



# Cibersegurança na Indústria 4.0



MATERIAL ELÉCTRICO & AUTOMATISMOS INDUSTRIAIS, LDA.

# Ciberegurança na Indústria 4.0

A “quarta revolução industrial” está a acontecer agora. Diz-se que esta vai trazer grandes mudanças na forma como a sociedade produz e faz negócios. Há uma esperança, de que estas mudanças conduzam a um salto na produtividade e na eficiência dos negócios. Como tal, a segurança é uma prioridade nesta nova era industrial

A primeira revolução industrial surgiu com a utilização de máquinas a vapor e de energia hidráulica nas fábricas. A segunda foi viabilizada pela utilização da electricidade e pela produção em massa. A terceira revolução industrial começou há não muito tempo, com a introdução dos computadores, melhorando os processos de automação e de fabrico. A quarta revolução industrial é conduzida pela “Internet das Coisas”, uma mistura de tecnologias que conduzem à criação de um ambiente de produção “cibernético-físico”, “inteligente” e altamente versátil. Envolve vários sensores inteligentes, robots ligados entre si, impressão 3D, uma vasta análise de dados e canais de comunicação que enviam enormes quantidades de dados de um lado para outro. A ideia é que, em conjunto, todas estas inovações permitirão criar produtos com maior qualidade e com elevado nível de personalização, de forma mais rápida e com um custo inferior o que tornará as linhas de produção mais eficientes.

Um dos maiores desafios para a implantação das fábricas inteligentes do futuro é representado pela cibersegurança. O problema é que muitas das tecnologias, conceitos e protocolos que colectivamente formam a Indústria 4.0 são antigos, sendo que a maioria não foi projectada para hiperconectividade omnipresente. E uma vez que estamos no início desta nova era inovadora, os riscos são bastante elevados - tal como aconteceu nas revoluções industriais um, dois e três.

## O que é a Internet das coisas?

A Internet das Coisas é um conceito tecnológico onde os objectos da vida quotidiana estão ligados à internet, agindo de forma inteligente e sensorial. Ao incorporarem electrónica, software e sensores, esses objectos que estão ligados à rede podem receber, enviar e trocar dados entre si.

Este conceito, cria oportunidades para uma integração mais directa do mundo físico com sistemas informáticos, resultando numa maior eficiência, precisão e benefício económico, para além da redução da intervenção humana.

Quando a Internet das Coisas é aumentada através da utilização de sensores e actuadores, a tecnologia torna-se um exemplo da classe mais geral de sistemas ciberfísicos, que abrange também tecnologias como redes inteligentes, casas inteligentes, transporte inteligente e cidades inteligentes. Cada “coisa” é identificável exclusivamente através do seu sistema de software incorporado e é capaz de interoperar dentro da infraestrutura de Internet existente.

Os especialistas estimam que a Internet das Coisas irá abranger quase 50 biliões de objectos até 2020.

Em cada uma das revoluções industriais anteriores, as novas tecnologias tornaram possível processar ou produzir de forma mais rápida, em volumes maiores, a temperaturas mais elevadas, em ambientes mais agressivos, etc.. Cada revolução industrial trouxe consigo, novos riscos. O facto de muitas fábricas operarem hoje em dia, 24 horas por dia e 365 dias por ano sem quaisquer incidentes, demonstra que as tecnologias utilizadas nelas, atingiram um elevado nível de fiabilidade.

Hoje em dia, as grandes corporações receiam a violação de dados em larga escala. O custo dos ciberataques de alto perfil é imenso. Mas no caso dos sistemas ciberfísicos, os danos potenciais causados por um ataque de computador podem ser ainda maiores. Se eventualmente, hackers maliciosos tentassem causar o máximo de danos possíveis numa grande fábrica química, o potencial de desastre seria avassalador.

Naturalmente, a tendência de tudo ao nosso redor tornar-se autónomo não vai parar. No entanto, os engenheiros que projectam novos equipamentos têm de ter em mente as implicações de segurança. Igualmente importante é desenvolver e implementar padrões de segurança para tecnologias ligadas entre si e principalmente para a Internet industrial.

# Ciberegurança na Indústria 4.0



## Segurança

O objectivo da Indústria 4.0 é a comunicação orientada ao último ponto da cadeia em todas as áreas dos sistemas envolvidos. Esta comunicação baseia-se no protocolo Internet (IP) e permite a transmissão de dados sem interrupções entre sistemas de nível de campo (sensores e atuadores) até ao nível de processos de negócios e as soluções ERP utilizadas nesse nível. Esta troca contínua de dados oferece muitas vantagens, mas também coloca vários desafios. Muitas empresas estão a investir em produtos inteligentes, que enviam dados de utilização e de erros de volta para essas mesmas empresas, de forma a poderem melhorar o desempenho e fiabilidade dos seus produtos.

No entanto, sempre que um dispositivo é ligado à Internet, esse mesmo dispositivo fica vulnerável a um acesso não autorizado. A Internet Industrial oferece enormes benefícios às empresas que o utilizam, mas também apresenta riscos de uso indevido e ataques cibernéticos.

### Detecção de malware desconhecido

Um cenário temido pela maioria das empresas é o acesso não autorizado a fórmulas armazenadas no sistema de controlo de uma máquina ou sistema, ou malware como o Stuxnet que pode reprogramar o software de controlo. Se os componentes de automação são sistemas baseados no Windows, os utilizadores podem assumir que o software antivírus que normalmente é instalado nos PC's fornecerá protecção suficiente. No entanto, geralmente não é o caso. Estes programas de software não podem ser utilizados devido ao comportamento em tempo real dos sistemas de automação e à falta de recursos. A necessidade constante de actualizar amostras de vírus em muitos computadores de máquinas e sistemas é ineficiente.

Através da monitorização de integridade CIFS (Common Internet File System), aparelhos de segurança oferecem uma solução para este problema. Esta tecnologia usa uma abordagem inovadora e industrial para monitorizar componentes de automação baseados no Windows para manipulação ou infecção por malware. A Monitorização de Integridade CIFS coloca pouca tensão nos recursos do sistema e pode ser utilizado sem necessidade de actualizar amostras de vírus em computadores. Mesmo os chamados vírus de "zero dias" podem ser detectados muito rapidamente.



## **Bloqueio imediato do tráfego de rede**

Para garantir uma proteção suficiente, o utilizador deve colocar um router de segurança na frente dos sistemas a serem protegidos. O componente de infra-estrutura monitoriza não apenas o tráfego de rede de entrada e de saída, mas também verifica se há alterações em determinadas áreas do sistema de arquivos dos componentes de automação baseados no Windows.

Para fazer isso, o acesso aos ficheiros Windows é fornecido ao router de segurança através do protocolo CIFS/SMB. O dispositivo analisa cíclicamente essas acções e calcula somas de verificação para os ficheiros. Se os ficheiros forem alterados, o router de segurança detectará isso com base nas somas de verificação que tenham sofrido alterações e bloqueia o tráfego de rede adicional.

Este processo também é uma boa solução para sistemas mais antigos, como aqueles que ainda funcionam com Windows 95, 98 ou XP, para os quais a Microsoft não disponibiliza mais actualizações. Se necessário, o router de segurança pode enviar ficheiros para programas anti-vírus no sistema de IT corporativo para que sejam verificados com amostras de vírus actualizadas.

## **Acesso restrito a dispositivos**

Outra fonte de risco potencial é o acesso concedido ao pessoal que presta serviço a máquinas ou sistemas. Hoje em dia, as instalações de produção apresentam aplicativos de diferentes fabricantes, e essas aplicações devem ser acessíveis pela rede ou mesmo pela Internet para fins de manutenção. Se o utilizador final conceder ao técnico de assistência técnica do fabricante da máquina acesso à rede, o técnico pode aceder a toda a sub-rede da máquina.

Para evitar isso, os “appliances” de segurança FL podem ter um firewall de utilizador que pode ser utilizado para modificar regras de firewall de acordo com o utilizador ligado no momento. Isso significa que o técnico de serviço entraria no router de segurança ao qual ele tem acesso. Só então o técnico teria acesso a dispositivos a jusante, e somente a componentes aos quais lhes foi concedido acesso.



# Ciberegurança na Indústria 4.0

## Redes cuidadosamente projectadas

As redes de comunicação devem ser, mais do que nunca, cuidadosamente planeadas e concebidas para garantir que o utilizador tenha sempre um controlo absoluto sobre os riscos que acompanham os sistemas abertos. Portanto, é absolutamente necessário que as redes cumpram a política de segurança implementada pela empresa de forma a garantir operações seguras.

Actualmente, estão também a ser desenvolvidos novos métodos de autenticação que utilizam certificados e gestão de chaves públicas, por forma a garantir que apenas exista troca de dados entre os dispositivos, através da utilização dos certificados dos dispositivos e certificados de sistema que garantam a autenticidade das partes que comunicam.

## Protecção em tempo real encriptada

Até ao momento, os estudos realizados têm demonstrado que os dispositivos de automação, como os sistemas de E/S, que estão ligados a uma rede baseada em Ethernet, podem ser mais facilmente protegidos de acesso não autorizado, utilizando os métodos existentes. Os recursos disponíveis para os componentes de campo são geralmente suficientes para garantir a transmissão segura de dados em tempo real.

Caso haja necessidade de uma maior protecção, o conceito pode ser melhorado encriptando a comunicação entre os participantes em tempo real. Neste caso, os sistemas de CPU de dispositivos de automação devem ter uma unidade de encriptação de hardware. O princípio da Indústria 4.0 é de que os sistemas de produção são auto-didáticos e auto-organizados e que podem ser ajustados de forma flexível às condições de produção conforme as necessidades. Isto requer que os sistemas de comunicação sejam flexíveis de ponta a ponta e que atendam a toda a gama de requisitos em relação à transmissão de dados em tempo real no campo, bem como o intercâmbio de dados através de soluções ERP. Por esse facto, a segurança cibernética deve ser considerada para garantir que as máquinas e os sistemas sejam protegidos de forma segura contra o acesso não autorizado.



## O que é o malware?

O termo malware é proveniente do termo em inglês Malicious software. Trata-se de um software concebido para se infiltrar num computador alheio de forma ilícita, com o intuito de causar algum dano ou roubar de informações (confidenciais ou não). Os vírus de computador, worms, cavalos de Tróia e spywares são considerados malware.

### Adware

Adware vem do inglês ad (anúncio) mais software. São programas que exibem uma grande quantidade de anúncios sem a autorização do utilizador, tornando o computador e a ligação lentos. Normalmente, assumem o formato de “pop-up”.

### Cavalo de Tróia

O cavalo de Tróia (do inglês Trojan Horse) é um tipo programa malicioso que pode entrar num computador disfarçado de programa comum e legítimo. É utilizado para criar uma “porta” que permite que utilizadores com más intenções possam invadir um PC e roubar informação. O seu nome deriva da história da Guerra de Troia e que levou à destruição dessa cidade. O cavalo de Tróia, feito de madeira, fora supostamente oferecido como um pedido de paz por parte dos gregos. Sendo um presente para o rei, os tróianos levaram o cavalo para dentro das muralhas da cidade. Durante a noite, quando todos dormiam, os soldados gregos que se escondiam dentro da estrutura oca de madeira do cavalo saíram e abriram os portões para que todo o exército entrasse e invadisse a cidade. Tal como na história, um cavalo de tróia faz-se passar por um programa que tem funcionalidades úteis, quando de facto, esconde um programa que pode causar danos aos computadores e aos seus utilizadores, ao abrir “portas” que possibilitam invadir e roubar, por exemplo, “passwords” dos utilizadores. A principal forma de propagação é feita através da internet, onde são oferecidos como ferramentas com funções úteis para os computadores.

### Spyware

O Spyware consiste em um programa automático de computador, que recolhe informações sobre o utilizador, sobre os seus costumes de navegação na Internet e transmite essas informações a uma entidade externa na Internet, sem o conhecimento e consentimento do utilizador. Ao contrário dos cavalos de Troia, os spyware não têm como objetivo que o sistema do utilizador seja dominado ou manipulado, por uma entidade externa, como um “hacker”. Os spywares podem ser desenvolvidos por firmas comerciais, que desejam monitorizar o hábito dos utilizadores por forma a avaliar os seus costumes e vender estes dados pela internet. Por outro lado, muitos vírus transportam spywares, que visam roubar certos dados confidenciais dos utilizadores. Roubam dados bancários, montam e enviam registos das actividades do utilizador.

# Ciberegurança na Indústria 4.0



## Stuxnet

### O primeiro vírus industrial

O Stuxnet foi o primeiro worm de computador projectado especificamente para atacar sistemas SCADA que controlam processos industriais.

O Stuxnet é um worm malicioso, identificado pela primeira vez em 2010 e que tem como alvo sistemas de computadores industriais com o sistema Scada desenvolvido pela Siemens. Este vírus foi responsável por causar danos substanciais no programa nuclear do Irão.

Apesar de nunca ter sido confirmado oficialmente por qualquer dos países, diversos peritos em informática dizem que este vírus foi desenvolvido pelos governos dos Estados Unidos da América e de Israel. Num artigo publicado no Washington Post, oficiais americanos de forma anónima indicaram que o vírus foi desenvolvido durante a administração do Presidente George W. Bush para sabotar o programa nuclear do Irão.





O Stuxnet foi escrito para atacar sistemas de controlo industrial SCADA, utilizado para controlar e monitorizar processos industriais. Este vírus explorava quatro vulnerabilidades do tipo “zero-dias” (denomina-se por vulnerabilidade “zero-dias”, uma falha existente num sistema que nunca foi identificada).

Stuxnet é composto por três módulos:

- um “worm” que executa todas as rotinas relacionadas com a carga principal do ataque;
- um arquivo de link que executa automaticamente as cópias propagadas do worm;
- um componente rootkit responsável por ocultar todos os arquivos e processos maliciosos, impedindo a detecção da presença do Stuxnet.



O Stuxnet normalmente é introduzido no ambiente de destino através de uma unidade flash USB infectada. Após ser introduzido num computador, o “worm” propaga-se através de redes que utilizem o sistema operativo Windows, à procura de computadores que possuam o software Step7 da Siemens para controlo de autómatos. Caso nenhuma destas condições se verifique, o Stuxnet fica dissimulado dentro do computador, sem qualquer manifestação. Se ambas as condições forem cumpridas, o Stuxnet introduz o “rootkit” infectado no software Step7 e no autómato, modificando os códigos e dando comandos inesperados ao autómato, enquanto transmite valores de sistema de operações normais, aos utilizadores e supervisores do sistema.

A central nuclear iraniana de Natanz, utilizava para controlo das centrífugas de enriquecimento de urânio, autómatos da Siemens que eram comandados pelo software Step7. Após ter infectado o sistema, o Stuxnet ia ter duas funções. A primeira delas era fazer com que as centrífugas iranianas comessem a girar 40% mais rapidamente por quinze minutos, o que causava fissuras nas centrífugas de alumínio. A segunda função era a de gravar dados telemétricos de uma típica operação normal das centrífugas nucleares, sem que o alarme soasse, para depois reproduzir esse registo para os operadores dos equipamentos de modo a que tudo parecesse normal, quando na verdade as centrífugas estavam literalmente a ser destruídas pela acção do Stuxnet. Estima-se que o Stuxnet terá destruído cerca de 1/5 das centrífugas nucleares iranianas.

Mas para além da central nuclear de Natanz, que crê-se ter sido o principal alvo quando da criação do vírus, este acabou por propagar-se de forma accidental pelo mundo inteiro. Esta propagação ocorreu quando um PC infectado pelo vírus na central, foi utilizado fora da mesma. Ao ligar-se à internet, o vírus espalhou-se pela rede, tendo sido encontrado em diversas partes do mundo. No entanto, este acabaria por não provocar danos, dado que foi especificamente criado, para as centrífugas de enriquecimento de urânio.

De acordo com um estudo da Symantec, 60% dos computadores infectados no mundo estavam localizados no Irão, o que vem corroborar o facto de que o vírus foi criado especificamente para a central de Natanz. Por sua vez, a Kaspersky Lab concluiu que o worm foi desenvolvido pelo governo de um país. Este ataque, em conjunto com outro tipo de ataques que ocorreram posteriormente, foi considerado como o início de uma ciberguerra e que veio a tornar-se numa preocupação para os governos de todo o mundo.

# Indusmelec

Material Eléctrico & Automatismos Industriais, Lda.

Rua António Sousa Bastos, N° 2/2A

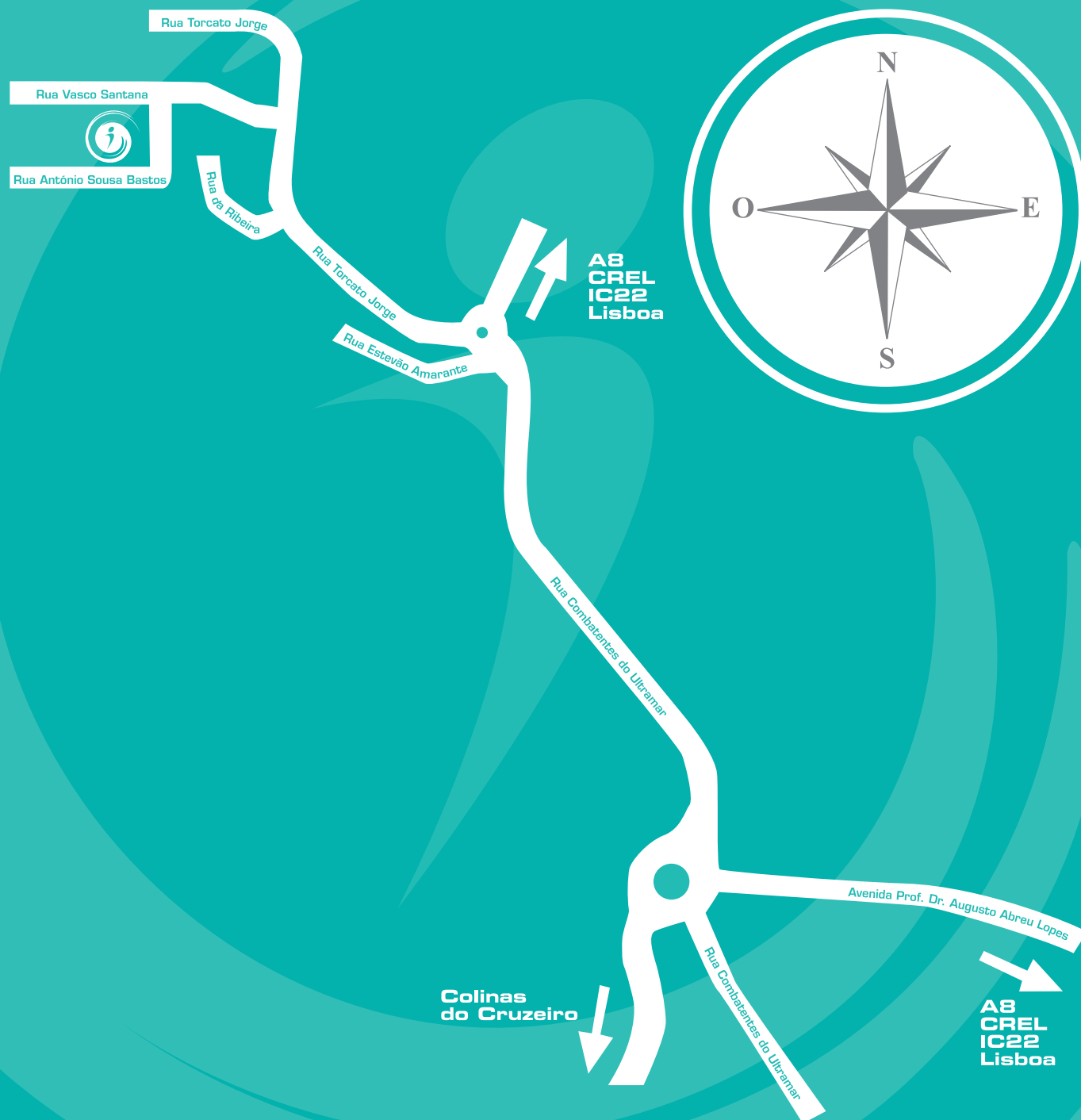
2620-419 Ramada

Tel.: 219 318 046/7/8 - 219 340 400 - 211 571 461 (6 acessos)

Fax: 219 318 049

Coordenadas GPS: N 38° 48' 7" W 9° 11' 34"

e-mail: geral@indusmelec.pt



||| | [www.indusmelec.pt](http://www.indusmelec.pt) ||| |