dispositivos inteligentes ou Internet das Coisas Industrial (IIoT)

Esta norma técnica fornece orientações gerais sobre SCIs. Se houver normas técnicas mais detalhadas para equipamentos ou processos específicos, elas prevalecerão sobre as orientações apresentadas neste documento.

Esta norma técnica não inclui:

- Detalhamento de projeto ou operação de equipamentos de SCI ou comunicações/redes
- Desempenho, compatibilidade ou funcionalidade de softwares
- Projeto, operação, inspeção, teste e manutenção de sistemas instrumentados de segurança (consulte a Norma Técnica 7-45, *Safety Controls, Alarms, and Interlocks*, da FM)
- Sistemas de tecnologia da informação utilizados em negócios em geral (ex., sistemas destinados a envio e recebimento de e-mails e sistemas com acesso à Internet)

1.1 Risco

Se o SCI não for devidamente gerenciado e mantido, pequenos problemas poderão se transformar em falhas graves e resultar em perda de produção e/ou danos patrimoniais potencialmente significativos. Muitos fatores podem contribuir para a falha do sistema de controle, incluindo atos cibernéticos com o objetivo de causar interrupções e a falta de ações de resposta a incidentes e recuperação após um incidente cibernético.

1.2 Mudanças

Julho de 2024. Revisão intermediária. Foram feitas alterações editoriais.

2.0 RECOMENDAÇÕES PARA PREVENÇÃO DE PERDAS

2.1 Introdução

Cada SCI tem um funcionamento diferente, dependendo da indústria em que é utilizado e, consequentemente, não existem dois SCIs iguais. Os SCIs são sistemas complexos de painéis de controle, solucionadores lógicos, motores, bombas, acionadores, equipamentos sensores e de monitoramento etc., todos conectados por redes de comunicação.

É essencial que a equipe responsável pelo SCI geral da unidade tenha uma ótima compreensão do sistema como um todo, dos requisitos operacionais, das necessidades de proteção, das redes de comunicação e das necessidades de software a fim de identificar coletivamente riscos e exposições relacionados ao SCI.

2.2 Construção e localização

2.2.1 Tenha salas de controle de processo e salas de equipamentos importantes associadas fora de áreas expostas a efeitos de riscos de explosão. Se não for possível, providencie construção resistente a pressão projetada de acordo com a Norma 1-44, *Damage-Limiting Construction*, da FM, considerando que a sobrepressão será aplicada sobre a superfície externa da sala de controle. Para as janelas, é recomendado o vidro aramado em conformidade com a ANSI Z97.1 (ASTM E1886 e E1996 ou FBC TAS 201 e 203 são alternativas aceitáveis) para resistência a impactos e com a ASTM E1300 para a sobrepressão exigida.

2.2.2 As salas de controle de processo e salas de equipamentos associadas não devem estar expostas a danos causados por líquidos igníferos ou corrosivos, vapores inflamáveis ou equipamentos mecânicos, como pontes rolantes.

2.2.3 Para salas de controle de processo elevadas e salas de equipamentos associadas que estejam expostas a riscos de incêndio, providencie revestimento à prova de fogo para o aço de suporte estrutural adequado à exposição (mínimo de uma hora).

2.2.4 Construa salas de controle de processo, centros de controle e salas de equipamentos de instrumentação de controle industrial associadas (ou seja, salas de entrada/saída) e/ou painéis de controle industrial com materiais incombustíveis. Esses itens incluem, entre outros, forros falsos, pisos elevados, divisórias, mobílias, materiais de isolamento de tubulações e ar condicionado e filtros de ar condicionado.

Se forem utilizados materiais plásticos, providencie materiais certificados pela FM Approvals ou cujas especificações sejam testadas apropriadamente utilizando as diretrizes a seguir:

A. Norma de aprovação da FM Approvals 4882, *Class 1 Interior Wall and Ceiling Materials or Systems for Smoke Sensitive Occupancies*

B. Norma de aprovação da FM Approvals 4884, *Panels Used in Data Processing Center Hot and Cold Aisle Containment Systems*

C. Norma de aprovação da ANSI/FM Approvals 4910, *Cleanroom Materials Flammability Test Protocol*

2.2.5 Instale uma separação com resistência ao fogo de no mínimo uma hora entre as salas de controle de processo e as áreas adjacentes, inclusive salas de equipamentos e salas de painéis de distribuição de baixa tensão. Essa recomendação não se aplica a equipamentos independentes localizados fora da sala de controle de processo.

2.2.6 Onde houver sistemas de controle de processo redundantes, instale os controles, equipamentos e cabeamento de cada sistema em áreas separadas, com resistência ao fogo.

2.2.7 Providencie áreas separadas para vestiários, refeitórios, cozinhas, salas de reunião, escritórios etc.

2.2.8 Vede aberturas em pisos e paredes pelas quais passam tubulações, fiações e cabos com selantes certificados pela FM Approvals que tenham tempo de resistência ao fogo equivalente ao do piso ou da parede.

2.2.9 Direcione drenos de telhado, linhas de água de consumo e outras linhas de líquidos ao redor de salas de controle de processo e salas de equipamentos associadas. Em edificações com vários andares, vede o piso acima para torná-lo estanque a líquidos. Se a tubulação não puder ser direcionada para longe dessas áreas, instale contenção (por exemplo, tubulações concêntricas) ou um recipiente de coleta e instale detecção de vazamento certificada pela FM Approvals com notificação por alarme conectada a local

com presença constante de pessoal. Consulte detalhes adicionais na Norma 1-24, *Protection Against Liquid Damage*, da FM.

2.2.10 Instale drenos de piso embaixo de pisos elevados se houver risco de acúmulo de água ou outros líquidos.

2.2.11 Construa painéis de controle industrial, inclusive portas e/ou painéis de acesso, usando materiais de construção incombustíveis. Siga padrões internacionais reconhecidos.

2.3 Proteção

2.3.1 Proteja salas de controle de processo, salas de equipamentos associadas e painéis de controle industrial contra exposições a incêndios externos de acordo com a Norma Técnica 1-20, *Protection Against Exterior Fire Exposure*.

2.3.2 Instale detecção de fumaça certificada pela FM Approvals em salas de controle de processo, centros de controle de processo e salas de equipamentos associadas, configurada para sinalizar um alarme em uma estação de trabalho ou um local com presença constante de pessoal.

2.3.3 Se for desejável um nível mais alto de detecção para sistemas críticos e/ou de segurança, instale um sistema de detecção de incêndio por aspiração na sala de equipamentos e/ou dentro do painel de controle industrial que sinalize em local com presença constante de pessoal. Use sistemas por aspiração ou sistemas inteligentes de detecção pontual de alta sensibilidade certificados pela FM Approvals, conforme apropriado, para o invólucro da área.

2.3.4 Instale detecção de fumaça certificada pela FM Approvals embaixo de pisos elevados e acima de áreas de teto com cabos.

2.3.5 Instale detecção de fumaça de acordo com a Norma Técnica 5-48, *Automatic Fire Detection*.

2.3.6 Instale proteção contra incêndio em salas de controle de processo, centros de controle ou salas de equipamentos de instrumentação de controle industrial como segue:

2.3.6.1 Salas com construção combustível

A. Instale um sistema de sprinklers automáticos de tubulação molhada ou pré-ação utilizando sprinklers automáticos de resposta rápida. Use demandas de projeto, demandas de hidrantes e durações de acordo com a Norma Técnica 3-26, *Proteção contra Incêndio para Ocupações de Uso Geral*.

B. Instale um sistema automático de água nebulizada em névoa (water mist) certificado pela FM Approvals especificamente para salas de equipamentos de processamento de dados e instalado de acordo com a Norma Técnica 4-2, *Water Mist Systems*, e com o manual de projeto, instalação, operação e manutenção do fabricante indicado na listagem da FM Approvals. Instale um suprimento de água para o sistema de água nebulizada em névoa (water mist) com duração de 60 minutos.

Para os itens A e B especificados anteriormente:

- Use a categoria de risco 1 (HC-1) para salas de controle de processo e centros de controle que tenham tetos com até 9 m (30 ft) de altura.
- Use a categoria de risco 2 (HC-2) para salas de equipamentos de instrumentação de controle industrial ou salas de controle de processo e centros de controle que tenham tetos com mais de 9 m (30 ft) de altura.

2.3.6.2 Salas de construção incombustível

Instale um sistema de extinção de incêndio por halocarbono ou gás inerte (agente limpo) projetado e instalado de acordo com as instruções do fabricante e com a Norma Técnica 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*. Proteção por sprinklers automáticos de tubulação molhada ou pré-ação ou por sistemas de água nebulizada em névoa (water mist) – de acordo com a Seção 2.3.6.1 acima – também é aceitável.

Para um sistema de extinção de incêndio por halocarbono ou gás inerte (agente limpo), assegure-se de que:

1. Haja detecção de incêndio por aspiração ou desligamento automático da sala e equipamentos (com exceção das luzes de emergência) em caso de detecção de fumaça, desde que uma análise de risco de processo ou avaliação equivalente comprove que um desligamento automático não danificará os equipamentos controlados (ou seja, os equipamentos de processo) e/ou não criará uma condição perigosa.
   a. No caso de desligamento automático, instale de acordo com as diretrizes para isolamento elétrico de equipamentos de processamento de dados e sistemas de ar condicionado da Norma Técnica 5-32.
   b. Ajuste o tempo de retardo do desligamento de forma que não exceda o tempo de retenção do sistema de extinção de incêndio por halocarbono ou gás inerte (agente limpo) com um fator de segurança igual a dois, a fim de retornar o processo a um estado seguro.
2. Haja detecção de incêndio por aspiração com alerta/sinal de supervisão para permitir tempo suficiente para uma investigação pelo operador ou pelo grupo de resposta antes da descarga do sistema de agente limpo.
3. Os compartimentos dos equipamentos sejam feitos de metal.
4. O uso de papel e outros materiais combustíveis seja mínimo na sala.
5. Não haja armazenagem de materiais de embalagem ou cassetes de plástico dentro da sala. **Obs.:** Essa exigência inclui todos os tipos de mídias combustíveis (por exemplo, rolos de fita).
6. Haja desligamento e/ou dampers em sistemas de ventilação que usam retorno de ar ou ar de reposição.

2.3.7 Providencie proteção para os equipamentos de controle de processo das instalações. Baseie essa proteção na criticidade do processo físico e no impacto da perda do sistema de controle de processo em caso de incêndio. Consulte a Seção 3.1, Proteção contra incêndio de equipamentos de controle industrial. Providencie um dos itens a seguir (A ou B):

A. Gabinetes incombustíveis com subdivisões para limitar os danos à menor configuração possível.

B. Um sistema de extinção de incêndio por halocarbono ou gás inerte (agente limpo) na sala, desde que os gabinetes sejam abertos/ventilados e/ou configurados para descarga direta dentro deles. Siga as orientações da Seção 2.3.6.2 acima.

2.3.8 Instale proteção por sprinklers automáticos de acordo com a Norma Técnica 3-26, *Proteção contra Incêndio para Ocupações de Uso Geral*, em todos os espaços do prédio adjacentes a salas e centros de controle (incluindo, entre outras, escritórios, áreas de descanso, salas de arquivos, áreas de autorização, salas de conferência, salas de treinamento, banheiros etc.) para a classificação de risco apropriada da ocupação.

2.3.9 Instale sistemas de proteção contra incêndio de acordo com a Norma Técnica 2-0, *Diretrizes de Instalação para Sprinklers Automáticos*, e com a norma técnica do sistema de proteção especial aplicável.

2.3.10 Proteja data centers associados a salas de controle de processo de acordo com a Norma 5-32, *Data Centers and Related Facilities*, da FM. Faça uma análise de risco de processo dos controles antes de permitir o desligamento automático.

2.3.11 Proteja geradores de emergência conforme a Norma 5-23, *Design and Protection for Emergency and Standby Power Systems*, da FM.

2.3.12 Proteja cabos agrupados e bandejas de cabos de acordo com a Norma 5-31, *Cables and Bus Bars*, da FM.

2.3.13 Instale extintores portáteis de dióxido de carbono ou agente limpo (Classe C) certificados para riscos elétricos energizados para proteger equipamentos eletrônicos de acordo com a Norma Técnica 4-5, *Portable Extinguishers*.

2.3.13.1 Não use extintores de pó químico em áreas onde houver equipamentos eletrônicos.

2.3.13.2 Para materiais combustíveis comuns, providencie extintores portáteis do tipo e ou na combinação adequados, conforme a Norma 4-5, *Portable Extinguishers*, da FM.

2.3.14 Elabore um plano pré-incidentes para resposta a incidentes e de incêndio em salas de controle de processo, centros de controle, salas de equipamentos de instrumentação de controle industrial associadas e/ou painéis de controle industrial.

2.3.14.1 Verifique se o pessoal de manutenção elétrica está capacitado para responder ao mesmo tempo que o pessoal de combate a incêndio e se está treinado para desenergizar ou isolar com segurança os painéis de controle de processo afetados e iniciar atividades de combate a incêndio.

2.3.14.2 Quando não for viável desenergizar todos os equipamentos elétricos em salas e painéis de equipamentos de instrumentação de controle industrial, assegure que a resposta ao alarme de incêndio inclua pessoal treinado e capacitado para diagnosticar as condições de incêndio/fumaça na área afetada e para implementar o plano pré-incidentes com o isolamento elétrico manual local, regional ou completo.

2.4 Fator humano

2.4.1 Programa de gerenciamento de mudanças

2.4.1.1 Administre os programas de gerenciamento e de segurança de SCI em conjunto com o programa de gerenciamento de mudanças.

2.4.2 Gerenciamento de SCI

O comprometimento da gerência é fundamental para o sucesso de programas de supervisão e gerenciamento de SCI. O sólido compromisso da gerência ajuda a garantir que todas as áreas de SCIs recebam a atenção, os fundos e recursos humanos necessários.

2.4.2.1 Equipe de supervisão de SCI

2.4.2.1.1 As organizações devem criar uma equipe de supervisão de SCI composta por indivíduos dos níveis corporativo e local da unidade que seja responsável por supervisionar a implementação de políticas de segurança cibernética relacionadas ao SCI.

2.4.2.2 Programa de gerenciamento de ativos

2.4.2.2.1 Estabeleça e implemente um programa de inspeção, teste e manutenção de SCI. Veja a Norma 9-0, *Integridade de Ativos*, da FM, para orientações sobre o desenvolvimento de um programa de integridade de ativos. Inclua os elementos a seguir no programa de gerenciamento de ativos, conforme aplicável:

A. Manter um inventário do hardware conectado à rede de SCIs que inclua as seguintes informações: fabricante, número de modelo e firmware, software e aplicativos instalados, com os números das versões.

B. Assegurar que a lista de inventário inclua uma classificação de criticidade de bens do SCI para priorizar esforços de segurança e manter atualizações de segurança aplicáveis.

C. Mantenha em arquivo os desenhos e a documentação do SCI (por exemplo, esquemas elétricos e de controle, desenhos de redes e, quando relevante, diagramas de tubulação e instrumentação). Manter esses documentos atualizados à medida que forem feitas mudanças no SCI.

D. Armazenar inventário de ativos, desenhos e documentação que detalham o projeto e a funcionalidade do SCI em local controlado e restrito. Dar acesso somente quando necessário. Se esses documentos forem digitais, proteja-os com senha e mantenha cópias de backup armazenadas em uma rede confiável. Criptografar esses arquivos onde possível. Todas as redes fora do ambiente de SCI/TO devem ser consideradas não confiáveis, inclusive a rede local de TI.

2.4.2.3 Programa de gestão da cadeia de suprimentos

2.4.2.3.1 Inclua os elementos a seguir em um programa de gestão de cadeia de suprimentos, quando aplicável:

A. Incluir requisitos de segurança cibernética para sistemas/aplicativos ou dispositivos como parte da documentação de proposta do fornecedor. Reavaliar os fornecedores aprovados pela unidade, inclusive prestadores de serviços terceirizados, com relação a suas políticas e seus procedimentos de segurança antes de assinar ou renovar qualquer contrato.

2.4.3 Segurança de SCI

Em qualquer processo, a disponibilidade do SCI é fundamental. Uma estratégia eficaz de segurança de SCI pode ter papel vital na manutenção dessa disponibilidade.

2.4.3.1 Programa de gerenciamento de acesso

2.4.3.1.1 Inclua os elementos a seguir em um programa de gerenciamento de acesso, conforme aplicável:

A. Usar credenciais do SCI para controlar seu acesso (ou seja, acessos à HMI/estação de trabalho do operador e às estações de trabalho da engenharia baseados na função). Além disso, limitar o acesso às estações de trabalho da engenharia aos que tiverem autoridade para mudar o processo. Para apoiar o acesso controlado ao SCI, adote as seguintes medidas:

1. IHMs/estações de operador (que não tenham a capacidade de mudar pontos de ajuste de alarmes e intertravamentos de dispositivos de segurança) podem usar credenciais de login compartilhadas.
2. Estações de trabalho de engenharia requerem login e senha únicos, específicos de cada usuário, para cada acesso ao sistema, e devem ter bloqueio automático quando a estação ficar ociosa por um período de 30 minutos ou menos.
3. As credenciais utilizadas para acessar o SCI são gerenciadas independentemente daquelas usadas para acessar sistemas de TI. Manter atualizadas as credenciais dos usuários do SCI em um repositório de usuários no ambiente de TO, revisar periodicamente as permissões de acesso e remover os acessos de pessoas que não o necessitam mais. Alternativamente, logins locais fora da rede podem ser aceitáveis.

B. Mude o nome de usuário e a senha padrão de fábrica de todos os sistemas, hardwares e softwares. Atualizar senhas rotineiramente ou quando ocorrerem mudanças de pessoal importante e/ou chave ou de prestadores de serviço. Evitar nomes de usuários genéricos e senhas fracas.

C. Proteja as comunicações sem fio por meio de autenticação e criptografia.

D. Tomar as seguintes precauções quanto a dispositivos portáteis que se conectam aos SCIs:

1. Antes de conceder acesso à unidade, providenciar treinamento em segurança cibernética de SCI para empresas contratadas e outros visitantes que entram na unidade em caráter temporário. Este treinamento deve incluir familiaridade com regras e procedimentos da unidade, de acordo com a Seção 2.4.3.1.1, partes D.2 a D.5.
2. Para dispositivos utilizados no ambiente de SCIs, como laptops (inclusive laptops, tablets etc. de terceiros), desabilitar conexões sem fio, manter e verificar atuais correções de segurança e software antivírus e sempre fazer varredura de vírus antes da conexão aos SCIs.
3. Para cartões de memória, pen drives USB, unidades de disco rígido externas etc., sempre fazer varredura de segurança antes da conexão aos SCIs.
4. Não permitir a conexão de telefones celulares ou quaisquer outros dispositivos móveis habilitados para rede aos SCI.
5. Desabilitar portas não utilizadas (USB, RJ45, seriais etc.) em equipamentos conectados ao SCI, sempre que possível.

2.4.3.2 Programa de gerenciamento de configuração

2.4.3.2.1 Inclua os elementos a seguir em um programa de gerenciamento de configuração, conforme aplicável:

A. Limitar os recursos/as funções de todos os dispositivos digitais conectados ao SCI a somente àqueles que sejam necessários para o suporte à operação do SCI. Isso inclui dispositivos de campo que tenham múltiplos ajustes e se comuniquem digitalmente, controladores que executem controle básico e de segurança de processo, dispositivos de supervisão, IHMs e estações de trabalho de engenharia, historiadores, servidores, equipamentos de rede, como gateways, chaves e roteadores, e equipamentos de proteção de rede, como firewalls, inclusive todos os dispositivos instalados dentro de uma zona desmilitarizada (DMZ) do SCI.

B. Verificar se a equipe de supervisão do SCI está analisando, validando e aprovando os impactos sobre a segurança de todas as mudanças antes da sua implementação, em qualquer dispositivo digital conectado com o SCI, como parte do programa de gerenciamento de mudança.

C. Fazer monitoramento do sistema para verificar quaisquer mudanças não autorizadas nos equipamentos de controle básico, de controle de segurança e da rede de TO.

D. Assegure que solucionadores lógicos, CLPs ou controladores utilizados como parte do sistema básico de controle de processo e do sistema de segurança tenham seleção de modo operacional (ou seja, execução/programação/remoto etc.) regulados de acordo com o ajuste recomendado pelo fabricante antes de habilitar o sistema e operar o SCI. Incluir mudanças do modo de operação na recomendação de monitoramento do sistema acima.

2.4.3.3 Programa de gerenciamento de correções de segurança

2.4.3.3.1 Inclua os elementos a seguir em um programa de gerenciamento de correções de segurança, conforme aplicável:

A. Assegurar que o programa de gerenciamento de correções de segurança inclua dispositivos de suporte e de comunicação, como servidores de acesso remoto, jump servers, historiadores, proteção contra vírus, redes privadas virtuais e outros componentes de rede, como firewalls etc. Incluir também qualquer equipamento utilizado para a manutenção do SCI, como laptops ou dispositivos portáteis, e equipamentos de escaneamento utilizados para verificar dispositivos portáteis, como quiosques USB etc.

B. Monitorar boletins e alertas de vulnerabilidades de segurança cibernética emitidos por fabricantes de sistemas e de dispositivos, integradores de SCI, agências governamentais e outros.

C. Ao tomar conhecimento de uma notificação de segurança cibernética, a equipe de supervisão de SCI deve determinar as ações necessárias para proteger o SCI da unidade, com base em sua criticidade e na exposição. Podem ser necessárias medidas adicionais de proteção contra vulnerabilidades do sistema até que uma correção de segurança de software possa ser instalada.

D. Verificar se a equipe de supervisão de SCI consulta o fornecedor do SCI antes da aplicação de uma correção de segurança. Onde possível, testar em uma simulação ou sistema virtual antes da instalação.

E. Providenciar medidas adicionais de proteção contra vulnerabilidades de segurança cibernética para equipamentos e/ou softwares obsoletos devido à falta de suporte do fabricante do equipamento.

2.4.3.4 Dispositivos de proteção de rede

2.4.3.4.1 Implemente acesso remoto seguro ao ambiente de SCI/tecnologia operacional (TO). Todas as redes fora do ambiente de SCI/TO devem ser consideradas não confiáveis, inclusive a rede local de TI. Siga as seguintes precauções conforme aplicável:

A. Verificar o acesso remoto ao SCI da seguinte maneira:

1. A partir de uma rede interna (conexão originada na rede corporativa), tal como a rede local de TI, use autenticação multifator (MFA) por meio de um jump server localizado em uma DMZ industrial (consulte a Seção 2.4.3.4.2 B).
2. A partir de qualquer rede externa (conexão originada fora da rede corporativa), use uma rede privada virtual (VPN) segura e autenticação multifator (MFA) por meio de um caminho exclusivo, utilizando sistemas corporativos para um sistema intermediário (jump host na DMZ industrial) antes da obtenção de acesso ao ambiente de SCI/TO.
3. Computadores pessoais ou qualquer outro dispositivo pessoal externo não podem ser utilizados para acesso remoto ao ambiente do SCI/TO.

B. Não permita conexões remotas a sistemas de segurança exclusivos.

C. Não permitir conexões remotas persistentes no ambiente de SCI/TO. Monitoramento remoto, coleta de dados e diagnósticos com fluxo de dados restrito em uma direção são adequados e não requerem limites de tempo na conexão com o SCI.

D. Substitua modems de conexão discada por métodos de comunicação modernos e seguros. Se não for possível, faça o seguinte:

1. Desligue e/ou desconecte os modems de conexão discada quando não estiverem em uso.
2. Tome medidas adicionais de proteção para os modems de conexão discada ativos (ex., configuração de retorno de chamada para um número de telefone designado, filtragem por identificadores de chamadas, desativação do atendimento automático).

2.4.3.4.2 Implemente os seguintes dispositivos de proteção de rede, conforme aplicável:

A. Providenciar separação entre as redes de SCI/TO e da TI ou outras redes de negócio com zona industrial desmilitarizada (DMZ) e direcionar todas as comunicações que entram e saem do SCI pela DMZ.

B. Providencie separação entre a rede do sistema básico de controle de processo e as redes de segurança por meio de segregação (arquitetura interfaceada ou com air gap ou fisicamente isolada) ou por segmentação (arquitetura integrada ou comum). Para orientações adicionais sobre sistemas de segurança, veja a Norma Técnica 7-45, *Safety Controls, Alarms, and Interlocks* (SCAI), da FM.

C. Verificar se as regras do firewall (portas abertas, protocolos permitidos etc.) são revisadas periodicamente por pessoal com experiência em rede e segurança cibernética. Mudanças nas regras do firewall devem ser implementadas a partir do ambiente do SCI/TO, e controladas por gerenciamento de mudanças sob a direção da equipe de supervisão do SCI.

D. Utilize ″allowlistis″ de aplicativos no ambiente do SCI, quando possível. Usar de cautela na implementação desta recomendação.

E. Empregar monitoramento e registro de atividades na rede do SCI (também conhecido como sistema de detecção de intrusão), juntamente com software de gerenciamento e correlação de eventos de segurança (SIEM), onde possível, para detectar atividades não autorizadas. Quando possível, monitorar o ambiente de TO a partir de um centro de operações de segurança (SOC).

F. Usar software de proteção antivírus no SCI e no ambiente de TO, incluindo sistemas SCADA. Trabalhar com o fornecedor ou prestador de serviços do SCI e ter cautela na seleção e implementação de soluções antivírus.

2.5 Operação e manutenção

A certeza de que o SCI está operando da maneira desejada é crítica para evitar danos significativos a equipamentos e/ou ao patrimônio que possam resultar em paradas prolongadas. A possibilidade de falhas relacionadas ao SCI e paradas prolongadas pode ser minimizada com procedimentos de monitoramento e notificação, planejamento viável de resposta/recuperação de emergências e de contingência de SCI, e operadores experientes e adequadamente treinados que sigam procedimentos padrão e operacionais de emergência documentados.

2.5.1 Operações de SCI

2.5.1.1 Programa de gerenciamento de alarmes

2.5.1.1.1 Inclua monitoramento de sistemas de equipamentos de SCI e de rede de TO se for determinado que essa é uma opção disponível segundo a Recomendação 2.4.3.2.1 C sobre gerenciamento de configuração:

A. Com o uso do monitoramento de sistemas, configure um alerta que seja acionado quando forem feitas mudanças não autorizadas em ajustes de configuração em equipamentos de SCI, inclusive sistemas de segurança, e equipamentos de rede de TO.

Obs.: Não está previsto que os alertas mencionados acima sejam implementados pelos operadores de processo. Em vez disso, esses alertas devem ser encaminhados ao pessoal responsável por monitorar os equipamentos da rede de TO e os equipamentos de SCI.

Para obter orientações adicionais sobre gerenciamento de alarmes, consulte a Norma 10-8, *Operators*, da FM.

2.5.1.2 Procedimentos operacionais de emergência

2.5.1.2.1 O planejamento e a preparação são vitais para o sucesso de um procedimento operacional de emergência cibernético/de SCI, o que inclui a identificação de pessoal e, se necessário, de consultores terceirizados ou outros especialistas com as habilidades necessárias para responder a um ataque cibernético.

A. Verifique se há funções e responsabilidades estabelecidas para o tratamento de incidentes cibernéticos.

B. Manter informações sobre prestadores de serviço autorizados/contratualmente obrigados a dar suporte durante um evento cibernético.

2.5.1.2.2 Inclua os seguintes elementos nos procedimentos operacionais de emergência de SCI/cibernética, conforme aplicável:

A. Assegure que haja um procedimento para mitigar o impacto ao SCI e à produção causado pela perda de um sistema ERP (Enterprise Resource Planning) ou de um sistema de execução de manufatura (MES).

B. Assegurar que sejam fornecidas orientações sobre como desligar o sistema e/ou processo (ou seja, conduzir o sistema para um modo seguro) quando o controle do SCI se comportar de modo suspeito ou parar de funcionar. Essas orientações devem incluir os seguintes incidentes cibernéticos conhecidos ou suspeitos, entre outros:

- Tela preta/tela HMI congelada
- Desligamento inexplicado da unidade
- Mensagens de ransomware que aparecem em estações de trabalho
- Cursores que se movem inesperadamente nas estações de trabalho sem ação do operador
- Mudança de configuração não reconhecida
- Problema ao configurar ou ajustar alguma parte do SCI

C. Verificar se existem procedimentos para operar equipamentos essenciais em modo manual.

D. Verifique se os procedimentos operacionais de emergência são praticados, no mínimo, em exercícios de simulação periodicamente.

2.5.1.3 Planejamento de contingência

2.5.1.3.1 Plano de contingência para equipamentos

Desenvolva e mantenha um plano documentado de contingência para o SCI, de acordo com a Norma Técnica 9-0, *Integridade de Ativos*. Veja o Anexo C dessa norma técnica para orientações sobre o processo de desenvolvimento e manutenção de um plano de contingência viável para o SCI. Consultar também na norma técnica orientações sobre estratégias de mitigação por sobressalentes, aluguel e redundância de equipamentos.

Além disso, incluir os seguintes elementos no processo do planejamento de contingência específico para o SCI:

A. Adote as ações necessárias para gerenciar desligamentos não intencionais e fazer a recuperação de possíveis paradas do SCI como parte do programa de resposta e recuperação de incidentes (consulte a Seção 2.5.1.4).

B. Testar e treinar o plano à frequência determinada pelo responsável pelo ativo e compatibilizá-lo com as exposições.

C. Com base no inventário de hardware (consulte a Seção 2.4.2.2.1), inclusive na criticidade dos componentes e nos planos de gerenciamento de vida útil, avalie a necessidade e o escopo de sobressalentes para falha de componentes do SCI.

2.5.1.3.2 Os planos de contingência de SCIs devem ser revisados anualmente.

2.5.1.4 Programa de recuperação de incidentes

2.5.1.4.1 Incluir os seguintes elementos em um programa de resposta e recuperação de incidentes como parte do planejamento de contingência do SCI, conforme aplicável:

A. Determinar a causa raiz de qualquer parada não programada antes de tentar reiniciar o SCI.

B. Manter registros eletrônicos para quando ocorrer parada não programada para avaliação pericial, tanto quanto possível.

C. Manter cópia viável e atualizada de todos os arquivos de configuração do SCI (por exemplo, última configuração confiável conhecida, configuração de referência) e a documentação necessária para um sistema totalmente funcional. Mantenha um histórico de arquivos de backup em local fisicamente seguro.

1. Se os arquivos de backup forem imutáveis (por exemplo, WORM – write once/read many, não podem ser atualizados), então:
    a. Armazenar os arquivos de backup imutáveis em uma unidade de rede confiável separada da rede de origem dos dados.
    b. Criar novos arquivos de backup quando ocorrerem mudanças no sistema e após qualquer atualização.
    c. Criar novos arquivos de backup antes do fim do período de retenção do arquivo imutável mais antigo.
2. Se os arquivos de backup não forem imutáveis (ex.: se puderem ser atualizados), então:
    a. No mínimo uma cópia de todos os arquivos de backup deve ser armazenada off-line em local fisicamente protegido.
    b. Criar novos arquivos de backup quando ocorrerem mudanças no sistema e após qualquer atualização.

D. Revise contratos de serviço com fabricantes e/ou fornecedores de equipamentos para identificar o tempo de entrega de componentes e determinar a estratégia ideal de recuperação e sobressalentes em caso de quebra de equipamentos.

E. Revisar o programa de resposta e recuperação de incidentes rotineiramente, a uma frequência compatível com as exposições, mas no mínimo anualmente. Atualizar o programa conforme necessário para manter sua eficácia.

Para orientações adicionais sobre planejamento pré-incidente, resposta e recuperação, consultar as Normas 9-1, *Supervision of Property*, 10-1, *Pre-Incident Planning*, e 10-5, *Disaster Recovery Planning*, da FM.

Para orientações adicionais sobre investigação de incidentes, veja as Normas Técnicas 10-8, *Operators*, e 7-43, Segurança de processos

2.6 Treinamento

2.6.1 Como parte do programa de treinamento de operadores da unidade, implemente um programa de treinamento e conscientização sobre políticas e procedimentos de segurança de SCI. O programa deve incluir normas de segurança cibernética e as melhores práticas da indústria.

2.6.2 Forneça treinamento específico a operadores e pessoal-chave da unidade que interagem com o SCI antes que eles recebam acesso ao sistema. Providenciar treinamento adicional para administradores do sistema ou pessoal que tenha nível privilegiado/mais alto de acesso (por exemplo, treinamento baseado na função) para a execução do seu trabalho.

2.6.3 Realize treinamento de segurança cibernética de SCI inicial e de atualização, anual e contínuo, para todo o pessoal do SCI.

2.6.4 Treine o pessoal de resposta a emergências de incêndio sobre combate a incêndios em controles de processo. Veja a Norma 5-32, *Data Centers and Related Facilities,* da FM, Seção 2.7.1.

Para orientações adicionais sobre operadores, consultar a Norma de Prevenção de Perdas Patrimoniais 10-8, *Operators*, da FM.

2.7 Utilidades

2.7.1 Providencie nobreaks e sistemas de energia elétrica de emergência para permitir a operação do SCI até que possa ser feito um desligamento seguro. Inclua suprimento de energia por nobreak para todos os sistemas de suporte, como ar de instrumentos (se utilizado) e ar condicionado, que possam ser necessários durante um desligamento seguro.

2.7.2 Execute atividades de inspeção e manutenção em sistemas de utilidades e suporte para SCIs (por exemplo, baterias, nobreaks, geradores e controle de temperatura) como parte do programa de integridade de ativos. Para obter orientações adicionais, consulte as Normas 5-28, *DC Battery Systems*, e 5-23, *Design and Protection for Emergency and Standby Power Systems* da FM.

2.7.3 Providencie um sistema confiável de ar de instrumentos se forem utilizados controles de ar pneumáticos (ex., um compressor de ar de instrumentos independente com reserva N+1 ou um receptor de ar adequadamente projetado).

2.7.4 Providencie um sistema confiável de aquecimento, ventilação e ar condicionado para manter as condições ambientais do espaço dos equipamentos de SCI necessárias às operações normais. Esta recomendação se destina a equipamentos de SCI considerados críticos para as operações.

3.0 AJUDA PARA RECOMENDAÇÕES

3.1 Proteção contra incêndio de equipamentos de controle industrial

Entenda que a proteção por sprinklers automáticos é feita, em grande parte, para proteger a estrutura da sala e ocupações adjacentes. Em uma sala pequena, todos os equipamentos podem ser perdidos, mesmo que o incêndio seja controlado por sprinklers ou sistemas de água nebulizada em névoa (water mist). Portanto, um sistema de extinção de incêndio por halocarbono ou gás inerte (agente limpo) pode ser uma opção melhor se o objetivo for proteger os equipamentos.

Um incêndio em gabinetes de equipamentos de controle de processo bem subdivididos provavelmente causará danos ao gabinete no qual o incêndio se originou e danos limitados a gabinetes adjacentes. Em contrapartida, um incêndio em um gabinete de equipamento de controle de processo que não tenha subdivisões provavelmente percorrerá toda a extensão do gabinete. O impacto da perda de equipamentos de controle de processo depende da extensão dos danos causados pelo incêndio e da criticidade do processo, da disponibilidade de peças de reposição etc.

3.2 Gerenciamento de SCI

O responsável pelo ativo ou um indivíduo identificado devem ter uma estratégia de segurança cibernética para proteger o SCI em toda a unidade.

3.2.1 Supervisão de SCI

Com a complexidade da automação, a interconexão de diferentes sistemas e redes, e a aquisição de dados para fins empresariais, um novo perigo foi introduzido no SCI: riscos cibernéticos. Para manter os processos da unidade em funcionamento, o SCI precisa de um indivíduo identificado com capacidade para proteger o SCI contra riscos cibernéticos e para entender como métodos, produtos e sistemas de segurança cibernética podem afetar o desempenho do SCI.

3.2.2 Programa de gerenciamento de configuração

Para manter a resiliência cibernética do SCI, as organizações devem saber o que está conectado à rede do SCI. Sem esse conhecimento, ela não consegue começar a identificar os dispositivos que expõem o SCI a riscos cibernéticos.

Os ativos que precisam ser incluídos no programa de gerenciamento de ativos são os dispositivos digitais conectados à rede do SCI. Considere estações de IHM/operador, estações de trabalho de engenharia, comutadores de rede, modems, roteadores, firewalls, servidores de aplicativos, impressoras, SDCDs, CLPs e outros controladores lógicos e dispositivos de campo inteligentes conectados à rede. Sistemas operacionais (ex., equipamentos utilizados no modelo Purdue de nível 3 em uma rede de TO) também devem ser incluídos no controle de ativos. Os itens normalmente encontrados nesse nível incluem historiadores agregados de plantas, sistemas de programação de operações, servidores de alarme e outros

aplicativos, serviços de TI específicos de operações, como DHCP, LDAP, DNS, e servidores de arquivos. Além disso, considere a Internet das Coisas Industrial (Iiot) e até mesmo dispositivos básicos da Internet das Coisas que possam erroneamente estar conectados à rede do SCI.

Bons programas de gerenciamento de ativos identificam dispositivos conectados à rede do SCI. Os dispositivos incluem, entre outros, IHMs, CLPs, estações de trabalho de engenharia, equipamentos de rede, servidores etc. A identificação do firmware, do software e dos aplicativos de cada dispositivo também é fundamental. Sem essas informações adicionais, não é possível determinar os recursos e serviços disponíveis para cada dispositivo, o que deixa o SCI vulnerável.

Muitos fornecedores no mercado oferecem soluções automatizadas, ativas e passivas, de mapeamento de ativos e redes. Onde possível, a utilização de soluções passivas de descoberta de rede é preferencial a técnicas manuais de gerenciamento de ativos.

3.2.3 Programa de gestão da cadeia de suprimentos

Um bom programa de gerenciamento de cadeia de suprimentos ajuda a assegurar que os equipamentos e o software adquiridos sejam configurados de maneira segura pelos fornecedores para atender aos requisitos de segurança da organização.

Antes de instalar qualquer novo controlador digital ou outro dispositivo digital, ou qualquer software e/ou aplicativo no SCI, a organização deve ter a segurança de que o dispositivo vem de uma cadeia de custódia confiável, que inclui o desenvolvedor, o fabricante, o fornecedor, a expedição e a armazenagem e também o comissionamento e o teste de aceitação.

3.3 Segurança de SCI

3.3.1 Programa de gerenciamento de acesso

Pontos de acesso não seguros estão entre os vetores de ataque mais vulneráveis em SCIs. Eles são vulneráveis a intrusões tanto deliberadas quanto não intencionais. Os criminosos cibernéticos sabem que o SCI deve dar suporte ao acesso remoto e procuram por pontos de fácil acesso para comprometer o sistema. O pior caso seria o comprometimento de um ponto de acesso por um período prolongado, o que permitiria o acesso ao SCI por terceiros não aprovados, que poderiam obter informações valiosas sobre o SCI e o processo da unidade, com tempo para planejar e iniciar um ataque cibernético.

3.3.2 Programa de gerenciamento de configuração

Dispositivos digitais e eletrônicos têm muitos recursos e opções de desempenho e/ou de comunicação em seu firmware e/ou software. Para reduzir a possível superfície de ataque cibernético, é usada a "blindagem" do equipamento (com base, por exemplo, na criticidade do ativo ou em uma análise de risco de processo cibernético) para limitar as opções e os recursos de dispositivos digitais/eletrônicos apenas aos necessários para a operação do SCI.

Quando a configuração desejada for definida e o sistema funcionar corretamente, essa configuração deve ser salva como referência ou como a última configuração confiável conhecida. Essa configuração de referência seria utilizada nos esforços para restabelecer o sistema em caso de interrupção, por danos físicos ou corrupção de firmware/software.

Uma vez definida a configuração de CLPs de segurança ou outros controladores, esses equipamentos devem ser colocados no modo de operação recomendado pelo fabricante (execução, programação, remoto etc.). Essa configuração, incluindo as definições e o modo de operação, seria bloqueada por meio da remoção da chave física ou da definição da chave digital. Esse método dá suporte ao programa de gerenciamento de acesso ao permitir o acesso apenas por pessoas com autoridade para ajustar as configurações de segurança.

O monitoramento dessas configurações identificará mudanças não autorizadas no SCI. Ela é útil para identificar e, possivelmente, evitar ameaças internas ou externas ao SCI.

3.3.3 Programa de gerenciamento de correções de segurança

O gerenciamento de correções de segurança é o processo de aplicação de atualizações de software, drivers e firmware para fornecer proteção contra vulnerabilidades. As correções de segurança devem ser avaliadas para determinar como podem afetar o processo.

Antes de instalar qualquer correção de segurança, faça a autenticação e a verificação da integridade do software para assegurar que ele esteja em sua forma original e que não tenha sido modificado. A origem do software também é importantíssima. Antes de baixar qualquer software, a confiabilidade da origem deve ser confirmada.

Se uma correção de segurança não trouxer benefícios do ponto de vista de segurança cibernética ou de desempenho, ela pode não ser necessária. O responsável pelo ativo deve trabalhar com o fornecedor do SCI para a implantação de correções de segurança no ambiente de SCI/TO.

3.3.4 Dispositivos de proteção de rede

Com os avanços da tecnologia, como o Industry 4.0, os ambientes de SCI/TO estão mais conectados do que nunca. Essa conectividade expandida expõe esses ambientes a ameaças cibernéticas que não existiam antes.

O acesso remoto passou a ser um método comum de suporte a fornecedores externos e é uma forma conveniente de os funcionários acessarem o ambiente de SCI/TO. As comunicações originadas externamente e que solicitam acesso ao ambiente de SCI/TO devem ser feitas por meio de uma VPN segura, com autenticação multifator feita através de uma DMZ, até chegarem a um jump server com acesso ao ambiente de SCI/TO. As comunicações originadas dentro do ambiente corporativo e que solicitam acesso ao ambiente de SCI/TO devem usar a autenticação multifator através de uma DMZ, até chegarem a um jump server com acesso ao ambiente de SCI/TO.

Uma DMZ (zona desmilitarizada) industrial é uma rede perimetral que adiciona uma camada extra de segurança à rede de TO interna de uma organização para defesa contra tráfego não confiável. Uma zona desmilitarizada (DMZ) é uma área definida nos limites de uma rede confiável que fornece recursos acessíveis a redes não confiáveis, como a Internet. Dessa forma, os recursos que precisam ser consumidos por usuários de áreas não confiáveis não terão acesso à rede considerada segura. Uma DMZ industrial fornece serviços que requerem conectividade à TI e à TO, como acesso remoto, aplicação de correções de segurança, antivírus, historiador, sistema de execução de manufatura (MES) e transferências de arquivos.

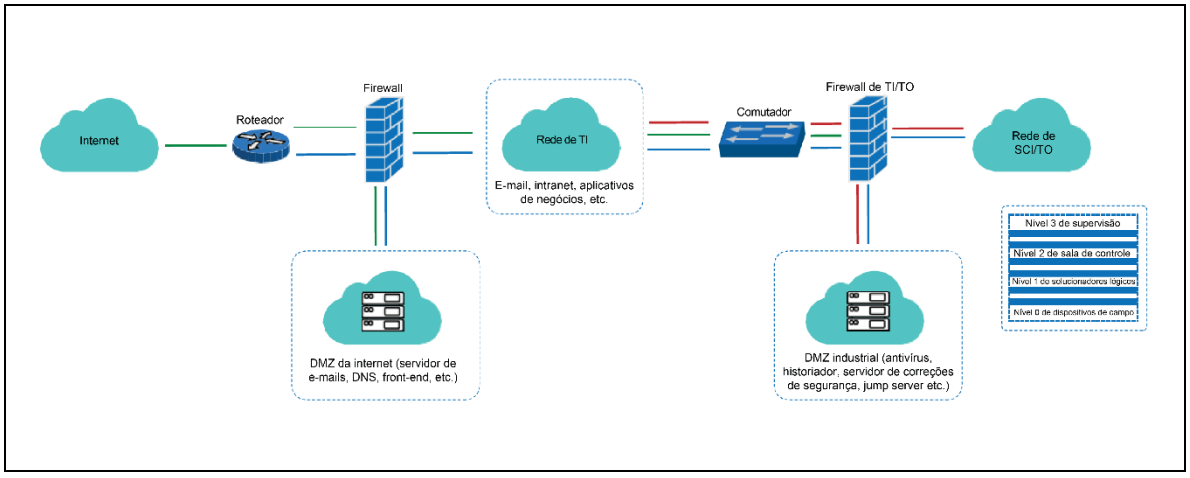

Fig. 3.3.4. Exemplo de caminho de comunicação que mostra a DMZ corporativa/de Internet e a DMZ de SCI/industrial

Os sistemas de detecção de intrusão são ferramentas de segurança de rede que monitoram o tráfego da rede e os dispositivos quanto a atividades maliciosas. Os alertas do SCI devem ser transmitidos a um centro de operações de segurança (SOC) para investigação mais aprofundada.

A detecção de intrusão baseada em assinaturas se concentra em pesquisar assinaturas (ou seja, padrões) para detectar uma intrusão. Essas assinaturas precisam ser atualizadas periodicamente para que sejam capazes de identificar os mais recentes padrões de ataque.

A detecção de intrusão baseada em anomalias se concentra em padrões inesperados de atividade para detectar uma intrusão, como um pico na atividade da rede, várias tentativas de logon com falha e atividades incomuns em portas de rede que são sinalizadas como atividades suspeitas, entre outros. Esses alertas são transmitidos ao centro de operações de segurança (SOC) periodicamente.

3.4 Exemplos ilustrativos de perdas

3.4.1 Rede de energia elétrica da Ucrânia

Malware de crash override. Um dos incidentes de violação de SCI mais notórios ocorreu na Ucrânia em 23 de dezembro de 2015, quando houve várias interrupções não programadas no suprimento de energia elétrica que afetaram aproximadamente 225 mil clientes. As interrupções foram causadas por intrusões cibernéticas remotas em três empresas regionais de distribuição de energia elétrica. Enquanto o suprimento era restaurado, as empresas envolvidas continuaram operando com restrições.

Supostamente, o ataque cibernético foi sincronizado e coordenado após uma extensa operação de reconhecimento das redes afetadas. Alguns relatórios sugerem que esse ataque ocorreu ao longo de um período de seis meses. Os relatórios afirmam que os ataques cibernéticos ocorreram em intervalos de 30 minutos entre cada uma das empresas e afetaram várias instalações. Durante o evento, vários disjuntores foram operados remotamente e sem autorização por várias entidades externas, tanto por meio de ferramentas de administração remota existentes no nível do sistema operacional quanto por software cliente remoto do sistema de controle industrial (SCI), via conexões de rede privada virtual (VPN). Segundo informado, as entidades externas adquiriram credenciais legítimas antes do ataque, a fim de facilitar o acesso remoto.

As três empresas de energia elétrica relataram que vários sistemas tinham sido apagados na conclusão do ataque cibernético com o malware Kill Disk. O malware apaga arquivos selecionados em sistemas e corrompe o registro de inicialização mestre, tornando os sistemas inoperantes. Além disso, as IHMs baseadas em Windows incorporadas a unidades terminais remotas também tinham sido sobrescritas pelo Kill Disk. Vários dispositivos com conexão serial-Ethernet nas subestações ficaram inoperantes devido à corrupção de firmware. Os nobreaks foram desconectados por meio de suas interfaces de gerenciamento remoto, o que interferiu nos esforços de recuperação previstos.

As três empresas relataram que tinham sido infectadas com o malware Black Energy, mas não se sabe ao certo se isso teve algum papel no ataque cibernético. Segundo informado, o malware foi introduzido por meio de e-mails de spear phishing com anexos maliciosos. Embora isso não tenha sido confirmado, o Black Energy pode ter sido usado para a obtenção de credenciais legítimas. No entanto, qualquer cavalo de troia de acesso remoto pode ter sido utilizado.

Após os ataques, as empresas não conseguiram rearmar remotamente os disjuntores. Portanto, foi preciso enviar o pessoal de operações para concluir o processo manualmente. Essa situação resultou em uma parada que durou entre quatro e seis horas. Deve-se notar que não foram relatados danos em nenhuma instalação de geração de energia elétrica como resultado desse incidente.

3.4.2 TRISIS

Em dezembro de 2017, pesquisadores de segurança identificaram um ataque por malware em sistemas instrumentados de segurança (SIS) e sistemas digitais de controle distribuído (SDCDs) de uma grande unidade industrial do Oriente Médio. Esse malware é conhecido como TRITON ou TRISIS pelas organizações de segurança cibernética, e como HATMAN pela equipe ICS-CERT do Departamento de Segurança Interna dos EUA. O malware afetou painéis de controle de segurança e IHMs Triconex Tricon da Schneider Electric e permitiu que um invasor lesse e modificasse o conteúdo da memória dos painéis de controle (ou seja, sobrescrevesse programas existentes por meio de uma conexão de rede remota).

Com base nas informações disponíveis, os invasores obtiveram acesso remoto a uma estação de trabalho de engenharia de sistema instrumentado de segurança e implantaram o malware: um arquivo executável para PCs com Windows para a comunicação com o controlador de segurança (Triconex) e um componente binário malicioso que foi baixado para o controlador. A Mandiant, empresa de segurança cibernética da

FireEye que foi chamada para investigar o incidente, afirmou em seu relatório [1] que “o malware conseguiu ler e gravar programas e consultar o estado do controlador”. Ele também conseguiu se comunicar com o painel de controle utilizando o TriStation, um protocolo proprietário utilizado pelo software TriStation (software de programação da Tricon) para a comunicação com sistemas de segurança Triconex. Aparentemente, o invasor estava familiarizado com o sistema Triconex e tinha testado o malware antes do ataque”.

Com base na análise da Mandiant, há evidências de que os invasores obtiveram acesso também ao SDCD da unidade, mas decidiram comprometer o sistema de segurança. Eles causaram acidentalmente um desligamento do sistema enquanto tentavam reprogramar os painéis de controle para causar danos físicos. O sistema entrou em modo à prova de falha devido a uma falha na verificação de validação entre os processadores, o que desligou o sistema e alertou o responsável. Segundo a Mandiant, “se o invasor tivesse assumido o controle do SDCD e do SCI, poderia ter causado um enorme impacto”.

A ICS-CERT e a Dragos afirmaram que o protocolo TriStation utilizado em painéis de controle mais antigos, como o que sofreu o ataque nesse evento, não tem um mecanismo de autenticação ou criptografia para contas de backdoor, algo vital para assegurar acesso no nível de administrador e controle sobre o dispositivo em caso de emergência. No entanto, as versões mais recentes dos sistemas Triconex têm um fator de autenticação para essas contas e são menos suscetíveis a ataques como esse. Uma notificação de segurança da Schneider Electric confirmou essa vulnerabilidade, e eles desenvolveram uma ferramenta para detectar e remover o malware em um controlador Tricon. Ela também afirmou que a chave principal do hardware que fornece o controle operacional físico foi deixada no modo “Program”, o que não é considerado uma prática aceitável quando o painel de controle não está sendo programado.

Os sistemas Triconex são sistemas de segurança altamente qualificados no mercado. O Tricon é baseado na tecnologia de TMR (redundância modular tripla). A TMR utiliza três sistemas de controle isolados e paralelos e de diagnósticos extensivos integrados em um único sistema. Ele permite uma operação de processo de alta integridade, livre de erros e ininterrupta, sem um único ponto de falha. A TMR aplica-se a entradas, saídas e lógica. Devido ao tamanho e ao custo do sistema, ele é usado principalmente para aplicações essenciais, como controles de turbinas (controle de sobrevelocidade) e, às vezes, como um SDCD. Embora esse malware tenha sido projetado especificamente para sistemas Triconex, as organizações de segurança cibernética acreditam que a capacidade e a metodologia do malware possam ser adaptadas pelos adversários para atingir sistemas de segurança de outros fornecedores. A convicção de que mesmo com o comprometimento do sistema de controle de processo o sistema de segurança evitará danos foi desafiada por esse incidente.

4.0 REFERÊNCIAS

4.1 FM

Norma Técnica 1-20, *Protection Against Exterior Fire Exposure*
Norma Técnica 1-44, *Damage-Limiting Construction*
Norma Técnica 2-0, *Diretrizes de Instalação para Sprinklers Automáticos*
Norma Técnica 3-26, *Proteção contra Incêndio para Ocupações de Uso Geral*
Norma Técnica 4-5, *Portable Extinguishers*
Norma Técnica 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*
Norma Técnica 5-11, *Lightning and Surge Protection for Electrical Systems*
Norma Técnica 5-23, *Design and Protection for Emergency and Standby Power Systems*
Norma Técnica 5-28, *DC Battery Systems*
Norma Técnica de Prevenção de Perdas Patrimoniais 5-31, *Cables and Bus Bars*, da FM
Norma Técnica 5-32, *Data Centers and Related Facilities*
Norma Técnica 7-43, *Process Safety*
Norma Técnica 7-45, *Safety Controls, Alarms, and Interlocks (SCAI)*
Norma Técnica 9-0, *Integridade de Ativos*
Norma Técnica 9-1, *Supervision of Property*
Norma Técnica 10-1, *Plano de Preparação para Incidentes e de Resposta a Emergências*
Norma Técnica 10-5, *Disaster Recovery Planning*
Norma Técnica 10-8, *Operators*

4.2 Outros

International Society for Automation (ISA). Série de normas e relatórios técnicos ISA/IEC 62443.

National Institute of Standards and Technology (NIST). *Guide to Industrial Control Systems (ICS) Security*. NIST SP 800-82, Revisão 2.

North American Electric Reliability Corporation (NERC). CIP Reliability Standards.

Electric Power Research Institute (EPRI), *Generation Cyber Security*.

US Department of Homeland Security, National Cybersecurity and Communications Integration Center's (NCCIC), ICS-CERT.

ANEXO A - GLOSSÁRIO DE TERMOS

Acesso físico: Acesso local e pessoal a hardware de computadores e redes ou a outras partes de uma instalação de rede.

Acesso remoto: Acesso por usuários (ou sistemas de informação) que se comunicam externamente com um perímetro de segurança do sistema de informação. (Fonte: NIST SP 800-53.) Uso de sistemas que estão dentro do perímetro da zona de segurança a partir de uma localização geográfica diferente, mas com os mesmos direitos do acesso físico no local. Exemplos de equipamentos utilizados no acesso remoto:

1. Modems que modulam e desmodulam os dados dentro e fora do aparelho. Essencialmente, eles convertem sinais elétricos analógicos de fora da rede em 1s e 0s digitais a serem manipulados pelo roteador e vice-versa.
2. Roteadores, que ficam a jusante do modem. Eles se conectam a uma rede de área ampla (WAN) ou à internet com um endereço IP público. Eles orientam e direcionam os dados da rede, enquanto priorizam os dados e escolhem a melhor rota a ser usada em cada transmissão.
3. Servidores de acesso remoto, que fornecem serviços para o gerenciamento de conexões remotas de fora da rede local (LAN). Comumente chamados de jump servers/hosts.

Acesso: A capacidade e os meios para se comunicar ou interagir de alguma forma com um sistema a fim de utilizar seus recursos. O acesso pode ser físico (autorização para acessar fisicamente uma área, posse de uma chave física, um código PIN ou um cartão de acesso ou atributos biométricos para permissão de acesso) ou lógico (autorização de conexão a um sistema e aplicativo por meio de uma combinação de meios lógicos e físicos).

Agente de ameaça: Entidade parcial ou totalmente responsável por um incidente que afeta a segurança de uma organização. Os exemplos de agentes de ameaça incluem hacktivistas, ameaças internas, estados-nações e crime organizado.

Allowlist: Uma lista de entidades distintas, como hosts ou aplicativos, que são conhecidamente benignas e aprovadas para uso dentro de organizações e/ou sistemas de informação. Exemplo: Permitir que apenas determinados aplicativos e serviços sejam executados em um host como parte de seu processo de hardening.

Ameaça interna: Ameaças (tanto maliciosas quanto não intencionais) de pessoas dentro da organização, como funcionários insatisfeitos, ex-funcionários, prestadores de serviços e parceiros de negócios, que têm informações internas relativas a práticas de segurança, dados e computadores da organização.

Arquivos de backup imutáveis: Arquivos que não podem ser alterados nem modificados de nenhuma maneira (WORM – write once/read many) nem excluídos até o fim do período de retenção. (A data final desse período de retenção deve ser configurada no momento da criação do arquivo imutável.) Como os arquivos imutáveis não podem ser alterados nem excluídos, o controle de versões é fundamental.

Ativo: Objeto físico ou lógico de propriedade ou sob custódia de uma organização que tem um valor percebido ou real para a organização.

Autenticação multifator (MFA): A autenticação multifator envolve dois ou mais fatores de autenticação (ou seja, algo que você sabe, como uma senha, algo que você tem, como um token estático/cronometrado, ou alguma característica sua, como uma impressão digital). A autenticação de dois fatores é um caso especial de autenticação multifator que envolve exatamente dois fatores.

Autenticação: O ato de comprovar uma afirmação, como a identidade de um usuário de sistema de computador. Em comparação com identificação, ou seja, o ato de indicar a identidade de uma pessoa ou coisa, a autenticação é o processo de verificação dessa identidade. Um meio típico de autenticação é uma senha fornecida por um usuário para fazer login.

Blindagem: Medida de segurança que inclui remoção ou desativação de recursos, funções, portas e serviços desnecessários e aplicação de controles de segurança cibernética para evitar uso não autorizado. Há dois tipos de blindagem:

1. Blindagem física: Desativação por meios físicos; remoção de portas de comunicação desnecessárias com o bloqueio do acesso a portas, drives etc.
2. Blindagem lógica: Desativação de protocolos de rede e comunicação, drivers de periféricos, servidores Web etc. que não são utilizados, seguida pela aplicação de controles de segurança cibernética, tais como ativação de proteção por senha para atualização de firmware e carregamento de programas, ativação de logs e alertas e ativação de tecnologias de segurança, como antivírus ou allowlists, fornecidos com o dispositivo.

Centro de controle de processo: Ver Sala de controle de processo.

Centro de controle SCADA: Centro de controle que utiliza computadores com o software SCADA para monitorar e operar equipamentos em um ou mais locais que estão geograficamente longe do centro de controle. Em geral fica em uma edificação sem controles de processo locais tais como SDCD ou CLP. Esses centros de controle têm tráfico bidirecional de dados e podem realizar mudanças operacionais em equipamentos geograficamente remotos.

Centro de controle: Ver Sala de controle de processo.

Centro de operações de segurança (SOC): Solução que engloba as pessoas, os processos e a tecnologia, inclusive a solução de SIEM, envolvidos no monitoramento de ambientes digitais (ou seja, TI e TO) para fins de proteção, na resposta a eventos que se convertem em incidentes, na pesquisa de ameaças conhecidas/desconhecidas, na resposta a incidentes e no compartilhamento de informações, entre outras coisas.

Comunicação unidirecional: Estratégias utilizadas para garantir comunicações unidirecionais seguras a partir de dispositivos ou através de diferentes redes/zonas de proteção, como:

1. Envio somente de um sinal analógico (amperagem ou tensão) de e para um dispositivo, em vez de dados digitais.
2. Uso de um diodo de dados/gateway unidirecional.
3. Uso de regras em um firewall ou uma DMZ para transmitir dados através de redes.

Confiabilidade A capacidade de um sistema de executar uma função necessária sob condições estabelecidas por um período especificado.

Controlador lógico programável (CLP): Os CLPs são controladores de automação com a capacidade de controlar processos complexos, e são muito utilizados em sistemas de supervisão e aquisição de dados (SCADA) e sistemas digitais de controle distribuído (SDCDs). Os CLPs também são utilizados como painéis de controle principais em configurações de sistemas menores. São muito utilizados em quase todos os processos industriais.

Controle de acesso baseado em função: Forma de controle de acesso baseado na identidade em que as entidades de sistemas que são identificadas e controladas são posições funcionais em uma organização ou processo.

Correção de segurança: Um complemento de software projetado para corrigir erros e problemas de segurança em sistemas operacionais ou aplicativos. Os riscos de segurança podem ser minimizados com a aplicação constante de correções de segurança ao software.

Credenciais: As credenciais incluem, no mínimo, um nome de usuário e uma senha, mas também podem ser um elemento biométrico físico ou humano, como uma impressão digital, Elas são utilizadas para autenticar um usuário durante o login no SCI. Permissões de acesso podem estar vinculadas às credenciais de um usuário. As credenciais de um usuário podem conceder acesso apenas à estação de um operador, ao passo que um nível mais alto de acesso para outro usuário pode conceder acesso a uma estação de trabalho de engenharia.

Criptografia: Desordenação dos dados, de modo a torná-los ilegíveis a qualquer um que não possua a “chave” utilizada para ordená-los. Transformação criptográfica de texto simples em texto cifrado que protege o significado original dos dados de forma a evitar que eles sejam conhecidos ou utilizados.

Defesa em profundidade: Prática de colocar camadas de vários controles de segurança sobrepostos para proteger ambientes de tecnologia da informação e tecnologia operacional.

Diodos de dados e gateways unidirecionais: Dispositivos de hardware com dois nós ou circuitos (um que apenas envia e outro que apenas recebe) que permitem o fluxo de dados em uma única direção, da origem ao destino. Eles usam um LED como transmissor de dados de um lado e um fotorreceptor do outro, tornando fisicamente impossível que os dados sejam transmitidos na outra direção. Alguns podem se referir a uma solução de software (por exemplo, por meio de uma configuração de firewall) ou mesmo a configurações de comutador ou roteador como gateways unidirecionais, mas um “verdadeiro” gateway unidirecional utiliza um ou mais diodos de dados unidirecionais como componentes para criar o gateway unidirecional. Segundo a NIST 800-82: gateways unidirecionais são uma combinação de hardware e software. O hardware permite que os dados fluam de uma rede para outra, mas é fisicamente incapaz de enviar qualquer informação de volta para a rede de origem. O software replica bancos de dados e emula servidores de protocolo e dispositivos.”

Diodos de dados/gateways unidirecionais: Veja Diodo de dados unidirecional.

Dispositivo de campo: Equipamento conectado ao lado do campo de um SCI. Entre os tipos de dispositivos de campo estão unidades terminais remotas (UTRs), controladores lógicos programáveis (CLPs), acionadores, sensores, interfaces homem-máquina (IHMs) e as comunicações associadas.

Dispositivo de entrada/saída (I/O): Termo genérico para o equipamento utilizado na comunicação com um computador ou sistema de controle.

Dispositivo não autorizado: Um dispositivo não autorizado que não tem permissão para acessar a rede e funcionar nela. Pode ser de natureza maliciosa e ser utilizado para contornar a segurança.

Equipamento de controle industrial: Ver Painéis de controle industrial.

Estação de trabalho de engenharia: Uma plataforma de computação geralmente confiável e de alto desempenho, projetada para configuração, manutenção e diagnóstico dos aplicativos e de outros equipamentos do sistema de controle. Normalmente, consiste no software específico de fornecedor necessário para programar dispositivos e nos arquivos de projeto utilizados para programar dispositivos, incluindo CLPs e IHMs.

Estação do operador: Fornece uma visão dinâmica de todos os processos da unidade necessários para operar sistemas de controle. Apresenta gráficos de controle, diagnósticos, tendências, alarmes e exibição de condições.

Firewall: Dispositivo de segurança de rede que monitora o tráfego de entrada e saída da rede e decide se permite ou bloqueia um tráfego específico com base em um conjunto definido de regras de segurança.

Gateway: Um mecanismo de retransmissão que conecta duas ou mais redes de computadores com funções similares, mas com implementações diferentes, e que permite que os computadores host de uma rede se comuniquem com os de outra.

Gerenciamento de configuração (GC): Políticas e procedimentos para controlar modificações em hardware, firmware, software e documentação, a fim de garantir que o sistema de informação esteja protegido contra modificações indevidas antes, durante e após a implementação do sistema.

Gerenciamento de eventos e informações de segurança (SIEM): Aplicativo que coleta dados de segurança de componentes do sistema de informação, normaliza trilhas de auditoria, registra testes em relação a um conjunto de regras de correlação que, quando acionado, cria eventos para análise e apresenta esses dados como informações acionáveis por meio de uma única interface.

Historiador: Um sistema de software especializado que coleta valores pontuais, eventos de alarme, registros em lote e outras informações de dispositivos e sistemas industriais e os armazena em um banco de dados específico, ou seja, um banco de dados centralizado que dá suporte à análise de dados por meio de técnicas de controle estatístico de processos.

Integridade: A qualidade de um sistema, que reflete a precisão lógica e a confiabilidade do sistema operacional, a exatidão lógica do hardware e do software que implementam os mecanismos de proteção e a consistência das estruturas de dados e da ocorrência dos dados armazenados.

1. Dispositivo eletrônico inteligente (IED): Qualquer dispositivo que incorpore um ou mais processadores com a capacidade de receber, enviar e controlar dados de e para uma fonte externa (como medidores multifuncionais eletrônicos, relés digitais e painéis de controle).

Interface homem-máquina (IHM):

1. Hardware ou software por meio do qual um operador interage com um painel de controle. Uma IHM pode ser desde um painel de controle físico com botões e luzes indicadoras até um PC industrial com monitor gráfico colorido executando softwares de IHM dedicados.
2. Software e hardware que permitem que usuários autorizados monitorem e controlem processos e/ou equipamentos, como exibição de status ou tendências históricas, modificação de configurações de controle e anulação manual em caso de emergência.

Invasor: Pessoa que cria e/ou modifica software e hardware de computador para cometer crimes ou obter ganhos financeiros. Os invasores geralmente tentam obter acesso a sistemas de computador para descobrir nomes de usuário e senhas.

Malware: Termo genérico usado para descrever softwares maliciosos, como vírus, cavalos de Troia, spywares e conteúdos ativos maliciosos.

Painéis de controle industrial (PCI): Um conjunto que compreende dois ou mais componentes do circuito de controle e do circuito de alimentação. Os componentes do circuito de controle incluem CLPs, módulos de entrada e saída, acionadores de motores e módulos de comunicação. Os componentes do circuito de alimentação incluem fontes de energia elétrica, nobreaks, relés, transformadores elétricos e conversores de tensão/corrente. Normalmente, os PCIs trabalham com tensão de 600 volts ou menos, embora as normas UL 508A e IEC aceitem 1.000 volts ou menos.

Phishing: Um tipo de ataque à segurança que convence as vítimas a revelar informações por meio de um e-mail falso, para atrair o destinatário a um site da Web que parece estar associado a uma fonte legítima.

Política: Um conjunto de regras que rege o tratamento de determinados procedimentos.

Procedimento: Etapas executadas para realizar uma determinada tarefa.

Protocolo: Sistema de regras utilizado por dois componentes que compartilham dados com a finalidade de entendê-los. Um protocolo não é uma “linguagem”, mas pode ser descrito mais adequadamente como a gramática e a sintaxe de comunicação dessa linguagem. No universo dos SCIs, muitos desses protocolos são exclusivos de cada fornecedor e foram projetados para fins de funcionalidade e confiabilidade, e não de segurança. Normalmente, eles são transmitidos em texto não criptografado. Isso aumenta a necessidade de separar os ambientes de TO e de TI. Alguns exemplos de protocolos de SCI comuns na indústria são Modbus RTU, Modbus TCP, Profibus, Profinet, DNP3 e ControlNet. No lado da TI, são comuns os protocolos baseados em TCP/IP (como FTP, DNS, HTTP e HTTPS).

Ransomware: Um tipo de software malicioso (malware) que desativa a operação ou bloqueia o acesso a dados até que o responsável ou operador responda a uma exigência de pagamento.

Rede de controle: Rede sensível ao tempo que está normalmente conectada a equipamentos que controlam processos físicos. A rede de controle pode ser subdividida em zonas, e pode haver várias redes de controle separadas dentro de uma empresa e uma unidade.

Rede de segurança: Rede que conecta sistemas instrumentados de segurança para a comunicação de informações relacionadas a segurança.

Rede de tecnologia da informação (TI): Uma rede comumente utilizada para a realização de negócios onde computadores são utilizados para criar, manipular, armazenar, recuperar e transmitir dados.

Rede de tecnologia operacional (TO): O termo TO é frequentemente utilizado de forma intercambiável com os termos sistema de controle industrial (SCI) ou rede de controle de processos. O termo tem o objetivo de diferenciar a rede de tecnologia da informação (TI) corporativa e a rede que controla os ativos operacionais (TO). O SCI compreende vários painéis de controle e instrumentos para monitorar e controlar

um processo físico, enquanto a TO inclui os sistemas de computação e a infraestrutura que gerenciam as operações industriais (inclusive o SCI).

Rede local (LAN): Rede de comunicações projetada para conectar computadores e outros dispositivos inteligentes em uma área geográfica limitada (normalmente, com menos de 10 quilômetros).

Rede privada virtual (VPN): Uma conexão segura entre uma rede pública (geralmente a internet) e uma rede privada.

Referência: Especificação ou produto que foi formalmente revisado e acordado e que, posteriormente, serve de base para desenvolvimento adicional e só pode ser alterado por meio de procedimentos formais de controle de mudanças.

Repositório de usuários: Sistema que armazena informações sobre usuários/membros para um determinado domínio com a intenção de assegurar recursos de autenticação e autorização por meio de uma abordagem centralizada. O Microsoft Active Directory é um exemplo comum de repositório de usuários comumente visto em redes de TI e TO.

Roteador: Um gateway entre duas redes na camada 3 do OSI que retransmite e direciona pacotes de dados através dessa interligação de redes. A forma mais comum de roteador opera em pacotes IP.

Sala de controle de processo: Uma sala isolada na qual o pessoal monitora e controla processos a partir de um local central ou remoto. A sala de controle de processo é normalmente separada, mas integrada a salas de equipamentos de controle industrial de modo a controlar o funcionamento dos equipamentos. O controle de processo é amplamente utilizado na indústria. Geralmente, permite a produção em massa de processos contínuos, como papel, produtos farmacêuticos, produtos químicos e energia elétrica, além de outros processos industriais. Em alguns cenários, salas e espaços técnicos para controle de processo podem se manter sem supervisão presencial e ser operados remotamente.

Salas de equipamentos de instrumentação de controle industrial: Salas nas quais estão localizados os equipamentos de controle de processo e que normalmente incluem diversos painéis de controle industrial e equipamentos de rede necessários para o funcionamento do processo físico.

Segmentação: Divisão de uma rede em seções menores e compartimentadas que ainda fazem parte da mesma rede geral. Dentro do SCI, a segmentação é geralmente obtida por meio de redes locais virtuais (VLANs) ou firewalls de hardware. A segmentação ajuda a retardar a propagação de malware ou a bloquear invasores. No entanto, o uso de VLANs não é um meio aceitável para separar a TI da TO.

Segregação: Desconexão total de uma rede das outras (air gap). Os sistemas instrumentados de segurança (SIS) em grandes instalações são segregados porque não são controlados pela rede do SCI que lida com o sistema básico de controle de processo.

Senha padrão: A senha fornecida em um sistema quando ele é inicialmente entregue ou instalado. Os usuários devem sempre alterar a senha padrão imediatamente.

Sensor:

1. Dispositivo que produz uma saída de tensão ou corrente representativa de alguma propriedade física medida (por exemplo, velocidade, temperatura, vazão).
2. Dispositivo que mede uma quantidade física e a converte em um sinal que pode ser lido por um observador ou instrumento.
3. Dispositivo que responde a uma quantidade inserida gerando uma saída funcionalmente relacionada, em geral na forma de um sinal elétrico ou óptico.

Separação: Particionamento adequado de diferentes redes que são consideradas não confiáveis umas pelas outras. A separação é geralmente feita com o uso de firewalls (e, preferencialmente, uma DMZ formal) ou de um gateway unidirecional. A separação da TI é essencial para redes de SCI.

Servidores de acesso remoto: Servidores de acesso remoto, que fornecem serviços para o gerenciamento de conexões remotas de fora da rede local (LAN). Comumente chamados de jump servers.

Sistema básico de controle de processo: Um sistema que gerencia equipamentos, produção e processos em uma unidade. Com base em uma ou mais condições predefinidas, esse sistema usa o feedback de circuitos de controle para automatizar e manter uma condição, um resultado ou um processo desejado.

Os sistemas básicos de controle de processo são personalizados para atender a qualquer necessidade de processo, desde sistemas muito grandes e complexos, como os de geração de energia elétrica ou de processamento químico, até sistemas muito simples, com apenas uma entrada e uma saída, tais como detectores de movimento ou sistemas de iluminação.

Sistema de controle industrial (SCIs):

1. Termo genérico que engloba vários tipos de sistemas de controle, como sistemas de supervisão e aquisição de dados (SCADA), sistemas digitais de controle distribuído (SDCDs) e outras configurações do sistema de controle, como controladores lógicos programáveis (CLPs) e solucionadores lógicos de segurança comumente encontrados nos setores industriais e em infraestruturas críticas. Um SCI consiste em vários componentes de controle (por exemplo, elétricos, mecânicos, hidráulicos e pneumáticos) que funcionam em conjunto para atingir um objetivo industrial (como fabricação e geração e transporte de matérias ou energia).
2. Conjunto formado por pessoas, hardware e software que pode afetar ou influenciar a operação segura e confiável de um processo industrial.

Sistema de detecção de intrusão: Um serviço de segurança que monitora e analisa eventos na rede ou no sistema para localizar e fornecer avisos em tempo real ou quase real de tentativas de acesso não autorizado a recursos do sistema. Um sistema de detecção de intrusão é capaz de detectar e alertar, mas não de bloquear nem rejeitar tráfego prejudicial.

Sistema de execução de manufatura (MES): Um sistema computadorizado que inclui software utilizado em ambientes de produção e manufatura para ajudar a rastrear inventários e outras informações de produção. Similar ao ERP, mas com foco mais especializado em manufatura (por exemplo, rastreamento e documentação de transformação de matérias-primas em produtos acabados).

Sistema de segurança: Sistema utilizado para implementar uma ou mais funções instrumentadas de segurança. É composto por qualquer combinação de sensores, solucionadores lógicos e acionadores.

Sistema de supervisão e aquisição de dados (SCADA): Utilizado para controlar ativos dispersos quando a aquisição centralizada de dados é tão importante quanto o controle. Os sistemas SCADA são utilizados em sistemas de distribuição, como os seguintes:

1. Sistemas de distribuição de água e coleta de água residual
2. Tubulações de óleo e gás natural
3. Sistemas de transmissão e distribuição de energia elétrica
4. Sistemas de transporte ferroviário e outros sistemas públicos de transporte

Os sistemas SCADA integram sistemas de aquisição de dados com sistemas de transmissão de dados e softwares de interface homem-máquina (IHM) para fornecer um sistema centralizado de monitoramento e controle para inúmeras entradas e saídas de processo. Os sistemas SCADA são projetados para coletar informações de campo, transferi-las para uma unidade central de computação, e exibir as informações para o operador de forma gráfica ou textual, permitindo, assim, que ele monitore ou controle um sistema inteiro a partir de um local central em tempo quase real. Dependendo da sofisticação e configuração do sistema, o controle de qualquer sistema, operação ou tarefa pode ser automático ou executado por comandos do operador.

Sistema digital de controle distribuído (SDCD): Um SDCD é um sistema de controle automatizado que controla processos distribuindo funções de controle entre vários componentes interconectados. Ele usa componentes distribuídos em vez de uma única unidade central. Observe que o termo “controlador de SDCD” aplica-se ao componente controlador físico, ao passo que o termo “SDCD” aplica-se a todo o sistema, inclusive a servidores de aplicativos, IHMs etc.

Sistema ERP (Enterprise Resource Planning): Software utilizado em ambientes corporativos. SAP e Oracle/PeopleSoft são exemplos desses sistemas. Eles direcionam ordens de produção, armazenagem e informações de transporte para a conclusão de pedidos.

Sistema operacional (OS): O software subjacente que permite a interação com um computador. O sistema operacional controla o armazenamento, as comunicações e as funções de gerenciamento de tarefas de computadores.

Software antivírus: Software que protege um computador contra vírus e malware. Uma vez detectada a presença de código malicioso, o software antivírus tenta limpar, excluir ou colocar em quarentena os arquivos, diretórios ou discos afetados.

Soluções de mapeamento de ativos:

1. Monitoramento passivo: Uma técnica de monitoramento silencioso e não intrusivo usado para capturar o tráfego de uma rede por meio da cópia do tráfego, muitas vezes a partir de uma porta SPAN ou espelhada, ou por meio de um TAP de rede. As soluções de detecção de intrusão baseadas em TO usam essa técnica para o mapeamento de ativos e também para detectar atividades não autorizadas.
2. Monitoramento ativo: Uma técnica intrusiva de monitoramento que faz consultas, no idioma nativo (protocolo) do controlador relevante, que variam ligeiramente, dependendo do fabricante. Uma abordagem de monitoramento ativo envolve a solicitação de informações detalhadas a um painel de controle (endereço IP e MAC, versão de firmware, configuração do backplane etc.).

Soluções de WAN: Uma rede de área ampla (WAN) é uma rede de computadores que abrange grandes regiões, países ou até mesmo o mundo todo. Os dados são transferidos entre redes que abrangem uma localização geográfica de várias maneiras, usando diferentes tipos de conexões para criar essas WANs. As soluções com fio incluem: MPLS, T1 e circuitos virtuais persistentes. Os serviços de comunicação sem fio incluem: 4G, 5G, Wi-Fi e redes via satélite.

Unidade terminal remota (UTR): Unidade projetada para dar suporte ao sistema digital de controle distribuído (SDCD) e a estações remotas de supervisão e aquisição de dados (SCADA). As UTRs são dispositivos de campo utilizados para monitorar parâmetros. Elas se comunicam com um painel de controle de supervisão utilizando recursos de comunicação remota, que podem incluir modem, celular, interfaces de rádio ou qualquer tecnologia de comunicação de área ampla. Algumas vezes, os CLPs são implementados como dispositivos de campo para atuar como UTRs. Nesse caso, o CLP costuma ser chamado de UTR. As UTRs são frequentemente instaladas em locais sem acesso fácil à energia elétrica, e podem ser alimentadas com energia solar.

Vetor de ataque: Método ou meio pelo qual um agente de ameaça obtém acesso ou prejudica os dados ou a rede de computadores de uma organização. Exemplos de vetores de ataque incluem negação de serviço (DoS), malware, acesso físico, ransomware e engenharia social.

Vulnerabilidade: Falha ou ponto fraco no projeto, na implementação, na operação e no gerenciamento de um sistema que podem ser explorados com a finalidade de violar a integridade ou a política de segurança do sistema.

War dialing: War dialer é um programa de computador usado para identificar os números de telefone capazes de estabelecer uma conexão com um modem de computador. O programa disca automaticamente um intervalo definido de números de telefone e registra e insere em um banco de dados os números que se conectam com êxito ao modem. Alguns programas também são capazes de identificar o sistema operacional específico em execução no computador e de fazer testes de penetração automatizados. Nesses casos, o war dialer percorre uma lista predeterminada de nomes de usuário e senhas comuns na tentativa de obter acesso ao sistema.

Zona desmilitarizada (DMZ industrial):

1. Uma interface em um firewall de roteamento semelhante às interfaces encontradas no lado protegido do firewall. O tráfego entre a DMZ e outras interfaces no lado protegido do firewall ainda passa pelo firewall e pode ter políticas de proteção de firewall aplicadas
2. Um segmento de host ou rede inserido como uma “zona neutra” entre a rede privada de uma organização e a Internet. A maior parte das DMZs industriais fica entre as redes de TI e TO de uma organização.
3. Um segmento da rede de perímetro situado logicamente entre redes internas e externas. Sua finalidade é garantir o cumprimento da política da rede interna de troca de informações externas, e restringir a fontes externas não confiáveis acesso a informações que podem ser divulgadas, sempre protegendo as redes internas contra ataques externos.

ANEXO B - HISTÓRICO DE REVISÕES DO DOCUMENTO

Neste anexo estão registradas as mudanças feitas neste documento em cada uma das vezes que ele foi publicado. Note que os números das seções se referem especificamente àqueles da versão publicada na data indicada (ou seja, os números das seções nem sempre são os mesmos entre as diferentes versões).

Julho de 2024. Revisão intermediária. Foram feitas alterações editoriais.

Janeiro de 2024. Revisão intermediária. Foram feitas pequenas alterações editoriais.

Julho de 2023. Revisão intermediária. As principais mudanças são as seguintes:

A. Esclarecimento e melhorias nas recomendações para proteção contra incêndio.

1. Melhorias nas orientações sobre proteção contra incêndio para ocupações e proteção contra incêndio para equipamentos.

B. Atualização de recomendações de segurança de SCI.

1. Orientações sobre conexões com centros de controle SCADA remotos.

C. Inclusão de termos no Anexo A - Glossário de Termos.

Janeiro de 2023. Revisão intermediária. As seguintes alterações foram feitas:

A. Esclarecimentos sobre recomendações para proteção contra incêndio.

B. Esclarecimentos sobre recomendações de gerenciamento de SCI.

C. Esclarecimentos e mudanças em recomendações sobre segurança de SCI, tais como:

1. Modificação em recomendações sobre configuração e monitoramento de sistemas para equipamentos de rede de SCI e TO.

2. Esclarecimentos sobre recomendações de gerenciamento de correções de segurança.

3. Esclarecimentos sobre recomendações relativas a proteções de rede.

D. Esclarecimentos e mudanças em recomendações sobre operações de SCI, tais como:

1. Esclarecimentos sobre recomendações de gerenciamento de alarmes.

2. Modificações no programa de recuperação de incidentes, especificamente os tipos de arquivos de backup aceitáveis.

E. Inclusão de termos no Anexo A - Glossário de Termos.

Julho de 2022. Revisão intermediária. Foram feitas pequenas alterações editoriais.

Outubro de 2021. Revisão intermediária. Atualização da referência a testes de baterias (Seção 2.7).

Julho de 2021. Revisão intermediária. Atualização e esclarecimentos sobre:

A. Segurança do SCI

i. Gerenciamento de acesso
ii. Gerenciamento de configuração
iii. Gerenciamento de correções de segurança
iv. Dispositivos de proteção de rede

B. Operações de SCI

i. Procedimentos operacionais de emergência

C. Recomendação sobre construção e incêndios

Julho de 2020. Revisão intermediária. Atualização da orientação sobre planejamento de contingência e sobressalentes.

Outubro de 2019. Esta é a primeira edição deste documento.