INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES

DISPOSITIVOS DE CONECTIVIDADE REMOTA ESTUDO, TESTES E ANÁLISE COMPARATIVA DE DESEMPENHO

TÂNIA CRISTINA DA COSTA NUNES
Outubro de 2021

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

DISPOSITIVOS DE CONECTIVIDADE REMOTA – ESTUDO, TESTES E ANÁLISE COMPARATIVA DE DESEMPENHO

Flexy 205- E-Won-HMS Networks

E-SR-2GT-LAN-Weidmuller

IXrouter 2415 IXON

Candidato: Tânia Cristina da Costa Nunes

Mestrado em Engenharia Eletrotécnica e de Computadores – Sistemas e Planeamento Industrial

Orientador: Prof. Filipe Alexandre de Sousa Pereira

2020/2021

Relatório elaborado para satisfação parcial dos requisitos da Unidade Curricular de Tese/Dissertação do Mestrado em Engenharia Eletrotécnica e de Computadores

Candidato: Tânia Cristina da Costa Nunes, nº 1191229, 1191229@isep.ipp.pt
Orientação científica: Prof. Filipe Alexandre de Sousa Pereira, fal@isep.ipp.pt

Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica e de Computadores

Área de Especialização em Sistemas e Planeamento Industrial

2021

Dedico este estudo a todos os leitores que tenham retido qualquer informação que tenha sido útil e a todos aqueles que procuram e que contribuem para um mundo virtual mais consciente dos riscos invisíveis e com uma maior postura crítica em relação à performance dos aparelhos que nos rodeiam.

Agradecimentos

Ao professor Filipe Alexandre De Sousa Pereira, orientador da dissertação, agradeço a presença e preocupação contínua para a realização deste trabalho, para além da motivação pelo conhecimento e postura crítica sobre o projeto.

Aos meus pais e restante família que estiverem sempre disponíveis, agradeço o amor e o apoio incondicional que sempre dispõe independentemente da situação.

À família que escolhi, as minhas amigas de Infância, Ana Isabel e Ana Paula, pelo apoio, motivação e palavras de reconforto nos momentos mais difíceis.

A vocês, que caminham ao meu lado em todas as fases da minha vida, o meu profundo e sentido agradecimento por viverem as minhas vitórias como se fossem próprias.

Resumo

Nos dias de hoje, vivemos cada vez mais uma realidade virtual, onde gradualmente tarefas manuais do dia a dia passam a ser substituídas por novas tecnologias capazes de realizar várias tarefas de forma independente. No mundo industrial esta nova realidade também se verifica, na medida em que a mão humana tem vindo a ser substituída por máquinas e robôs, que têm não só a capacidade de realizarem as tarefas às quais foram projetadas, como também apresentam a capacidade de se adaptarem ao ambiente e de aprenderem de forma autónoma. Esta evolução tecnológica carrega vantagens no que toca à diminuição do esforço físico e mental do ser humano, à prevenção e deteção prévia de falhas, bem como uma maior eficiência dos processos industriais e menores custos associados. No entanto, esta nova era virtual exige uma maior partilha de dados e uma constante comunicação entre os sistemas com recurso à Internet. Desta forma, torna-se essencial o conhecimento e a execução de avaliações periódicas dos equipamentos, quanto à sua velocidade e segurança de comunicação entre os diferentes equipamentos envolvidos nos processos industriais, para garantir que estes apresentam o melhor desempenho possível.

O presente trabalho tem como ambição realçar a importância da testagem de equipamentos que estão projetados para permitir a comunicação remota entre os diferentes equipamentos.

Palavras-Chave:

Redes Industriais: Rede de Computadores; Indústria 4.0; *Internet of Things*; Acesso remoto;

INDICE

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos

OSS - Open Software Source

OSI- Open Source Initiative

OSI- Open System Interconnection

ISO- Internal Organization for Standardization

DoD- Department of Defense

TCP - Transmission Control Protocol

CLL- Controlo de Link Lógico

CAM- Controlo de Acesso ao Meio

ARPA - Advanced Research Projects Agency

WAN- Wide Area Network

HTML- HyperText Markup Language

WWW- World Wide Web

URL - Uniform Resource Locator

CAN - Controller Area Network

IoT- Internet of Things

LAN- Local Area Network

ISACA - Information Systems Audit and Control Association

PLC- Controlador Lógicos Programável

HMI- Interfaces humano-máquina

VPN - Virtual Private Network

SSL - Secure Scoket Layer

ISEP- Instituto Superior de Engenharia do Porto

IdCI - Internet das coisas Industrial

TIC- Tecnologias da Informação e Comunicação

KPI - Key Performance Indicators

1. INTRODUÇÃO

Espaços de trabalho virtuais, onde colaboradores podem trabalhar e comunicar entre si e com os seus superiores, tem-se tornado um cenário cada vez mais familiar. Um estudo realizado nos Estados Unidos demonstrou um aumento do número de colaboradores a trabalhar de forma remota de cerca de 115% entre os anos de 2005 e 2015, devido à revolução digital da informação e da comunicação tecnológica, como os *smartphones* e a computação baseada em *cloud* [1]. Nas atividades industriais, tecnologias e soluções inteligentes passaram a fazer parte da gestão das operações. Este fator, iniciou-se na terceira revolução industrial, onde foram desenvolvidas novas tecnologias com o objetivo de reduzir a intervenção do ser humano nos processos de produção [2]. Estas soluções envolviam a introdução de novos dispositivos eletrónicos nas máquinas industriais, como os controladores lógicos programáveis (PLC), robôs, e a utilização das tecnologias da informação e comunicação (TIC), que tinham como função a integração de todos os processos industriais com as máquinas e as pessoas. Após este período, dá-se a quarta revolução industrial, indústria 4.0, na qual se foca no desenvolvimento de um sistema mais inteligente, sobretudo na resolução de problemas sem a necessidade de intervenção humana. Neste campo, as TIC desempenham um papel fundamental na indústria 4.0, pelo facto de possibilitarem a comunicação simultânea dos processos entre si, criando um ambiente cyber-físico, a união do mundo físico e o mundo virtual [1].

A adaptação a esta nova realidade de ambiente de trabalho, exige uma maior segurança. Com cada vez menos pessoas presentes no local de trabalho, aumenta a procura pela gestão remota dos equipamentos, a recolha de dados em tempo real e a tomada de decisões com base na inteligência artificial [3]. Para que os dispositivos tecnológicos usados em automação possam conferir a devida integridade e segurança, é necessário garantir que estes aparelhos executam as suas funções com o melhor

desempenho possível, dentro de vários aspetos, como por exemplo, a qualidade de conexão entre eles, velocidade de processamento, percentagem de falhas, etc.

1.1. Siemens- Soluções de conexão remota

A empresa Siemens tem mostrado cada vez mais relevância no mercado em áreas distintas, como a energia, indústria, mobilidade e tecnologias para edifícios. Dentro da automação e comunicação industrial a Siemens oferece o *Teleservice*, onde o seu principal foco é a troca de informações entre sistemas de forma remota, apresentando funções de deteção de erros, análise de diagnóstico, realização de manutenção e melhorias no âmbito industrial [4]. O SINEMA Remote Connecting é um software de acesso remoto da Siemens, onde apresenta a possibilidade de funcionar como um servidor, através da sua instalação num computador ou na *cloud*. Através deste *software* é possível configurar os utilizadores e máquinas, isto é, a relação entre os utilizadores que terão a permissão ou não de utilizar a máquina. Na Figura 1 encontra-se apresentado pela Siemens um modelo relativo às formas de conexão entre as diferentes máquinas constituintes da rede.

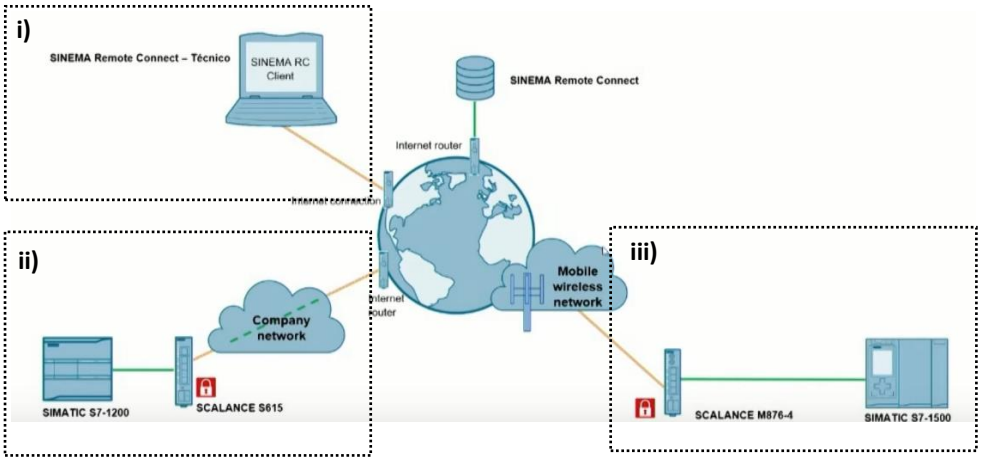

Figura 1. Formas de conexão entre os utilizadores e máquinas [5].

Assinalado com a letra i), tem-se o SINEMA *Remote Connect Client* instalado num computador, onde apenas é necessário estar conectado à internet para poder ter acesso ao servidor.

Quanto à conexão com às máquinas existem diferentes formas de conexão. Como assinalado na Figura 1, verifica-se que para estabelecer uma ligação com servidor é necessário atravessar toda a estrutura de tecnologia de informação do cliente final, com recurso ao *software* SCALANCE S615 (ii). Em situações em que não é possível estabelecer ligação através da estrutura do cliente, como alternativa, utiliza-se o *software* SCALANCE M876-4, uma tecnologia móvel que permite estabelecer o acesso ao servidor (iii) [5].

1.2. Objetivo

Para que os sistemas de acesso remoto permitam a monitorização e manutenção em tempo real, é crucial uma avaliação pormenorizada dos aparelhos tecnológicos projetados na arquitetura de acesso remoto. Os aparelhos devem ser testados segundo métricas que garantam a melhor qualidade de funcionamento do aparelho.

Este projeto surgiu pela necessidade de avaliação da performance de três aparelhos de conectividade remota, mais especificamente a velocidade da comunicação e conexão entre os diferentes aparelhos envolventes. O dispositivo que apresentar melhores resultados de desempenho, irá ingressar numa uma bancada didática de acesso remoto para os alunos do Instituto Superior de Engenharia do Porto (ISEP). Será realizada uma análise comparativa do desempenho dos dispositivos em estudo, com o intuito de alinhar os conceitos teóricos relacionados e o encontro da melhor solução para a linha de montagem da bancada.

2. REFERENCIAL HISTÓRICO

2.1. Rede de Computadores

Atualmente, torna-se indispensável para a sociedade o uso tecnologias tendo como suporte o uso de rede de computadores. As pessoas procuram dispositivos que se conectem à internet de forma rápida, para que possam usufruir dos seus serviços, quer sejam estes por motivos pessoais ou profissionais. Os dispositivos de uma rede de computadores são ativos tangíveis com a capacidade de tratamento de informação/dados, como por exemplo, *smartphones*, câmaras de segurança, computadores, etc. Estes dispositivos dizem-se autónomos porque são capazes de realizar as suas tarefas de forma independente [6]. A comunicação e a transferência de informações entre estes ativos pressupõem a existência de uma rede de computadores.

Para que este facto seja possível, é necessário que todos os dispositivos sejam projetados para comunicar de acordo com a mesma tecnologia, isto é, que todos sigam um padrão pré-definido [7].

2.1.1. CONSTITUINTES DE UMA REDE DE COMPUTADORES

O desenvolvimento de uma rede de computadores implica a existência de três elementos essenciais, tal como representado na Figura 2 [6][7].

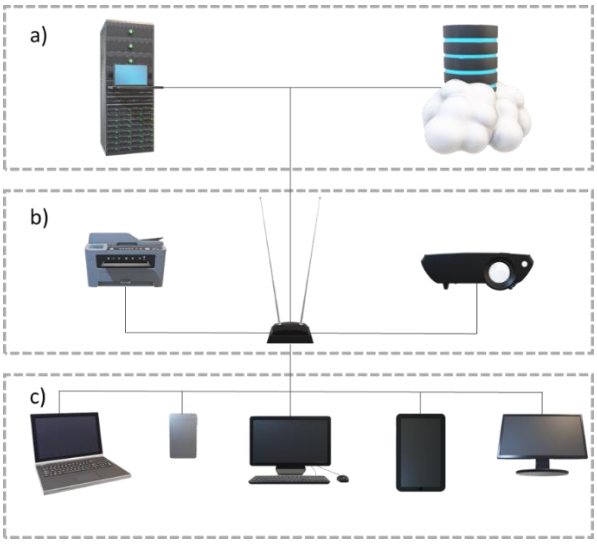

Figura 2. Exemplificação de uma rede de computadores.

Na parte superior da Figura 2, assinado com a letra a encontram-se os dispositivos denominados de servidores, que englobam todos os dispositivos projetados para executar algum tipo de serviço na rede.

O elemento central da Figura 2, assinalado com a letra b, o router, tem a responsabilidade de estabelecer a ligação entre os dispositivos da rede e onde através deste, serão fornecidas informações entre os dispositivos e funcionalidades [7].

Os dispositivos que tencionam usufruir destes serviços encontram-se identificados na parte inferior da Figura 2, identificado com letra c, representando os clientes.

2.1.2. Modelo OSI e Modelo de Referência TCP/IP

A *Internal Organization for Standardization* (ISO), na década de 1970, criou um padrão universal de troca de informações dentro e entre redes, incentivando a padronização de redes e controlo dos processos, resolvendo desta forma a incompatibilidade entre os fabricantes [6]. Durante o processo de definição do modelo *Open System Interconnection* (OSI), o Departamento de Defesa dos Estados Unidos da

América (DoD- *Department of Defense*) desenvolveu um outro modelo com o objetivo de manter os seus equipamentos conectados, modelo de referência TCP/IP [6]. Numa ligação TCP/IP existe um servidor que permite a comunicação entre duas pontas (fonte/destino ou cliente/servidor). O cliente inicia a ligação ao enviar um pacote TCP com a *flag* `SYN` ativa, sendo que esta flag funciona como sinalização. O próximo passo consiste no servidor em aceitar a ligação enviando um pacote *SYN+ACK*. O estabelecimento da ligação dá-se por concluído quando por parte do cliente é confirmada a aceitação do servidor, respondendo-lhe com um pacote `ACK`, como é possível observar na Figura 3.

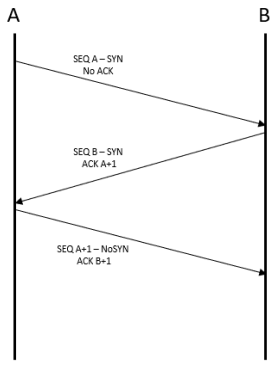

Figura 3. Esboço de uma ligação TCP/IP.

Se dentro de um determinado espaço de tempo o pacote enviado pelo cliente não for recebido, ocorre uma interrupção e o pacote *SYN* é reenviado [8]. Durante estas comunicações, ocorrem trocas de números iniciais que servem para identificar os dados que estão a ser partilhados ao longo do fluxo, bem como para contabilizar os bytes que estão a ser transmitidos [8]. A arquitetura do protocolo TCP/IP é dividido em quatro camadas: Aplicação; Transporte; Rede e Interface Rede [9].

É através da camada Aplicação que os programas comunicam. Por exemplo, o serviço *email* utiliza o protocolo SMPT, o FTP para a transferência de documentos e o protocolo HTTP para a navegação *Web*.

Depois de processada a requisição do programa, o protocolo na camada Aplicação irá comunicar com outro protocolo da camada de Transporte, na qual é responsável por assegurar a entrega sequencial dos dados. Podem ser usados 2 protocolos distintos, o TCP e o UDP. Enquanto o protocolo TCP é orientado à conexão, o UDP funciona como segunda opção, uma vez que não garante a entrega de pacotes de forma sequencial [9].

Na camada de Rede é realizado o endereçamento, onde é adicionado ao pacote recebido um endereço virtual, nominado por endereço IP, que contém informação sobre o endereço do computador que está a enviar os dados e o endereço do computador que irá receber. Por fim, os pacotes são enviados para a camada Interface com a Rede, na qual o que se encontra nesta camada depende do computador que está a ser utilizado. Usualmente encontramos um tipo de rede chamada de Ethernet, que funciona como um Controlo de Link Lógico (LLC), Controlo de Acesso ao Meio (CAM) e as características físicas da comunicação [9].

2.1.3. EXTRANET E INTRANET

Tendo por base o projeto realizado pela Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos da América (ARPA) [6], a Internet é constituída por uma série de redes menores, interligada através de routers, funcionando como uma única rede. A Internet, com o "I" maiúsculo refere-se à rede que lhe deu origem, na ARPANET, enquanto internet com "i" minúsculo se refere a uma rede que é composta por diversas redes menores, que utiliza o mesmo protocolo de comunicação [6]. Existem ainda internets isoladas, tais como, Intranets e Extranets.

A Intranet trata-se de uma rede de carácter privado, que possibilita o acesso aos mesmos serviços da rede mundial Internet. É construída sobre a arquitetura do protocolo TCP/IP e os seus serviços apenas se encontram disponíveis para os utilizadores com acesso à rede local [6].

A Extranet é uma rede geograficamente distribuída (WAN- *Wide Area Network*). A sua construção é baseada em protocolos de comunicação privados e comunicação TCP/IP. Os serviços oferecidos por esta são bastante similares à rede Internet e geralmente é usada para interligar as sedes de diferentes corporações que utilizam a Intranet [6].

O principal serviço fornecido pela internet representa um suporte de informação. Este serviço permite ao utilizador realizar compras virtuais, ler jornais e repositórios eletrónicos bem como a consulta de banco de dados. Para além disso, permite ainda o acesso a diversos documentos, através de *hyperlinks* disponíveis em páginas escritas em HTML (*HyperText Markup Language*), linguagem de desenvolvimento de páginas estáticas) [6]. A informação disponibilizada encontra-se organizada em páginas que podem conter diferentes formatos de informação, tais como, textos, imagens, sons, programas, etc. Com esta tecnologia, as empresas tiveram a possibilidade de transportar seus negócios para o digital e tornar a relação com o cliente mais prática, pelo facto de evitar em muitos casos, a deslocação do cliente ao espaço físico da empresa.

2.2. Redes Industriais

Tal como mencionado na secção 2.1., as redes têm a capacidade de armazenar e tratar de inúmeros processos, através da troca de informações entre os ativos fixos. As redes industriais surgiram para tornarem os processos contínuos (indústria de processo) e as linhas de processo discretos (indústria de manufatura) mais flexíveis, promovendo expansões futuras e tornando mais acessível quando comparado ao sistema centralizado [10]. Existem diferentes redes industriais no mercado. Cada uma delas apresenta um conjunto de regras e particularidades específicas na qual regem o tratamento de dados.

Ao transportar este cenário para os dias de hoje, verifica-se uma realidade bem diferente no que toca à automação industrial, onde numa linha de produção é possível a construção de automóveis de cores, modelos diferentes, pacotes de acessórios específicos de cada modelo, rastreio da produção e requisitos em relação a padrões de qualidade. A procura pela automação industrial tem vindo a ganhar uma maior relevância no mercado. Tal procura, está associada a diferentes níveis de negócio, desde o pequeno empresário até grandes empresas já consolidadas no mercado, bem como diferentes aspetos do segmento onde se inserem, isto é: velocidade; quantidade de dados; níveis de produtividade, qualidade e flexibilidade nos processos [11].

Na Tabela 1 que se segue, encontra-se um quadro resumo com os diferentes tipos de redes industriais, os seus respetivos objetivos, áreas de atuação e algumas recomendações [10] [12]:

Tabela 1. Quadro resumo sobre os diferentes tipos de redes industriais.

Redes Industriais		Objetivo	Recomendações
Fieldbus	AS - Interface	Controlo da passagem de informação;Conexão entre os diferentes dispositivos existentes na rede	Utilização em máquinas de pequeno porte.
	Profibus DP	Transmissão de informações de forma rápida e eficaz.	Equipamentos de médio a grande porte.
	Profibus PA	Transmissão dos sinais de componentes da rede, por exemplo, temperatura.	Indústria de processos contínuos
	Profibus FMS	Troca de dados entre equipamentos regidos por padrões diferentes;	Não é recomendada redes amplas e complexas.
	DeviceNet	Baseado em rede Controller Area Network (CAN) Controlo de transmissão de informação com capacidades multi-mestre, isto é, vários "nós" podem requisitar acesso a meio da transmissão.	Comunicações em série
Ethernet	Ethernet IP	Partilha de dados digitais entre os computadores conectados à rede.	-
	LAN	Conexão entre redes locais através de fios (LAN-Local Area Network).	Empresa, escola,etc
	WAN	Ligação entre diferentes dispositivos conectados à rede dispersos geograficamente	Entre países e continentes
	I/O Link	Comunicação entre dispositivos I/O, como por exemplo sensores, dispositivos de interface e controladores.	Identificação mais rápida em falhas elétricas.

2.3. Indústria 4.0.

As revoluções industriais têm sofrido alterações cada vez mais tecnológicas, como se pode verificar na Figura 4. O termo *Indústria 4.0* representa a quarta revolução industrial, trazendo um novo modelo de organização e controlo do ciclo de vida de um produto. O principal objetivo da indústria 4.0 consiste no atendimento das necessidades e requisitos do cliente em áreas distintas que vão desde a gestão de encomendas, desenvolvimento e produção, até à reciclagem dos produtos [13].

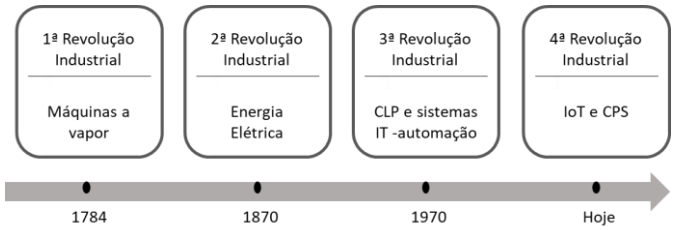

Figura 4. Revoluções Industriais ao longo do tempo.

2.3.1. PILARES DA INDÚSTRIA 4.0.

Em meados de 2013, surge o modelo *Industrie 4.0 Working Group*" [13]. Os pilares da indústria 4.0 residem em: *Big data analytics;* Robôs autónomos; Simulação, Integração do sistema (vertical e horizontal); *Internet of things* (IoT); *The cloud;* Manufatura aditiva; Realidade aumentada e Cybersegurança.

Big data analytics insere-se na tecnologia da informação que engloba a análise de um grande número de dados que precisam de ser processados e armazenados. Num contexto de Indústria 4.0, a avaliação de uma grande quantidade de dados de diferentes fontes, isto é, vários equipamentos e sistemas de produção de gestão empresarial,

contribui para um método padrão do estudo comportamental do processo de produção, para além de que auxilia a tomada de decisão em tempo real [14].

O funcionamento dos robôs autónomos, passa pela recolha de informação do ambiente onde se insere, deslocação entre pontos de controlo e execução da sua tarefa [15]. Este facto confere aos robôs a vantagem de aprenderem a executar tarefas de forma independente e a desenvolverem outras capacidades sem ajuda externa. Estes robôs têm ainda a possibilidade de interagirem entre si, colaborando em conjunto para executarem uma determinada tarefa.

A simulação na Indústria 4.0. consiste em testar continuamente os processos de forma dinâmica e com o objetivo de otimizar os processos de produção. As ferramentas digitais que executam esta análise permitem uma visão pormenorizada do sistema de produção e a sua autoconfiguração, o que facilita um planeamento estratégico ajustado às necessidades. Este planeamento é feito com dados adquiridos em tempo real [14].

A integração e a auto-organização são os principais focos no que diz respeito à organização industrial. Dentro deste conceito temos duas dimensões a analisar: horizontal e vertical. A dimensão horizontal trata-se de uma integração cruzada entre os sistemas de informação de produção com os dispositivos automatizados nas várias etapas do processo de produção. A vertical refere-se à integração dos sistemas que são possíveis de reconfigurar, desde o processo de produção do produto até à sua manufatura [14]. Nesta integração, são usados normalmente dados recolhidos por sensores em diferentes níveis do processo, com o objetivo de se obter uma reconfiguração flexível e adaptável à manufatura de diferentes produtos [16].

O termo *Internet of things* refere-se à revolução tecnológica que compreende todos os aparelhos que tenham a capacidade de estarem conectados à internet e de comunicarem entre si. A sua principal função consiste em estabelecer a conexão entre os diferentes aparelhos e recolher dados destes mesmos. Esta recolha de dados permite a computadores ou dispositivos de nível superiores terem a capacidade de tomada de decisão sobre as operações [14]. Esta interligação não se limita apenas aos

equipamentos que se encontram na linha de produção e aos produtos que estão a ser fabricados no momento, envolve também os centros logísticos que são capazes de interagir de forma autónoma.

Segundo a definição apresentada pela Microsoft, o termo *cloud* não se refere a uma entidade física, mas sim a uma rede global de servidores que se encontram global e remotamente disponíveis, onde cada um dos servidores se destina a uma função específica. Estes servidores estão projetados para armazenar e gerir dados, executar aplicações e fornecer conteúdos e serviços. Esta tecnologia permite aceder à informação onde quer que esteja a qualquer altura, isto é, em vez de aceder aos ficheiros num computador local ou pessoal, está a aceder de forma online a partir de um dispositivo com acesso à Internet [14]. As empresas diferem na forma de implementação dos recursos da *cloud*. Existem quatro métodos: pública; privada; híbrida e da comunidade. A *cloud* pública disponibiliza recursos e serviços ao público enquanto a *cloud* privada fornece serviços apenas dentro de uma rede privada, geralmente alocada no local específico. A *cloud* híbrida permite a partilha de serviços entre *cloud's* públicas e privadas de acordo com o objetivo. A *cloud* da comunidade partilha recursos entre organizações, como por exemplo o governo [17]. O uso de *software* baseado em *cloud* nas empresas, exige uma maior partilha de dados entre locais, ao mesmo tempo que alcança um menor tempo de reação. A implementação dos dados e funcionalidades na *cloud* promove uma virtualização dos recursos e serviços, que não só traz vantagens ao nível da integração e centralização de informação, como facilita a gestão e administração dos sistemas de controlo num sistema virtual, atendendo às necessidades dos diferentes tipos de utilizadores [15].

A Manufatura Aditiva consiste num conjunto de tecnologias que permitem a produção de produtos personalizados com recurso à impressão 3D através de modelos digitais [15]. A forma mais comum de produção são a construção de protótipos e os métodos de impressão 3D para produzir pequenos lotes e manter uma produção elevada. Este tipo de produção traz como vantagens [14]:

- a diminuição do custo de produção, devido à substituição de um conjunto de máquinas por uma impressora 3D;
- a criação de produtos com geometrias complexas;
- personalização dos produtos de acordo com as necessidades;
- a redução dos recursos utilizados, que por sua vez geram um menor volume de resíduos;

A realidade aumentada estabelece o cruzamento entre o mundo virtual e o mundo físico. Um exemplo prático e fácil de entender o que é a realidade aumentada é o uso do QR Code em pontos turísticos. Com apenas um *smartphone* que tenha instalado a aplicação móvel de leitura do QR code e que esteja conectado à Internet, é possível ter acesso a outros pontos turísticos de referência da zona e qual a rota que deve ser seguida [18]. No caso do setor industrial, a realidade aumentada permite o acompanhamento em tempo real dos processos de produção, procedimentos de manutenção e segurança dos equipamentos e das infraestruturas, bem como a tomada de decisão.

A quarta revolução industrial é caracterizada por uma grande partilha de informações entre dispositivos cada vez mais sofisticados, onde os sistemas se encontram interligados, quer seja através da internet, quer por um serviço de *cloud* ou até mesmo uma conexão com o mundo externo. Toda esta acessibilidade de informação exige uma maior preocupação em relação à segurança da informação, daí a cibersegurança se caracterizar por ser um dos pilares da indústria 4.0. De acordo com a associação *Information Systems Audit and Control Association* (ISACA), cyberegurança define-se como: "Proteção dos ativos de informação, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transportada pelos sistemas de informação que estão interligados." [19]. Uma falha de segurança trata-se de um incidente que permite o acesso não autorizado a informações confidenciais em aplicações, redes ou dispositivos do computador. Em segurança de computadores, uma vulnerabilidade trata-se de uma falha do sistema segurança, que

pode ter origem na forma como é projetada a arquitetura do sistema de informação ou aquando é feita a sua implementação (Oliveira, 2021). Esta imperfeição no sistema pode resultar num ataque, permitindo a entrada de intrusões no sistema, a destruição ou roubo de dados bem como pôr em causa a integridade do sistema (Costa, 2018). De forma a perceber melhor um sistema se encontra protegido, são realizados testes de penetração ou *pentests,* na qual são realizadas simulações de ataques reais de forma a avaliar o risco associado às falhas de segurança no sistema. O principal objetivo é detetar e explorar vulnerabilidades de um sistema de forma a validar a eficácia dos mecanismos de segurança. Quando um ataque é bem-sucedido pode resultar em prejuízos irreversíveis, quer sejam de natureza física ou moral, como tal, é essencial para o negócio a existência de planos de Cyber segurança de forma a aumentar a proteção de dados.

2.3.1. BANCADAS DIDÁTICAS NA INDÚSTRIA 4.0.

O avanço tecnológico no âmbito da automação tem vindo a ser um fator de competitividade entre as indústrias pela redução de custos ao automatizar os processos anteriormente realizados de forma manual. Tendo por base a linha S7300 da Siemens, desenvolvida pela EXSTO, empresa que se foca na satisfação das necessidades de equipamentos voltados para o ramo de tecnologia didática [20], foi desenvolvido um kit didático para dar a possibilidade a estudantes de explorar as características básicas deste sistema, permitindo o desenvolvimento de competências em diversos aspetos relacionados com a automação industrial, como compreender o "cérebro" deste sistema, o PLC [20]. Os estudantes ao estarem em contacto com esta bancada, tinham a possibilidade a operar e programar com o PLC, bem como interagir com diversos equipamentos externos comumente encontrados em situações de operação reais. Estes kits didáticos, também conhecidos como "bancadas didáticas" consistem num sistema eficiente que é capaz de envolver vários equipamentos eletrónicos, na qual há a possibilidade de simular de situações reais de trabalho em diversas áreas de atuação.

De uma forma geral, a estrutura física destas bancas baseia-se num quadro em alumínio, com uma parte inferior que permite a sua deslocação. Geralmente estão também inseridos instrumentos de medição e fonte de energia, de fácil utilização e não facilmente danificados. Estas bancadas possuem ainda um circuito modular que se encontra totalmente configurado e usado em combinação com outros equipamentos bem como um sistema de segurança integrado [24].

Estas características trabalhadas em conjunto, possibilitam a realização tangível de soluções que melhoram tarefas do dia a dia na automação, tal como é o caso da bancada didática onde irá ser inserido um dos dispositivos de teste neste estudo. Uma das ambições deste estudo é também realçar para os estudantes de automação, a postura crítica a adotar quanto à avaliação da velocidade e segurança da comunicação dos diferentes equipamentos que se inserem em bancadas didáticas.

2.4. Acesso remoto

Dentro do contexto de Indústria 4.0., um elemento fundamental é a conectividade. Quer sejam fabricantes ou utilizadores de máquinas industriais, a possibilidade de observar o seu comportamento enquanto operam resulta numa maior valia para o negócio bem como para a satisfação do cliente [21]. Geralmente, o controlo remoto de máquinas industriais permite programar e solucionar problemas relacionados com os PLC's, na qual dizem respeito a dispositivos projetados para o controlo de processos industriais e que possuem a capacidade de automatizar processos específicos [22]. Para além disso, o controlo remoto industrial possibilita ainda a visualização e o controlo à distância dos painéis que permitem a interação entre o utilizador e máquina, Interfaces humano-máquinas (HMI'S), a assistência técnica com recurso a uma *webcam* e o apoio técnico na integração de novos equipamentos [21].

De uma forma simples, o acesso remoto trata-se de uma tecnologia que possibilita o acesso entre computadores ou outros dispositivos eletrónicos, a uma rede sem a

necessidade de uma ligação de natureza física entre os diferentes aparelhos. Para que a conexão seja estabelecida com sucesso, é necessário que a máquina local tenha o software de cliente remoto instalado e a máquina remota ter o software de servidor instalado [23].

2.4.1. VIRTUAL PRIVATE NETWORK (VPN)

Geralmente o acesso remoto é feito com recurso a uma VPN, onde é possível estabelecer uma ligação direta entre um determinado computador e o servidor de destino, e na qual é criado uma espécie de "canal protegido" na Internet. A construção de uma VPN pode ser feita por duas formas: através do protocolo *secure scoket layer* (SSL) ou softwares. No primeiro tipo de ligação, esta pode ser estabelecida com apenas um navegador *web* e um serviço de *cloud*. No segundo caso, sendo este método mais comum, é necessário um *software* que utiliza o protocolo IPseg para fazer a ligação direta entre dois computadores, ou entre um computador e o servidor.

Do ponto de vista de segurança a utilização de um router industrial e uma infraestrutura baseada em *cloud* torna-se numa alternativa interessante na medida em que impõe uma segregação de rede lógica entre a máquina e a LAN do cliente. Desta forma, o utilizador não tem acesso à LAN da fábrica, mas apenas aos dispositivos que estão conectados ao router de acesso remoto [21].

3. CONTEXTUALIZAÇÃO

Ao longo deste capítulo serão abordadas informações técnicas sobre os dispositivos em estudo, bem como os resultados da realização dos testes de performance.

3.1. Materiais e Métodos

Neste projeto, a solução encontrada será para uma rede de nível intermédio, com conexão a um PLC e a uma HMI. Como tal, foram escolhidos dispositivos que têm a capacidade de criar o acesso remoto a este tipo de rede industrial, sendo estes do mesmo fornecedor: OMRON. Tratando-se de uma bancada didática, na qual o seu principal propósito é a educação e possibilitar aos estudantes a simulação de situações reais, teve-se em especial atenção a velocidade de conexão e transferência de informação entre os diferentes dispositivos. Com o intuito de avaliar a velocidade da comunicação entre os diferentes equipamentos, foram cronometrados os seguintes tempos:

I) Cronometragem do tempo de abertura do canal VPN;
II) Teste *Packet Inter-Network Groper* (PING);
III) Cronometragem do tempo de transferência de um projeto para o PLC;
IV) Cronometragem do tempo de transferência de um projeto para a HMI;
V) Cronometragem do tempo de mudança de valor de uma variável (neste caso, *On/Off* LED).

O primeiro teste foi realizado para analisar o tempo que cada um dos dispositivos demora a estabelecer o canal VPN, onde através deste estabelece uma ligação direta entre um computador cliente e o servidor de destino.

O teste de `ping` foi realizado na linha de comandos do computador de teste com o intuito de identificar os pacotes de dados de rede, analisar o tempo de envio destes e verificar a resposta das máquinas que estão ligadas na mesma rede. Para além disso, o teste de `ping` permite ainda verificar a percentagem de pacotes perdidos durante a ligação . Nesta avaliação é necessário ter informação sobre os endereços IP de cada um dos dispositivos inseridos na rede .

Os testes de avaliação de transferência de um projeto, tanto para o PLC como para a HMI, foram realizados nos *softwares* específicos de cada um dos dispositivos, Cx-Programmer e NB Designer, respetivamente. Nesta testagem, é também necessário deter da informação dos endereços IP de cada um dos dispositivos.

O último teste, realizado no software Cx-Programmer, consistiu no desenvolvimento de uma ordem para o PLC acender um LED numa determinada posição.

Estes testes foram realizados segunda a estrutura apresentada na Figura 5, sendo a variável de estudo os dispositivos de conectividade remota.

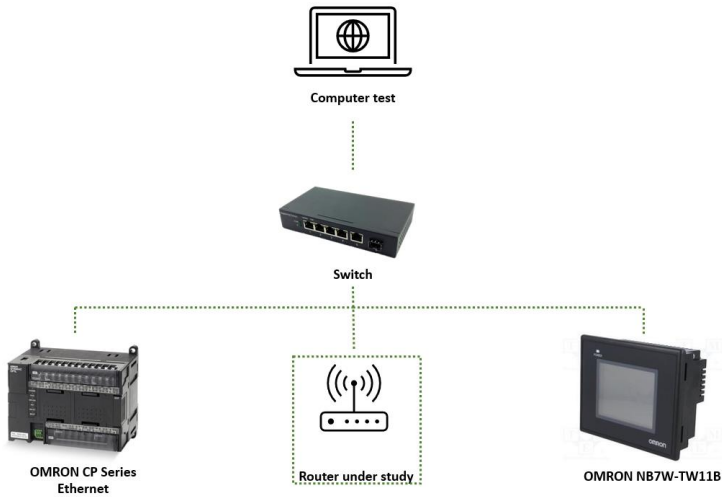

Figura 5. Esboço da estrutura seguida no presente estudo.

3.1.1. DISPOSITIVO DE CONECTIVIDADE REMOTA 1: FLEXY 205- E- WON- HMS NETWORKS FUNCIONAMENTO E CONEXÃO COM DIFERENTES MÁQUINAS

A Ewon é uma marca europeia, fundada em 2001 na Bélgica. É um dos principais fornecedores de dispositivos de acesso remoto baseados em internet, apresentando ainda a capacidade de se conectarem a CLP'S e outros sistemas de automação [25].

O Ewon Flexy 205 é um dispositivo que funciona como um portão entre duas redes, isto é, um router de acesso remoto muito utilizado no mundo industrial (Internet das coisas Industrial (IdCI)), e que permite uma comunicação universal independentemente do protocolo utilizado [26]. Para além de possibilitar o acesso remoto VPN com serviços de conectividade remota (eWON Talk2M), este aparelho permite a ativação de notificações de alarme, a leitura e armazenamento de dados de máquinas, constante monitorização de indicadores de performance (KPIs- *Key Performance Indicators*). Este router estabelece uma ligação segura de rede, de carácter privado (VPN- *Virtual Private Network*), da máquina para qualquer outro lugar através da *cloud* do Ewon, designada por Talk2M [26]. O router comunica de forma eficiente na área local de rede (LAN- *Local Area Network*) com o PLC e a interface do utilizador, num sistema de controlo de fabrico ou de processo, com recurso a uma *ethernet*. Na máquina ao lado, um Ewon deve ser instalado e será ligado a um PLC, a um PC industrial, ou a qualquer outro dispositivo automatizado. Juntos, a solução permite a ligação remota com o PC, laptop, tablet ou até mesmo com um *smartphone*. A conta Talk2M é uma conta gratuita onde é possível criar usuários com e sem restrições de acesso. A versão gratuita permite apenas uma conexão direta, não sendo permitidas conexões simultâneas ao portal Talk2M [26].

Na Figura 6, encontra-se representada a forma de funcionamento e conexão com os diferentes dispositivos relativamente ao primeiro dispositivo de estudo.

Figura 6. Funcionamento Flexy 205 E-Won – HMS Networks [25].

A EWON oferece 3 alternativas de conexão com as máquinas (Jacobsen & Miller):

- Talk2M Software cliente – eCatcher [28];
- Talk2M Aplicação móvel- eCatcher Mobile [27];
- Talk2M *Web* portal- M2*Web* [29].

Na perspetiva do cliente, basta instalar a aplicação do *software* do cliente, designado por eCatcher, num PC que execute o Microsoft Windows. Este *software* estabelece uma ligação VPN através da internet entre o PC e Talk2M, como ilustrado na Figura 6. Quanto à aplicação móvel, esta permite o acesso remoto de qualquer *smartphone* iOS ou Android. Como alternativa, é possível apenas usar uma página *web*, como o Google Chrome, Microsoft Internet ou Mozilla Firefox, sem ser necessário a instalação de alguma aplicação para conectar com as máquinas [28]. Existem várias formas de conexão com as máquinas através da Internet com o objetivo de comunicar com o servidor Talk2. Esta ligação pode ser estabelecida através o uso de uma LAN, que é financeiramente mais amigável, de acesso viável e de velocidade eficaz. A maioria dos sites têm uma LAN que é conectada à Internet, e por este motivo é o método mais utilizado para ligar máquinas. Em contrapartida, as LANs apresentam políticas de segurança complexas que podem não permitir a conexão das máquinas ao servidor Talk2M. Nestes casos, é recomendado as ligações Wi-Fi ou através de *smartphones*. As ligações Wi-Fi estão a ficar cada vez mais comuns em diversas áreas, incluindo no mundo

industrial. À semelhança das LANS, as ligações por Wi-Fi também são tipicamente livre de custos e a conexão também apresenta uma alta velocidade. No entanto, a conectividade e a cobertura da ligação Wi-Fi podem ser postas em causa em áreas industriais com sinais que podem interferir com os sinais Wi-Fi, como por exemplo áreas barulhentas [27]. Quando não há a possibilidade de estabelecer uma ligação por Wi-Fi ou LAN, o uso das tecnologias móveis representam uma boa alternativa. Este serviço móvel está disponível geograficamente em diferentes velocidades. As desvantagens neste tipo de conexão, passam por elevadas taxas de uso de dados móveis e pela possibilidade de o sinal ficar comprometido em algumas áreas remotas, limitando assim o seu uso e fiabilidade. Por estes motivos, é dada uma maior preferência pelas ligações LAN e Wi-Fi quando possível.

As especificações técnicas do dispositivo foram seguidas consoante as informações disponibilizadas pelo fornecedor [26]. Tal como qualquer outro dispositivo conectado à Internet, o Flexy 205 também apresenta um IP padrão, como demonstrado na Tabela 2, que pode ser alterado durante a sua configuração através de um browser .

Tabela 2. Configurações do Dispositivo 1.

Características	**Valor (es)**
LAN IP *Address*	10.0.0.53
LAN *Subnet Mask*	255.255.255.0
Gateway	0.0.0.0

3.1.2. Dispositivo de conectividade remota 2: IE-SR-2GT-LAN-Weidmuller

A Weidmuller é uma empresa alemã, que oferece produtos no âmbito industrial de energia, sinalização e dados [25].

Este dispositivo, IE-SR-2GT-LAN-Weidmuller, fornece um sistema de gestão de acesso remoto seguro, com base em routers *Ethernet* Industrial, o *mWatcher* (*machine Watcher*). Este sistema permite o acesso de forma segura e privativa, bem como a realização de manutenções preventivas e avaliações online do estado da instalação [30]. O sistema mWatcher tem por base um sistema de redes privadas OpenVPN e uma base de dados MySQL. Enquanto as redes privadas virtuais (Virtual Private Network (VPN)), tal como mencionado na secção 2.4.1., dizem respeito a um conjunto de tecnologias de rede que permitem uma extensão segura da rede local, o sistema OpenVPN é um *software* de código aberto e que está baseado num protocolo SSL, protocolo este que é utilizado no comércio eletrónico e que funciona segundo uma codificação de chaves privadas e públicas. Neste tipo de comunicações, uma das partes atua como cliente e a outra como servidor [31]. A aplicação OpenVPN reconhece os dados a enviar por um dos utilizadores e decifra-os antes de os enviar. No outro lado da comunicação, o mesmo programa é também responsável de receber os dados enviados e decifrá-los. Todos os dados são encriptados e decifrados para que se estabeleça um canal seguro. Este sistema da Weidmuller é responsável pela manutenção do servidor na nuvem para cada cliente. Trata-se de uma simples aplicação de software de computador portátil, que permite a aceder a instalações de toda a parte do mundo, que se atualiza automaticamente. Em termos de segurança, como existe uma base de dados em MySQL com um sistema de utilizadores e respetivas passwords, o acesso está limitado apenas aos equipamentos identificados e aprovados.

Os routers industriais da Weidmuller são configurados de forma simples, diretamente da aplicação, sem a necessidade de aceder a um menu ou interface *web*.

Apenas é necessário a junção do router na conta e a introdução dos dados de acesso necessários. A Weidmuller oferece duas versões unicamente com conexão WAN, e outro com as 3 funções WAN, 3G E WiFi no mesmo dispositivo, sendo que o preço desta segunda versão é significativamente mais dispendioso [25]. Neste estudo será usado um dispositivo que se enquadra no primeiro cenário descrito. Existem dois tipos de utilizadores, os administradores e os utilizadores. Na perspetiva do administrador são geridas as licenças, na qual a partir de um único IP se tem acesso ao sistema e a todo o computador que não está na listagem e que não tem acesso ao ID e *password*, bem como o grupo de utilizadores, isto é, conjunto de utilizadores de diferentes categorias. No caso dos utilizadores, é possível visualizarem-se todos os routers e estabelecer conexões entre eles através de um canal seguro VPN [30]. Para além das características técnicas do dispositivo [32] este apresenta ainda funções adicionais, tais como, a criação de um servidor que permite comunicar diretamente com outros routers já existentes e configurados na rede [25].

O U- Link trata-se de uma ferramenta de *cloud* da Weidmuller para serviço de acesso remoto [25]. É usado como ponto de encontro entre o PC e o dispositivo de acesso remoto. Através dele é criado um canal VPN que estabelece uma conexão entre o PC do fornecedor e a máquina que está inserida na rede do cliente. O *software* responsável por estabelecer esta conexão também é denominado por U-Link, onde liberta uma parte do canal VPN, para criar uma outra conexão entre o PC do distribuidor e o ponto de encontro. A outra parte da conexão é feita através do portal, onde basta apenas o router estar conectado à internet para se tornar visível no portal [25]. A conta de acesso ao portal U-link é gratuita, no entanto existem duas versões. Tanto na versão gratuita como na versão padrão o número de utilizadores é ilimitado, no entanto a versão padrão apresenta um maior número de router conectados e uma taxa de comunicação maior. A versão gratuita só permite a criação de um grupo, enquanto a versão padrão permite a criação de vários grupos [25].

3.1.3. DISPOSITIVO DE CONECTIVIDADE REMOTA 3: IXON IXROUTER 2415

A IXON foi fundada no ano de 2014, com o propósito de corresponder à crescente procura de fornecedores de máquinas com a possibilidade de se ligaram à cloud [33]. Ixon *cloud* e IXrouter apresentam uma solução do de manutenção e gestão remota com outros dispositivos (como por exemplo um CLP), apresentando uma plataforma *web* gratuita. O IXrouter trata-se de um router VPN industrial com conectividade IoT. Este dispositivo conecta-se de forma simples e automática à Ixon *cloud*, permitindo o acesso a todos os equipamentos que se encontram configurados na rede. Procura automaticamente o serviço requisitado e encontra o servidor mais rapidamente disponível. Para além disso, o dispositivo possui ainda uma firewall integrada, onde divide a rede do aparelho da rede da empresa, o que confere uma maior segurança ao cliente [34].

Os routers da IXON permitem o uso de conexões VPN para um número ilimitado de utilizadores sem a necessidade da instalação adicional de um software cliente VPN. A IXON apresenta a possibilidade de ter acesso e controlar remotamente os dispositivos através da adição de um serviço HTTP ou um serviço VNC (*Virtual Network Computing*), que é um sistema que executa a partilha da tela do computador que está a ser controlado remotamente [35], como se pode observar na Figura 7.

Figura 7. IXON: Serviço remoto e Plataforma IoT-conexões [34].

Para além disso, permite o controlo a partir da conexão com um servidor *web* ou através de um *smartphone*, tudo isto apenas com a compra de um IXrouter [36].

3.1. Comparação de Preços

Após uma breve pesquisa nos sites online de vendas deste tipo de dispositivos industriais, foi possível definir uma margem de custo dos dispositivos, verificando-se em alguns casos que o preço unitário varia de acordo com a quantidade de compra [37] [38] [39].

Tabela 3. Tabela de preços dos três dispositivos em estudo [37] [38] [39].

Características	**Preço unitário (€)**
IE-SR-2GT-LAN-Weidmuller	912 - 1400€
Flexy 205- E- Won- HMS networks	460- 685€
Ixon IXrouter 2415	≈ 350€

3.2. Testes

Durante este subcapítulo serão abordados os testes realizados para testar o desempenho dos dispositivos de conectividade remota.

3.1.1. FLEXY 205- EWON- HMS NETWORKS

Após estabelecidas todas as ligações físicas, procedeu-se à configuração dos parâmetros necessários para uma correta ligação, tendo por base o guia de configuração do professor Filipe Pereira [44]. Com o router Ewon conectado ao portátil através de um cabo de rede, alterou-se o endereço IP da máquina para a mesma gama de endereço de rede do dispositivo através do *software* eBuddy, na qual foi desenvolvido para facilitar as configurações de dispositivos Ewon [40]. Para além de permitir um conjunto de ações relativas a configurações técnicas de dispositivos, permite ainda visualizar informações relevantes sobre os aparelhos que se encontram disponíveis na rede, como demonstrado na Figura 8.

+

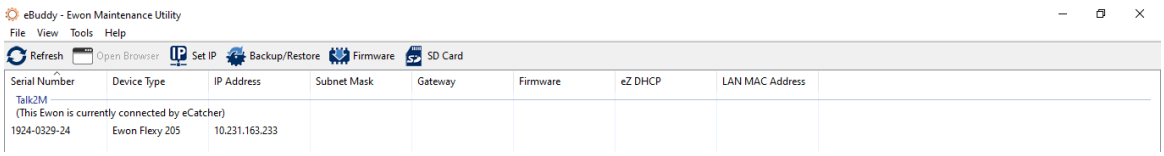

Figura 8. Informação apresentada na página principal eBuddy. após realizadas as configurações.

Na fase seguinte teve-se por base os passos recomendados no guia de configuração [40], onde numa primeira instância é necessário instalar o *software* eCatcher. Tal como

mencionado anteriormente, é um *software* que permite aos utilizadores estabelecer ligações remotas com as suas máquinas e criar uma conta no Talk2M [28]. Depois de criada uma conta, realizam-se testes de configuração ao Sistema, Internet e VPN na página do Flexy 205, na qual se tem acesso direto a partir dos dados introduzidos no eBuddy, numa das opções do menu, denominada por "Open Browser". Antes de se realizar o último teste, adiciona-se o router no eCatcher, onde é gerada uma chave de ativação, que ao ser introduzida na página do router irá permitir a criação do canal VPN. Posteriormente, assim que concluída a testagem à VPN verifica-se na secção "Summary" da página do router se a ligação e configuração VPN foi realizada com sucesso ou não, através de dois ícones assinalados com a cor verde, no canto inferior direito, como observado na Figura 9. Verifica-se ainda no eCatcher, a mudança do estado do aparelho adicionado para "*online*".

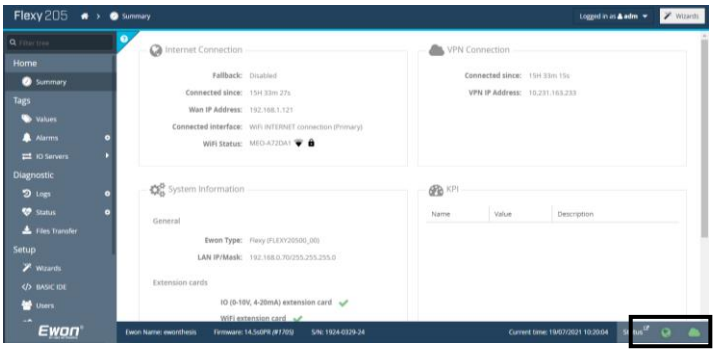

Figura 9. Ligação e configuração VPN com sucesso.

É importante mencionar que, para a realização de testes à VPN, foi usada uma rede privada doméstica, com menos barreiras de firewall para se poder estabelecer a conexão.

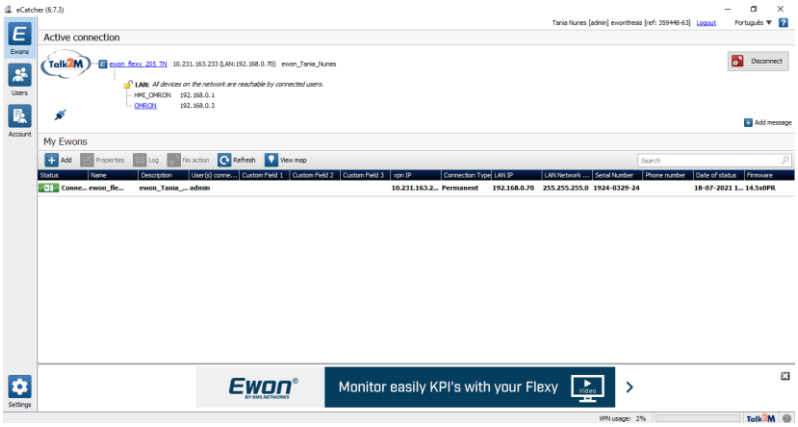

Figura 10. Router *online* no eCather.

O primeiro teste realizado foi a cronometragem do tempo que o router demora a estabelecer o canal VPN. Este teste é feito com recurso ao eCatcher, logo após concluídas as configurações de ligação, isto é, assim que chegamos ao estado online (ver Figura 8). Existem duas opções para dar a ordem de abertura do canal VPN: duplo clique na linha onde está identificado o router, ou selecionar o router e carregar no quarto botão denominado por "Connect". Para se efetuar uma contagem mais precisa, foi escolhida a segunda opção por diminuir o tempo gasto na ordem do utilizador.

Tabela 4. Tempo de abertura do canal VPN por parte do router Ewon.

Dispositivo	**Tempo (s)**
Ewon Flexy 205	Aproximadamente 2.50s

O teste de ping [41], trata-se de um comando que está disponível em quase todos os sistemas operacionais e funciona como um localizador de pacotes na rede de internet, e a sua função consiste na análise do tempo de envio de um pacote de dados e a resposta entre as máquinas que estão conectadas na mesma rede. Para além de nos dar informação sobre o tempo médio de conexão, dá também informação sobre a percentagem de pacotes que são perdidos durante a conexão. Para se efetuar esta

análise, recorreu-se à linha de comandos e fez-se “ping” aos seguintes dispositivos mencionados na Tabela 5 e obteve-se os resultados apresentados na Figuras, 11, 12 e 13.

Tabela 5. Informações necessárias para a realização do teste de tempo médio de conexão e percentagens de falhas.

Dispositivo	**Endereço IP**
Router Ewon	192.168.0.70
PLC OMRON	192.168.0.3
HMI OMRON	192.168.0.1

```
        C:\Users\tania> ping 192.168.0.70
 Reply from 192.168.0.70: bytes=32 time=79ms TTL=64
 Reply from 192.168.0.70: bytes=32 time=76ms TTL=64
 Reply from 192.168.0.70: bytes=32 time=75ms TTL=64
 Reply from 192.168.0.70: bytes=32 time=75ms TTL=64
        Ping statistics for 192.168.0.70:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
  Minimum = 75ms, Maximum = 79ms, Average = 76 ms
```

Figura 11. Resultados do tempo médio de conexão e percentagem de pacotes perdidos (router Ewon com IP: 192.168.0.70).

```
          C:\Users\tania> ping 192.168.0.3
      Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.70: Destination host unreachable.
Reply from 192.168.0.70: Destination host unreachable.
Reply from 192.168.0.70: Destination host unreachable.
Reply from 192.168.0.70: Destination host unreachable.
          Ping statistics for 192.168.0.3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figura 12. Tempo médio de conexão e percentagem de pacotes perdidos (PLC OMRON com IP:192.168.0.3).

```
          C:\Users\tania> ping 192.168.0.1
      Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.70: Destination host unreachable.
Reply from 192.168.0.70: Destination host unreachable.
Reply from 192.168.0.70: Destination host unreachable.
Reply from 192.168.0.70: Destination host unreachable.
          Ping statistics for 192.168.0.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figura 13. Tempo médio de conexão e percentagem de pacotes perdidos (HMI OMRON com IP: 192.168.0.1)

Através da observação dos dados obtidos nas Figuras 11 ,12 e 13, foi possível concluir que o tempo médio de conexão com o router foi cerca de 76 ms e não foram registadas percentagens de falhas quanto aos pacotes transferidos.

De forma a analisar o tempo de transferência de um projeto para cada um dos dispositivos, recorreu-se aos softwares de automatização específico de cada um. No caso do PLC, foi usado o *software* Cx-Programmer, que é o software de programação usado para todas as séries PLC da Omron [42]. O PLC foi configurado segundo os passos recomendados no guia de configuração do professor Filipe Pereira [45]. Foi simulado um projeto exemplo, e procedeu-se à transferência para o PLC segundo os passos demonstrados na Figura 14.

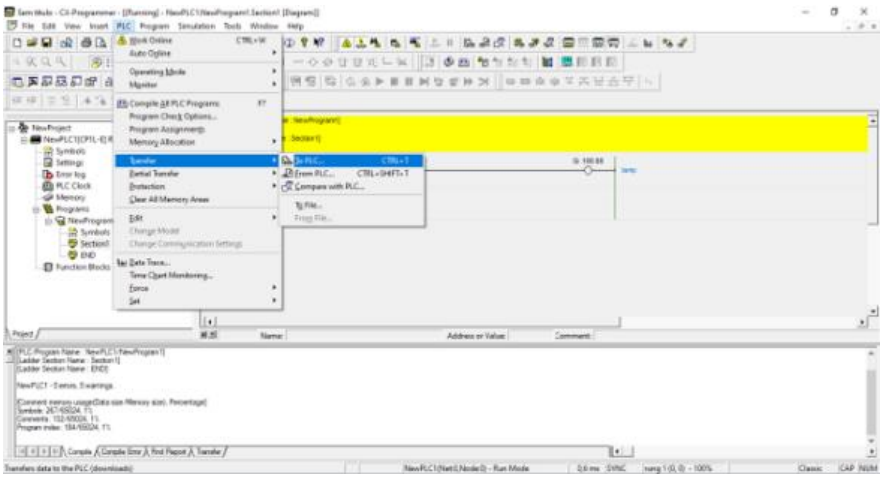

Figura 14. Transferência de projeto para o PLC.

A transferência está concluída quando se obtém uma janela de informação, como demonstrado na Figura 15.

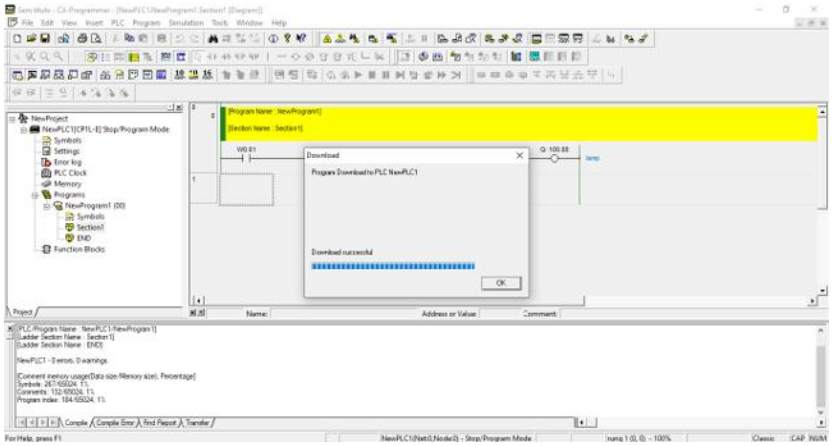

Figura 15. Transferência para o PLC concluída.

Para a transferência de projeto para a HMI, foi usado o *software* NB Designer [43], que é o software que permite criar a aplicação HMI pretendida, e configurada na mesma gama de valores de endereço IP dos restantes dispositivos inseridos na rede [46]. Foi criado um projeto simples no NB Designer, um interruptor ligado a uma lâmpada,

como se pode observar na Figura 16, e posteriormente procedeu-se à transferência desta simulação seguindo os passos da Figura 17.

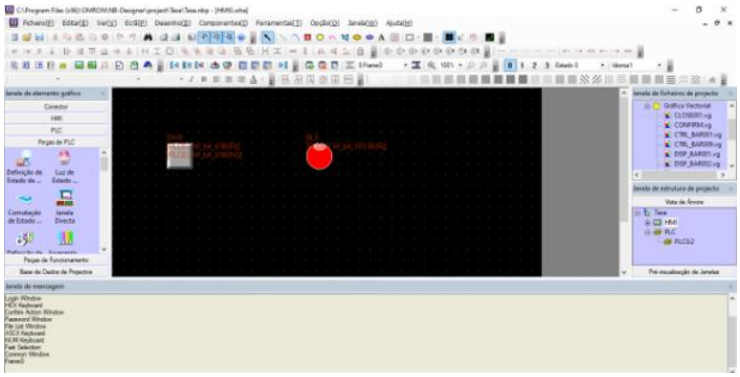

Figura 16. Simulação com um interruptor ligado a uma lâmpada.

É importante mencionar que o dipositivo HMI deve estar conectado ao computador de teste através de um cabo USB para se poder realizar a transferência com sucesso, Figura 17.

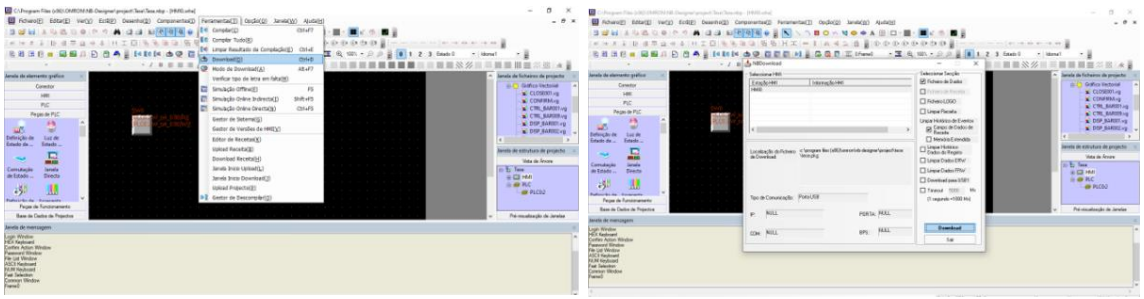

Figura 17. Passos a seguir para a transferência.

Depois de concluída a transferência é despoletada uma janela indicando o sucesso da operação, Figura 18.

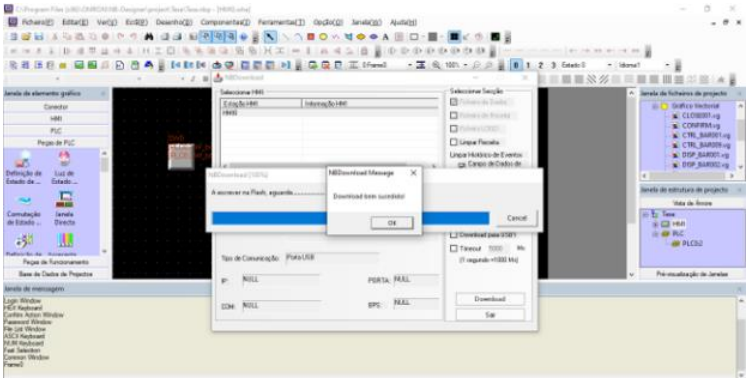

Figura 18. Conclusão da transferência para a HMI.

Com recurso a um cronómetro online foram registados os seguintes tempos de download como demonstrado na Tabela 6.

Tabela 6. Resultados obtidos na cronometragem do tempo de transferência de projetos para os diferentes equipamentos.

Software	**Tempo (s)**
Cx Programmer (transferência para o PLC)	5.775 s
Nb Designer (transferência para a HMI)	3.571 s

Para analisar o tempo de resposta do PLC quando este é ordenado a ligar/desligar um LED, forçou-se uma variável a 1, na qual se pretende acender um LED na posição 0 da parte inferior "OUT" do PLC. No programa Cx-Programmer foi criada uma linha de conexão entre um interruptor (assinalado com a letra a) e uma lâmpada (assinalado com letra b), como demonstrado na Figura 19. Ao fazer duplo clique no interruptor, coloca-se no campo "value" o valor de 0 com o intuito de desligar o LED. No caso de se pretender ligar o LED, basta inserir no campo "value" o valor 1. Na Figura 19, está apresentado o resultado desta última configuração. Efetuou-se a cronometragem do

tempo de confirmação do LED a um valor de 0 e 1, onde nos dois casos se pode afirmar que o tempo de resposta do PLC é instantâneo.

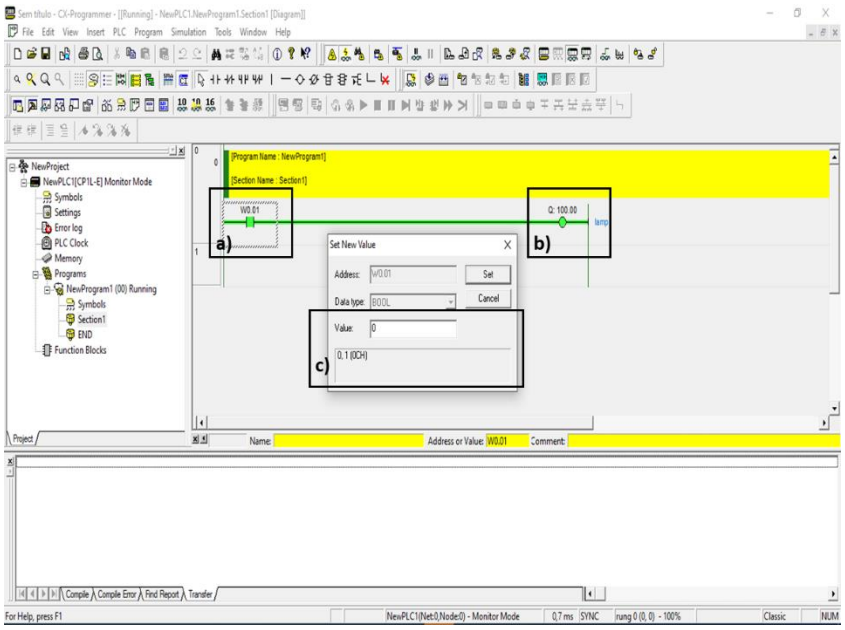

Figura 19. Forçar uma variável a zero no Cx Programmer.

Figura 20. PLC após configuração de variável a um valor de 1.

3.1.2. E-SR-2GT-LAN-WEIDMULLER

Após estabelecidas todas as ligações físicas necessárias para a conexão entre os diferentes equipamentos, segue-se os passos fornecidos pelo manual disponibilizado pela Weidmuller [47]. O primeiro passo para a configuração do router passa pela definição do endereço IP do computador de teste na mesma gama de valores do endereço do equipamento, fornecidos pelo fornecedor, como demonstrado na Figura 21. No aparelho em estudo, é fornecido um folheto com algumas informações básicas e onde podemos encontrar o IP de origem do equipamento.

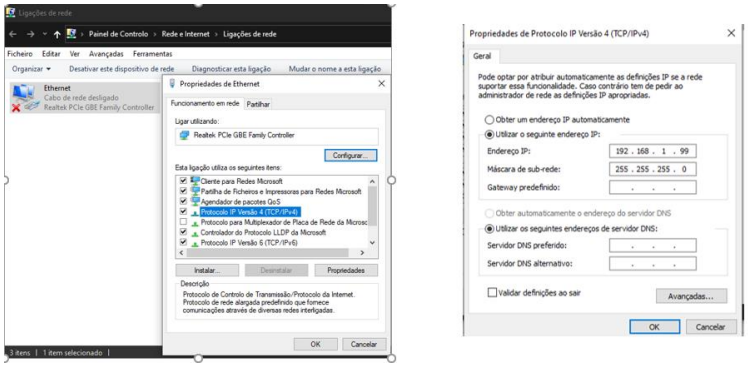

Figura 21. Configuração do endereço IP do computador de tese.

Depois de definido o endereço IP nos diferentes equipamentos, estes já se encontram aptos para comunicar entre si. A partir deste ponto, é possível abrir a página *Web* do router em estudo, onde basta apenas inserir o seguinte endereço IP em qualquer *browser*: 192.168.1.110 (endereço de origem disponibilizado pelo fornecedor). É despoletada uma janela com a requisição de credencias que irão permitir avançar com as restantes configurações para uma comunicação com sucesso, sendo estas também fornecidas no folheto. Assim que efetuado o *login,* é necessário configurar os campos

de rede. Para isso, acede-se à categoria das configurações, nomeadamente "*IP Configuration*". É importante mencionar que o router foi ligado a um *switch*, que por sua vez se liga ao computador teste por um cabo de rede, através da porta LAN. Como se pode observar na Figura 22, é definido um endereço IP para essa mesma porta e no caso da WAN, é selecionado o protocolo DHCP (*Dynamic Host Configuration Protocol*), que se trata de um protocolo que permite às máquinas a obtenção de IP's de forma automática [48].

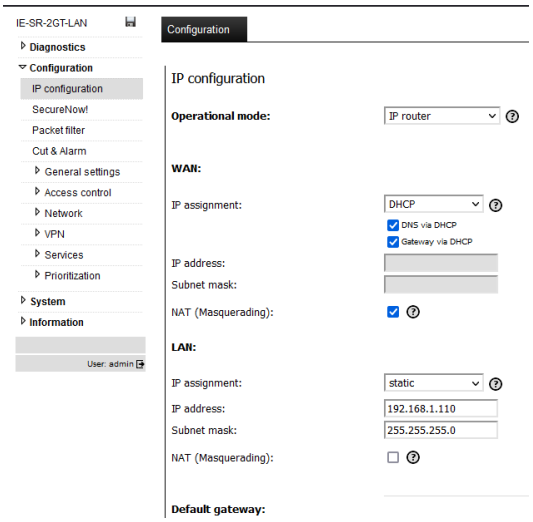

Figura 22. Configurações de rede na página do router Weidmuller.

De forma a verificar se o equipamento tem ou não acesso à internet foi realizado um teste de `ping` estando esta opção disponível na secção denominada por "Diagnostics". Foram colocados endereços conhecidos tais como "8.8.8.8" e "www.google.com", onde se verificou o sucesso da conexão com a internet. Para que este ponto seja possível, é necessário que o router Weidmuller esteja a receber internet de um outro router através de um cabo de rede, visto que não apresenta a possibilidade de conexão via Wi-Fi [47]. O próximo passo, consiste na abertura de um canal VPN, na qual o *software* responsável por esta ligação é o U-Link. Para tal, recorre-se à opção "U-Link" localizado na secção das configurações no campo "VPN" e segue-se os passos de acordo com a numeração da Figura 23, de forma a permitir o estabelecimento do canal VPN. No ponto 4, é necessário a inserção de um código de ativação fornecido no início

do registo da conta do utilizador, onde é identificada a máquina em estudo. É também possível encontrar este mesmo código na página *Web* do U-Link na categoria de "Device Management", como se pode observar na Figura 24 [47].

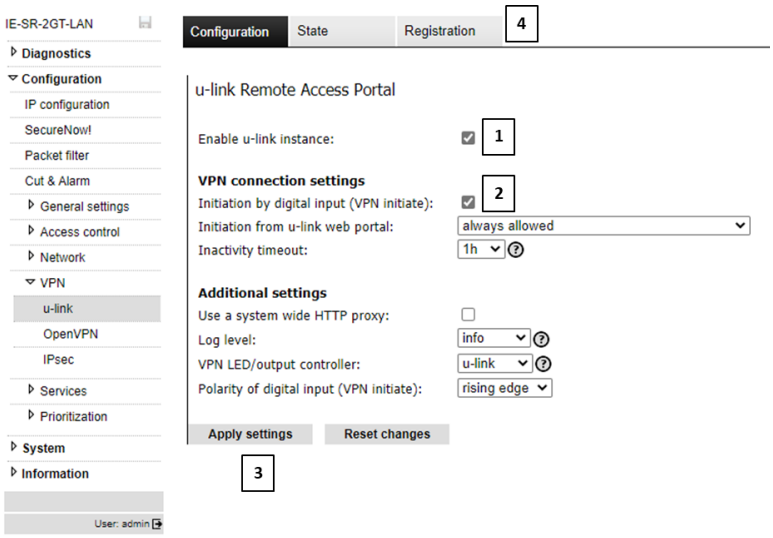

Figura 23. Configurações VPN.

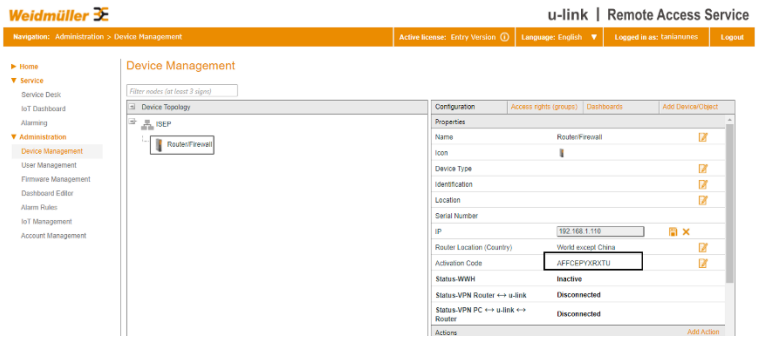

Figura 24. Código de ativação.

Para verificar o correto funcionamento da ligação VPN, recorre-se ao campo "state", onde é possível verificar o corrente estado da conexão e forçar a abertura do canal VPN, como se pode observar na Figura 25.

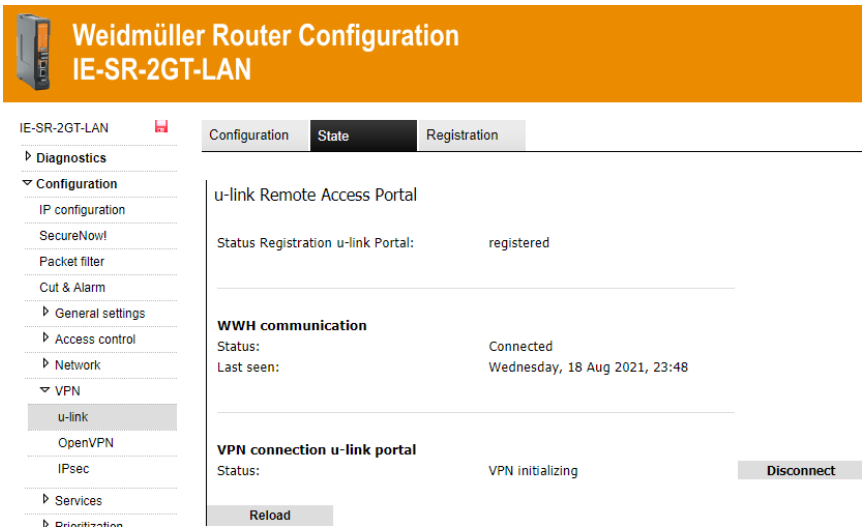

Figura 25. Estado da ligação VPN.

O primeiro teste realizado foi a cronometragem do tempo que o router demora a estabelecer o canal VPN. Este teste é feito com recurso ao software U-Link VPN Client, após a conclusão de todas as configurações de ligação. Depois de seguidos todos os passos do tutorial disponibilizado no site de serviço de acesso remoto da Weidmuller, apresentado na Figura 26.

Figura 26. Página *Web* Weidmuller- u-Link- Remote Access Service.

Efetuou-se a cronometragem do tempo de abertura do canal VPN, após o clique na opção “Connect VPN” como demonstrado na Figura 27, registando-se os seguintes tempos apresentados na Tabela 7.

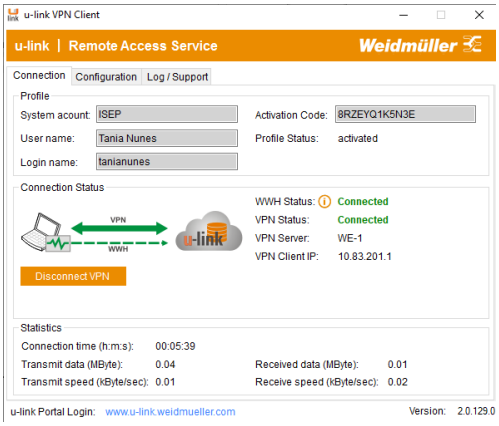

Figura 27. Canal VPN estabelecido.

Tabela 7. Tempo de abertura do canal VPN por parte do router Weidmuller.

Dispositivo	**Tempo (s)**
E-SR-2GT-LAN-Weidmuller	Aproximadamente 17.40 s

À semelhança do router da Ewon, testou-se também o tempo médio de conexão entre os diferentes dispositivos e a percentagem de falhas relacionadas com os pacotes partilhados. Assim sendo, recorreu-se à linha de comandos e efetuou-se testes “ping” aos diferentes endereços IP, descritos na Tabela 8.

Tabela 8. Informações necessárias para a realização do teste de tempo médio de conexão e percentagens de falhas.

Dispositivo	Endereço IP
Router Weidmuller	192.168.1.110
PLC OMRON	192.168.1.3
HMI OMRON	192.168.1.1

```
        C:\Users\tania> ping 192.168.1.110
Reply from 192.168.1.110: bytes=32 time=79ms TTL=64
Reply from 192.168.1.110: bytes=32 time=76ms TTL=64
Reply from 192.168.1.110: bytes=32 time=75ms TTL=64
Reply from 192.168.1.110: bytes=32 time=75ms TTL=64
        Ping statistics for 192.168.1.110:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Figura 28. Tempo médio de conexão e percentagem de pacotes perdidos (router Weidmuller com endereço IP:192.168.1.110).

```
         C:\Users\tania> ping 192.168.1.3
 Reply from 192.168.1.3: bytes=32 time=5ms TTL=30
 Reply from 192.168.1.3: bytes=32 time=4ms TTL=30
 Reply from 192.168.1.3: bytes=32 time=4ms TTL=30
 Reply from 192.168.1.3: bytes=32 time=3ms TTL=30
         Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 3ms, Maximum = 5ms, Average = 4ms
```

Figura 29. Tempo médio de conexão e percentagem de pacotes perdidos (PLC OMRON com endereço IP: 192.168.1.3).

```
          C:\Users\tania> ping 192.168.1.1
  Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
  Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
  Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
  Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
          Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 30. Tempo médio de conexão + percentagem de pacotes perdidos (HMI OMRON com endereço IP:192.168.1.1).

Através da observação dos dados obtidos nas Figuras 28,29 e 30 foi possível concluir que o tempo médio de conexão com o router foi cerca de 1 ms e não foram registadas percentagens de falhas quanto aos pacotes transferidos.

Para efeitos de cronometragem do tempo de transferência de um projeto para as diferentes máquinas, HMI e PLC, foram seguidos os mesmos passos de transferência realizados no dispositivo de conectividade remota 1, sendo que neste caso os diferentes aparelhos encontram-se conectados através do router Weidmuller. Foram registados os tempos de transferência de um projeto para cada um dos dispositivos, como se pode observar na Tabela 9:

Tabela 9. Resultados obtidos na cronometragem do tempo de transferência de projetos para os diferentes equipamentos

Software	**Tempo (s)**
Cx Programmer (transferência para o PLC)	7.44 s
Nb Designer (transferência para a HMI)	6.26 s

Para analisar o tempo de resposta do PLC ao ligar e desligar um LED, na posição 0 da parte inferior “OUT” do PLC, efetuou-se o mesmo procedimento descrito no subcapítulo 3.3.1., onde se verificou igualmente uma resposta imediata.

3.1.3. IXON IXROUTER 2415

Após estabelecidas todas as ligações físicas, as configurações do router da Ixon começam pela criação de uma conta gratuita no portal Ixon Cloud [49]. Esta conta permite adicionar um número ilimitado de utilizadores ou clientes. O segundo passo consiste em gerar um ficheiro de configurações (formato wizard), onde são definidas as opções de rede. Neste caso, foi definido que o router receberia rede através de uma rede Wi-Fi de carácter doméstica, visto que este dispositivo apresenta essa possibilidade de ligação com a Internet. Este ficheiro foi transferido para uma Pen USB (fornecida juntamente com a máquina), que por sua vez é colocada no dispositivo, e onde este é automaticamente adicionado ao portal. A abertura do canal VPN é feita de forma instantânea assim que o dispositivo é adicionado ao portal. Tal como mencionado no subcapítulo 3.1.3, nesta fase a firewall interna separa a rede do dispositivo da rede doméstica, o que confere uma maior segurança à máquina ao mesmo tempo que se encontra remotamente acessível. Para que os diferentes dispositivos comuniquem entre si, é necessário que sejam alterados os endereços IP de cada aparelho. No portal, é possível consultar qual o endereço IP do router da Ixon (192.168.0.50), na secção de "Fleet Manager" e alterar nos respetivos softwares das máquinas conectadas à rede (HMI- NB Designer (192.168.0.1) e PLC- Cx Programmer (192.168.0.3) o seu endereço para a mesma gama.

Dado que a introdução do router no portal é realizada de forma automática assim que se insere a Pen USB no dispositivo, a abertura do canal VPN é executada de forma instantânea. Este facto representa uma vantagem sobre os restantes dispositivos em estudo, na medida em que não exige a instalação de um software de utilização, basta apenas a utilização do portal da Ixon Cloud.

Como nos anteriores dispositivos, testou-se também o tempo médio de conexão entre os diferentes dispositivos e a percentagem de falhas relacionadas com os pacotes

partilhados. Assim sendo, recorreu-se à linha de comandos e efetuou-se testes "ping" aos diferentes endereços IP, descritos na Tabela 10.

Tabela 10. Informações necessárias para a realização do teste de tempo médio de conexão e percentagens de falhas.

Dispositivo	**Endereço IP**
Router Ixon	192.168.0.50
PLC OMRON	192.168.0.3
HMI OMRON	192.168.0.1

```
        C:\Users\tania> ping 192.168.0.50
Reply from 192.168.0.50: bytes=32 time=79ms TTL=128
Reply from 192.168.0.50: bytes=32 time=76ms TTL=128
Reply from 192.168.0.50: bytes=32 time=75ms TTL=128
Reply from 192.168.0.50: bytes=32 time=75ms TTL=128
        Ping statistics for 192.168.0.50:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 31. Tempo médio de conexão e percentagem de pacotes perdidos (router Ixon com endereço IP:192.168.0.50).

```
        C:\Users\tania> ping 192.168.0.3
  Reply from 192.168.1.3: bytes=32 time=1ms TTL=30
  Reply from 192.168.1.3: bytes=32 time=2ms TTL=30
  Reply from 192.168.1.3: bytes=32 time=2ms TTL=30
  Reply from 192.168.1.3: bytes=32 time=1ms TTL=30
        Ping statistics for 192.168.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Figura 32. Tempo médio de conexão e percentagem de pacotes perdidos (PLC OMRON com endereço IP:192.168.0.3).

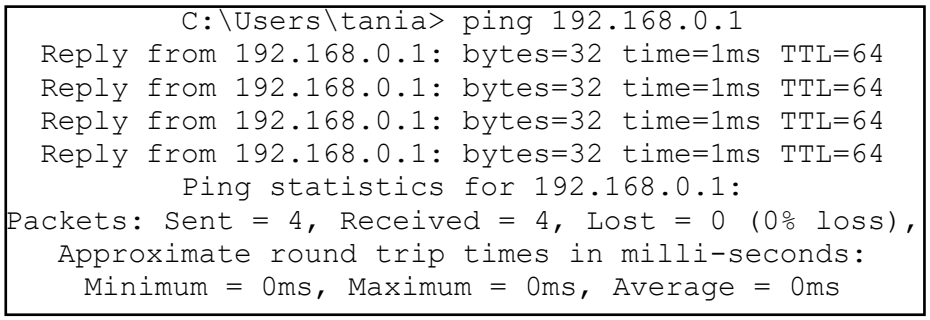

Figura 33. Tempo médio de conexão e percentagem de pacotes perdidos (HMI OMRON com endereço IP:192.168.0.1).

Através da análise dos dados obtidos nas Figuras 31.32 e 33, foi possível concluir que o tempo médio de conexão com o router é praticamente instantâneo e não foram registadas percentagens de falhas quanto aos pacotes transferidos.

Para efeitos de cronometragem do tempo de transferência de um projeto para as diferentes máquinas, HMI e PLC, foram seguidos os mesmos passos de transferência realizados nos outros dispositivos, sendo que neste caso os diferentes aparelhos encontram-se conectados através do router da Ixon, pela qual se registaram os seguintes tempos, como se pode observar na Tabela 11:

Tabela 11. Resultados obtidos na cronometragem do tempo de transferência de projetos para os diferentes equipamentos.

Programa	**Tempo (s)**
Cx Programmer (transferência para o PLC)	7.93 s
Nb Designer (transferência para a HMI)	3.48s

Para analisar o tempo de resposta do PLC ao ligar e desligar um LED, na posição 0 da parte inferior “OUT” do PLC, efetuou-se o mesmo procedimento descrito no subcapítulo 3.2.1.4., onde se verificou igualmente uma resposta imediata.

3.2. Comparação de resultados

Concluídos os testes de performance dos dispositivos de conectividade remota, é possível averiguar qual é que apresenta o melhor desempenho.

Tendo em conta os modos de conexão à internet, aquele que apresenta uma maior desvantagem em relação aos restantes dispositivos é o router da Weidmuller, pelo facto de necessitar de receber internet através de um cabo de rede ligado a outro router. Tanto o router da Ewon como da Ixon, apresentam diferentes formas de ligação. O Flexy 205 da Ewon, apresenta várias opções de conexão à internet: WAN, WiFi e 3G [26], tal como o router da Ixon: Ethernet, WiFi e 4G [34].

Em relação ao portal de utilização e respetivas configurações necessárias para o seu funcionamento, tanto o Flexy 205- Ewon- HMS Networks como o E-SR-2GT-LAN-Weidmuller apresentam um carácter intuitivo e simples, no entanto, implicam um elevado número de passos de configurações e dados de *setup* do dispositivo antes do estabelecimento de conexão, pelo que se evidencia nos dois casos como pontos de melhoria. Este cenário não se enquadra no router da Ixon, pelo facto de ser o mais rápido e com poucos passos de configuração.

Quanto à abertura do canal VPN, apesar do router da Weidmuller registar um tempo maior na abertura do canal VPN, como se pode observar na Tabela 12, supera mais facilmente os obstáculos da firewall quando comparado ao Flexy 205, na qual foi necessário reduzir no software do eCatcher o índice de barreira da firewall durante a sua utilização. A abertura do canal VPN verificou-se forma instantânea no dispositivo de conectividade remota da Ixon (Tabela 12).

Relativamente à criação de registos nos diferentes aparelhos, o router da Weidmuller verificou-se como o mais prático, ao exigir apenas a criação de utilizador no Portal de Acesso remoto da U-Link, quando comparado ao router da Ewon, que exige a

criação de uma conta no *software* M2*Web* e Talk2M, sendo os dados deste último também inseridos no software eCatcher. No entanto, ambos apresentam um maior número de fases de registo, quando comparado ao router da Ixon.

Quanto às versões de acesso, em todos os dispositivos estudados são gratuitas, no entanto alguns deles apresentam certas limitações. No caso da Ewon, não permite ligações simultâneas, isto é, apenas permite um utilizador por sessão. Quanto à Weidmuller, tanto na versão gratuita como na versão padrão, o número de utilizadores é limitado. No caso da Ixon, não se verifica nenhuma limitação relativamente ao número de utilizadores inseridos no portal.

Tabela 12. Resultados obtidos dos testes de desempenho.

Testagem	**Flexy 205- E- Won- HMS networks**	**E-SR-2GT-LANWeidmuller**	**Ixon Ixrouter 2415**
Mudança de estado para online (s)	2.50s	17.40 s	Instantâneo
Tempo médio de conexão (s)	76 ms	1 ms	0 ms
Percentagem de falhas (%)	0%	0%	0
Tempo de transferência de um projeto para o PLC (s)	5.775 s	7.44 s	7,93 s
Tempo de transferência de um projeto para a HMI (s)	3.571 s	6.26 s	3,48 s
Forçar variáveis – Ligar/Desligar LED	Resposta imediata	Resposta Imediata	Resposta Imediata
Preço (€)	460€ - 685€	912€ - 1400€	≈ 350€
Tipo de conta	Gratuíta	Gratuíta	Gratuíta

3.3. Balanço do estudo realizado

A realização do presente estudo apresenta como requisitos teóricos, o conhecimento de redes de computadores, redes industriais, indústria 4.0 e acesso remoto. Para além disso exige um conhecimento básico sobre como ligar, fisicamente, os diferentes dispositivos inseridos na rede.

Quanto a conhecimento operacional, é necessário um computador de teste, fios elétricos, dispositivos de conectividade remota, uma HMI e uma PLC. O computador de teste deverá apresentar a capacidade de execução dos diferentes programas do dispositivo.

A nível de tratamento e registo de dados, é necessária a utilização de Microsoft Word e Microsoft Excel.

3.4. Conclusão

Através da realização deste estudo, verifica-se que as soluções testadas garantem os requisitos necessários para solucionar o acesso remoto da bancada didática. No entanto, é necessário ter em conta fatores que promovem o melhor desempenho da bancada didática no que toca à possibilidade de acesso remoto.

Tendo em conta os modos de conexão à internet, assume-se como grande importância a possibilidade de escolha no que toca às formas de ligação, visto que o dispositivo escolhido será inserido numa bancada didática de acesso remoto aos alunos de uma instituição de ensino superior. Os dispositivos que cumprem com maior satisfação este requisito são os routers: Flexy 205- Ewon- HMS Networks e Ixon IXrouter 2415, pelo facto de não apresentarem como obrigatoriedade uma ligação física de rede.

Quanto à praticidade de utilização dos softwares incorporados em cada dispositivo, aquele que se verificou ser o mais simples e intuitivo, foi o router da Ixon, por despender de menos tempo no que toca a configurações necessárias para a sua utilização. Para além disso, este aparelho executa a abertura do canal VPN de forma automática assim que é inserido no portal da Ixon Cloud, enquanto os restantes dispositivos exigem a instalação de softwares de utilização extra para ordenar a abertura do canal.

Dado ao principal objetivo destes dispositivos, que é conferir o acesso remoto aos alunos do Instituto Superior de Engenharia do Porto, a segurança é um fator crucial a ter em conta na escolha do dispositivo. Neste sentido, aquele que cumpre com uma maior satisfação este requisito é, novamente, o router da Ixon, na medida em que, assim que aberto o canal VPN, o dispositivo separa a rede da máquina da rede do cliente, como mencionado no capítulo 3.1.3.1., o que confere uma maior segurança na conexão. Observando os resultados dos testes de cronometragem do tempo de mudança de estado, o Ixon IXrouter 2415 apresenta um melhor tempo (quase instantâneo), quando comparado aos restantes dispositivos de estudo.

Quanto à criação de registos, tanto o dispositivo da Ewon como da Weidmuller, apresentam um maior número de fases para a conclusão da criação de uma conta de utilizador, quando comparado ao dispositivo de conectividade remota número 3, que apenas exige a criação de uma conta no portal da Ixon Cloud.

Ao analisar os resultados obtidos nos testes de performance dos dispositivos em estudo, a praticidade de utilização, a possibilidade de escolha no modo de ligação com a rede, preço e a segurança de ligação remota, de uma forma geral aquele que cumpre de uma forma mais satisfatória e que apresenta um melhor desempenho é o router Ixon Ixrouter 2415.

BIBLIOGRAFIA

1. Zareh A. Demirdjian – To Evaluate the Efficiency and Performance of Virtual Workplaces in SMEs in Lebanon, página 13, Capítulo 1.1. (Maio 2018). [Última consulta: 10 de Outubro de 2021]. Disponível em: To Evaluate the Efficiency and Performance of Virtual Workplaces in SMEs in Lebanon

2. Paulo Souza, Silvio Junior, Geraldo Neto – Indústria 4.0: Contribuições para o setor produtivo moderno (Outubro 2017). [Última consulta: 10 de Outubro de 2021]. Disponível em: Indústria 4.0: Contribuições para o setor produtivo moderno

3. Parker Brazil Team – Trabalho remoto eficiente no ambiente industrial. Brasil. [Última consulta: 10 de Outubro de 2021]. Disponível em:Trabalho remoto eficiente no ambiente industrial

4. Siemens – TeleService V6.1 SP3 – Service Software SIMATIV S7 and C7 (2010). [Última consulta: 10 de Outubro de 2021]. Disponível em: Teleservice

5. Siemens – Acesso remoto seguro e simplificado (2020). [última consulta: 10 de Outubro 2021]. [Última consulta: 10 de Outubro de 2021]. Disponível em: SIEMENS

6. Douglas Mendes – Redes de Compuradores (Teoria e Prática), NOVATEC. [Última consulta: 10 de Outubro de 2021]. Disponível em: Redes de Computadores

7. Ricardo Macedo, Roberto Franciscatto, Guilherme Cunha, Cristiano Bertolini- Redes de Computores, p. 196, UAB/NTE/UFSM (2018). [Última consulta: 10 de Outubro de 2021]. Disponível em: Redes de Computadores

8. ISSAM IBRAHIM – Conjunto de protocolos TCP/IP e suas falhas, (2011), p.34. [Última consulta: 10 de Outubro de 2021]. Disponível em: Protoclos TCP/IP e suas falhas

9. Ilma Vienazindyte, NordVPN – TCP vs UDP:Comparando Protocolos (2020). [Última consulta: 10 de Outubro de 2021]. Disponível em: TCP vs. UDP (NordVPN)

10. Alexandre Lugli, Max Santos – Redes Industriais para automação industrial (AS-I, Profibus e Profinet), p.176, Érica. [Última consulta: 10 de Outubro de 2021]. Disponível em: Redes Industriais para Automação Industrial

11. Balluff – Tipos de redes industriais e suas principais aplicações no mercado (2019). [Última consulta: 10 de Outubro de 2021]. Disponível em: Tipos de redes industriais - Aplicações no mercado

12. Bruna Rasmussen – LAN, WLAN, MAN, WAN, PAN: conheça os principais tipos de redes (2013), Canaltech. [Última consulta: 10 de Outubro de 2021]. Disponível em: Principais tipos de redes

13. Saurabh Vaidya, Prashant Ambad, Santosh Bhosle – Industry 4.0. – A Glimpse, (2018), p.6. [Última consulta: 10 de Outubro de 2021]. Disponível em: Industry 4.0 - A Glimpse

14. Gizem Erboz – How to define industry 4.0: the main pillars of industry 4.0 – (2017), p.8. . [Última consulta: 10 de Outubro de 2021]. Disponível em: Pilares da indústria 4.0

15. Michael Rubmann, Markus Lorenz, Philipp Gerbert, Manuela Waldner, Pascal Engel, Michael Harnisch, Jan Justus – Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries (2015). [Última consulta: 10 de Outubro de 2021]. Disponível em: BCG Industry 4.0

16. *Shiyong Wang, Jiafu Wan, Di Li – Implementing Smart Factory of Industrie 4.0: An Outlook (2016).*). [Última consulta: 10 de Outubro de 2021]. Disponível em:Industry 4.0

17. Rômulo Martins – Pública, Privada, Comunidade ou Híbrida? Conheça os modelos de *Cloud Computing*, Qi Network.). [Última consulta: 10 de Outubro de 2021]. Disponível em: Tipos de *cloud*

18. André Cintra – O que é realidade aumentada e como ela funciona?, *Post* Digital.). [Última consulta: 10 de Outubro de 2021]. Disponível em: Realidade aumentada

19. Miguel Mendoza – Cybersegurança ou segurança da informação? Explicando a diferença (2017). [Última consulta: 10 de Outubro de 2021]. Disponível em: Cybersegurança

20. Exsto Tecnologia – XC132 – Banco de Ensaios para PLC Siemens (S7 – 300), p.11. [Última consulta: 10 de Outubro de 2021]. Disponível em: Soluções EXSTO em Educação Tecnológica

21. Francisco Lemos – Controlo remoto de conversor de potência no âmbito da Indústria 4.0, Lisboa (2018), p.134. [Última consulta: 10 de Outubro de 2021]. Disponível em: Controlo remoto - Indústria 4.0

22. Alfaco MP – PLC – O que é e como funciona o controlador lógico programável. [Última consulta: 10 de Outubro de 2021]. Disponível em: PLC

23. TechLib – Acesso Remoto. [Última consulta: 10 de Outubro de 2021]. Disponível em: Acesso Remoto

24. Jinan Should Shine Import and Export Co. – Basic Electronis Training Bench Educational Equipment, Teaching Equipment. . [Última consulta: 11 de Outubro de 2021]. Disponível em: Didatic Bench

25. Bruno Ferreira – Estudo e teste de dispositivos de acesso remoto aplicado a máquinas industriais (2017), p.83. . [Última consulta: 11 de Outubro de 2021]. Disponível em: Dispositivos de acesso remoto

26. Ewon by HMS Networks– Ewon Flexy 205. [Última consulta: 11 de Outubro de 2021]. Disponível em: Flexy 205

27. Jon Jacobsen, Lawrence Miller – Secure Remote Access for Industrial Machines (2017), p.61, Ewon.

28. Ewon by HMS Networks – eCatcher. [Última consulta: 11 de Outubro de 2021]. Disponível em: eCatcher

29. Ewon by HMS Networks – M2*Web*: portal to your machines. [Última consulta: 11 de Outubro de 2021]. Disponível em: M2*Web*

30. Weidmuller – mWatcher: seguro sistema de gestão de acesso remoto a máquinas e instalações. [Última consulta: 11 de Outubro de 2021]. Disponível em: mWatcher

31. Weidmuller – Router de acesso remoto u-link da Weidmuller. [Última consulta: 11 de Outubro de 2021]. Disponível em: U-link Weidmuller

32. Weidmuller – Product Catalogue: Industrial Ethernet. [Última consulta: 11 de Outubro de 2021]. Disponível em: Weidmuller product catalogue

33. Ixon – Ixon our story. [Última consulta: 11 de Outubro de 2021]. Disponível em: Ixon

34. Ixon – O edge gateway para IXON Cloud. [Última consulta: 11 de Outubro de 2021]. Disponível em: IXrouter

35. Bradley Mitchell – What is Virtual Network Computing (VNC)? (2020), LifeWire. [Última consulta: 11 de Outubro de 2021]. Disponível em: VNC

36. Noortje Vollenberg – IXouter: Industrial VPN Router for PLC Remote Access and Data (2021), Ixon. . [Última consulta: 11 de Outubro de 2021]. Disponível em: IXrouter

37. Electronic, A Master Electronics Company – Weidmuller Canada. [Última consulta: 11 de Outubro de 2021]. Disponível em: Weidmuller

38. Industrial Networking Solutions, Industrial & Enterprise IoT Solutions. [Última consulta: 11 de Outubro de 2021]. Disponível em: Flexy 2025

39. SMC, Our Knowledge is your power. [Última consulta: 11 de Outubro de 2021]. Disponível em: Flexy 205

40. Ewon Machines can talk – Application User Guide; eBuddy, p.16. [Última consulta: 11 de Outubro de 2021]. Disponível em: eBuddy

41. Exfo Glossary- Packet Internet or Inter-Network Groper (PING): [Última consulta: 11 de Outubro de 2021].Disponível em:PING

42. OMRON – CX- Programmer: A programação e depuração de PLC nunca foi mais fácil. [Última consulta: 11 de Outubro de 2021]. Disponível em:Cx-Programmer

43. OMRON – Série NB, O HMI económico e repleto de funcionalidades. [Última consulta: 11 de Outubro de 2021]. Disponível em:NB Designer

44. Filipe Pereira – Guia rápido E-won Flexy 205.

45. Filipe Pereira - E-won Flexy 205, Guia confiração PLC's.

46. Joaquim Rosell – NB Designer: Comunicació per Ethernet. OMRON. [Registo Vídeo], (2020). [Última consulta: 11 de Outubro de 2021]. Disponível em: NB Designer: Comunicação por Ethernet

47. Weidmuller – Industrial Security Router /Firewall: IE-SR-2GT-LAN, IE-SR-2GT-UMTS/3G, Setembro (2013), p.103. [Última consulta: 11 de Outubro de 2021]. Disponível em: Weidmuller IR-SR-2GT-LAN manual

48. Efficient iP – What is DHCP? Dynamic Host Configuration Protocol. [Última consulta: 11 de Outubro de 2021]. Disponível em: DHCP

49. IXON – Ixon Cloud. [Última consulta: 11 de Outubro de 2021]. Disponível em: Ixon Cloud