Cibersegurança em Sistemas de Controlo Industrial (janeiro de 2023)

Filipe Bagagem Nº 2220558 e Pedro Marques Nº 2220562,
Estudantes do Mestrado em Cibersegurança e Informática Forense do Instituto Politécnico de Leiria

***Resumo* — Nos últimos tempos, o termo cibersegurança tem sido cobiçado nas mais diversas áreas, até nos ICS *(industrial control systems)*, que significa Sistemas de Controlo Industrial, não são uma exceção. Existem vários tipos de ICS, os mais conhecidos são os DCS (Sistemas de Controlo Distribuído), SCADA (Controlo de Supervisão e Aquisição de Dados), PLCs (Controladores Lógicos Programáveis) e SIS (Sistemas Instrumentados de Segurança). Por vezes, a segurança do ICS também é abordada por Segurança SCADA ou Segurança do Sistema de Controlo Industrial. Todos eles são usados para monitorizar e controlar processos em todos os tipos de indústrias e setores, como por exemplo: plataformas de petróleo/gás, minas, refinarias de petróleo, fábricas de manufatura, fábricas de papel, redes elétricas, abastecimento de redes de água e muitas outras áreas. Muitos desses sistemas são sistemas antigos, já com décadas e vulneráveis a ataques cibernéticos.**

***Termos de* Índice: Cibersegurança, Controlo Industrial, Sistema, ICS, Segurança, DCS, SCADA, OT, IT.**

I. Introdução

Os Sistemas de Controlo Industrial referem-se a uma vasta gama de sistemas que monitorizam e medem parâmetros, controlam e/ou automatizam processos na maior parte das indústrias e setores. Muitos destes sistemas foram projetados numa época em que as ameaças à segurança eram inexistentes, porque a única forma de atacar um sistema destes era o criminoso fazê-lo presencialmente.

Geralmente, estes sistemas estão localizados em Salas de Controlo que têm uma segurança de perímetro muito boa e com controlos de acesso. Tipicamente, estes sistemas antigos têm computadores (terminais de operadores e de engenharia) com versões de sistemas operativos já descontinuados pelo fabricante (Windows CE e Windows XP), porque não necessitarem de versões mais recentes para executar as tarefas do dia a dia. Os responsáveis pelas operações (como os operadores de fábrica) controlam e monitorizam todo o sistema através destes terminais existentes numa Sala de Controlo, como por exemplo: iniciar/parar bombas, abrir/fechar válvulas, etc., é o típico posto de trabalho de um operador DCS. Os terminais de engenharia são utilizados para programar os controladores, os *dashboards*, entre outro tipo de parametrização.

Os Sistemas de Computação referidos anteriormente fazem parte da Tecnologia Operacional, dentro destes é que surge o ICS (Sistemas de Controlo Industrial), que por sua vez podem ter os vários tipos, conforme ilustrado na figura 1.

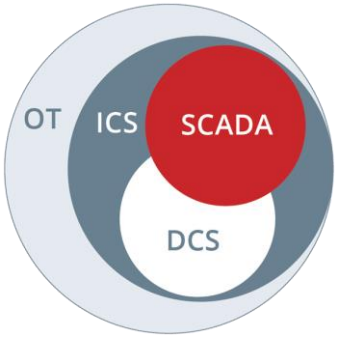

Figura 1 - Tecnologia Operacional

Neste artigo, descrevemos o que é um **Sistema de Controlo Industrial** no Capítulo II e no Capítulo III apresentamos os **Tipos de Sistemas de Controlo Industrial**. No Capítulo IV e V indicamos quais são os **Componentes de um Ambiente de ICS** e as **Comunicações Dentro do ICS**, respetivamente. No Capítulo VI e VII elencamos as **Vulnerabilidades de Segurança do ICS** e as **Ameaças Comuns aos ICS**, respetivamente. No Capítulo VIII listamos as **Considerações de Cibersegurança** que entendemos serem as mais emergentes, e a diferença entre a defesa ativa e passiva. No Capítulo IX, indicamos alguns dos **Impactos dos Eventos de Cibersegurança** podem trazer às organizações. No Capítulo X listamos as **Boas Práticas e Recomendações** e um resumo dos fatores mais cruciais com a cibersegurança nos ICS. No Capítulo XI, apresentamos um **Ambiente de Simulação**. No Capítulo XII, os **Testes e Resultados** obtidos no Ambiente de Simulação. E por último, para finalizar o artigo, apresentamos o que há a fazer como **Trabalho Futuro**.

II. Sistema de Controlo Industrial (ICS)

Sistema de Controlo Industrial (ICS) é um termo utilizado para descrever diferentes tipos de sistemas de controlo e instrumentação associada à Indústria, que incluem dispositivos, sistemas, redes e controlos utilizados para operar e/ou automatizar processos industriais.

Dependendo do setor, cada ICS funciona de maneira diferente e é projetado para gerir tarefas eletrónicas com eficiência. Atualmente, os dispositivos e protocolos utilizados num ICS são aplicados de forma transversal a todos os setores industriais e infraestruturas críticas, como manufatura, transporte, energia e indústrias de tratamento de água.

III. TIPOS DE SISTEMAS DE CONTROLO INDUSTRIAL

Existem vários tipos de ICS, sendo os mais comuns os sistemas de controlo distribuído (DCS) e os sistemas de controlo de supervisão e aquisição de dados (SCADA). As operações locais são frequentemente controladas pelos chamados Dispositivos de chão de fábrica que recebem comandos de supervisão das estações remotas.

Controlo de Supervisão e Aquisição de Dados (SCADA)

O SCADA não é um sistema que oferece controlo total. Pelo contrário, as suas capacidades concentram-se em fornecer apenas controlo ao nível da supervisão. Os sistemas SCADA são compostos por dispositivos, geralmente controladores lógicos programáveis (PLC) ou outros módulos de hardware. Os sistemas SCADA podem recolher e transmitir dados, e estão integrados com uma Interface de Máquina Humana (HMI) que fornece monitorização e controlo centralizado para inúmeras entradas e saídas de processos, conforme ilustrado na Figura 2.

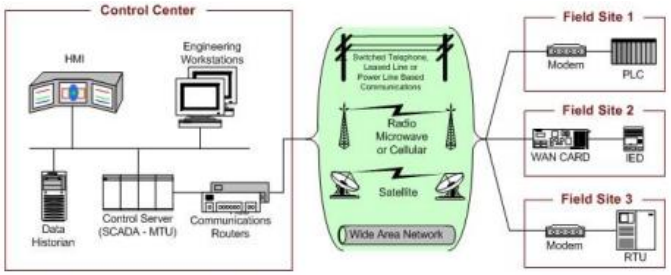

Figura 2 - Arquitetura SCADA
Fonte: https://nvlpubs.nist.gov/

O objetivo principal da utilização do SCADA é a monitorização e controlo de longa distância dos locais de chão de fábrica através de um sistema de controlo centralizado. Em vez de os trabalhadores terem de percorrer longas distâncias para executar tarefas ou recolher dados, um sistema SCADA automatiza estas tarefas. Os dispositivos de chão de fábrica controlam operações locais como a abertura ou o fecho de válvulas e/ou disjuntores, e permitem a recolha de dados dos sensores para uma monitorização efetiva de todo o ambiente, e se necessário alarmar o operador. [1]

Sistema de Controlo Distribuído (DCS)

O DCS é utilizado para controlar os sistemas de produção na mesma localização geográfica, nas mais diversas indústrias.

Num DCS, é enviado um ponto de *setpoint* (ponto de ajuste) ao controlador e este tem a capacidade de instruir as válvulas, ou mesmo um atuador. Os dados do chão de fábrica podem ser guardados para referência futura, utilizados para um simples controlo de processos, ou mesmo utilizados para posteriormente tomar outro tipo de decisões.

Cada DCS utiliza um ciclo centralizado do controlo de supervisão para gerir vários controladores ou dispositivos locais que fazem parte do processo global de produção. Isto permite que as indústrias tenham a capacidade de aceder rapidamente aos dados de produção e operação. Permite também utilizar vários dispositivos dentro do processo de produção, um DCS tem a capacidade de reduzir o impacto de uma falha pontual, dentro de todo o sistema industrial.

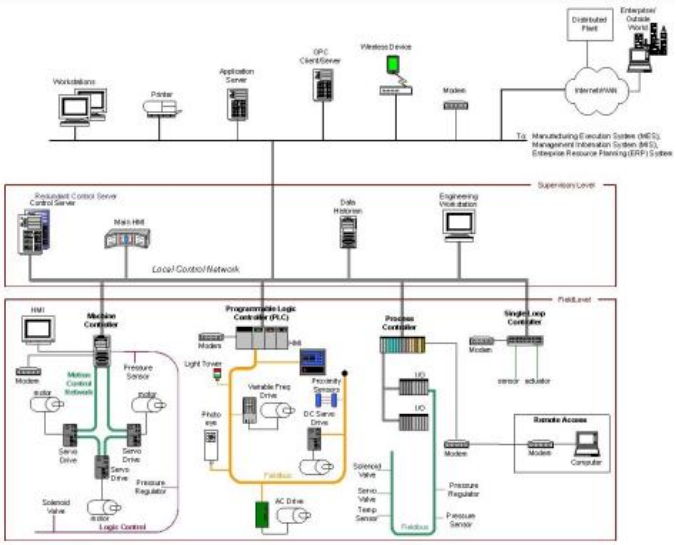

Figura 3 - Arquitetura DCS
Fonte: https://nvlpubs.nist.gov/

IV. COMPONENTES DE UM AMBIENTE ICS

IT (Tecnologia da Informação) e OT (Tecnologia Operacional)

A Tecnologia Operacional (ou, em inglês, Operational Technology - OT), tem como variáveis, protocolos específicos e sistemas de hardware e software que monitorizam e controlam dispositivos físicos no chão de fábrica. As tarefas OT variam de indústria para indústria, cada uma tem as suas especificações.

A Tecnologia da Informação (ou, em inglês, Information Technology — IT) pode ser definida como o conjunto de todas as atividades e soluções provenientes de recursos computacionais que permitem obter, armazenar, proteger, processar e gerir a informação. Na figura abaixo é possível verificar as diferenças entre uma tecnologia e outra.

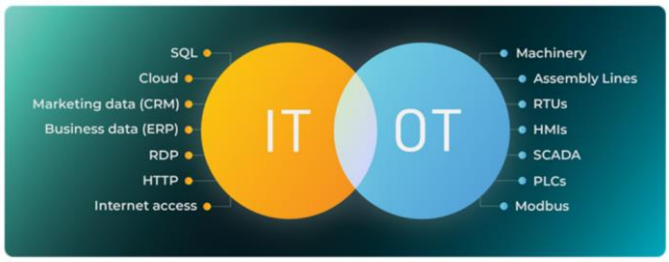

Figura 4 - Diferenças IT e. OT

A junção das redes IT com as redes OT proporcionam às empresas uma maior integração dos sistemas, em muitos casos permite tomar decisões rápidas porque têm uma visão global de todo o sistema e permite obter dados precisos. Por outro lado, a junção destes dois componentes (OT com IT) torna os sistemas ICS mais vulneráveis a ataques cibernéticos. Infelizmente, continuam a ser muitas as organizações que têm a infraestrutura OT exposta a ciberataques.

Controlador lógico programável (PLC)

Este é um tipo de hardware que é utilizado tanto em sistemas DCS como em sistemas SCADA como um componente de controlo. Também fornece a gestão local de processos que estão a ser executados através dos dispositivos de controlo, permitindo obter o feedback dos sensores e atuadores.
No SCADA, um PLC fornece a mesma funcionalidade que as Unidades de Terminal Remoto (RTU). No DCS, os PLCs são utilizados como controladores locais no âmbito de um regime de controlo de supervisão. Os PLCs também são implementados como componentes primários em configurações de sistema de controlo de menor dimensão.

Unidade de Terminal Remoto (RTU)

Um RTU é um dispositivo de chão de fábrica controlado por microprocessadores que recebe comandos e envia informações de volta para a MTU (*Master Terminal Unit*).

Ciclo de controlo

Cada ciclo de controlo é composto por hardware como PLC's e atuadores. O circuito de controlo interpreta sinais dos sensores, válvulas, disjuntores, interruptores, motores e outros dispositivos semelhantes. Os valores dos sensores são transmitidos ao controlador para este realizar uma tarefa e/ou completar um processo.

Interface da Máquina Humana (HMI)

Uma aplicação gráfica de interface de utilizador (GUI) que permite a interação entre o operador humano e o hardware do controlador. Também pode apresentar informações de estado e histórico de dados recolhidos pelos dispositivos no ambiente do ICS. Também é utilizado para monitorizar, configurar *setpoints*, algoritmos de controlo, ajustar e definir novos parâmetros para os controladores.

Diagnóstico remoto e manutenção

Este é um termo usado para identificar, prevenir e recuperar de operações anormais ou falhas.

Servidor de Controlo

Um servidor de controlo acolhe o software de controlo de supervisão DCS ou PLC e comunica com dispositivos de controlo de nível inferior.

Servidor SCADA ou Unidade de Terminais Principais (MTU)

Este é um dispositivo que emite comandos para RTUs.

Dispositivo Eletrónico Inteligente (IED)

É um dispositivo inteligente com a capacidade de obter dados, comunicar com outros dispositivos e processar a informação de forma autónoma. A utilização de IED em sistemas de controlo como o SCADA e o DCS permite que os controlos a nível local sejam automatizados.

Histórico de Dados

Um histórico de dados é uma base de dados centralizada para registar toda a informação dos processos num ambiente ICS. Os dados guardados são então utilizados para análise de processos, controlo de processos estatísticos e para se definirem estratégias empresariais.

Na figura 5, é possível verificar como os componentes descritos anteriormente, estão relacionam num ICS. [2]

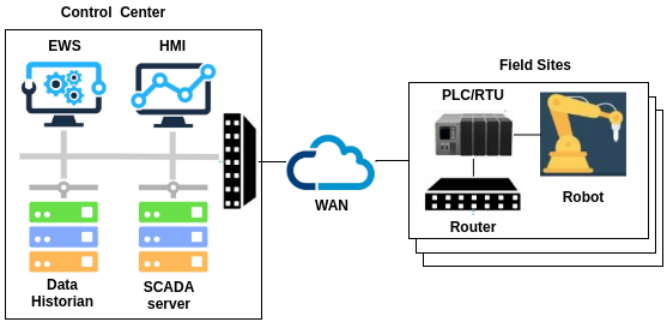

Figura 5 - O típico sistema SCADA

V. COMUNICAÇÃO DENTRO DOS ICS

Os dispositivos e módulos de controlo nos sistemas ICS transmitem informações através de protocolos de comunicação. Existem vários protocolos de comunicação que são utilizados nos mais diversos ambientes ICS. A maioria destes protocolos são projetados para fins específicos como automatização de processos, automação de edifícios, automatização de sistemas de energia, e muito mais. Estes protocolos foram também desenvolvidos para garantir a interoperabilidade entre diferentes fabricantes. No entanto, existem alguns protocolos proprietários que só permitem integração com outras tecnologias do próprio fabricante. Na figura 6, é possível observar a quota de mercado que cada protocolo tinha em 2017.

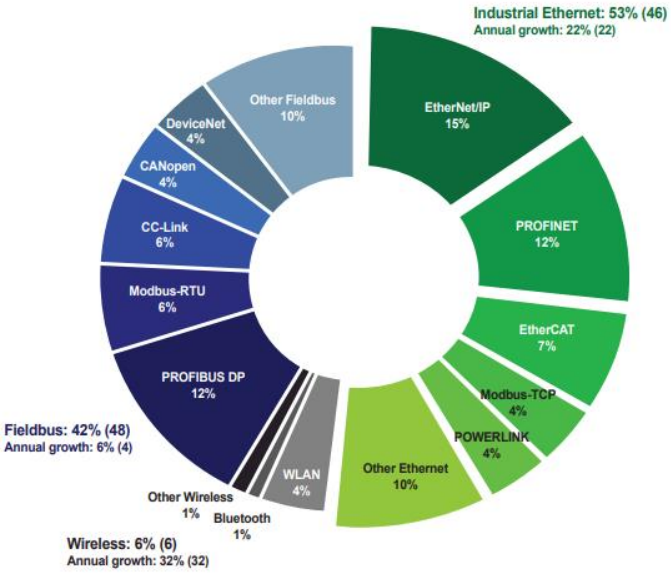

Figura 6 - Quota de Mercado – Rede Industrial (2017)
Fonte: HMS

Os protocolos ICS normalmente utilizam:

Process Field Bus (PROFIBUS)

Profibus utiliza RTU para MTU, MTU para MTU, e RTU para comunicações RTU no chão de fábrica. Existem duas variantes disponíveis: Profibus DP (periféricos descentralizados), que

são utilizados para operar sensores e atuadores através de um controlador central, e a Profibus PA (automatização de processos), que é utilizador para monitorizar equipamentos de medição através de um sistema de controlo de processos**.**

Protocolo de Rede Distribuído (DNP3)
Este é um protocolo com três camadas, que opera na camada ligação de dados, aplicação e transporte. Este protocolo é amplamente utilizado em estações elétricas e de tratamento água.

Modbus
Desde a sua introdução em 1979, o Modbus é considerado um dos mais antigos protocolos do ICS. A Modbus utiliza comunicações em série com os PLCs e tem sido o protocolo de comunicações mais utilizado nos ambientes ICS. Existem dois tipos do Modbus: Serial Modbus – que utiliza a norma de controlo de ligação de dados de alto nível (HDLC) para transmissão de dados, e a Modbus TCP – que utiliza a pilha de protocolar TCP/IP para transmitir os dados.

Comunicação de plataforma aberta (OPC)
O OPC tem série de normas e especificações para comunicações industriais. A especificação OPC baseia-se em tecnologias desenvolvidas pela Microsoft, para o sistema operativo Windows (OLE, COM e DCOM).

Redes de Automação e Controlo de Edifícios (BACnet)
Trata-se de um protocolo de comunicação concebido para controlar o aquecimento, ventilação e controlo do ar condicionado (AVAC); iluminação; e deteção de incêndios.

Protocolo Industrial Comum (CIP)
Um CIP é um conjunto de serviços e mensagens para controlo, segurança, sincronização, configuração, informação, etc. O CIP pode ser integrado nas redes de Ethernet. O CIP permite também a integração com diferentes tipos de redes.

Ethernet para Tecnologia de Automação de Controlo (EtherCAT)
Um protocolo de comunicações de código aberto usado para incorporar o Ethernet em ambientes industriais. O EtherCAT é utilizado em aplicações de automação com ciclos de atualização curta (≤ 100µs) e com nervosismo ≤ 1µs.

VI. Vulnerabilidades de segurança do ICS

No mundo de hoje, os sistemas de controlo industrial que suportam a infraestrutura crítica estão cada vez mais vulneráveis, pelas seguintes razões:

Dispositivos expostos à Internet: Ligar o ICS à Internet sem implementar medidas de segurança, dá a possibilidade dos atacantes identificarem vulnerabilidade e *backdoors* nos sistemas que estão implementados no ambiente ICS.

Validar as configurações padrão: as configurações dos equipamentos ICS por omissão, não oferecem segurança suficiente, mas as empresas nem sempre têm os recursos preparados para lidar com *patches* e criar políticas para reconfigurar os dispositivos.

Segmentação de redes entre IT e OT: A forte segregação entre ambientes é um passo crítico para impedir que os ataques se espalhem da rede IT para sistemas OT.

Pontos fracos dos aplicativos ICS: os aplicativos ICS e HMI podem ser particularmente vulneráveis a ataques como captura de credenciais e sessões, manipulação de parâmetros e comandos de *SQL injection*.

Treino ao nível da segurança insuficiente: os funcionários/operadores podem facilmente ser vítimas de todos os tipos de ataques, como por exemplo: engenharia social, *phishing*, entre outros bem conhecidos. Os funcionários devem ser treinados para desenvolver uma consciência básica na área da segurança.

Como é possível verificar na figura 7, o número de recomendações tem aumentado de ano para ano. Embora se verifique um crescimento exponencial em 2021. As recomendações ICS-CERT são publicadas quando uma vulnerabilidade do ICS é conhecida. [3]

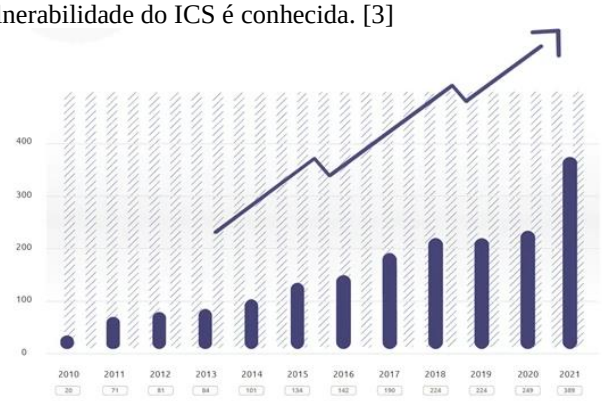

Figura 7 - Recomendações ICS-CERT por ano
Fonte: trendmicro.

VII. Ameaças comuns aos ICS

Por estarem subjacentes a infraestruturas críticas, os sistemas de controlo industrial são particularmente apelativos para a prática de ciberataques. A importância diária das empresas petrolíferas, gás, serviços de água e das fábricas manufatura, posicionam os ambientes ICS como alvos de alto valor e lucrativos aos olhos dos mal-intencionados. Os ataques a sistemas críticos, como os ICS, já não são uma novidade, na figura 8, é possível verificar os ataques com maior relevância compreendidos entre o ano 2010 e 2020.

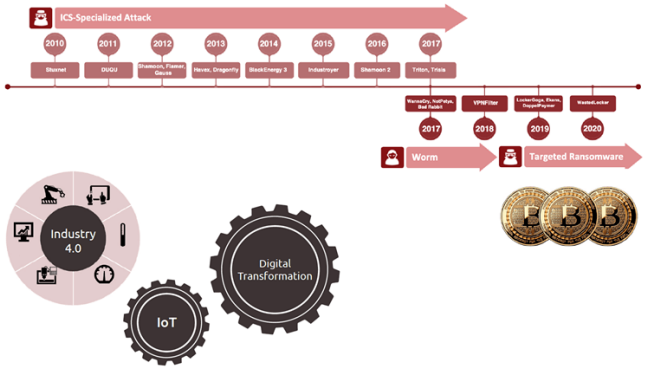

Figura 8 - Timeline das ameaças cibernéticas do ICS de 2010 a 2020
Fonte: trendmicro.

As ameaças mais populares à segurança do ICS incluem:

Ataques de malware: É relativamente fácil, um funcionário transportar malware através de um dispositivos de armazenamento externo, do escritório/casa para um ambiente ICS; Por exemplo, o Stuxnet foi introduzido pela primeira vez na Siemens quando um funcionário utilizou uma unidade USB infetada no ambiente ICS.

Ataques de negação de serviço: Os sistemas ICS dependem de alta disponibilidade para funcionarem, logo as interrupções de serviço são muito dispendiosas. Os ataques do DoS a componentes individuais (como PLCs) ou à infraestrutura de rede ICS (com fios ou sem fios) podem causar grandes interrupções dos serviços operacionais.

Ataques internos: O comportamento dos funcionários pode levar a ataques internos, sejam eles por negligência ou intencionais. Funcionários descontentes, que têm rendimentos baixos, funcionários sem formação em segurança, são alguns dos exemplos que representam sérias ameaças.

VIII. CONSIDERAÇÕES DE CIBERSEGURANÇA

À medida que as empresas adotam novas tecnologias para melhorar a eficiência operacional, estas devem estar cientes dos riscos na segurança cibernética que as tecnologias OT, IT, IoT e IIoT podem acrescentar.

Entre os riscos, estão:

- Expansão da superfície de ataque do ICS, o que pode levar a um aumento de eventos de insegurança.
- Eliminação da segmentação de rede dos sistemas OT com as redes IT, resultando numa maior exposição dos sistemas críticos.
- Sistemas cada vez mais suscetíveis a contrair *malware* e *ransomware* devido à transição digital nas redes IT, o que pode levar a uma interrupção de processos físicos.

Defesa cibernética passiva e ativa

As tecnologias e práticas defensivas recomendadas pelos consultores de segurança não são suficientes para impedir ataques aos sistemas, porque não existem sistemas 100% seguros, mas são um ponto de partida. Os Sistemas de Controlo Industrial requerem um programa de defesa ativo para enfrentar ataques avançados e direcionados, por estarem classificados como um ambiente crítico.

Os ciberataques são uma grande preocupação para as organizações industriais de todo o mundo. A maior parte das organizações reconhece que é necessário investir em tecnologia, seguindo as recomendações dos consultores de segurança, para aplicar segurança defensiva. Embora não seja suficiente, aplicar só medidas de segurança passiva, porque na maior parte dos casos não é suficiente para parar ataques avançados e/ou direcionados.

Para lidar com estes riscos, as organizações industriais necessitam de um programa de defesa ativo, orientado por inteligência. O Instituto SANS define a defesa ativa como "*the process of analysts monitoring for, responding to, and learning from adversaries internal to the network*". A defesa ativa requer pessoas experientes, processos comprovados e tecnologia *fit-foruse*. As pessoas certas têm conhecimentos especializados em cibersegurança, sistemas de controlo e processos industriais. Os processos certos refletem uma compreensão do comportamento do atacante e das boas práticas do defensor. A tecnologia certa integra a deteção de comportamentos suspeitos com capacidades para uma investigação e resposta eficazes e eficientes, conforme ilustrado na figura 9.

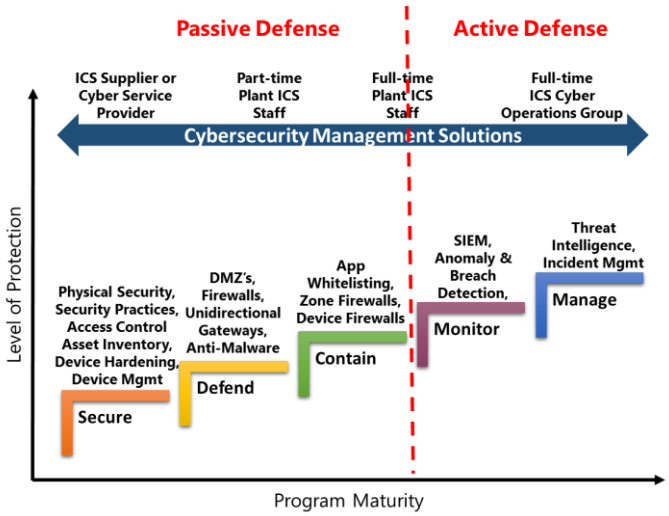

Figura 9 - Modelo de Cibersegurança - Defesa Passiva e Ativa
Fonte: arcweb

O modelo da ARC divide a cibersegurança num conjunto de etapas que reduzem gradualmente os riscos cibernéticos. Cada etapa aborda um problema de segurança específico, como **proteger** dispositivos individuais, **defender** *plants* de ataques externos, **conter** malware que pode vir a entrar num sistema de controlo, **monitorizar** os sistemas para tentar identificar atividades suspeitas e **gerir** ativamente as ameaças sofisticadas e incidentes cibernéticos. Cada etapa tem um conjunto associado de ações e tecnologias que podem ser utilizadas para atingir um objetivo específico. O modelo também mostra os recursos humanos e as ferramentas necessárias para sustentar e utilizar os investimentos em tecnologia de forma eficaz. [4]

IX. IMPACTOS DOS EVENTOS DE CIBERSEGURANÇA

Impactos a curto prazo

- Interrupções operacionais, não intencionais
- Perda da visibilidade sobre os sistemas de produção e segurança
- Perda financeira devido a interrupções e tempo de inatividade
- Roubo de propriedade intelectual
- Riscos de saúde e segurança pessoal
- Danos e destruição de bens e equipamentos
- Perda de disponibilidade
- Perda de controlo
- Negação de serviço

Impactos a longo prazo

- Custos significativos de mão de obra, que não estava prevista, como horas extras e equipamentos inativos
- Seguro aumentado ou negado pela Seguradora
- Desempenho e qualidade dos equipamentos degradados
- Taxas e processos judiciais por negligência ou incumprimento
- Perda de clientes
- Redireccionamento das despesas organizacionais para a recuperação dos sistemas

X. BOAS PRÁTICAS E RECOMENDAÇÕES

Apresentamos um conjunto de recomendações técnicas associadas ao cumprimento de padrões, boas práticas e configurações, e cuja respetiva implementação contribui decisivamente para o incremento dos níveis de cibersegurança das organizações. [5]

Gestão de risco

- Identificar ameaças à organização.
- Manter o inventário de ativos ICS atualizado com todas as tecnologias de hardware, software e ativos da infraestrutura de rede.
- Desenvolver políticas, procedimentos, treino e materiais educacionais de cibersegurança que se apliquem de forma transversal a toda a organização.
- Desenvolver e aplicar os procedimentos de resposta a incidentes, tanto em processos IT como OT.

Segurança física

- Em casos de emergência, bloquear a eletrónica do chão de fábrica e configurar mecanismos de alerta para automatizar dispositivos, como corte da energia, reiniciar os dispositivos.
- Certificar que apenas as pessoas autorizadas têm acesso a espaços onde se encontram os equipamentos ICS.
- Utilizar autenticação multifator, para controlar o acesso lógico e físico aos equipamentos e instalações ICS.

Rede ICS - Arquitetura

- Utilizar a segmentação de redes sempre que possível.
- Implementar uma topologia de rede para ICS com várias camadas, para que as comunicações mais críticas ocorram na camada mais segura e confiável.
- Utilizar *data-diodes* sempre que possível, nas comunicações (unidirecionais) para evitar acessos do exterior.
- Configurar zonas desmilitarizadas (DMZ) para criar uma sub-rede física e lógica, para evitar a exposição de dispositivos críticos.
- Implementar protocolos e serviços de rede confiáveis e seguros sempre que possível.

Rede ICS – Segurança do Perímetro

- Configurar a(s) firewall(s) para controlar o tráfego entre a rede OT (ICS) e a rede IT (Cooperativa)
- Ativar o bloqueio geográfico de IP, permitir só as localizações necessárias.
- Reforçar os níveis de segurança com as ligações externas à organização, em situações pontuais só com recurso a uma ligação por VPN.
- Utilizar servidores de salto (intermédios) como um local de autorização central entre zonas de segurança da rede ICS.
- Não permitir ligações remotas do fornecedor ou do colaborador à rede de controlo.
- Catalogar e monitorizar todas as ligações remotas à rede.

Segurança no alojamento

- Promover uma cultura de atualização e gestão de vulnerabilidades.
- Testar todas as atualizações em ambientes de teste isolados antes de aplicar as atualizações nos ambientes de produção.
- Implementar a lista de aplicativos em interfaces homem-máquina.
- Dispositivos de chão de fábrica reforçados, tais como tablets e smartphones.
- Substituir os dispositivos que possam ter o software e/ou hardware descontinuado.
- Desativar portas e serviços não utilizados nos dispositivos ICS, após testes para garantir que não afeta as operações dos ICS.
- Implementar e testar os sistemas de backups e processos de recuperação.
- Configurar encriptação e segurança nos protocolos ICS.

Monitorizar a Segurança

- Medir a linha de base das operações normais e do tráfego de rede nos ICS.
- Configurar os Sistemas de Deteção de Intrusão (IDS) para criar alarmes para qualquer tráfego de rede ICS fora dos padrões normais.

- Investigar e monitorizar os registos das auditorias nas áreas mais críticas dos ICS.
- Configurar a monitorização de incidentes e eventos de segurança (SIEM) para monitorizar, analisar e correlacionar registos de eventos de toda a rede ICS para identificar tentativas de intrusão.

Gestão da Cadeia de Abastecimento

- Ajustar o processo de aquisição do ICS para avaliar fortemente a cibersegurança como parte da metodologia de classificação e avaliação.
- Investir antecipadamente em produtos ICS seguros, avaliando a segurança contra ameaças atuais e futuras durante a vida útil do produto/projeto.
- Estabelecer acordos contratuais para todos os serviços subcontratados que garantam: tratamento e *report* adequados de incidentes, segurança das interconexões e especificações e processos de acesso remoto.
- Considerar a integridade e a confidencialidade da segurança da informação nos ICS ao contratar um provedor de serviços na Cloud.
- Aproveitar os laboratórios de simulação para testar o software disponibilizado pelo fornecedor com código malicioso e/ou defeituoso, antes da implementação nos dispositivos de produção.

Elemento Humano

- Emitir políticas que descrevam as regras de segurança do ICS, incluindo as regras de comportamento esperadas e controlos necessários.
- Emitir procedimentos que estabeleçam como os colaboradores devem operar os ICS de forma segura.
- Treinar os operadores do IT, os operadores do OT e os outros elementos envolvidos na segurança para terem conhecimento dos indicadores dum potencial comprometimento e quais as etapas a seguir para garantir que uma investigação cibernética seja bem-sucedida.
- Promover uma cultura de diálogo e troca de informações entre os elementos que estão envolvidos com a segurança dos sistemas, incluindo o IT e OT.

Alguns factos importantes em resumo

1. Quando se trata de cibersegurança, não há 100% de garantia. É necessário treinar as pessoas e os sistemas para detetar e prevenir o mais cedo possível.
2. Vista geral do Sistema de Controlo Industrial. Se não conseguem ver o que transita nas redes, não vão conseguir evitar os ataques.
3. Não é suficiente resolver todos os problemas de segurança de uma empresa apenas com uma Tecnologia. É necessário envolver as pessoas, os processos, a própria tecnologia.
4. O investimento em cibersegurança, normalmente, resulta numa maior disponibilidade dos Sistemas.
5. Reduzir o risco proveniente dos fornecedores. Considerar os requisitos de cibersegurança, dos componentes mais críticos, nos RFQ (Request for Quotation).
6. Correlacionar as redes IT com as redes OT para obter os logs e tráfegos, é uma das principais medidas para se ter uma vista geral de todo o ambiente IDS.
7. Muito se pode fazer para proteger os sistemas de controle industrial com medidas não intrusivas.

XI. Ambiente de Simulação

Com a inovação da Indústria 4.0 as empresas de produção têm a oportunidade de implementar sistemas que lhes permite automatizar as suas linhas de produção, rentabilizando equipamentos e recursos humanos. Desta forma a questão da cibersegurança ganha uma importância vital para a preservação de dados, processos e ativos.

O ambiente de simulação (AS) proposto pretende fazer um estudo da implementação de cibersegurança em sistemas de controlo industrial, servindo de linhas orientadoras na implementação deste tipo de sistema. Pretende também verificar a implementação de medidas de segurança que permitam mitigar o risco de ataques cibernéticos. Na figura 10, apresentamos uma captura da Interface da Máquina Humana (HMI), do ambiente de simulação.

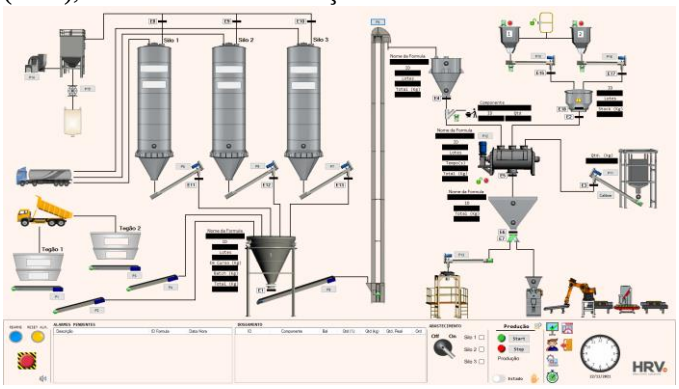

Figura 10 – Ambiente de Simulação (HMI)

O AS é uma linha de produção automatizada de compostos para pavimentos na área da construção civil que integra os seguintes equipamentos:

- **Linha de Produção**: 3 silos, 2 tegões, 1 balança, 1 elevador, 1 misturadora, 1 deposito superior, 1 deposito inferior, 1 adição manual com balança, 1 adição por tempo, 1 linha de ensaque robotizada.
- **Automação**: PLC (Programmable Logic Controllers) Siemens Simatic S7 – 1500.
- **Gestão de Produção e Supervisão**: HRVDOSWIN (Programa de Gestão Industrial e Controlo), MSSQL Server.
- **Comunicações**: Ethernet, Profinet (Padrão de comunicação Ethernet Industrial), Ixon IX 2400 (VPN Router & Gateway), Sophos UTM
- **Protocolos**: TCP, MQTT, S7.

Os equipamentos da linha de produção são totalmente controlados pelo PLC que tem a função de controlar os inputs e outputs dos equipamentos da linha e controlo da gestão do processo que compreende a sequência de encadeamento da

produção desde o início até ao fim do ciclo produtivo. A rede de automação está isolada através do equipamento Ixon IX 2400 (VPN Router & Gateway) que permite ligações remotas através de uma VPN.
O HRVDOSWIN é a aplicação que controla a fase produtiva e de gestão. Através do ecrã de supervisão são controlados todos os equipamentos e mostrados os valores dos vários sensores. O ecrã de gestão permite fazer toda a gestão de produto final, matérias-primas, realizar pedidos de produção, extrair relatórios e integrar com o ERP. O modelo físico utilizado no Ambiente de Simulação está representado na figura 11.

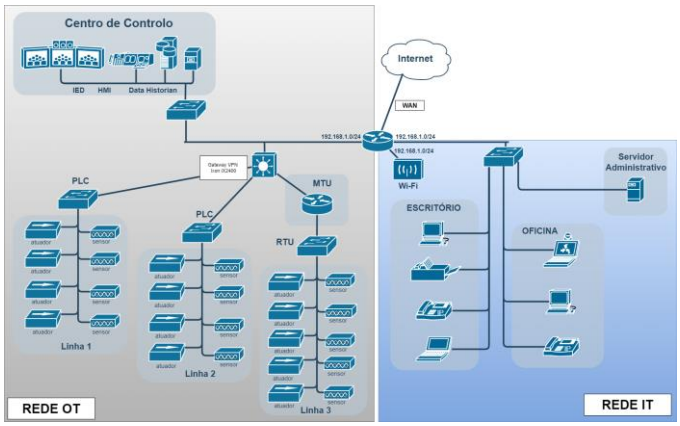

Figura 11 – Modelo Físico (AS)

XII. TESTES E RESULTADOS

Com o ambiente de testes apesentado pretendeu-se de uma forma prática e num ambiente próximo do real implementar uma solução de segurança baseado em testes funcionais, demonstrando desta forma as limitações e dificuldades da implementação da solução, nomeadamente as de segurança. As soluções e equipamentos aplicados no AS mostraram-se eficazes na arquitetura inicial conseguindo cumprir com a confidencialidade, integridade, privacidade e disponibilidade dos dados, para este teste recorreu-se ao Wireshark (figura 12).

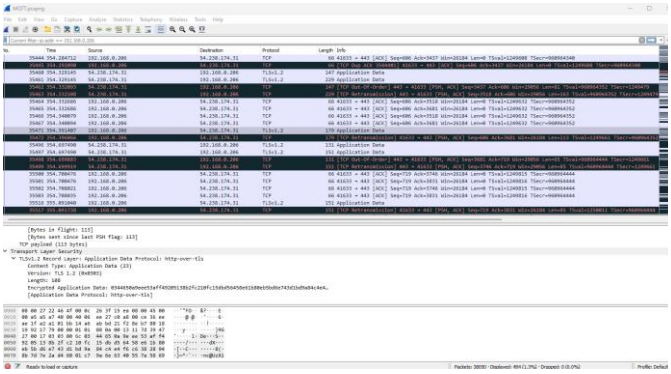

Figura 12 – Captura de Pacotes (Wireshark)

Foram, no entanto, identificados alguns pontos de falha que poderiam resultar no comprometimento do computador de gestão/supervisão, este computador tem duas placas de rede permitindo a ligação à rede da automação e à rede corporativa, o comprometimento deste equipamento poderá levar ao comprometimento também da rede de automação e consequentemente ao comprometimento da linha de produção. Identificou-se ainda uma vulnerabilidade ao nível dos PLC que poderia comprometer a rede de automação, conforme ilustrado na figura 13. [6]

Figura 13- Vulnerabilidade PLC Siemens S7-1500

A segmentação da rede por forma a isolar rede de automação, através do equipamento IXON permite-nos mitigar ataques diretos direcionados ao PLC e/ou dispositivos da rede de automação.
De seguida apresentamos um novo modelo físico, para a mesma infraestrutura de rede (OT e IT), mas com níveis de segurança mais elevado, conforme é possível verificar na figura 14.

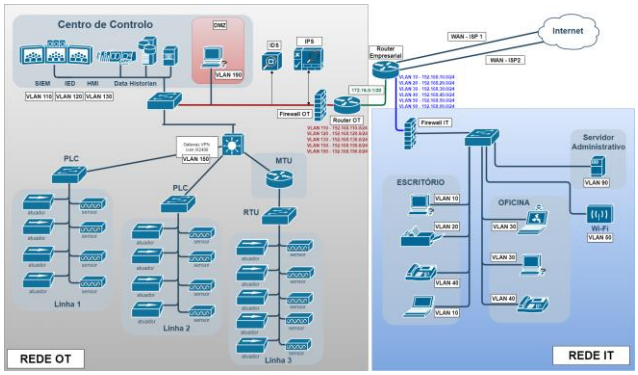

Figura 14 - Arquitetura Final

XIII. CONCLUSÕES

À medida que as ICS crescem em complexidade e se ligam a redes empresariais e externas, o número de potenciais problemas de segurança e os seus riscos associados também aumentam. A grande variedade de vetores de ataque que visam múltiplos recursos em sistemas de controlo industrial podem dar origem a ataques assíncronos durante um longo período de tempo e podem visar múltiplas fraquezas dentro de um ambiente de sistemas de controlo industrial. As organizações não podem depender de uma única contramedida para mitigar todas as questões de segurança. Para proteger eficazmente os ICS de ataques cibernéticos, as organizações devem aplicar múltiplas contramedidas, reduzindo assim o risco recorrendo a

uma série de técnicas de mitigação da segurança. Note-se que as medidas de defesa em profundidade não protegem nem podem proteger todas as vulnerabilidades e fraquezas num ambiente ICS. As técnicas são aplicadas, principalmente, para dificultar a tarefa dos atacantes, permitindo assim os responsáveis pela segurança (IT e OT), possam ser alertados para darem resposta às ameaças em curso.

XIV. TRABALHO FUTURO

Como trabalho futuro, e em complemento a este artigo, gostaríamos de aprofundar quais as vantagens e desvantagens ao nível da cibersegurança, em aplicar, de forma global (interempresas), a inteligência artificial para automatizar o controlo de sistemas industriais.

XV. BIBLIOGRAFIA

[1] NIST, “NIST,” [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[2] medium, “medium,” [Online]. Available: https://laurentbalmelli.medium.com/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633.

[3] trendmicro, “trendmicro,” [Online]. Available: https://www.trendmicro.com/pl_pl/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

[4] arcweb, “arcweb,” [Online]. Available: https://www.arcweb.com/blog/ics-cybersecurity-requires-passive-active-defense.

[5] CISA, “CISA,” [Online]. Available: https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[6] thehackernews, “thehackernews,” [Online]. Available: https://thehackernews.com/2023/01/over-100-siemens-plc-models-found.html?m=1.

XVI. AUTORES

Filipe Bagagem nasceu em Leiria, Portugal em 1985. Licenciou-se em Engenharia Informática no Instituto Politécnico de Leiria, em 2015. Diretor Técnico / Operações na MICROABREU, Lda.

Pedro Marques nasceu em Portalegre em 1976. É Mestre em Engenharia Informática– Computação Móvel pelo Instituto Politécnico de Leiria em 2012. Responsável pelo Departamento de TI da HRV – Equipamentos de Processo S.A.

Link para o vídeo >>
https://www.youtube.com/watch?v=k2avE0Ezl6c