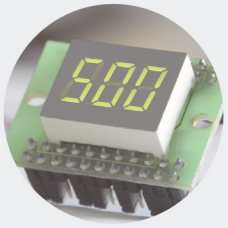
INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES






SISTEMA SEGURO DE CONTROLO DE BARREIRA PARA PASSAGENS DE NÍVEL

JORGE GONZALEZ BEATO
julho de 2021

POLITÉCNICO
DO PORTO

Politécnico do Porto
Instituto Superior de Engenharia do Porto

SISTEMA SEGURO DE CONTROLO DE BARREIRA PARA PASSAGENS DE NÍVEL

Jorge González Beato

Mestrado em Engenharia Electrotécnica e de Computadores
Área de Especialização em Automação e Sistemas

Departamento de Engenharia Eletrotécnica
Instituto Superior de Engenharia do Porto

Julho, 2021

Esta dissertação satisfaz, parcialmente, os requisitos que constam da Ficha de Unidade Curricular de Tese/Dissertação, do 2º ano, do Mestrado em Engenharia Electrotécnica e de Computadores, Área de Especialização em Automação e Sistemas.

Candidato: Jorge González Beato, Nº 1160697, 1160697@isep.ipp.pt

Orientação Científica: Manuel Gericota, mgg@isep.ipp.pt

Empresa: Efacec

Orientador: José Mário Fonseca, jose.fonseca@efacec.com

Departamento de Engenharia Eletrotécnica
Instituto Superior de Engenharia do Porto
Rua Dr. António Bernardino de Almeida, 431, 4200–072 Porto

Julho, 2021

Agradecimentos

Em primeiro lugar, quero agradecer ao meu orientador da faculdade Eng. Manuel Gericota pela orientação, disponibilidade e ajuda prestada na realização da Tese, ao longo do ano.

Gostaria também de agradecer à equipa da Efacec pela amabilidade e ajuda prestada. Em especial, ao meu orientador da Efacec Eng. José Mário Fonseca, pela paciência, seguimento e orientação ao longo da realização deste projeto, ao Eng. João Marques Martins, pela disponibilidade e material de suporte prestado nas tarefas de aprendizagem, ao Eng. André Arruela, pela disponibilidade e ajuda na aprendizagem do software PLCNext Engineer e do PLC da Phoenix, ao Eng. Miguel Cabral, pela ajuda técnica no acoplamento e ligação do controlador ao sistema de barreira e a todos os que contribuíram para a realização deste trabalho na Efacec.

Queria agradecer também ao Eng. António Vasconcelos, pelo seu tempo disponibilizado na transmissão de conhecimento sobre os sistemas e normas relativos aos caminhos de ferro e às passagens de nível.

Por último, deixo aqui os meus agradecimentos à minha família e amigos, especialmente à minha mãe, pai e avós, pelo apoio e valores que me transmitiram ao longo do meu percurso e por me guiarem no sentido certo.

Resumo

A automação de trabalhos está cada vez mais presente na sociedade. Tarefas que antigamente eram realizadas de forma manual são atualmente realizadas com apenas alguns cliques, ou mesmo de forma autónoma. Uma aplicação possível para a automação é a das barreiras presentes nas passagens de nível, como é o caso do mecanismo de barreira XBarrier 100, criado pela Efacec.

Nenhum sistema está completamente imune a falhar e esta circunstância é aplicável ao XBarrier 100, que é comandado por um controlador externo situado nas proximidades da passagem de nível. A fiabilidade deste sistema é um dos aspetos mais importantes que devem ser tidos em conta no desempenho da sua função. Mesmo em caso de falha, o seu funcionamento deve oferecer a maior segurança possível. Desta forma, procura-se melhorar as suas funções de controlo e automação. Para isso, pretende-se incorporar ao sistema um novo controlador interno que faça parte das funções de operação que atualmente executa o controlador externo, que inclua novas funcionalidades, que aporte um maior grau de automatização e tudo isso com garantia de segurança e fiabilidade. Para além disso, e consequentemente, é necessária a intercomunicação do novo controlador interno com o controlador externo atual e também com os restantes dispositivos do sistema.

Tendo em conta o problema descrito, a solução é projetada e desenvolvida de forma a obter um sistema seguro antifalhas, com a adequada escolha de um PLC que garanta uma série de condições específicas de segurança e, posteriormente, a sua programação com diversas funcionalidades e requisitos selecionados pela empresa Efacec. Além disso, foi escolhido e configurado um protocolo de comunicação industrial capaz de intercomunicar o novo PLC interno, com o PLC externo atual e outros dispositivos do sistema.

Em suma, é implementada uma solução de controlo interno de barreira para otimizar as funcionalidades de automação e segurança do sistema XBarrier 100 atual.

Palavras-Chave: Automação, Controlo de barreira, Passagem de nível, Segurança funcional.

Abstract

Automation is becoming more and more present in society. Tasks that used to be manual are now done with just a few clicks or even autonomously. A possible automation application is the level crossing barriers, such as the XBarrier 100 barrier mechanism created by Efacec.

No system is completely immune to failure and this circumstance is also applicable to the XBarrier 100, which is controlled by an external controller located near the level crossing. The reliability of this system is one of the most important aspects that has to be taken into account when performing its function. Even in case of failure, its operation must offer the greatest possible security. It is thus always desirable to improve its control and automation functions. For that purpose, a new internal controller shall be incorporated in the system in order to perform some operating functions that external controller currently performs, and also new features, globally bringing a greater degree of automation with guaranteed security and reliability. In addition, and consequently, intercommunication between new internal controller and current external controller and also other devices in the system shall be ensured.

The solution is designed and developed, taking into account the described problem, wich aim is a safe, fail-safe system, with the appropriate choice of a PLC, that guarantees a series of specific safety conditions. Subsequently, its programming with various features and requirements selected by the Efacec company is performed. Beside that, an industrial communication protocol capable of ensurig intercommunication between new internal PLC, the current external PLC and other system devices was chosen and configured.

In short, an internal barrier control solution is implemented to optimize the automation and safety features of the current XBarrier 100 system.

Keywords: Automation, Barrier control, Level Crossing, Security.

Índice

Lista de Figuras

Lista de Acrónimos

AC	Corrente Alternada
ALARP	*As Low As Reasonably Practicable*
CAN	*Controller Area Network*
CCF	*Common Cause Failure*
CIP	*Control Information Protocol*
CPU	Unidade Central de Processamento
DC	Corrente Continua
DC	Cobertura de Diagnóstico
DEE	Departamento de Engenharia Eletrotécnica
DI	*Digital Inovation*
DP	*Decentralized Peripherals*
ERP	*Enterprise Resource Planning*
FAR	*Fatal Accident Rate*
FBD	*Function Block Diagram*
Grafcet	*Graphe Fonctionnel de Commande Étapes Transitions*
HMI	Interface Homem-Máquina
IEC	*International Electrotechnical Commission*
IL	*Instruction List*
IoT	*Internet of Things*
IP	*Internet Protocol*
IRT	*Isochronus Real Time*
ISA	*International Society of Automation*
ISEP	Instituto superior de Engenharia do Porto
IT	Tecnologia da Informação
LD	*Ladder*
LED	*Light Emitting Diode*
LOPA	*Layer Of Protection Analysis*
MES	*Manufacturing Execution System*
MTBF	*Mean Time Between Failures*
MTTF	*Mean Time To Failure*
MTTFd	*Mean Time to Dangerous Failure*
MTTR	*Mean Time to Repair*

OSHA	Administração de Segurança e Saúde Ocupacional
OSI	*Open Systems Interconnection*
OT	Tecnologia Operacional
PAC	Controlador de Automação Programável
PC	*Personal Computer*
PFD	*Probability of Failure on Demand*
PFHd	Probabilidade Média de Falhas perigosas por hora
PID	Proporcional Integral Derivativo
PL	*Nível de Desempenho*
PLC	Controlador Lógico Programável
PLr	Nível de desempenho Exigido
PN	Passagem de Nível
PNO	*Profibus User Organization*
RAMS	*Reliability Avaliability Mantainability Safety*
RCS	*Redundant Control System*
RRF	*Risk Reduction Factor*
RT	*Real Time*
SCADA	Controlo de Supervisão e Aquisição de Dados
SFC	*Sequencial Flow Chart*
SIF	*Funções Instrumentadas de Segurança*
SIL	*Safety integrity Level*
SIS	*Safety Shutdown System*
SRP/CS	*Safety-Related Parts of Control System*
ST	*Structured Text*
TCP	*Transmission Control Protocol*
TEDI	Tese e Dissertação
UDP	*User Datagram Protocol*

Capítulo 1

Introdução

Este relatório descreve o projeto desenvolvido no âmbito da unidade curricular de Tese e Dissertação (TEDI) do 2º ano do Mestrado em Engenharia Eletrotécnica e de Computadores na área de especialização de Automação e Sistemas, no Departamento de Engenharia Eletrotécnica (DEE), do Instituto Superior de Engenharia do Porto (ISEP).

Este trabalho foi desenvolvido ao longo de aproximadamente 8 meses, nas instalações da Efacec, na Maia, no Instituto Superior de Engenharia do Porto e em teletrabalho. Assim, através da pesquisa e da realização de um modelo de trabalho, é possível aplicar de forma prática os conhecimentos ao longo do percurso académico, com a finalidade de expor este trabalho, inerente ao projeto proposto no âmbito da presente unidade curricular.

A empresa para a qual foi desenvolvido o projeto foi a Efacec. É uma empresa portuguesa com um perfil exportador e presença internacional em mais de 65 países, com mais de 70 anos de marca. A missão da empresa é criar soluções de Energia, Ambiente e Transportes, através da integração de diferentes competências e tecnologias, tendo também como visão criar soluções para uma nova época energética. As principais áreas de foco são a energia, a mobilidade e o ambiente, sendo alguns dos ramos mais prestigiados os seguintes: transformadores, automação, aparelhagem, sistemas, serviços, mobilidade elétrica e transportes [1].

Neste capítulo é feita uma contextualização histórica do tema, são definidos os objetivos propostos que se pretendem alcançar e, por fim, é descrita a estrutura do relatório, apresentando um resumo de cada capítulo.

1.1 Contextualização

A primeira linha de caminho de ferro com tração a vapor para serviço público foi inaugurada em Inglaterra, no ano de 1825, entre Stockton e Darlington. Em Portugal, as obras da primeira ligação ferroviária só se iniciaram em 1853. O primeiro troço, entre Lisboa e o Carregado, entrou ao serviço em 1856, tendo a linha sido concluída com a chegada à fronteira espanhola, em 1863. Por outro lado, a linha do Norte foi concluída com a chegada a Porto Campanhã em 1877. Os caminhos de ferro são um sistema de transporte que consiste num rolamento sobre carris metálicos com guias de rodas dos veículos, proporcionando uma baixa resistência ao avanço e grande segurança de marcha a velocidades elevadas. Este sistema oferece a possibilidade de atrelar um grande número de veículos, formando comboios de elevada capacidade de transporte, quer de passageiros, quer de carga. Tendo beneficiado da invenção da máquina a vapor, o uso deste meio de transporte generalizou-se, constituindo um elemento fundamental do crescimento económico que teve lugar com a Revolução Industrial.

No cruzamento entre estas linhas de ferro e um caminho ou estrada, localizadas ao mesmo nível, encontram-se as passagens de nível. O comboio tem quase sempre prioridade face a qualquer outro veículo, devido a razões económicas e de segurança.

Antigamente as passagens de nível (PN) possuíam barreiras onde o seu movimento rotativo era acionado de forma manual. Este devia-se a um mecanismo com uma manivela acoplada que permitia abrir ou fechar a barreira. Esta movimentação da barreira era feita por uma pessoa encarregue de o fazer cada vez que o comboio passava, fechava a barreira, levantava uma bandeira vermelha enrolada, que significava que a passagem estava livre para o comboio passar. Depois deste passar, voltava a abrir a barreira.

Hoje em dia as barreiras das passagens de nível têm vindo a evoluir e na sua maioria têm incorporadas funções que permitem que a sua movimentação seja feita de forma automática. Esta nova funcionalidade permite uma maior segurança, tanto do comboio, como do transeunte e tem também a vantagem de não exigir que nenhuma pessoa esteja fisicamente a fazer o controlo da barreira [2].

1.2 Objetivos

Este projeto vai ser desenvolvido sobre o sistema de barreira, XBarrier 100, criado pela empresa Efacec, que atualmente é gerido por um controlador externo localizado nas proximidades da passagem de nível. Por isso, numa primeira fase é necessário compreender os seus componentes e o seu funcionamento.

O trabalho tem dois objetivos principais:

- Projetar e programar um controlador interno ao XBarrier 100, com caraterísticas de segurança e funcionalidades que otimizem o seu desempenho;
- Selecionar e configurar um protocolo de comunicação industrial que permita fazer a comunicação entre o controlador escolhido e outros equipamentos externos ao XBarrier 100.

Para alcançar estes objetivos é necessário estudar os principais fatores e normas que determinam a segurança em processos de automação, assim como, conhecer os tipos de autómatos de segurança existentes no mercado aplicáveis ao tema a abordar. Analisados estes fatores é necessário estudar os protocolos de comunicação normalmente usados no contexto de automação e o seu funcionamento.

1.3 Organização do Documento

O relatório está estruturado em 7 capítulos.

No capítulo 1, introduz-se o propósito que alude à razão do projeto, é apresentada uma contextualização, bem como os objetivos que se pretendem atingir.

No capítulo 2, é feita uma breve introdução à pirâmide de automação, é abordado o tema da segurança na indústria de automação, distinguindo os diferentes pontos e formas de classificação de segurança e é feita uma análise e estudo da cibersegurança na atualidade.

No capítulo 3, é feita uma descrição global do problema, onde é apresentado o mecanismo de barreira, no qual se vai implementar o controlador lógico de segurança, e são descritos os requisitos para a elaboração deste projeto.

No capítulo 4, é exibida uma proposta de solução do problema, onde inicialmente é feita uma listagem dos controladores existentes no mercado que têm uma aplicação

ao problema em causa e posteriormente é selecionado e descrito aquele que se adequa mais aos requisitos do projeto. Posteriormente, são estudados alguns dos protocolos de comunicações industriais mais utilizados e é escolhido o mais adequado.

No capítulo 5, é feita a implementação da solução, descrevendo os passos e a maneira como se desenvolveu até à solução final.

No capítulo 6, é mostrada a fase dos resultados onde são apresentados os testes elaborados na sequência do desenvolvimento do projeto.

Por fim, no capítulo 7, a conclusão, onde é analisado o presente trabalho e são elencadas algumas propostas para trabalho futuro.

Capítulo 2

Estado de Arte

Neste capítulo é feita uma breve descrição da pirâmide de automação, além de incidir sobre a parte de segurança, os cuidados e métodos que se devem ter em conta para garantir um entorno de segurança. Para projetar e desenvolver uma solução que permita o movimento automático de uma barreira é necessário ter em conta vários fatores de segurança. Estes, garantem não só a sua segurança, como também das pessoas que estão direta ou indiretamente ligadas a ele, tal como, por exemplo, um transeunte na área da passagem de nível. Por outro lado, é feita uma análise e estudo da cibersegurança na atualidade.

2.1 Pirâmide de Automação

Como em todos os sistemas autónomos, a pirâmide de automação está presente em todos os projetos de automação e sistemas que contêm dispositivos de automação.

A pirâmide de automação é uma forma representativa de exibir as camadas de automação dentro de uma fábrica ou num projeto de automação, definida pela norma ISA-95. Esta pirâmide contém 5 camadas ou níveis que dependem dos dispositivos integrados e da tecnologia usada.

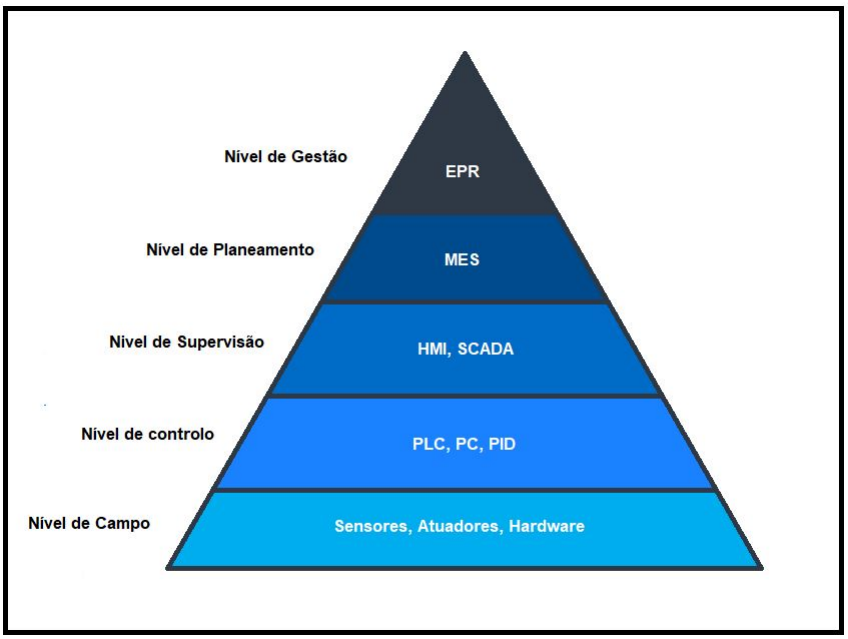


Figura 2.1: Pirâmide de Automação

A base da pirâmide, ou **nível 0**, é conhecido como o nível de campo. Neste escalão estão incluídos todos os dispositivos de hardware, atuadores e sensores que estão presentes no espaço físico onde está incorporado o sistema autónomo. Assim, no nível de campo estão incluídos os equipamentos de automação que fazem o trabalho físico de monitorização. Entre eles, motores elétricos, atuadores hidráulicos e pneumáticos, interruptores de proximidade, interruptores fotoelétricos, sensores de temperatura, entre outros.

O **nível 1** é o nível de controlo. Neste nível estão incluídos os PLCs, computadores pessoais (PCs) e os controladores proporcional integral derivativo (PIDs). Estes dispositivos são usados para controlar e acionar os dispositivos do nível de campo que fazem o trabalho físico. Estes recebem informações de todos os sensores, interruptores e outros dispositivos de entrada para tomar as decisões sobre quais as saídas a ativar para realizar uma tarefa programada.

O **nível 2** da pirâmide de automação é o nível de supervisão. Em comparação com o nível anterior que utiliza PLCs, este nível utiliza o Sistema de Controlo de Supervisão e Aquisição de Dados (SCADA) para fazer um controlo desses mesmos PLCs. O SCADA é essencialmente a combinação dos níveis anteriores usados para ter acesso aos dados e aos sistemas de controlo de um único local. Além disso, neste nível é geralmente adicionada uma interface gráfica do utilizador, ou interface homem-máquina (HMI), para controlar funções remotamente. O sistema SCADA

pode monitorizar vários sistemas a partir de um único local e não está limitado a uma única máquina como a HMI, embora ambos façam parte deste nível.

O **nível 3** é o nível de planeamento. Este nível utiliza um sistema de gestão computacional conhecido como *Manufacturing Execution System* (MES) ou sistema de execução de manufatura. O MES monitoriza todos os processos de manufatura numa planta, fábrica ou espaço onde está implementado o sistema de automação, desde a matéria-prima até o produto acabado. Isto permite gerir e ver o que se passa com o sistema e permite também que sejam tomadas decisões, com base nessas informações e assim ajustar os pedidos de materiais ou planos de envio, com base nos dados reais recebidos nestes sistemas.

O **nível 4**, e último, é conhecido como nível de gestão. Este nível utiliza o sistema de gestão integrado da empresa, um sistema de gestão computacional conhecido como *Enterprise Resource Planning* (ERP). É neste nível que a alta administração de uma empresa pode ver e controlar as suas operações. O ERP é geralmente um conjunto de diferentes aplicações computacionais que podem ver todo o processo ativo de uma empresa. A principal diferença deste nível e do anterior é que este nível, ao contrário do outro, tem acesso a todas as áreas de trabalho de uma empresa. Utiliza a tecnologia dos níveis anteriores e mais alguns softwares para realizar esse nível de integração. Com isto, a empresa é capaz de gerir todos as etapas de negócio, desde a fabricação, vendas, compras, finanças e folhas de pagamento, entre muitas outras. A integração do ERP é capaz de promover, de uma forma organizada, a eficiência e a transparência dentro de uma empresa [3] [4].

2.2 Segurança na Automação

Este subcapítulo é dedicado à análise de normas e conceitos de segurança necessários para escolher e/ou projetar equipamentos aplicáveis à indústria da automação.

2.2.1 Segurança em PLCs

Um controlador lógico programável de segurança é um PLC de segurança projetado para uso em aplicações de missão crítica ou relacionados à segurança para proteger um sistema contra falhas que podem resultar em danos às pessoas, equipamentos ou meio ambiente. Este PLC é projetado para, no caso da ocorrência de uma falha, não pôr em perigo nenhum destes agentes. Desta maneira, quando ocorrer uma condição perigosa específica, o PLC de segurança deve responder colocando o sistema que esteja a controlar, numa condição de segurança [5] [6].

Um PLC de segurança suporta as mesmas aplicações que um PLC padrão. No entanto, um PLC de segurança contém recursos extras com redundância e funções de segurança adicionais que seguem um nível de integridade de segurança específico (SIL) [6].

Para a deteção de um curto-circuito o PLC de segurança utiliza uma rotina de diagnóstico por meio de micropulsos e monitorização do estado lógico das saídas. Com isto, em caso de curto-circuito do sistema, o PLC permite dar um alarme.

Outra forma de proteção, em caso de falhas, é a incorporação de um segundo transístor em série incorporado na saída do PLC, com um entravamento com o circuito de monitorização, chamado de "watchdog", que compara o estado de ambos os transístores de saída. A Figura 2.2, representa um esquema deste sistema incorporado nos PLC de segurança.

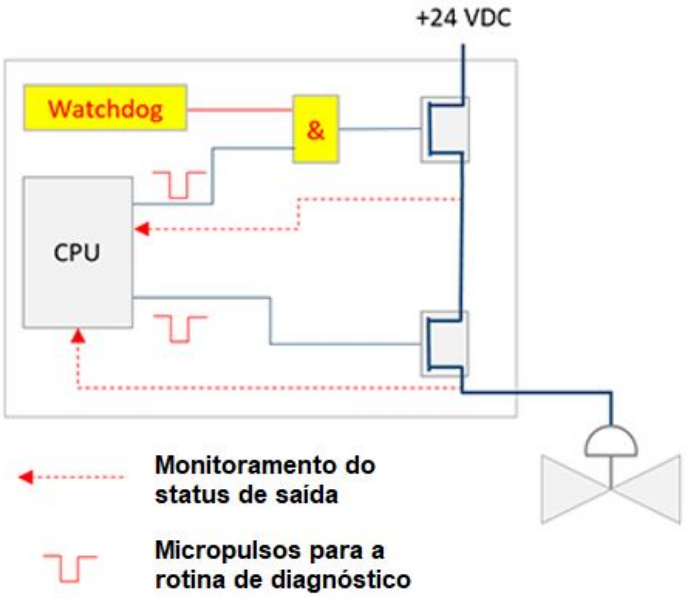


Figura 2.2: Circuito com Watchdog [7]

Desta forma, obtemos um circuito de saída seguro, *fail safe*, tolerante a falhas do ponto de vista da segurança. Para obter um maior nível de segurança, são também utilizadas arquiteturas redundantes. Neste exemplo da figura 2.3, é feita a ligação em paralelo de dois circuitos que controlam uma mesma saída.

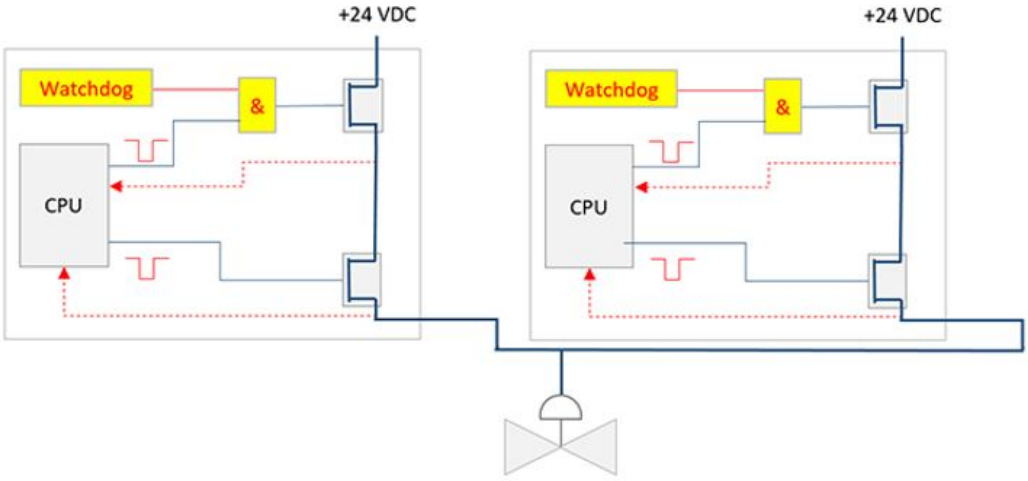


Figura 2.3: Circuito em paralelo [7]

A redundância é uma forma de aumentar a fiabilidade do sistema e reduzir situações de risco, mas por outro lado acrescenta um custo adicional. O seu principal objetivo num sistema de controlo é eliminar a dependência de um único módulo, para desta maneira, fornecer várias opções em caso de falha de um componente. Além destas funções, existem muitas outras de diagnóstico no PLC de segurança, tanto a nível de Unidade Central de Processamento (CPU), como de memória, como de entradas, saídas e comunicações [7].

No entanto, existem algumas desvantagens em usar um PLC de segurança. O custo inicial é mais alto, por isso, este tipo de PLC não é ideal para aplicações mais simples e que não supõem nenhum perigo. Desta maneira é necessário saber identificar o contexto e a aplicação em questão, para assim, escolher o PLC que se adeque em função da necessidade de possuir um sistema seguro.

Assim, é possível distinguir 2 tipos de falhas num sistema, as perigosas e as não perigosas. As primeiras, falhas perigosas, no hipotético caso de acontecer um erro no sistema, representam uma ameaça para o próprio sistema e para as pessoas, num estado onde não é possível parar o processo se isto vier a ser necessário, resultando no não desempenho da função de segurança, como é o caso das passagens de nível. Por exemplo, um sistema de uma barreira dar um sinal que está fechada, sendo que na realidade está aberta, podendo assim deixar passar carros ou peões, não havendo condições para isso. Para estas situações, é necessário um PLC com condições de segurança.

As falhas não perigosas, ou falhas seguras, levam o processo para uma situação onde não existe perigo para o sistema, pessoas ou o ambiente.

Como por exemplo, um sistema de barreira dar um sinal que a barreira se encontra aberta, estando na verdade na posição fechada. Neste caso, não existe um perigo para o sistema, ou seja, nem para o comboio nem para os carros ou peões. Nestas situações são usados PLCs comuns, sem características de segurança [8] [9] [10].

Desta maneira podem ser considerados 2 objetivos principais que um PLC de segurança deve cumprir. Falhar o menos possível, e se for inevitável, que falhe apenas de maneira previsível e segura, através de diagnósticos integrados que permitem monitorizar continuamente as entradas e saídas. Se uma falha interna ou outra falha for detetada, dá-se por norma geral um *shutdown* no sistema [11].

2.2.2 Requisitos e Normas em PLCs

Para que um PLC seja considerado de segurança, deve atender a um conjunto de normas internacionais rigorosas. Entre elas a *International Electrotechnical Commission* (IEC) 61508 (Segurança Funcional de Sistemas Elétricos / Eletrónicos / Eletrónicos Programáveis relacionados à Segurança). Esta norma cobre design, métodos de design e testes de hardware e software, além de definir processos de certificação rígidos para minimizar riscos [8].

Esta norma é dividida em 7 partes, onde as 4 primeiras são obrigatórias e as outras 3 atuam como diretrizes:

- Parte 1: Requisitos gerais;
- Parte 2: Requisitos para sistemas relacionados à segurança E / E / PE;
- Parte 3: Requisitos de software;
- Parte 4: Definições e abreviações;
- Parte 5: Exemplos de métodos para a determinação dos níveis de integridade de segurança;
- Parte 6: Diretrizes sobre a aplicação de IEC 61508-2 e IEC 61508-3;
- Parte 7: Visão geral das técnicas e medidas.

Outra norma muito utilizada é a IEC 61131, publicada pela *International Electrotechnical Commission* (IEC) em 1992, a qual estabelece padrões para Controladores Programáveis. Esta norma é atualizada a cada certo período de tempo e é dividida em várias partes:

- 61131-1 – Informações gerais;
- 61131-2 – Requisitos e testes de equipamentos;
- 61131-3 – Linguagens de programação;
- 61131-4 – Guia de orientação ao usuário;
- 61131-5 – Comunicação;
- 61131-6 – Comunicação via Fieldbus;
- 61131-7 - Programação de controlo FUZZY;
- 61131-8 – Implementação das Linguagens.

A parte 2 da norma é uma das mais importantes do ponto de vista de segurança. Estabelece requisitos funcionais de compatibilidade eletromagnética e funcional e testes de verificação relacionados para qualquer produto onde o intuito é desempenhar a função de equipamento de controlo industrial, incluindo controladores programáveis e os seus periféricos associados [12].

Assim, a norma determina como principais objetivos, estabelecer as definições e identificar as principais caraterísticas relevantes para a seleção e aplicação de PLC e seus periféricos associados e especificar os requisitos mínimos funcionais elétricos, mecânicos, ambientais e caraterísticas de construção, condições de serviço, segurança, *ElectroMagnetic Compatibility* ou Compatibilidade EletroMagnética (EMC), programação do utilizador e testes aplicáveis a PLCs e periféricos associados [13].

Os equipamentos contidos neste padrão são para o uso da categoria II de *overvoltage* (sobrecarga) (IEC 60664-1), em instalações de baixa tensão, onde a tensão elétrica nominal não exceda os 1000V a 50/60Hz em corrente alternada (AC) ou 1500V em corrente contínua (DC) [13].

Outro ponto definido por esta parte da norma são as memórias de backup: tipos, especificação e capacidades. Por consequência das definições de hardware, a parte 2 define também todos os testes necessários à certificação de um determinado PLC conforme estipulado por esta norma. Assim, esta norma aplica-se a qualquer produto que exerça função de um PLC e aos periféricos associados [14].

A parte 3 da norma define 5 linguagens de programação. Estas linguagens são as mais utilizadas no mundo para a programação de PLCs. Entre elas existem 2 linguagens escritas: *Structured Text* (ST), linguagem de alto nível e *Instruction List* (IL), linguagem de baixo nível. As outras 3 são baseadas em linguagens gráficas, *Ladder* (LD), originalmente desenvolvida para construir e melhorar a documentar

circuitos a relés, *Function Block Diagram* (FBD) sendo esta uma linguagem que utiliza blocos lógicos e a *Sequencial Flow Chart* (SFC) que é uma linguagem parecida com os diagramas funcionais *Graphe Fonctionnel de Commande Étapes Transitions* Grafcet ou fluxogramas [15].

2.2.3 *Safety Shutdown System* (SIS)

Um PLC de Segurança é uma das 3 partes de um Sistema Instrumentado de Segurança (SIS). O SIS também pode ser referido como *Safety Shutdown System*. O Sistema Instrumentado de Segurança (SIS) é um sistema que monitoriza um equipamento ou processo, e caso ocorra uma condição de risco inaceitável ou insegura, este sistema garante uma paragem de emergência [16].

O objetivo principal é evitar acidentes dentro e fora das fábricas, como incêndios, explosões, danos a equipamentos, proteção de produção e, sobretudo, evitar danos à saúde pessoal e situações de risco de vida. Nenhum sistema está completamente imune a falhar e, mesmo em caso de falha, este deve fornecer uma condição segura [16] [17].

Organismos como a Administração de Segurança e Saúde Ocupacional (OSHA) a *International Society of Automation* ISA, a IEC e entre outros, criaram normas para definir riscos, não como linhas de processamento isoladas, mas como riscos associados às funções de processamento como um todo. As normas ISA 84 (*Instrumented Sys To Achieve Functional Safety*) e IEC 61508 foram desenvolvidas em torno do conceito de segurança funcional. Desta maneira, a forma como a segurança funcional é abordada num sistema a fim de reduzir os riscos funcionais é instalar um Sistema de Segurança separado e bem projetado [8] [16] [18].

A camada do SIS deve fornecer uma redução de risco de pelo menos 10 vezes no risco da operação. Essa diminuição de risco é chamada de fator de redução de risco *Risk Reduction Factor* (RRF) e deve ser igual ou superior a 10. Uma maneira de medir o risco é através do *Fatal Acidente Rate* (FAR), taxa de acidentes fatais. Por exemplo, a indústria química tem FAR de aproximadamente 4, a condução de um carro tem um FAR de sensivelmente 40.

Um Sistema Instrumentado de Segurança é composto por 3 partes: sensores, *logic solvers* e elementos de controlo final, com o objetivo de levar o processo a um estado seguro quando as condições de segurança são violadas. Isto significa que o SIS é um conjunto separado de dispositivos do sistema de controlo de processo básico. Então, para ter um fator de redução de risco maior do que 10, este não

pode ser interligado com o sistema de controlo básico e com qualquer uma das deficiências desse sistema. O *logic solver*, ou PLC de segurança, é um PLC reforçado e especializado que pode ter vários processadores a executar o programa em paralelo para garantir a integridade da lógica e da ação resultante [16].

O SIS é projetado relativamente a funções individuais no sistema chamadas funções instrumentadas de segurança (SIF). Estas funções são camadas de proteção cujo objetivo é alcançar um estado seguro do processo quando um evento perigoso específico ocorre. O SIF é implementado no SIS, que normalmente é composto por várias funções de segurança [19] [20]. Como por exemplo, o logic solver, que obtém as entradas do SIS e determina qual deve ser o estado das saídas do SIS para um determinado SIF [16].

Pode ser usada uma matriz de risco, também conhecida por *Risk Graph*, *Risk Matrix* ou *Layer Of Protection Analysis* (LOPA), detalhadas e definidas pelas normas IEC 61508/61511 para identificar o nível de risco que é tolerável e até que ponto uma função exige que um SIF seja definido. Isso pode ser feito qualitativamente, como representado na matriz de risco da Figura 2.4, sendo que ALARP, significa *as low as reasonably practicable*, ou seja, tão baixo quanto razoavelmente praticável.

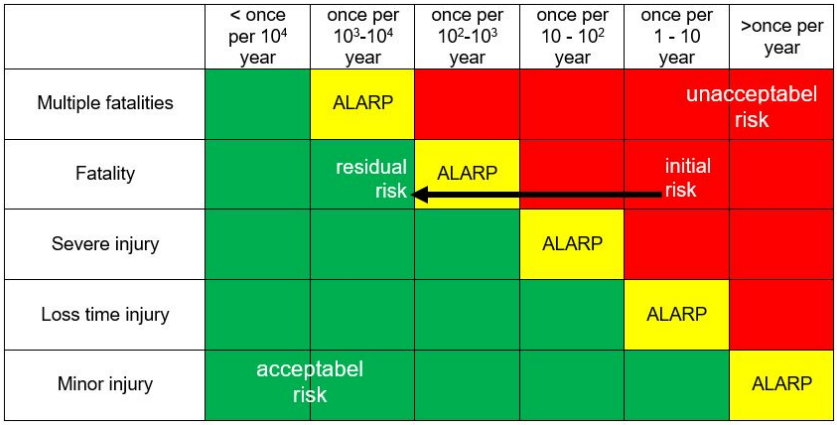


Figura 2.4: *Risk Matrix* [21]

Também pode ser feito quantitativamente, atribuindo valores numéricos à frequência e gravidade esperadas do risco, tal como representado na Figura 2.5

		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequences	5 Catastrophic	5 Moderate	10 High	15 Extreme	20 Extreme	25 Extreme
	4 Major	4 Moderate	8 High	12 High	16 Extreme	20 Extreme
	3 Moderate	3 Low	6 Moderate	9 High	12 High	15 Extreme
	2 Minor	2 Low	2 Moderate	6 Moderate	8 High	10 High
	1 Negligible	1 Low	2 Low	3 Low	4 Moderate	5 Moderate

Figura 2.5: *Risk Matrix* [22]

Mas até um SIS tem probabilidade de falhar. A probabilidade que um dispositivo, quer seja de entrada, saída, ou *logic solver*, falhe, fazendo com que o SIF não responda quando chamado, é chamada de Probabilidade de Falha sob Demanda ou PFD (*Probability of Failure on Demand*). O PFD de cada instrumento é definido previamente pelo fabricante. Este valor é inversamente proporcional ao *Risk Reduction Factor* (RRF), se ambos utilizarem a mesma unidade de tempo, normalmente expressa em anos:

$$PFD = \frac{1}{RRF} \tag{2.1}$$

[23]

Onde:

RFD - *Probability of Failure on Demand*

RRF - *Risk Reduction Factor*

2.2.4 *Safety Integrity Level* (SIL)

Sempre que um bem se encontra a desempenhar as suas funções de segurança nas condições estabelecidas e durante um período de tempo determinado, designa-se por integridade da segurança.

O Safety integrity level (SIL) é definido como um nível relativo de redução de risco, dada por uma função específica, ou para especificar um nível de redução de risco.

Assim, o SIL é uma medida de desempenho necessária para uma função de segurança. Os requisitos para um SIL variam conforme os padrões de segurança funcional. Nos padrões de segurança funcional baseados na norma IEC 61508 e IEC 61511 são definidos 4 níveis, sendo o SIL 4 o mais confiável e o SIL 1 o menos. Figura 2.6 [8] [24].

SIL Levels According IEC 61508 / IEC 61511

SIL Safety Integrity Level	PFDavg Average probability of failure on demand per year (low demand mode)	RRF Risk Reduction Factor	PFDavg Average probability of failure on demand per hour (high demand or continuous mode)
SIL 4	$\geq 10^{-5}$ and $< 10^{-4}$	100000 to 10000	$\geq 10^{-9}$ and $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ and $< 10^{-3}$	10000 to 1000	$\geq 10^{-8}$ and $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ and $< 10^{-2}$	1000 to 100	$\geq 10^{-7}$ and $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ and $< 10^{-1}$	100 to 10	$\geq 10^{-6}$ and $< 10^{-5}$

Figura 2.6: Níveis SIL [25] [8] [24]

Assim, a cada intervalo de valores do PFD corresponde um valor de SIL. Quanto menor for o PFD, maior vai ser o SIL e mais seguro é o sistema.

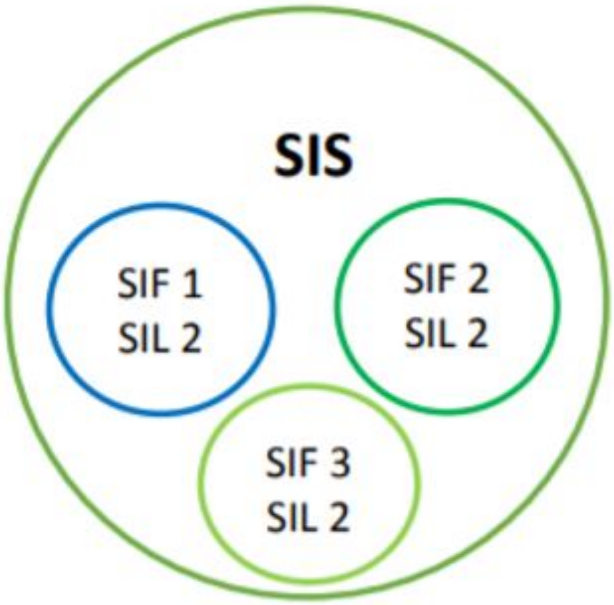


Figura 2.7: Diagrama de Venn do SIS [26]

Cada SIS tem uma ou mais funções de segurança (SIFs) e cada uma oferece uma medida de redução de risco indicada pelo seu nível de integridade de segurança (SIL). O SIS e um equipamento individual não têm um SIL atribuído [26].

2.2.5 *Reliability Avaliability Mantainability Safety* (RAMS)

RAMS é um acrónimo de *Reliability Avaliability Mantainability Safety* (Fiabilidade, Disponibilidade, Manutenibilidade, Segurança) que consiste na aplicação de um conjunto de conceitos de engenharia, métodos, cálculos e técnicas estabelecidas ao longo do ciclo de vida de um produto, como pode ser o caso de um PLC, ou sistemas, referentes a aplicações ferroviárias ou passagens de nível.

De acordo com a Norma Portuguesa NP EN 50126:2000 de Aplicações ferroviárias – Especificação e demonstração de Fiabilidade, Disponibilidade, Manutenibilidade e Segurança (RAMS), "Os objetivos de segurança e de disponibilidade de um sistema em funcionamento só podem ser alcançados se estiverem satisfeitos todos os requisitos de fiabilidade e de manutenibilidade e se as atividades de manutenção e de exploração forem controladas ao longo do ciclo de vida do sistema, assim como o meio ambiente em que se insere". Desta maneira, o RAMS é um método que integra as características de fiabilidade, disponibilidade, manutenibilidade e segurança de um equipamento, daí que, o objetivo final é a maximização da produtividade e do lucro, a redução de riscos de avaria ou acidente e a redução dos custos [27].

Para entender os conceitos do RAMS como fiabilidade ou disponibilidade, é necessário conhecer alguns fatores importantes utilizados no seu cálculo, como é o exemplo do *Mean Time Between Failures* (MTBF), ou o *Mean Time to Repair* (MTTR).

O MTBF é o tempo médio que um equipamento funciona corretamente entre falhas, dado pela seguinte expressão matemática [28].

$$MTBF = \frac{Número \quad de \quad horas \quad operacionais}{Número \quad de \quad falhas} \tag{2.2}$$

[29]

Assim, o MTBF é usado para antecipar a probabilidade de um ativo falhar, num determinado período de tempo. Este número é útil quando comparado com outras estratégias de manutenção, como códigos de falha e análise de causa raiz, e métricas de manutenção adicionais, como o *Mean Time to Repair* (MTTR) [29].

O MTTR é o resultado do tempo total de manutenção corretiva a dividir pelo número de ações de manutenção durante um determinado período de tempo. Este é um importante indicador para verificar como é que uma empresa ou organização consegue responder a um problema e resolvê-lo de forma eficiente. Para este cálculo assume-se que as tarefas são realizadas sequencialmente e por pessoal devidamente treinado. A fórmula matemática encontra-se representada na equação 2.3 [28].

$$MTTR = \frac{Tempo \quad Total \quad de \quad Manutenção \quad Corretiva}{Número \quad de \quad Ações \quad de \quad Reparação} \tag{2.3}$$

[30]

Por exemplo, se a manutenção não planeada de um PLC demora 50 horas, e supondo que avariou 8 vezes ao longo de um ano, o tempo médio de reparação será de 6,25 horas, ou seja, 6 horas e 15 minutos. De maneira simplificada, pode considerar-se este número como uma média de tempo que um determinado equipamento gasta para ser reparado, ao longo de um intervalo [28].

Taxa de Falhas

A taxa de falhas pode ser definida como o número previsto de vezes que um equipamento falha num período de tempo específico. É um valor calculado que fornece uma medida de confiança a um produto. Um fabricante de componentes pode fornecer uma taxa de falhas especificada, geralmente com base em dados de teste de campo ou laboratório. Da mesma forma, um fabricante também pode fornecer uma taxa de falhas específica para uma montagem [31]. Esta taxa de falhas é normalmente representada pela letra grega λ.

Esta taxa de falhas também pode ser representada como o inverso do MTBF, ou seja o MTBF é o inverso da taxa de falhas λ.

$$MTBF = \frac{1}{\lambda} \tag{2.4}$$

Reliability

A **fiabilidade** (*reliability*) é um conceito que é definido pela probabilidade de um equipamento desempenhar certas funções corretamente durante um determinado período de tempo sob condições específicas [32] [33].

Teoricamente não se pode prever quando um produto ou equipamento irá falhar, mas pode-se prever a probabilidade que esse produto tem de falhar num determinado intervalo de tempo [34].

A fiabilidade, pode ser calculada como uma função de probabilidade de declínio exponencial que depende da taxa de falha. Uma vez que a taxa de falhas pode não permanecer constante ao longo do ciclo de vida operacional de um componente, as quantidades médias baseadas no tempo, como *Mean Time To Failure* (MTTF) ou *Mean Time Between Failures* (MTBF), também podem ser usadas para calcular a fiabilidade. A função matemática é definida pela expressão 2.5.

$$Realiability, R(t) = \mathrm{e}^{-\lambda \cdot t} \tag{2.5}$$

[23]

Ou também definida pela expressão 2.6:

$$Realiability, R(t) = \mathrm{e}^{-\frac{t}{MTBF}} \tag{2.6}$$

[34]

Onde:

R - Fiabilidade

λ - Taxa de falhas

t - tempo decorrido

MTBF - tempo médio entra falhas

A fiabilidade de um produto é de 100% apenas se não se usar o produto, pois à medida que o valor de t começa a aumentar, o R vai diminuir e a taxa de mudança depende do design do produto, materiais, entre outros [34].

Para uma taxa de falhas constante, a fiabilidade tem uma distribuição exponencial, ou seja, uma distribuição de Poisson para k = 0.

$$Realiability, R(t) = \mathrm{e}^{\int_0^t \lambda(t)\,dt} = \mathrm{e}^{-\lambda(t)} \tag{2.7}$$

Onde:

λ(t) = taxa de falhas dependente do tempo de vida

Mas as taxas de falhas dos componentes não costumam ser rigorosamente constantes ao longo da vida dos equipamentos. Este comportamento é descrito por uma distribuição *bathtub* (em forma de banheira) que vai buscar o seu nome ao aspeto gráfico da sua função taxa de falhas de três troços, conforme se ilustra na figura 2.8.

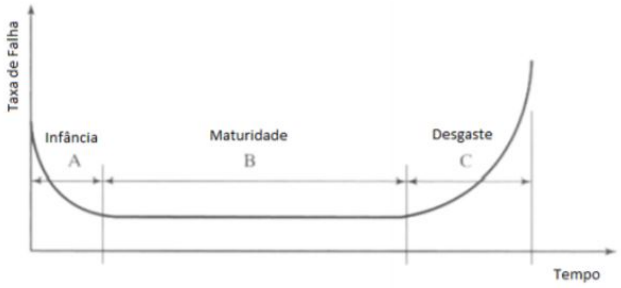


Figura 2.8: Curva de vida de um equipamento [35]

No período inicial (infância) essa taxa é tipicamente maior devido aos defeitos de projeto e fabrico. No chamado período de vida útil ou maturidade, o seu valor médio mantém-se razoavelmente estacionário. Após essa fase, na fase do envelhecimento, a taxa de falhas volta a subir (período de desgaste), porque o componente já ultrapassou o seu período de vida útil [35].

Uma conclusão pratica é que "a fiabilidade de um sistema em série é sempre menor do que a fiabilidade de qualquer um dos seus componentes" [36].

Availability

A **disponibilidade** (*availability*) é a capacidade de um equipamento ou unidade industrial estar apta para cumprir uma função requerida, sob dadas condições

e num determinado momento ou intervalo de tempo, assumindo que os recursos externos necessários são fornecidos [37].

De acordo com a norma portuguesa NP EN 13306 (2007) de Terminologia da Manutenção, disponibilidade é a "Aptidão de um bem para cumprir uma função requerida sob determinadas condições, num dado instante ou durante um dado intervalo de tempo, assumindo que é assegurado o fornecimento dos necessários recursos externos", sendo que esta aptidão depende da combinação da fiabilidade e da adequabilidade da manutenção [33] [38].

A disponibilidade determina o desempenho instantâneo de um componente num determinado momento, com base na duração do tempo entre a falha e a recuperação. Desta maneira a disponibilidade depende do MTBF e do MTTR, calculada usando a fórmula 2.8:

$$Availability, A(t) = \frac{MTBF}{MTBF + MTTR} \tag{2.8}$$

[23]

Onde:

A(t) – Disponibilidade

MTBF – tempo médio entre falhas

MTTR – tempo médio de reparação

Mantainability

A **Manutenibilidade** (*mantainability*) é a probabilidade de uma ação ativa de manutenção para um elemento sob determinadas condições de utilização poder ser executada dentro de um intervalo de tempo estabelecido, quando a manutenção é realizada nas condições preestabelecidas e com a utilização de procedimentos escritos e recursos predefinidos.

O cuidado com a Manutenibilidade deve ter-se em conta a partir da fase de projeto. Desta maneira, uma vez que os requisitos operacionais do sistema estejam definidos, deve ser feita uma análise que permita avaliar a sua Manutenibilidade. Esta será uma vantagem para os projetistas que poderão saber quais as áreas que precisam de ser revistas, e consequentemente melhoradas, modificadas ou até mesmo suprimidas [33] [37].

Safety

O termo *Safety*, traduzido para português como Segurança funcional, é o estado ou condição de estar protegido, imune de danos ou resultados indesejáveis e a conservação da vida humana, da sua eficácia e a prevenção de danos causados aos equipamentos.

Assim, *Safety* é usado para se referir à condição de estar protegido dos aspetos que podem causar danos, ou seja, é a prevenção de acidentes, que podem ou não envolver agentes humanos, sendo estes não intencionais [32].

Por outro lado, o termo *Security* representa um conceito diferente de *Safety*. Sendo estes dois termos confundidos normalmente como uma segurança geral que engloba qualquer tipo de proteção.

O termo *Security* é utilizado para se referir à proteção de indivíduos ou organizações contra ameaças externas e atividades criminosas executadas por pessoas (assaltos, furtos, roubos, atividades terroristas, etc.). Assim, *security* é a segurança focada nas ações que põem em risco a integridade de um indivíduo, ou de uma organização.

2.2.6 Performance Level (PL)

A norma ISO 13849-1 (Segurança de máquinas – Partes relacionadas à segurança de sistemas de controlo – Princípios gerais para projeto), fornece requisitos de segurança e orientação sobre os princípios para o projeto e integração de peças relacionadas com a segurança de sistemas de controlo, ou *Safety-Related Parts of Control System* (SRP/CS), incluindo o projeto de software. Para essas partes do SRP/CS, especifica características que incluem um nível de desempenho necessário para realizar funções de segurança. Aplica-se a SRP/CS para alta demanda e modo contínuo, independentemente do tipo de tecnologia e energia utilizada (elétrica, hidráulica, pneumática, mecânica, etc.), para todos os tipos de máquinas [39].

Esta norma foi revista em 2006. Nesse plano de revisão, as peças semicondutoras, como transístores, foram colocados em uso nas máquinas de segurança que compõem as partes relacionadas à segurança dos sistemas de controlo, o que representa uma mudança nos métodos de controlo por meio de fios para o controlo através de software. Convencionalmente eram usadas categorias, sendo a segurança determinada de acordo com as arquiteturas de sistema (estruturas) que usavam dispositivos de segurança mecânica e relés. Nessas circunstâncias, foram feitas tentativas de regular a segurança mecânica de acordo com as funções e confiabilidade por volta do ano 2000. Esta forma de pensar é chamada de "segurança funcional". Sendo que a

ISO 13849-1: 2006 é uma norma que revisa a ISO 13849-1: 1999, que foi baseada na norma convencional EN 954-1, adicionando detalhes da IEC 61508 (IEC 62061), que definiu a segurança funcional. Em suma, a segurança funcional é uma parte de segurança integral de um sistema ou equipamento, sendo caraterizada pela ausência de riscos e situações perigosas devido ao mau funcionamento de sistemas técnicos [40].

O nível de desempenho (PL) foi introduzido na ISO 13849-1: 2006, que é quantitativamente expresso como a fiabilidade das partes relacionadas à segurança de um sistema de controlo, incluindo cobertura de diagnóstico (DC) ou taxa de falha.

Assim, PL é um valor usado para definir a capacidade das partes relacionadas à segurança dos sistemas de controlo para executar uma função de segurança sob condições previsíveis. A situação de perigo é dividida em 5 níveis, conforme a Probabilidade Média de Falhas perigosas por hora, PFHd (1/h), conceito este introduzido pela norma IEC 61508. Portanto, a cada nível de desempenho, corresponde um intervalo de valores de PFH D, sendo que o PLa é o nível menos confiável e com valores mais altos de PFH D e PLe o mais confiável e com valores mais baixos, conforme representado na Figura 2.9 [40].

Performance Level (PL)	Probability of Dangerous Failure per Hour (PFHd) 1/h
a	$\geq 10^{-5}$ and $<10^{-4}$ ⟨0.001% to 0.01%⟩
b	$\geq 3 \times 10^{-6}$ and $<10^{-5}$ ⟨0.0003% to 0.001%⟩
c	$\geq 10^{-6}$ and $<3 \times 10^{-6}$ ⟨0.0001% to 0.0003%⟩
d	$\geq 10^{-7}$ and $<10^{-6}$ ⟨0.00001% to 0.0001%⟩
e	$\geq 10^{-8}$ and $<10^{-7}$ ⟨0.000001% to 0.00001%⟩

Figura 2.9: Relação entre o PL e PFHd [40]

A norma EN ISO 12100 define procedimentos importantes de sistemas relevantes para a segurança ou componentes de máquinas e comandos de instalações referidos à segurança. Desta maneira, a norma define algumas etapas para determinar e comprovar o nível de desempenho desejado num projeto [41].

Determinação do nível de desempenho exigido (PLr)

O nível de desempenho exigido (PLr) é usado para atingir a redução de risco necessária para cada função de segurança. Portanto, o nível de desempenho (PL) das peças relacionada à segurança de um sistema de controlo deve ser igual ou superior ao nível de desempenho exigido (PLr).

Considerando o exemplo de uma pessoa que entra numa área onde uma máquina potencialmente perigosa está a operar, estima-se o risco usando o gráfico de risco qualitativo, ou fluxograma, para atribuir um nível de desempenho exigido (PLr), com base em três critérios. Os parâmetros a serem considerados são:

Gravidade da lesão:

S1: Leve;

S2: Grave (com lesões irreversíveis e morte);

Frequência e/ou tempo de exposição ao perigo:

F1: Raramente a menos frequente e/ou o tempo de exposição é curto;

F2: Frequentemente a contínuo e/ou o tempo de exposição é longo;

Possibilidade de evitar o perigo ou limitar os danos:

P1: Possível em condições específicas;

P2: Dificilmente possível.

A figura 2.10 representa um gráfico de risco qualitativo, para atribuir um nível de desempenho requerido (PLr), segundo a norma ISO 13849-1 [39].

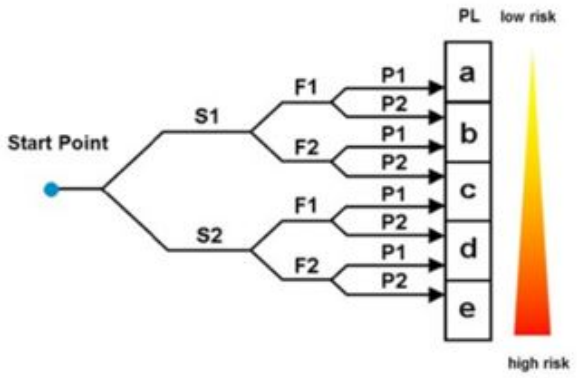


Figura 2.10: Nível de Desempenho requerido [42]

Para cada critério é escolhido um número, 1 ou 2, sendo que o 1 é o menos grave e o 2 é o mais grave, a conjunção destes critérios permite a atribuição de um nível de desempenho exigido *Required Performance Level* (PLr).

Os seguintes critérios são usados para cada parâmetro de acordo com a norma AISI / RIA R15.06 [43].

S: Num caso que exija mais do que primeiros socorros, incluída ausência no trabalho, será designado de S2.

F: Num caso onde a exposição típica ao perigo é mais de um por hora, deve ser atribuído o F2

P: Num caso onde a velocidade do mecanismo é maior do que 250 mm 9,84 /s, será atribuído o P2.

Projeção de funções de segurança

Para cada parte relacionada à segurança do sistema de controlo ou à combinação das mesmas que desempenha uma função de segurança, o nível de desempenho (PL) deve ser determinado pela estimativa dos seguintes aspetos:

- Categoria;
- Cobertura de Diagnóstico (DC);
- *Mean Time To Failure* (MTTFd);
- *Common Cause Failure* (CCF).

A "categoria" de segurança foi definida na ISO 13849-1: 1999. É a classificação das partes relacionadas à segurança de um sistema de controlo em relação à sua resistência a falhas e ao seu comportamento subsequente na condição de falha e que é alcançada pela estrutura e disposição das peças e/ou pela sua fiabilidade. Estas categorias também são conhecidas como categorias arquitetónicas.

Existe uma escala de 5 categorias ("B", 1, 2, 3, 4) sendo a B o menos seguro e o 4 o mais seguro.

Na figura 2.13 está representada uma tabela, que indica os resumos dos requisitos para pertencer a uma determinada categoria.

Categoria	Resumo dos requisitos	Comportamento do sistema
B	As partes relacionadas à segurança dos sistemas de controle e seus equipamentos de proteção devem ser projetadas, construídas, selecionadas, montadas e combinadas de acordo com as normas pertinentes, de modo que possam suportar a influência esperada.	A ocorrência de uma falha pode levar à perda da função de segurança.
1	Os requisitos de B devem ser aplicados. Devem ser usados componentes bem testados e princípios de segurança comprovados. *	A ocorrência de uma falha pode levar à perda da função de segurança, mas a probabilidade de ocorrência é menor do que para a categoria B.
2	Os requisitos de B e o uso de princípios de segurança comprovados devem ser aplicados. A função de segurança deve ser verificada em intervalos adequados pelo sistema de controle da máquina.	A ocorrência de uma falha pode levar à perda da função de segurança entre as verificações. A perda da função de segurança é detectada pela verificação.
3	Os requisitos de B e o uso de princípios de segurança comprovados devem ser aplicados. As peças relacionadas à segurança devem ser projetadas de modo que - uma única falha em qualquer uma dessas peças não leve à perda da função de segurança e - sempre que razoavelmente praticável, a falha única seja detectada.	Quando ocorre uma única falha, a função de segurança é sempre executada. Algumas, mas não todas, as falhas serão detectadas. O acúmulo de falhas não detectadas pode levar à perda da função de segurança.
4	Os requisitos de B e o uso de princípios de segurança comprovados devem ser aplicados. As peças relacionadas à segurança devem ser projetadas de modo que - uma única falha em qualquer uma dessas partes não leve à perda da função de segurança e - falhas únicas sejam detectadas na ou antes da próxima solicitação da função de segurança, mas que se esta detecção não for possível, um acúmulo de falhas não detectadas não deve levar à perda da função de segurança.	Quando as falhas ocorrem, a função de segurança é sempre executada. As falhas serão detectadas a tempo de evitar a perda da função de segurança.

Figura 2.11: Categorias arquitetónicas [39]

Diagnostic Coverage (DC)

Outro fator importante é o *Diagnostic Coverage* (DC). Este fator, conforme usado na norma ISO 13849-1, é importante para analisar a qualquer função de segurança válida em qualquer projeto [44].

Desta forma, este parâmetro é importante na utilização de vários equipamentos de segurança. No entanto, uma vez que os circuitos de segurança de canal único, em particular, mas também de dois canais, frequentemente funcionam mal ou podem estar com defeito, um DC ajuda a interpretar tais estruturas adequadamente [45].

Para o cálculo da cobertura de diagnóstico deve-se ter em conta dois conceitos:

- Falha perigosa detetada: Falhas que podem levar à perda da função de segurança, somente falhas que são detetadas.
- Falha perigosa: Todas as falhas que podem levar à perda da função de segurança, falhas detetadas e não detetadas.

Assim, o DC é uma medida de eficácia de diagnóstico, que pode ser determinada pela razão entre a taxa de falhas perigosas detetadas e a taxa de falhas perigosas totais.

$$DC = \frac{\sum \lambda dd}{\sum \lambda dd + \sum \lambda du} \tag{2.9}$$

[23]

Sendo que :

λdd – Número de falhas perigosas detetadas

λdu – Número de falhas perigosas não detetadas

Uma vez calculado o DC, é classificado e atribuída uma denotação em função do seu valor, como representado na figura 2.12 da norma ISO 13849-1.

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

Figura 2.12: Classificação do *Diagnostic Coverage* [44]

Mean Time to Dangerous Failure **(MTTFd)**

O MTTFd (tempo médio para falha perigosa) é uma expectativa do tempo médio para falha perigosa de um sistema relacionado à segurança. O MTTFd é

fornecido para cada canal, como "I" (dispositivo de entrada), "L" (lógico) e "O" (dispositivo de saída). As três denotações mostradas na tabela à direita são fornecidas na ISO 13849-1.

Designação	MTTFd
Baixo	3 anos ≤ MTTFd < 10 anos
Médio	10 anos ≤ MTTFd < 30 anos
Alto	30 anos ≤ MTTFd < 100 anos

Figura 2.13: MTTFd [40]

Common Cause Failure (CCF)

A CCF refere-se à falha de causa comum, resultante de um único evento, onde as falhas não são consequências umas das outras. A norma ISO 13849-1 fornece um processo de pontuação e quantificação de medidas. Este parâmetro nem sempre é usado para a obtenção do PL.

Determinação do nível de desempenho (PL) e comparação com o (PLr)

O nível de desempenho PL pode ser determinado combinando a categoria de arquitetura, com medidas quantitativas de cobertura de diagnóstico DC e com o tempo médio para falhas perigosas (MTTF).

Dado que as categorias não podem atingir a mesma fiabilidade, o PL e as categorias estão vinculadas conforme mostrado na Figura 2.14. Este diagrama resume a relação dos parâmetros centrais da norma ISO 13849-1.

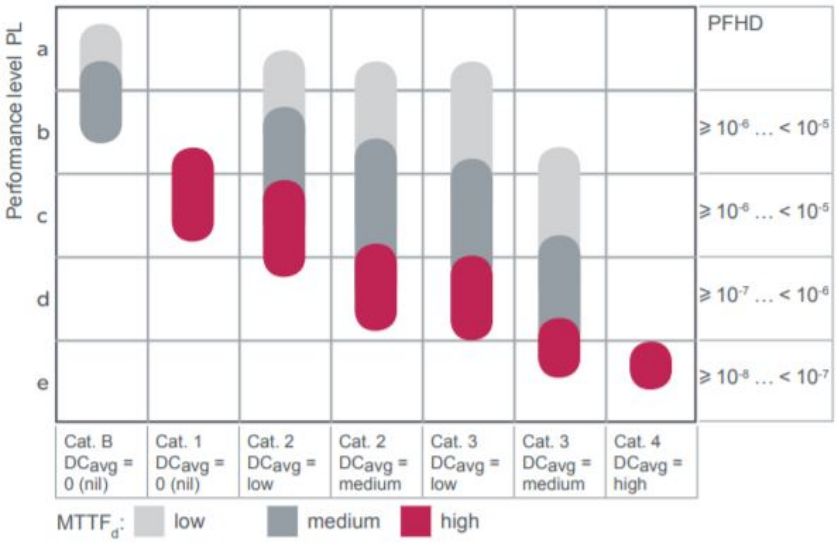


Figura 2.14: Gráfico de atribuição de PL [39]

O MTTFd diminui nos canais à medida que a cobertura de diagnóstico aumenta. O projeto compensa a fiabilidade mais baixa nos componentes aumentando a cobertura de diagnóstico e adicionando redundância. A partir da Figura 2.15, pode-se definir qualquer um dos parâmetros e selecionar outros conforme apropriado.

Por exemplo, para uma categoria 4, um MTTF > 30 anos e com um DC maior ou igual a 99% pode-se concluir pelo gráfico da Figura 2.15 que estamos perante um PLe.

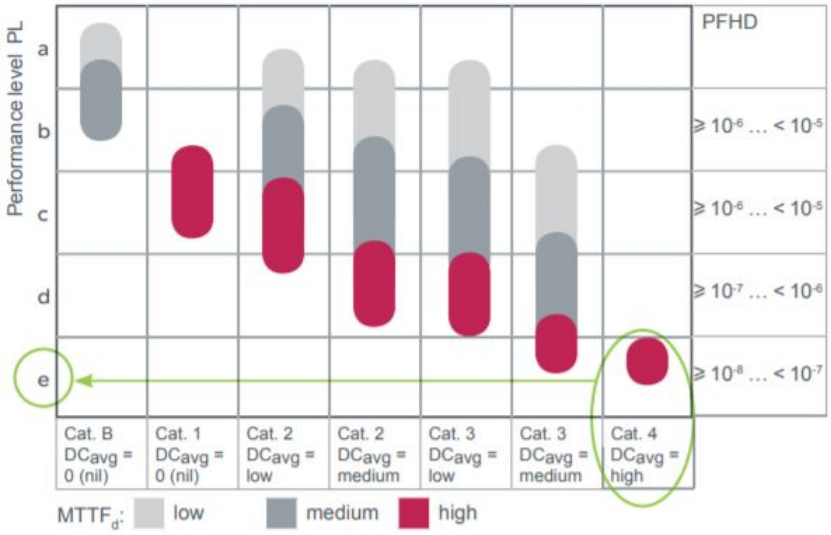


Figura 2.15: Gráfico de atribuição de PL indicativo [39]

Uma vez determinado o PL, procede-se à comparação do valor com o (PLr). Se (PL≥PLr) pode-se dizer que o nível de desempenho exigido foi conseguido.

Assim como a norma EN/ISO 13849 define níveis de desempenho, a norma EN/IEC 62061 também especifica parâmetros de medição de SIL, que têm uma relação direta com os parâmetros da norma EN/ISO 13849. A Figura 2.16 mostra a relação entre esses 2 conceitos.

Performance level (PL)	Average probability of a dangerous failure per hour (1/h)	Safety integrity level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Figura 2.16: IEC/TR 62061 – 1:2010 [46]

2.3 Cibersegurança

Atualmente a segurança da informação tem sido uma preocupação constante das diversas instituições e países que utilizam recursos computacionais para a comunicação e oferta de serviços. Os ataques cibernéticos continuam a evoluir, tonando-se cada vez mais complicados de detetar e de prevenir. Por este motivo, a necessidade de modernizar a forma como essas ameaças são tratadas deve ser uma prioridade.

São conhecidos métodos de proteção para redes tradicionais que são frequentemente utilizados, tais como, *firewalls* e detetores de intrusões. Para os sistemas de controlo e aquisição de dados SCADA, no ambiente industrial o processo é semelhante. No início, estes sistemas eram baseados em mainframes e arquitetura fechada, ou seja, dependentes dos fabricantes e consequentemente isolados de outros sistemas. Nos dias atuais, os sistemas SCADA estão a convergir cada vez mais para plataformas baseadas em sistemas abertos e com a sua arquitetura fortemente apoiada em conectividade, sendo assim usual a interligação destes sistemas com uma rede corporativa e em alguns casos com a própria internet. Para isto é necessário criar mecanismos ou programas que permitam ter uma segurança no sistema.

Quanto mais fácil for monitorizar a atividade da rede, mais rápido uma instalação poderá responder quando um ataque for detetado, o que reduzirá o impacto

do ataque. Portanto, esta é uma das etapas mais importantes na proteção de controladores lógicos programáveis (PLCs) e controladores de automação programáveis (PACs) contra ameaças à segurança. Assim, este processo de cibersegurança deve começar antes que um ataque seja detetado [47].

2.3.1 Convergência entre OT e IT

Nos dias de hoje, cada vez mais se tem vindo a afiliar a tecnologia operacional (OT) e a tecnologia da informação (IT). A tecnologia operacional (OT) controla o equipamento, a tecnologia da informação (IT) controla os dados. Especificamente a IT concentra-se em garantir a confidencialidade, integridade e disponibilidade dos sistemas e dados.

Tradicionalmente a cibersegurança de OT não era necessária porque estes sistemas não estavam ligados à internet, por isso, nunca foram expostos a ameaças externas. Conforme as iniciativas de *Digital Inovation* (DI) se foram expandindo e as redes de OT e IT convergiram, as organizações tiveram a necessidade de reforçar as suas soluções pontuais para tratar de questões relacionadas com a cybersegurança. Essas abordagens à segurança de OT resultaram numa rede complexa onde as soluções não podiam partilhar informação e fornecer visibilidade total [48].

Assim, a convergência entre a OT e a IT é fundamental, pois tem uma relação direta com a conectividade industrial entre os equipamentos, um maior volume de dados e uma maior automatização e segurança. A ligação com a internet permite uma visibilidade em tempo real de todos os processos, inclusive à distância, o que traz uma grande praticidade para os analistas técnicos e também para a gestão, que pode utilizar informações atualizadas em eventos externos à industrial [49].

2.3.2 Risco à Segurança

São inúmeros os problemas e ameaças que surgem da capacidade de conectividade entre os equipamentos e o mundo exterior. A maioria das ameaças são fatores externos ao organismo ou sistema. Um dos ataques mais conhecidos e comuns nas redes industriais é o *attack vector*. Este é um método usado para ter acesso a um sistema e poder controlar ou executar ações, como é o caso de ataques de manipulação de máquinas sendo este o caso mais comum nas passagens de nível, podendo dar sinais para abrir uma barreira quando o movimento não é pedido, ou dar informações falsas aos sensores, afetando assim o normal e desejado funcionamento do sistema, pondo em risco a segurança do mesmo. Desta maneira, alguém que tenha acesso à estrutura de TI da organização, pode instalar um código malicioso

que pode controlar remotamente a infraestrutura de TI, saber informações de uma organização em questão, ou até roubar dados ou recursos. Os *attack vector* podem ser feitos por uma variedade de grupos de pessoas, desde um ex-funcionário descontente com a empresa que deseja comprometer os negócios da mesma, até ao serviço de inteligência de um governo [50].

No entanto, proteger de ameaças externas não é suficiente, visto que também podem existir ameaças internas. Um *Malicious Insider*, pode ser um utilizador com acesso a dados e redes confidenciais, podendo causar danos extensos por meio do uso indevido de privilégios, como pode ser o caso de um funcionário que expõe informações privadas da empresa ou que pode causar danos intencionados a um controlador da empresa. Também pode existir o fator de erro humano, como pode ser um carregamento incorreto do código ou uma má programação. Estes fatores podem causar danos tão prejudiciais como os ciberataques [51].

2.3.3 Prevenção e Limitação de Danos

Não importa o quão preparada esteja uma empresa, os ataques e violações de segurança podem sempre ocorrer. Portanto, é importante não apenas evitar que eles ocorram, mas também garantir que, caso ocorram, o dano seja o mínimo possível. Exemplos de algumas medidas passíveis de serem utilizadas são:

- A segmentação de redes em zonas lógicas ajuda a impedir ameaças internas que, embora sejam menos comuns, costumam resultar em maiores danos.
- Uma maneira de limitar os danos à rede é ter mais do que um controlo de segurança. Por isso, uma abordagem robusta em camadas com controlos de segurança em muitos níveis independentes é mais difícil de um invasor comprometer todo o sistema.
- Outra forma de limitar os efeitos de uma violação é utilizando redundância ou incluindo componentes de backup num sistema, para que possa continuar a funcionar em caso de falha do componente ou em caso de violação da segurança.
- No mínimo, as instalações devem garantir a implantação segura com *firewalls* e segmentação para bloquear o tráfego de entrada não solicitado, bem como isolar as redes para restringir a transferência de dados para os seus locais pretendidos. O uso de *firewalls* avançados ou de camada de aplicativo é uma boa abordagem para aumentar esse recurso.

- Bloquear todas as portas de comunicação não utilizadas e desligar todos os serviços não utilizados são outras etapas simples que devem ser tomadas para reduzir a área de superfície que pode ser atacada.
- As instalações devem trabalhar com fornecedores que tenham certificações comprovadas de sistemas PLCs e PACs que abrangem os requisitos técnicos de segurança de projeto e engenharia para um sistema de controlo. As certificações permitem que os fornecedores de sistemas de controlo ilustrem formalmente a conformidade dos seus sistemas de controlo produzidos com requisitos de segurança cibernética.
- Monitorizar a comunicação da máquina dentro de uma instalação é outra etapa crítica para garantir que um ataque não ocorra. Todas as comunicações devem ser feitas com segurança por meio de protocolos para automação industrial que oferecem segurança robusta que consiste em autenticação e autorização, criptografia e integridade de dados. Ao monitorizar as comunicações de rede, as portas ou protocolos recém-abertos em uso alertam os usuários sobre potenciais ameaças.
- Finalmente, uma das maneiras mais importantes de limitar o impacto da violação de segurança é estabelecer uma continuidade de negócios eficaz e sólida ou processos e políticas de recuperação, para que uma violação possa ser tratada antes que o seu impacto tenha a chance de se espalhar e provocar ameaças futuras.

2.3.4 Isolamento da Rede PLC

O maior risco representado pelo acesso remoto à rede é que o mesmo possibilita a um *hacker* obter acesso mais profundo a uma organização de fora dela e, quando o faz, torna-se complicado evitar *shutdowns* não planeados, perda de controlo, ou até perda de dados. As empresas também devem auditar a sua rede de PLC para localizar quaisquer vetores de acesso obscuros que um *hacker* possa usar e monitorizar regularmente os pontos de acesso. Uma empresa pode implementar a autenticação multifator, que exige que um utilizador apresente com sucesso duas ou mais evidências, ou fatores, a um mecanismo de autenticação para ter acesso a um dispositivo, aplicativo ou informação.

A autenticação de dois fatores é um subconjunto normalmente usado de autenticação multifator. Este método confirma a identidade reivindicada de um utilizador usando uma combinação de dois dos seguintes fatores diferentes: algo que eles sabem, como uma senha e algo que eles têm, como um cartão-chave ou token de software, ou algo que eles são, como apresentar uma impressão digital ou identificação facial.

2.3.5 Gestão e Autenticação do Utilizador PLC

Os comportamentos não intencionais podem ser uma das ameaças mais críticas para uma organização. Para mudar isto, é importante adotar os melhores comportamentos e educar os trabalhadores para diminuir os riscos. Por exemplo, uma das maiores ameaças à segurança é a seleção de senha. Num mundo onde algumas das senhas mais comuns são "password" ou 123456, nunca é demais enfatizar a enorme importância que tem instruir os utilizadores a selecionar senhas fortes e oferecer orientações sobre como fazê-lo e uma exigência automática da mudança da mesma periodicamente.

A autenticação multifator e o controlo de acesso são as melhores opções que um sistema pode oferecer suporte a esse nível de segurança [52].

2.3.6 Fabricantes

Além destes cuidados a ter para prevenir ou limitar danos, existem vários fabricantes e empresas que se dedicam a criar sistemas de proteção e cibersegurança, que têm como objetivo proteger o sistema de ciberataques. Entre eles, empresas multinacionais como a Microsotf, IBM, McAfee, Fortinet, Cisco, etc.

2.4 Conclusão

Neste capítulo são descritos e apresentados os parâmetros e normas de segurança tipicamente utilizados num projecto de automação. Por outro lado, é discutida a crescente importância das preocupações de cibersegurança na indústria, como também são apresentados alguns dos riscos e medidas de prevenção a ter em conta. Com isto é possível conhecer alguns dos conceitos que são essenciais para o projeto do sistema de controlo analisado no capítulo 3.

Capítulo 3

Descrição do Problema

Neste capítulo é feita a descrição do sistema atual de barreira, Xbarrier 100, de forma a compreender o problema que se pretende abordar. Em seguida, são apresentados os objetivos para a realização deste projeto, nomeadamente quanto aos seus componentes: o controlador da barreira e protocolo de comunicação industrial. Por último, é apresentada a lista dos requisitos para o controlo do mecanismo de barreira conforme solicitado pela empresa Efacec.

3.1 Sistema de Barreira Atual

Este sistema baseia-se num mecanismo que atua em passagens de nível e faz parte do sistema de segurança ferroviária galardoado com os prémios Red Dot Awards, na categoria Product Design 2021[53], pela conjugação de design e segurança. Este sistema foi desenvolvido e fabricado pela empresa Efacece e está representado na Figura 3.1.

Figura 3.1: XBarrier 100

O principal objetivo deste mecanismo é proteger os veículos na área da passagem de nível, ao controlar o seu tráfego, em função da passagem de veículos ferroviários e dando a indicação de abrir ou fechar a barreira, minimizando o tempo de espera do transeunte, mas dando sempre prioridade à segurança deste.

O sistema básico de funcionamento consiste em dois movimentos ativos, um de subida e outro de descida, ambos acionados por um motor, e este último não se deve à força da gravidade. O mecanismo permite um acionamento manual, além do seu funcionamento automático.

O sistema XBarrier 100 é constituído por:

- Um sistema de transmissão mecânica;
- Uma caixa/carcaça que obedece à norma EN aplicável;
- Um conjunto de dispositivos para monitorizar a posição da barreira;
- Um conjunto de elementos que deteta o acesso ao interior do mecanismo;
- Um motor elétrico;
- Um sistema elétrico para permitir o funcionamento automático;
- Uma barreira cilíndrica;

- Um conjunto de luzes na barreira (opcional);
- Um sistema de iluminação interior da caixa (opcional);
- Uma saia metálica na barreira (opcional);
- Um suporte para a luz na barreira (opcional).

Atualmente, o mecanismo é alimentado por uma fonte de alimentação externa e gerido por um controlador externo localizado num armário lógico situado nas proximidades da passagem de nível, representado na Figura 3.2.

Figura 3.2: Armário lógico da Efacec

3.2 Objetivos do Projeto

O projeto consubstancia-se em dois grandes objetivos:

- Projetar um **controlador da barreira** que se adeque ao sistema atual descrito no subcapítulo 3.1 e que cumpra com os requisitos de segurança dados pela Efacec. Posteriormente, fazer a programação do controlador com funções específicas predeterminadas, de acordo com os requisitos estabelecidos pela Efacec e descritos no subcapítulo 3.3.

- Escolher um protocolo de comunicação industrial que permita fazer a comunicação entre o controlador da barreira e o resto dos dispositivos que vão ser ligados a uma mesma rede e, por sua vez, fazer a configuração deste protocolo no PLC da barreira.

3.2.1 Controlador Interno da Barreira

O primeiro objetivo consiste em projetar um controlador interno que vai estar localizado no interior da caixa do XBarrier 100 que está representada na Figura 3.3.

Figura 3.3: Caixa do XBarrier 100

Este controlador vai estar integrado na gama de dispositivos que faz parte do segundo nível da pirâmide de automação, ou seja, nível de controlo, onde estão incluídos os PLCs, PCs e PIDs, embora esteja diretamente relacionado com os elementos do primeiro nível desta pirâmide, descrita no subcapítulo 2.1

O objetivo é implementar funções à barreira que sejam independentes do controlador externo e, desta maneira, descentralizar a arquitetura de PLCs do sistema, passando a serem realizadas algumas das funções que antes eram feitas pelo controlador externo, pelos controladores internos das barreiras. Com isto, é possível reduzir o número de funções do controlador externo, assim como o número de cabos antes existentes entre o armário lógico e o XBarreier 100. Um exemplo gráfico representativo de uma possível localização dos PLCs na passagem de nível é mostrado na Figura 3.4.

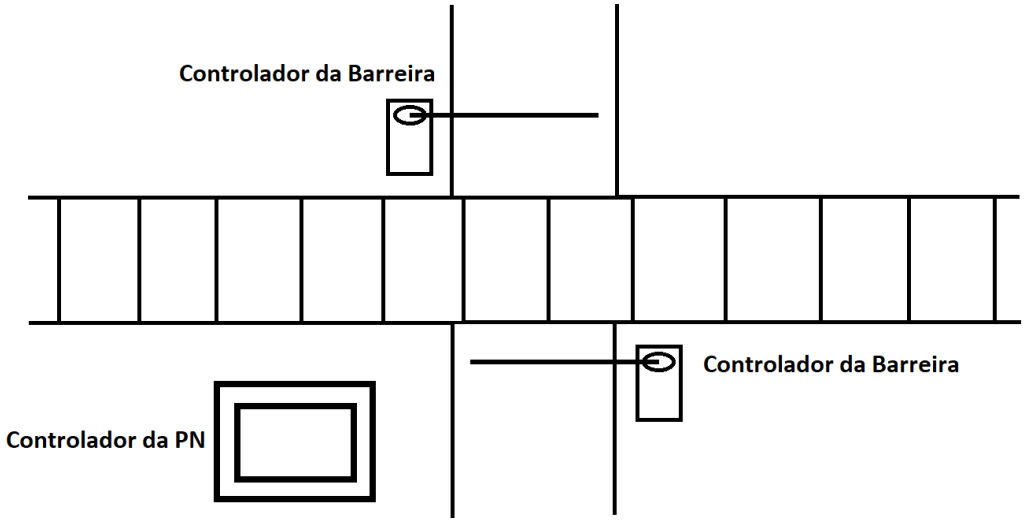


Figura 3.4: Localização dos PLCs na PN

Os PLCs das barreiras, o PLC externo e outros dispositivos do sistema da ferrovia serão ligados a uma mesma rede, o que permitirá uma intercomunicação entre todos eles. Os sinais e comandos dados pelo sistema da ferrovia como, por exemplo, a aproximação de um comboio à passagem de nível, são recebidos pelos PLCs da barreira através da rede.

Também é possível reduzir o número de cablagens necessárias para fazer a ligação entre as entradas e saídas à barreira e o armário lógico.

O esquema da Figura 3.5 representa um esboço da rede e dos dispositivos a ela pertencentes.

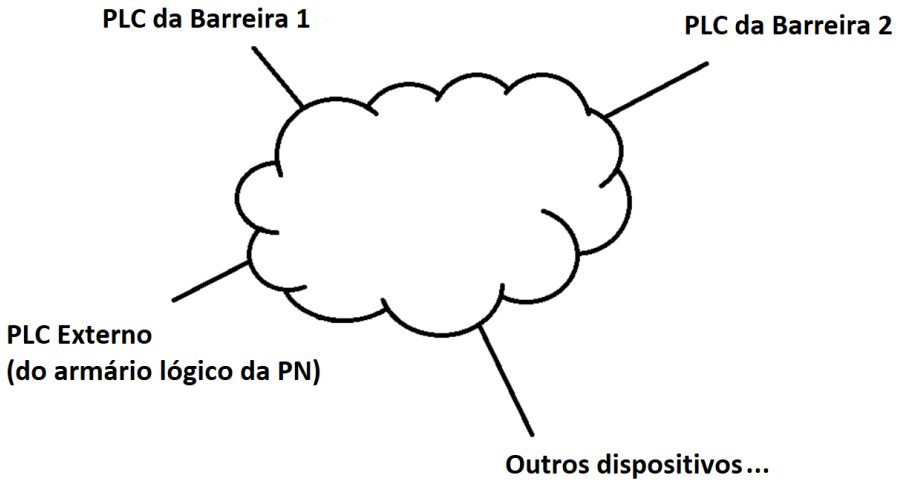


Figura 3.5: Rede de PLCs

Um requisito importante que deve cumprir o PLC que se escolha para implementar esta solução é o cumprimento de normas e requisitos de segurança que se estabelecem no subcapítulo 3.3.

Assim, o primeiro passo é selecionar um PLC com as funcionalidades e características de segurança que melhor se adeque para dar solução ao problema e que cumpra as normas e requisitos propostos pela empresa.

O segundo passo é programar o controlador com os requisitos e funções descritas no subcapítulo 3.3.

3.2.2 Protocolo de Comunicação

O segundo objetivo deste trabalho é selecionar um protocolo de comunicação industrial que permita a adequada e segura comunicação entre os dispositivos que estarão ligados à rede.

Para fazer a comunicação entre dois ou mais dispositivos industrias, como é o caso dos PLCs, sensores, ou atuadores é necessário estabelecer um protocolo de comunicação industrial que seja adequado ao paradigma do problema. Um protocolo de comunicação, tecnicamente, é um conjunto de regras normalizadas que caracterizam o formato, a sincronização, a sequência e, ainda, a deteção de erros e falhas na comutação de pacotes de dados, isto é, na transmissão de informação entre dois dispositivos.

Durante a última década, as redes de comunicação são as que tiveram uma maior evolução na área de controlo industrial e de sistemas, à semelhança de outros ramos de atividade como as telecomunicações móveis, a Internet, a comunicação sem fios, entre outros. A utilização das redes permite uma comunicação rápida entre equipamentos que, hoje em dia, se tornou um fator fundamental na produtividade industrial.

Dentro deste contexto, é cada vez mais importante definir os protocolos de comunicação para o bom funcionamento de um sistema industrial, tendo em conta vários parâmetros que definem os protocolos e alguns aspetos, tais como:

- Facilidade de uso;
- Velocidade de transmissão;
- Número máximo de estações;
- Compatibilidade de equipamentos;

- Tamanho do pacote;
- Tipos de correção de erros;
- Mapeamento de endereços;
- Processos de reconhecimento;
- Controlo de fluxo;
- Controlo de sequência de pacotes.
- Formatação do endereço.

Com base nestes parâmetros, consegue-se definir o tipo de aplicação para a qual se vai implementar o protocolo de comunicação para, desta maneira, selecionar, utilizar e configurar o protocolo que mais se adapte às características do sistema de automação em causa [54].

Por sua vez, e uma vez escolhido o protocolo de comunicação, é necessário proceder à sua configuração e determinação de alguns parâmetros do protocolo.

3.3 Lista de Requisitos da Solução Global

Neste subcapítulo são apresentados os requisitos selecionados pela empresa Efacec que o sistema XBarrier 100 deve cumprir.

A Figura 3.6 apresenta um esboço do XBarrier 100, incluindo a terminologia usada. Além disso, permite representar os ângulos críticos que a barreira pode atingir, desde -10º até 90º. A razão do ângulo da barreira ir até um mínimo de -10º, deve-se ao facto de, compradores de alguns países exigirem que a barreira esteja paralela ao solo e, quando há superfícies inclinadas, isto só é possível se a barreira for inferior a 0º de inclinação.

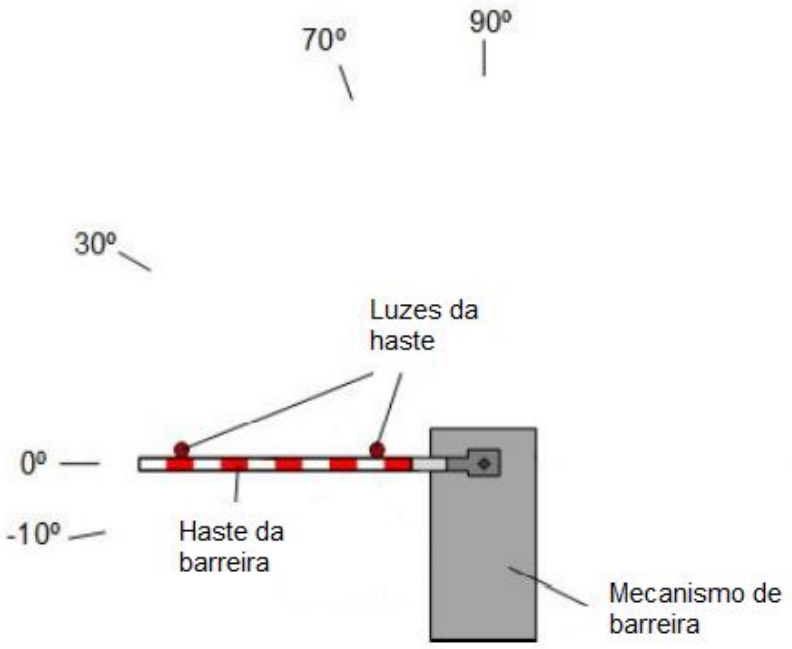


Figura 3.6: Designações e ângulos da barreira

Nos subcapítulos seguintes são transcritos os requisitos globais para o projeto, que a proposta de solução do controlador deve ter em conta.

3.3.1 Normas Aplicáveis

- EN 50126-1:2017 - Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safery;
- EN 50121-4 2016 - Railway applications Electromagnetic compatibility. Emission and immunity of the signalling and telecommunications apparatus;
- EN 50124-2:2017 - Railway applications Insulation coordination. Overvoltage's and related protection;
- EN 50125-3:2003 - Railway applications. Eviromental conditions for equipment. Equipment for signalling and telecomunications;
- EN 60529:1992 - Degrees of protection provided by enclouseres (IP code);
- EN 62262:2002 - Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code);

- Directive 2006/42/EC on machinery.

3.3.2 Requisitos Gerais

- O desenvolvimento do processo deve seguir a norma EN 50126-1:2017;
- O sistema de barreira deve ser projetado de modo que o tempo estimado de qualquer instalação seja de, pelo menos, 30 anos;
- O MTBF da barreira deve ser, no mínimo, de 500 000 operações;
- A barreira deve ser dimensionada para que seja capaz de resistir a 300 operações por dia;
- A execução não solicitada de qualquer movimento devido a falhas de componentes (mecânicos, elétricos, etc.) deve ter uma taxa de falha máxima de $10^{-9}.\mathrm{h}^{-1}$.

3.3.3 Requisitos Ambientais

- Os requisitos ambientais devem estar de acordo com a norma EN 50125-3:2003, sempre que aplicável;
- A temperatura máxima de operação da barreira deve ser, no mínimo , +70ºC;
- Em conformidade com o limite superior da classe climática T1, de acordo com a norma EN 50125-3:2003;
- A temperatura mínima de operação da barreira deve ser, no máximo, -40ºC;
- Atendendo ao limite inferior da classe climática T2, de acordo com EN 50125-3:2003;
- Não é permitido ter resistências de aquecimento para suportar esta temperatura. Se considerado economicamente relevante, a faixa entre -40ºC e -20ºC pode ser vista como opcional;
- A altitude máxima de operação da barreira deve ser, no mínimo, 1000m;
- Em conformidade com a classe de altitude A2, de acordo com a norma EN 50125-3:2003;
- A humidade mínima de operação da barreira deve ser, no máximo, 5%;
- A humidade máxima de operação da barreira deve ser de 100%;

- Em conformidade com a classe climática T1, de acordo com a norma EN 50125-3:2003;
- O efeito da radiação solar deve ser considerado, de acordo com a norma 50125-3:2003;
- O efeito da poluição deve ser considerado, ao nível4 C2 de acordo com a norma EN 50125-3:2003;
- O efeito de choque e vibração deve ser considerado para posicionar "fora da pista" de acordo com a norma EN 50125-3:2003.

3.3.4 Requisitos Elétricos

- O controlador deve ser alimentado com uma tensão nominal de 24 V DC +/- 20%;
- O sistema deve suportar um pico de corrente de 100A;
- O sistema deve suportar uma corrente constante de 10A.

3.3.5 Requisitos de Interface

- A interface do controlador de passagem de nível e do controlador de barreira deve ser implementada com uma conexão IP;
- O protocolo escolhido deve ser compatível com o nível de segurança alto.

3.3.6 Requisitos Funcionais

- O controlador tem de estar apto para dar o comando, ao motor, de abrir a barreira;
- O controlador tem de estar apto para dar o comando, ao motor, de fechar a barreira;
- Cada movimento ativo deve ter um comando independente do controlador da passagem de nível;
- Se a posição para a qual o mecanismo é comandado não for atingida após um tempo limite configurável, o controlador deve parar de alimentar o motor;
- Este tempo deve ser configurado para entre 5 e 60 segundos;

- Quando o controlador parar a barreira após um tempo limite, se a posição para a qual o mecanismo é comandado não for alcançada, o controlador deverá efetuar outra tentativa de mandar sinal após um determinado período de tempo;
- Esse tempo deve ser configurado para entre 5 a 60 segundos;
- O número máximo de tentativas deve ser configurado de entre 0 a 10;
- Quando a barreira está em modo manual, o controlador não pode dar nenhum comando de movimento ao motor;
- A barreira só se pode mover quando lhe for ordenado fazê-lo;
- A ativação da indicação "prova que está fechado" quando a barreira estiver num estado diferente, devido a uma falha de componentes (mecânicos, elétricos, etc.), deve apresentar uma taxa de falha máxima de $10^{-9}.\mathrm{h}^{-1}$;
- As ligações elétricas das luzes devem permitir a ligação independente de dois grupos de luzes;
- Por exemplo, a iluminação independente da luz da ponta das demais;
- A abertura da caixa do mecanismo de barreira deve cortar a energia do mecanismo;
- Um painel de manutenção deve ser equipado com indicações para sinalizar o status de operação do mecanismo da barreira;
- A operação deste painel de manutenção deve inibir o modo de operação automática;
- Os comandos e indicações devem estar prontos para a interface com um painel externo, com as mesmas funcionalidades;
- O controlador deve permitir a configuração do tempo de abertura;
- O controlador deve permitir a configuração do tempo de fecho;
- O valor mínimo para o tempo de abertura deve ser, no máximo, 6 segundos;
- O valor máximo para o tempo de abertura deve ser, no mínimo, 12 segundos;
- O valor mínimo para o tempo de fecho deve ser, no máximo, 6 segundos;
- O valor máximo para o tempo de fecho deve ser, no mínimo, 12 segundos;
- O controlador deve comandar a luz interna do mecanismo;

- O controlador deve ter uma entrada para receber a informação de que a barreira está na posição aberta;
- O controlador deve ter uma entrada para receber a informação de que a barreira está na posição fechada;
- O controlador deve ter uma entrada para receber a informação de que a posição da barreira está acima do meio;
- O controlador deve ter entradas para receber as informações sobre a abertura das portas do mecanismo;
- O controlador deve ter uma entrada para receber a informação de que o mecanismo foi mudado para a operação manual.

3.3.7 Conclusão

Este capítulo foca-se principalmente nos detalhes do sistema em estudo, na compreensão do mecanismo de barreira e da problemática ligada à implementação do PLC, assim como do protocolo de comunicação aplicável. A boa compreensão do problema, passa pela definição de objetivos e pela listagem dos requisitos definidos que irão ser a base da proposta de solução, a desenvolver no próximo capítulo 4.

Capítulo 4

Proposta de solução

Na procura da proposta de solução é inicialmente feita uma listagem dos controladores de segurança, aplicáveis ao mecanismo de barreira, disponíveis na indústria. Posteriormente, é feita uma análise e estudo de forma a escolher o controlador que mais se adeque ao problema em causa. Por outro lado, são estudados e listados os protocolos de comunicação industrial mais utilizados de forma a selecionar o mais adequado para fazer a comunicação do controlador barreira com outros dispositivos.

4.1 Controlador da Barreira

Este subcapítulo está dividido em duas partes:

- Listagem dos PLC de segurança com as caraterísticas apropriadas para este projeto;
- Posteriormente, é escolhido o PLC aplicável em função dos critérios de seleção, é descrita a arquitetura do PLC proposto, é feita uma análise do cumprimento dos requisitos globais do projecto e, por fim, é apresentado o custo dos componentes do sistema;

4.1.1 Listagem de Controladores

Neste subcapítulo são selecionados e estudados alguns dos PLCs/módulos de segurança, dentro das diferentes marcas existentes na indústria e fornecedores presentes em Portugal, de acordo com as necessidades e exigências que se enquadram neste projeto. Desta maneira, foram listados e analisados os PLCs que possuem as condições de segurança exigidas para este projeto, tendo também em consideração o desempenho e fiabilidade e ainda o seu custo associado.

A lista dos controladores que são analisados é a seguinte:

- ABB;
- Allen Bradley;
- HIMA;
- Mitsubishi;
- Shneider;
- Phoenix Contact.

Além destes 6 controladores listados, também é recolhida informação de outras empresas fabricantes de PLC, mas não são tidos em conta porque não se adequavam aos requisitos do projeto, entre eles, as marcas Delta Group, Kojo, Telemecanique, Siemens, Omron e Pilz.

De seguida, vão ser analisados com mais detalhe cada um dos 6 PLCs selecionados e a sua empresa fabricante.

ABB

A ABB é uma empresa que atua no setor de energia e automação, com sede na Suiça. Esta empresa tem no mercado um conjunto PLC dedicado à segurança, como é o AC500–S. Este PLC é uma melhoria do PLC AC500, mas com requisitos de segurança adicionados. Atinge um nível (SIL3, PLe) e é projetado para aplicações de segurança envolvidas na área de automação de fábrica, maquinaria ou processo. Normalmente utilizada para implementar e gerir soluções de segurança complexas. É certificado para aplicações de segurança SIL3 (IEC 61508, IEC 62061, IEC 61511) e PLe (ISO 13849-1) [55].

O seu módulo de segurança, representado na Figura 4.1, SM560-S, atinge um nível SIL3. O módulo de entradas e saídas, DX581-S, possui 8 canais de saída digital

de segurança até SIL3 ou PL e 8 canais de entrada digital de segurança até SIL2 ou PL d, ou então 4 canais duplos até SIL3 ou PL e com 4 saídas de pulso de teste. Todos os canais (incluindo saídas de pulso de teste) são protegidos contra polaridade inversa, alimentação inversa, curto-circuito e sobretensão contínua de até 30 V DC.

Figura 4.1: Safety PLC da ABB [55]

Allen Bradley

Allen-Bradley é o nome de marca de uma linha de equipamentos de automação, atualmente de propriedade da Rockwell Automation. Dentro dos diferentes produtos existem alguns especializados na segurança, como:

- Controladores programáveis de segurança;
- Módulos (I/O) de segurança;
- *GuardLink Technology*;
- Conceções de segurança;
- *Safety Drivers*;
- Sensores de presença de segurança;
- *Safety realms*, entre outros.

Entre eles, o último PLC de segurança lançado no mercado, o Controlador ControlLogix 5580, ilustrado na Figura 4.2.

Este controlador usa o ambiente de design Studio 5000® como estrutura padrão. Essa estrutura administra o movimento integrado sobre EtherNet/IP para aplicações de movimento de alta velocidade e soluções de segurança SIL2 / PLd e SIL3 / PLe. Assim, é ideal para aplicações que requerem comunicações de alto desempenho

e elevado número de entradas e saídas.

Figura 4.2: Safety PLC da Allen Bradley [56]

Este produto atinge o nível SIL 2 / PLd com o controlador primário e atinge o nível SIL 3 / PLE com o controlador primário mais uma adição de segurança [56].

Algumas das caraterísticas térmicas:

- Operação de -25ºC a 70ºC;
- Projeto de arrefecimento por convecção;
- Testado para a ANSI / ISA-S71.04-1985: Padrões de classe G3.

HIMA

A HIMA é uma empresa alemã fundada em 1908, que tem o seu foco na área da tecnologia de automação e segurança, que produz equipamentos de segurança para sistemas e espaços industriais.

Em 2002 a HIMA introduziu no mercado o HIMatrix, o primeiro sistema de segurança certificado pela TÜV, com comunicação segura via Ethernet para passagens de nível protegidas na indústria ferroviária, entre outras. Além disso, como primeiro produtor mundial de sistemas de segurança, a empresa tem o certificado IEC 61508 para a gestão de segurança funcional da TÜV [57], representado na Figura 4.3.

O controlador de segurança e módulos de E/S da série HIMatrix, juntamente com a comunicação *safe ethernet* são certificados para uso até SIL 3 e PLe (Cat. 4), de acordo com a norma IEC 61508. A configuração e a programação do HIMatrix são executadas através da ferramenta de programação SILworX.

Figura 4.3: Safety PLC HIMAtrix [57]

Mitsubishi

A Mitsubishi é uma empresa multinacional com sede no Japão. É uma empresa especializada na produção automóvel, embora ao longo dos últimos anos tenha começado a investir na indústria de automação.

O PLC MELSEC-QS Series é um controlador programável de segurança, constituído por um conjunto de módulos, que está em conformidade com os padrões de segurança internacionais, EN ISO 13849-1 Categoria 4 / PLe e IEC 61508 SIL 3. É utilizado para sistemas de controlo de segurança de médio a grande porte [58]. Este controlador encontra-se representado na Figura 4.4.

Os módulos de alimentação QS061P-A1 e QS061P-A2 têm capacidade de receber uma tensão nominal de 120V AC e 240V AC e tranformar à saída para uma tensão de 5VDC.

Os módulos de comunicação permitem estabelecer protocolos de comunicação baseados em Ethernet e os protocolos CC-link IE e CC-link Safety.

Figura 4.4: Safety PLC da Mitsubishi [58]

Schneider

A empresa Schneider é um grupo multinacional francês, atualmente ativa no mercado de gestão de energia e automação.

O modelo Preventa XPS MF é o PLC especializado em segurança fabricado pela HIMA e vendido pela Schneider. Utiliza o software XPSMFWIN para fazer a sua programação. Alcança um Categoria 4 em conformidade com a norma EN 954-1 e SIL3 em conformidade com a norma IEC 61508. Permite uma comunicação com outros módulos de entradas e saídas via Safe Ethernet lPermite uma comunicação com PLCs *standard* ou HMI via Modbus *Transmission Control Protocol* (TCP), Modbus ou Profibus *Decentralized Peripherals* (DP).

Existem 2 tipos de PLC de segurança deste modelo, representados na Figura 4.5:

- Compacto com (I/O) integrados;
- Modular, em rack com 6 slots para vários módulos de (I/O) separados[59].

Figura 4.5: Safety PLC Preventa XPS MF [59]

Phoenix Contact

A Phoenix Contact é uma empresa alemã fabricante de soluções de automação industrial, interconexão, interface, componentes, sistemas e soluções relacionadas com a área de engenharia elétrica e eletrónica. Atualmente possuem uma rede global em mais de 100 países.

A Phoenix desenvolveu uma nova tecnologia, PLCnext, que consiste num ecossistema aberto e exclusivo para automação moderna, desenhado para atender aos desafios do mundo da *Internet of Things* (IoT). Esta consiste numa plataforma de controlo aberta (*open source*), software de engenharia modular e integração sistémica em nuvem (*cloud*) que permite uma adaptação simples às características da procura em constante mudança e a utilização eficiente de serviços de software.

Com a PLCnext a Phoenix Contact oferece à comunidade PLCnext uma plataforma de troca aberta para as suas funções de software.

Esta empresa desenvolveu e lança ao mercado este ano, 2021, um módulo de *Central Processing Unit* (CPU) com caraterísticas de segurança, "*Axioline F module with integrated safety logic and safe digital outputs*", representado na Figura 4.6.

Algumas das carateristicas deste módulo são, a resistência a uma temperatura de operação de entre -35°C a 60°C, atinge um SIL máximo de 3, de acordo com a norma IEC 61508 e tem um máximo de PLe e Categoria 4, de acordo com a norma EN ISO 13849 [60].

Figura 4.6: Módulo de Segurança com CPU da Phoenix Contact [60]

Os módulos de entrada AXL F SSDI8/4 1F e de saída AXL F SSDO8/4 1F, permitem a ligação de 4 entradas e 4 saídas de canal duplo com redundância e podem ser acoplados ao módulo CPU de segurança até um máximo de 13 módulos de entradas e saídas.

4.1.2 Controlador Aplicável

Todos os seis controladores listados no subcapítulo 4.1.1, adequam-se em termos de segurança ao projeto, mas apenas um, é o PLC escolhido para desempenhar as funções no sistema da barreira. Para a decisão final e escolha do PLC aplicável, foram comparados e tidos em conta vários parâmetros tendo em consideração vários fatores segundo é explicado de seguida.

Critérios de Seleção

Neste subcapítulo são detalhados os critérios tidos em conta para a seleção do controlador.

- **Cumprimentos dos requisitos do projeto**, assim como as suas caraterísticas de segurança aplicáveis, descritos no subcapítulo 3.3;
- **Custo de aquisição baixo**, relativamente à oferta existente no mercado;
- **A familiarização, o conhecimento e a experiência com a marca e com os seus dispositivos**. A Efacec atualmente possui e trabalha com controladores e módulos da HIMA e da Phoenix Contact para aplicações ferroviárias. Em consequência já existe uma adaptação ao funcionamento de ambos estes PLCs e às suas plataformas de programação.

- **Relação comercial**. A Efacec já tem estabelecida uma relação comercial tanto com a HIMA, como com a Phoenix Contact, que facilita a comunicação entre as empresas.

Para além destes critérios é tido em conta o número de **entradas e saídas** que foram estabelecidas na fase de implementação da solução, descritas no subcapítulo 5.1.

A Figura 4.7 representa esquematicamente o diagrma de blocos da solução implementada detalhando as ligações de entradas e saídas necessárias:

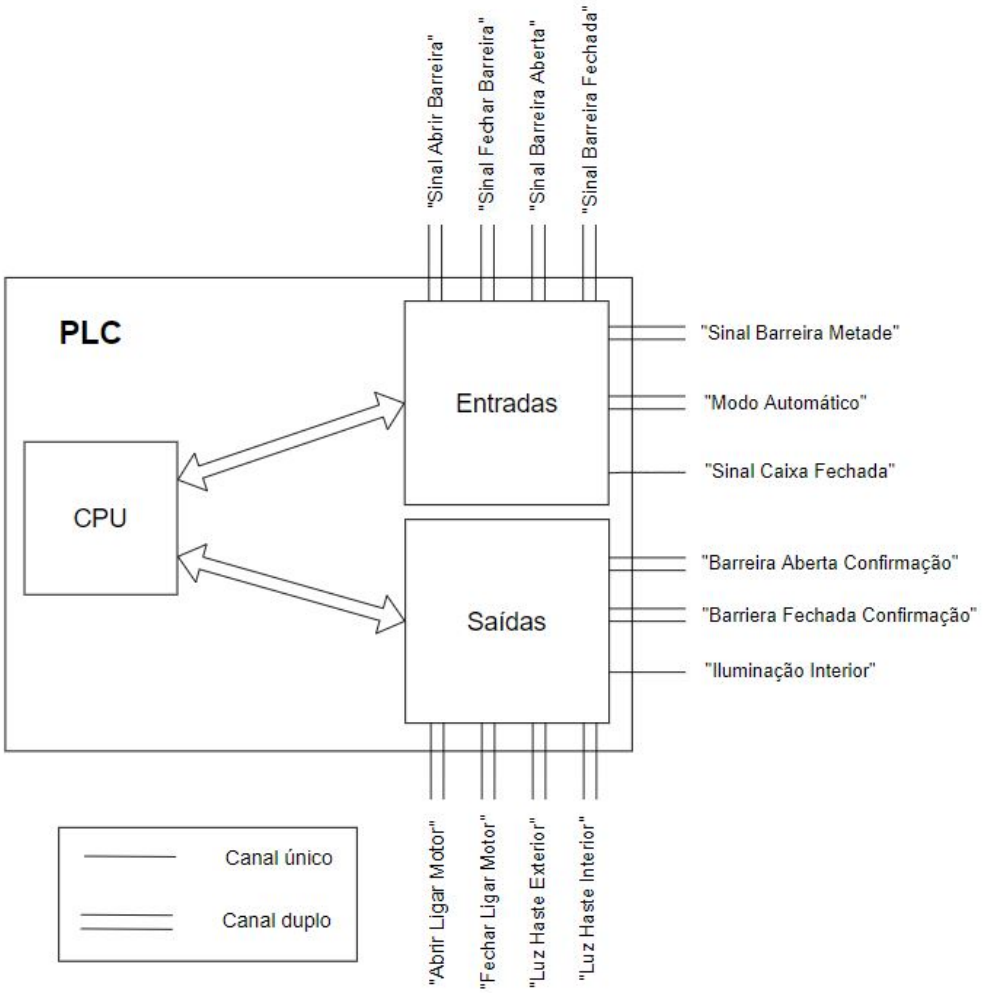


Figura 4.7: Diagrama de Blocos da Solução

Tendo em conta os fatores descritos e por indicação da Efacec a escolha final decaiu sobre o **PLC da marca Phoenix Contact** que estará composto pelos módulos representados a seguir no subcapítulo 4.1.2.

Descrição do PLC Proposto

A seguir é apresentada e descrita a arquitetura projetada do conjuto do PLC. Entre eles foram escolhidos os seguintes módulos:

- Um modulo **AXC F 2152**, que é um processador *standard* que pode ser acoplado ao LPSDO. Atualmente a empresa já possui um, onde é carregada a lógica do programa;
- Um módulo **AXL F LPSDO8/3 1F** é um processador de segurança (Fail Safe). O LPSDO, não funciona de forma individual (*stand alone*), precisa de estar acompanhado por um autómato AXC standard;
- Dois módulos **AXL F SSDI8/4 1F**, cada um com espaço para 4 entradas digitais de canal duplo, ou 8 de canal único;
- Um módulo **AXL F SSDO8/3 1F**, com espaço para 4 saídas digitais de canal duplo, ou 8 de canal único;
- Um módulo **AXL F DI8/1 DO8/1 1H**, com capacidade para ligação de 8 entradas e 8 saídas de canal único (opcional).

A imagem 4.8 representa uma possível ordem de acoplamento dos diferentes módulos escolhidos.

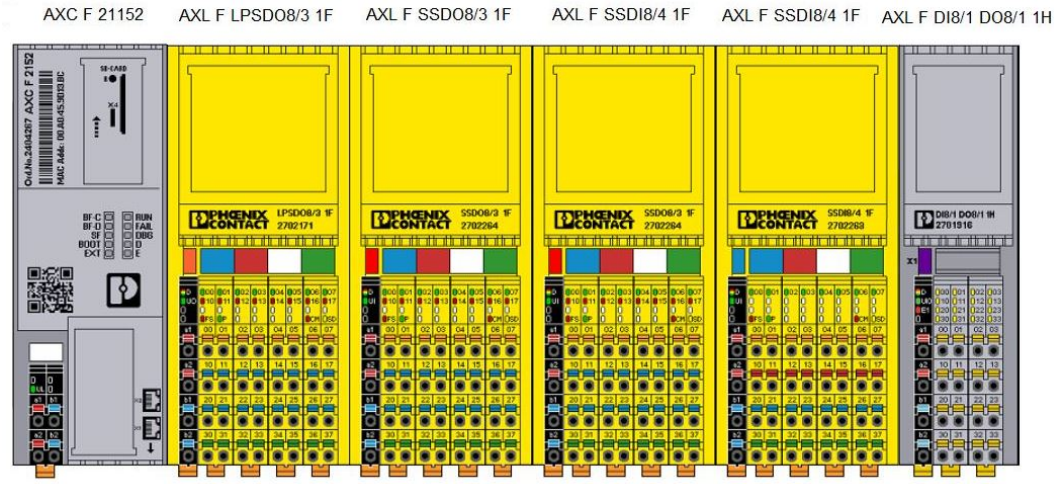


Figura 4.8: Proposta da arquitetura do PLC modular

CPU

A *Central Process Unit* (CPU) pode ser considerado o componente hardware mais importante do PLC, responsável por calcular e realizar tarefas determinadas pelo utilizador, através de um sistema de computação lógica e de processamento de números. Normalmente a CPU também é conhecida como o processador ou controlador do PLC. A unidade de processamento do PLC pode estar embutido na unidade PLC, no caso de um controlador fixo, ou no caso dos PLC modulares e PLC distribuídos, esta faz parte de um dos módulos de incorporação [61].

O processador contém 2 componentes principais:

- A CPU do PLC (Unidade Central de Processamento);
- Memória PLC.

A **unidade central de Processamento** é um microprocessador semelhante a uma CPU de um computador. No entanto, esta CPU não está programada para realizar multitarefas como a CPU de um computador, mas sim para realizar tarefas especificas. Desta maneira a CPU tem como funções principais, correr um programa (como lógica ladder), execução de programas, manipulação de armazenamento de dados, direcionamento de fluxo de dados e controlo da comunicação entre as várias interfaces [61].

A **memória do PLC** é composta por uma memória de programa, memória de dados e firmware. O PLC usa essa memória para armazenar o programa para ser processado pela CPU e para armazenar dados para processamento e execução de entrada e saída [61].

O módulo escolhido para desempenharem a função de CPU é o módulo AXC F 2152. Este módulo é responsável pelo processamento e armazenamento de memória. Possui um processador dual core, Arm® Cortex®-A9 2x 800 MHz, com capacidade de memória RAM de 512 Mbyte. Além disso, tem uma interface de comunicação integrada, compatível com vários dos protocolo de comunicação industriais [60].

Função de Segurança

Este módulo deve permitir através da sua composição interna e capacidade de redundância níveis de segurança de acordo com os requisitos do projeto.

O módulo de segurança, AXL F LPSDO8/3 1F, não tem capacidade de fazer a gestão do barramento entre os dispositivos do conjunto do PLC. Tem uma CPU de segurança incorporada, mas esta CPU não faz uma gestão completa da arquitetura, apenas permite fazer uma gestão dos módulos de entradas e saídas de segurança.

Este módulo contém 4 saídas de canal duplo incorporadas, para aumentar a redundância do sistema, tendo por isso disponíveis 8 saídas de canal único.

Este dispositivo tem um comprimento de 126,1mm, uma largura de 53,6mm, uma espessura de 54mm e um peso de 222g. Tem 8 saídas digitais de canal único, com 4 pontos de canal duplo.

Atinge um nível SIL3 para canal duplo, segundo a norma IEC 61508, como representado na Figura 4.9.

Safety Integrity Level (SIL)	max. 3 (two channel; dependent in parameterization and wiring)

Figura 4.9: SIL do controlador [60]

Atinge Categoria 4 para canal duplo, segundo a norma EN ISO 13849.

Category	max. 4 (two channel; dependent in parameterization and wiring)

Figura 4.10: Categoria do controlador [60]

Tem um *Diagnostic Coverage* de 99%, atendendo ao subcapítulo 2.2.6 e representado na Figura 4.11.

Diagnostic coverage (DC)	99%

Figura 4.11: *Diagnostic Coverage do módulo de segurança* [60]

Tem um MTTFd de 100 anos, logo apresenta um MTTFd de designação Baixo, como explicado no capítulo 2.2.6, e representado na especificação técnica da Figura 4.12.

Mean time to dangerous failure (MTTFd)	100 years

Figura 4.12: MTTFd do módulo de segurança [60]

Além disso, este controlador possui uma camada de proteção de IP20.

Degree of protection	IP20

Figura 4.13: Grau de proteção IP módulo de segurança [60]

Entradas e Saídas

Num sistema de controladores, os módulos de entrada e saída são uma interface comum entre os dispositivos de campo e o processador do PLC.

Para esta interface, são escolhidos alguns módulos, dependendo da necessidade de utilização de entradas/saídas com requisitos de segurança, ou simplesmente sem requisitos de segurança. Para este projeto foram utilizadas 6 entradas e 6 saídas com requisitos de segurança e 1 entrada e 1 saída simples, como exemplificado na Figura 4.7.

Para as aplicações que precisam de uma segurança elevada, são escolhidos módulos de entradas e saídas com caraterísticas de segurança e canal duplo. Consideram-se assim, dois módulos de entradas seguras, AXL F SSDI8/4 1F que permitem a ligação de 4 entradas digitais seguras de canal duplo ou 8 de canal simples, cada um.

Para a ligação das saídas seguras, considera-se o módulo de segurança escolhido para o projeto, o AXL F LPSDO8/3 1F, que por sua vez, permite a ligação de 4 saídas digitais de canal duplo ou 8 saídas de canal simples. Além deste, foi escolhido outro módulo de saídas de segurança de canal duplo, o AXL F SSDO8/3 1F, com 4 saídas de canal duplo, ou 8 saídas simples, de forma a permitir completar um total de 8 saídas de canal duplo ou 16 de canal único.

Para a utilização dos módulos de entrada e saída segura é necessária a utilização do módulo AXL F LPSDO8/3 1F, que contém o CPU que por sua vez faz o seu processamento, como explicado no ponto 4.1.2.

Para as aplicações que não necessitam de uma segurança elevada, foi escolhido um módulo de entradas e saídas de canal único, o AXL F DI8/1 DO8/1 1H. Este módulo pode ser considerado opcional, uma vez que atualmente existem um pontos de entradas e saídas exato ao número de ligações necessárias para o sistema que se pretende.

Por isso, a escolha destes módulos é sobredimensionada de maneira a dar folga a possíveis pontos de entradas e saídas que podem vir a perspectivar-se num futuro desenvolvimento da aplicação.

Interface de Comunicação

A interface de comunicação faz parte o módulo de CPU AXC 2152. Este módulo possui um sistema de barramento integrado (*local bus*) que permite fazer a ligação a outros dispositivos através de vários protocolos de comunicação industrial Algumas das caraterísticas da interface de comunicação do AXC 2152 estão representadas na Figura 4.14.

Interface	Axioline F local bus
Number	1
Connection method	Bus base module
Transmission speed	100 Mbps
Interface	Ethernet
Number	2
Connection method	RJ45 jack
Transmission speed	10/100 Mbps (full duplex)

Figura 4.14: Dados técnicos da interface de comunicação do módulo AXC F 2152 [60]

Análise do Cumprimento dos Requisitos

Seguidamente são analisadas as caraterísticas e especificações técnicas do PLC da Phoenix escolhido e vão ser comparadas com os requisitos globais do projeto, que estão diretamente relacionados ao controlador da barreira.

Requisitos Gerais:

Tendo em conta a norma EN 50126-1:2017 (Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1), foram analisados alguns dos seguintes pontos do subcapítulo 3.3.2, relativos aos Requisitos Gerias.

O período de vida estimado do PLC é de 20 a 25 anos, tendo em conta o módulo menos resistente, como representado na Figura 4.15. De acordo com o ponto do subcapítulo 3.3.2 "O sistema de barreira deve ser projetado, de modo que, o tempo estimado de vida de qualquer instalação seja de pelo menos 30 anos", o controlador da barreira faz parte da instalação, pelo que o PLC não atinge este parâmetro. Da mesma maneira, não foi possível encontrar um equipamento, de entre os outros PLCs listados mais acima no subcapítulo 4.1.1, que cumpra integralmente este requisito.

Permissible duration of use	20 years, 25 years with a low demand rate

Figura 4.15: Período de vida estimado do PLC [60]

De seguida é analisando o requisito do projeto que refere que o MTBF do sistema da barreira deve ser no mínimo de 500 000 operações, representado no subcapítulo 3.3.2. Se em 1 hora se executarem x operações, 500 000 operações levam $\frac{500000}{x}$ horas

para serem executadas. Desta maneira pode concluir-se que o MTBF dos requisitos é de $\frac{500000}{x}$, sendo que x é o número de operações que se fazem numa hora.

Por outro lado, é conhecido o requisito que especifica que a barreira deve ser dimensionada para que seja capaz de resistir a 300 operações por dia.

É por isso expectável que cumpra estes requisitos, pois o módulo de CPU de segurança apresenta um nível SIL3 segundo a norma IEC 61508, ou seja, um PFD de até 10^{-8}.

Requisitos Ambientais

Analisando os pontos do subcapítulo 3.3.3, sobre os requisitos ambientais, e tendo em conta a norma EN 50125-3:2003 (Railway applications - Environmental conditions for equipment - Part 3: Equipment for signalling and telecommunications), foram comparados alguns dos pontos.

As gamas de resistência a temperaturas de operação dos módulos, segundo as informações técnicas disponíveis nos respetivos manuais, são as seguintes [60]:

- AXC F 2152: de -25° a 60° e -40° a 70° em determinadas condições específicas;
- AXL F LPSDO8/3 1F: de -35° a 60° em qualquer posição de montagem;
- AXL F SSDI8/4 1F: de -35° a 60° em qualquer posição de montagem;
- AXL F SSDO8/3 1F: de -35° a 60° em qualquer posição de montagem;
- AXL F DI8/1 DO8/1 1H: de -25° a 60°.

O módulo de segurança menos resistente, AXC F 2152, suporta temperaturas de operação entre os -25°C e +60°C. Sendo que o requisito do sistema global é resistir a temperaturas de operação entre os -40°C e +70°C, estima-se que se a temperatura ambiente for de -40°C, a temperatura no interior da caixa do mecanismo vai ser superior a -40°C, devido ao calor dissipado pelo PLC, e devido ao funcionamento do PLC e consequente aquecimento interno por convecção. Desta maneira, seria necessário testar o PLC em condições reais de funcionamento para saber se chega a uma temperatura inferior aos -25°C, ou a uma temperatura que permita a operação do PLC.

Quanto à temperatura máxima, se a temperatura no interior da caixa do mecanismo de barreira for de +70°C, poderia existir a possibilidade de instalar uma fonte refrigeradora de maneira a diminuir a temperatura do PLC.

As gamas de pressão de operação admissível dos módulos, segundo as informações técnicas disponíveis nos respetivos manuais, são as seguintes [60]:

- AXC F 2152: 70 kPa até 106 kPa (até cerca de 3000m acima do nível do mar);
- AXL F LPSDO8/3 1F: 70 kPa até 108 kPa (até cerca de 3000m acima do nível do mar);
- AXL F SSDI8/4 1F: 70 kPa até 108 kPa (até cerca de 3000m acima do nível do mar);
- AXL F SSDO8/3 1F: 70 kPa até 108 kPa (até cerca de 3000m acima do nível do mar);
- AXL F DI8/1 DO8/1 1H: 70 kPa até 106 kPa (até cerca de 3000m acima do nível do mar).

Prevê-se que o PLC suporta uma pressão do ar de operação de 70 kPa a 106 kPa (até cerca de 3000m acima do nível do mar), o que está de acordo com a altitude máxima de operação de 1000m imposta pelos requisitos.

As gamas humidade de operação dos módulos, segundo as informações técnicas disponíveis nos respetivos manuais são as seguintes [60]:

- AXC F 2152: 5% até 95%;
- AXL F LPSDO8/3 1F: 10% até 75% em média e até 85% ocasionalmente;
- AXL F SSDI8/4 1F: 10% até 75% em média e até 85% ocasionalmente;
- AXL F SSDO8/3 1F: 10% até 75% em média e até 85% ocasionalmente;
- AXL F DI8/1 DO8/1 1H: 5% até 95%.

Este controlador suporta taxas de humidade de operação de 10% a 75%, no pior dos casos, e os requisitos globais do sistema impõem que o mecanismo suporte taxas de 5% a 100%, segundo a classe climática T1. Desta maneira, pode concluir-se que o controlador não está integralmente de acordo com este ponto dos requisitos. Porém a humidade dentro da caixa do mecanismo teria de ser testada em condições de operação, podendo esta ser amenizada. Em caso de urgência pode ser ponderada a utilização de um desumidificador se assim se justificar o preço e o espaço.

Para saber se cumpre requisitos relacionados com os efeitos de radiação solar, ou da poluição, este PLC necessita ser submetido a testes específicos, em condições específicas e já acoplado e ligado ao XBarrier 100, para saber se está de acordo com estes requisitos. Para atender a esta condicionante, a caixa do sistema da barreira foi projetada para atender a estas necessidades.

O requisito de choque e vibração pode ser analisado, tendo acesso à norma EN 50125-3:2003 do requisito do projeto e às normas IEC 60068-2-6 e IEC 60068-2-27, das especificações do controlador.

Todos os módulos permitem uma vibração e choque em condições operacionais representadas na Figura 4.16.

Vibration resistance according to EN 60068-2-6/ IEC 60068-2-6	5g
Shock testing according to EN 60068-2-27/IEC 60068-2-27	30g

Figura 4.16: Resistência ao choque e vibração [60]

Requisitos Elétricos

O requisito do projeto do subcapítulo 3.3.4 refere que o controlador deve ser alimentado com uma tensão nominal de 24 V DC +/- 20%. Na pior das hipóteses, o conjunto do PLC admite uma tensão de alimentação de 19,2 V a 30 V DC, ou seja, 24V +25% - 20% como representado na Figura 4.17. Sendo assim, este parâmetro encontra-se dentro do esperado.

Permissible voltage range	19.2 V DC to 30.0 V DC (including all tolerances, ripple included)

Figura 4.17: Tensão entrada admissível do PLC [60]

"O sistema deve suportar uma corrente constante de 10A e um pico de corrente de 100A." Este requisito é referido ao motor que aciona o mecanismo. A corrente do motor não passa diretamente no PLC, passa através de um relé/contactor (ou variador eletrónico) que deve garantir estes níveis de corrente. Este projeto não aborda esta parte do sistema pelo qual estes requisito não é analisado.

Requisitos de Interface:

Este PLC possui uma interface de comunicação IP, cumprindo o primeiro requisito do subcapítulo 3.3.5.

Neste projeto é escolhido um protocolo compatível com o PLC, de maneira a testar a correta comunicação. Num trabalho futuro, irá ser implementado e configurado um protocolo com um nível de segurança alto.

Custo dos Componentes do Sistema

De seguida, são apresentados os preços individuais de cada módulo escolhido que forma parte do conjunto do PLC, assim como o preço total de todo o conjunto, disponíveis na Figura 4.18. Estes preços estão de acordo com o distribuidor de energia eléctrica e automação, **eibabo**[62], podendo variar o seu preço dependendo do distribuidor.

Artigo	Custo (€)
AXC F 2152	729,40
AXL F DI8/1 DO8/1 1H	133,95
AXL F LPSDO8/3 1F	596,88
AXL F SSDI8/4 1F	310,51
AXL F SSDO8/3 1F	442,78
Total	2271,43

Figura 4.18: Custo dos componentes do sistema

4.2 Protocolo de Comunicação

Na sequência deste capítulo, é feita uma listagem dos protocolos de comunicação mais usados em contexto de automação. Seguidamente, é apresentado e descrito um protocolo de comunicação que pretende dar solução ao problema em causa.

4.2.1 Listagem de Protocolos

As redes industriais são tipicamente muito distribuídas e variam consideravelmente em todos os aspetos, incluindo a camada de enlace e os protocolos de rede utilizados, bem como a topologia. No entanto, nas redes de negócios, as redes Ethernet e *Transmission Control Protocol* (TCP)/*Internet Protocol* (IP) são omnipresentes, usando uma variedade de topologias de estrelas ou árvores [63] [54]. Cerca de 70% das redes industriais atualmente são do tipo Ethernet e têm vindo cada vez mais a aumentar. As restantes 30% são redes de campo.

Existem dois grandes grupos de redes industrias: as redes de campo e as redes Ethernet. Dentro das redes de campo existem 3 grupos: SensorBus, DeviceBus e FieldBus.

SensorBus

A principal função deste tipo de protocolos é permitir a ligação de sensores digitais e atuadores a uma rede. Transmitem dados de pequeno tamanho à rede, exigindo um processamento mínimo por parte dos sensores. Estas redes não cobrem áreas de longa distância graças aos equipamentos mais simples. Um exemplo deste protocolo é o ASInteface.

AS-Inteface

Este protocolo possui uma interface de simples utilização, podendo ser instalado sem necessidade de qualquer requisito especial. O sistema AS-Interface foi concebido para reduzir as fontes de erro, aquando da instalação. O perfil especial do cabo AS-Interface impede a inversão dos polos ao ligar dispositivos, reduzindo a frequência de erro[64].

Caraterísticas:

- **Tipo de rede:** Sistema de comunicação mestre/escravo;
- **Tipologia:** Bus, Anel Estrela, ou árvore;
- **Velocidade de transmissão:** 167 kbit/s;
- **Número máximo de estações:** 1 mestre e até 31 escravos.

DeviceBus

A função deste tipo de protocolos é intermediar a transferência de dados, entre o Sensorbus e o Fieldbus, e assim fazer com que os sinas analógicos e os sinais digitais transmitam os dados para os controladores. Estes protocolos são capazes de atingir distâncias de até 500m e fazer uma rápida transferência de dados. Alguns exemplos destes tipos de protocolos são: Modbus, Profibus *Decentralized Peripherals* (DP), DeviceNet, entre outros.

Modbus

O Modbus é um protocolo de comunicação de dados utilizado em sistemas de automação industrial. Este protocolo destaca-se pela sua facilidade de utilização.

Foi criado originalmente no final da década de 1970, pela fabricante de equipamentos Modicon. É um dos mais antigos e até hoje mais utilizados protocolos em redes PLC para aquisição de sinais (0 ou 1) de instrumentos e comandar atuadores.

A Schneider Electric (atual controladora da Modicon) transferiu os direitos do protocolo para a Modbus Organization (Organização Modbus) em 2004 e a utilização é livre de taxas de licenciamento. Por esta razão e também por se adequar facilmente a diversos meios físicos, é utilizado em milhares de equipamentos existentes e é uma das soluções de rede mais baratas a serem utilizadas em Automação Industrial [65].

Caraterísticas:

- **Tipo de rede:** Sistema de comunicação mestre/escravo;
- **Tipologia: Características:**
  - RS-232: ligação "peer-to-peer" entre mestre e escravo;
  - RS-485: topologia em linha com segmentos de até 32 dispositivos. Cada segmento será encerrado no começo e fim;
- **Velocidade de transmissão:** Depende do meio físico;
- **Número máximo de estações:** 1 mestre e até 246 escravos.

Profibus DP

O Profibus *Decentralized Peripherals* (DP) é a primeira versão de protocolos da Profibus. Foi criada para a sua utilização em plantas industriais, onde existe um grande volume de informações e existe a necessidade de uma alta velocidade de comunicação [66].

Caraterísticas:

- **Tipo de rede:** Multi-mestre / sistema de comunicação escravo;
- **Tipologia:** linear, anel ou estrela;
- **Velocidade de transmissão:** De 9,6 Kbits/s até 12 Mbits/s;
- **Número máximo de estações:** Até 32 estações (mestres ou escravos) por segmento. Até 126 estações por rede.

DeviceNet

O protocolo de comunicação DeviceNet foi desenvolvido originalmente pela Rockwell Automation e está de acordo com a norma IEC 61158. Esta rede é utilizada ao nível operacional e permite a integração em redes de aparelhos, tais como, disjuntores, variadores de velocidade, detetores, relés de proteção de motores, entre

outros, permitindo comunicações e troca de informações entre sistemas de fabricantes diferentes. Outra das vantagens deste protocolo, é a possibilidade de remover e substituir equipamentos em redes sob tensão e sem necessidade de utilizar um aparelho de programação, bem como, a possibilidade de poder alimentar os equipamentos através do próprio cabo de rede. Assim, este protocolo é mais usado de forma complementar ou opcional [67].

Caraterísticas:

- **Tipo de rede:** Comunicação baseado em *Controller Area Network* (CAN);
- **Tipologia:** linear ou com derivações;
- **Velocidade de transmissão:** De 125 Kbits/s a 500 Kbits/s;
- **Número máximo de estações:** Até 64 estações.

FieldBus

Este tipo de rede faz a ligação entre equipamentos de entrada e saída mais inteligentes e cobre maiores distâncias que o SensorBus e o DeviceBus. Este sistema de comunicação permite a interligação em rede de múltiplos instrumentos, realizando funções de controlo e de monitorização de processos e estações de operação HMI. Alguns exemplos deste tipo de protocolos são: Profibus PA, CC-link, entre outros.

Profibus PA

Profibus PA (*Process Automation*) é uma versão do Profibus especializada em processos de automação. Este protocolo permite o tráfego de dados pelo cabo físico de alimentação DC, o que economiza tempo de instalação, espaço e custos. Além disso é caracterizado por ser intrinsecamente seguro [66].

Caraterísticas:

- **Tipo de rede:** Multi-mestre / sistema de comunicação escravo;
- **Tipologia:** árvore, estrela ou mista;
- **Velocidade de transmissão:** De 9,6 Kbits/s até 12 Mbits/s;
- **Número máximo de estações:** Até 32 estações (mestres ou escravos) por segmento. Até 126 estações por rede.

CC-link

CC-Link é a rede de campo de alta velocidade capaz de lidar simultaneamente com dados de controle e informações. O CC-Link pode atingir a distância máxima de transmissão de 100 metros e ligar-se a 254 estações [68].

Caraterísticas:

- **Tipo de rede:** Alta velocidade Ethernet;
- **Tipologia:** estrela, linear, anel, misto;
- **Velocidade de transmissão:** Até 1 Gbits/s;
- **Número máximo de estações:** Até 254 estações.

Redes Ethernet

A rede Ethernet é atualmente a mais utilizada no mundo para troca de informações entre PCs, devido a estar de acordo com normas para redes industriais. Estes tipos de redes têm vindo a evoluir e a ser cada vez mais utilizadas que as redes de campo e a sua velocidade de transmissão pode chegar até 10Gbits/s.

A Ethernet é compatível entre equipamentos de diferentes fabricantes. As redes "proprietárias" colocam o cliente final em suas mãos, dificultando muito a substituição do fornecedor. É de implementação simples, com custos mais baixos relativamente às outras, permite uso de diversos protocolos, está em constante evolução, pode ser aplicada tanto em ambientes domésticos como industriais e é interoperável e escalável. Alguns tipos de protocolos que utilizam este princípio são: Profinet, Ethernet/IP, EtherCat, Modbus TCP, entre outros.

Profinet

Profinet é uma norma aberta para a Ethernet Industrial, tendo sido desenvolvida pela Siemens e pela Profibus User Organization (PNO). Com o Profinet podem ser implementadas soluções de automação de processos, aplicações de segurança, controlo de movimento, entre outros. O Profinet foi desenvolvido seguindo as normas IEC 61158 e IEC 61784 [66].

Este protocolo oferece um desempenho escalável com três níveis de desempenho:

- TCP/IP para aplicações que não sejam em tempo real;
- Real Time (RT): para transferência em tempo real de dados de processo;

- Isochronus Real Time (IRT): para aplicações de controlo de movimento.

Caraterísticas:

- **Tipo de rede:** sistema de comunicação escalável com base em Ethernet:
- **Tipologia:** linear, estrela ou em árvore;
- **Velocidade de transmissão:** 100 Mbit/s;
- **Número máximo de estações:** praticamente ilimitada.

Ethernet/IP

Este protocolo é normalmente usado em aplicações industriais e usado na maioria dos sistemas de passagem de nível. Desta maneira a empresa Efacec sugeriu a utilização deste protocolo.

Ethernet/Industrial Protocol (Ethernet/IP) é um protocolo de rede industrial que utiliza o *Control Information Protocol* ou modelo CIP, o modelo Produtor/Consumidor, a arquitetura TCP/IP e o IEEE 802.3 Ethernet. Este protocolo é utilizado no âmbito industrial e sistemas de tempo real, pois permite a troca de informação entre dispositivos industriais que possibilita a execução de aplicações de tempo real e pode ser usado para oferecer suporte a aplicações de controlo de dados [69].

Caraterísticas:

- **Tipo de rede:** Ethernet com protocolo de aplicação CIP;
- **Tipologia:** linear, estrela ou em árvore;
- **Velocidade de transmissão:** 10, 100, 1000 Mbits/s;
- **Número máximo de estações:** praticamente ilimitada.

EtherCat

O EtherCAT é uma rede Ethernet que se baseia na metodologia mestre/escravo em tempo real desenvolvido inicialmente pela Beckhoff. Atualmente é um protocolo aberto gerido pelo grupo de tecnologia EtherCAT. O princípio fundamental do EtherCat é o de leitura de "pass-through". Isto significa que as mensagens não são destinadas a um único nó e consumidos por esse nó [70].

Caraterísticas:

- **Tipo de rede:** Rede mestre/escravo baseada em Ethernet;
- **Tipologia:** linear, estrela ou em árvore;
- **Velocidade de transmissão:** 100 Mbit/s;
- **Número máximo de estações:** 65535 estações.

Modbus TCP

O Modbus TCP é um protocolo de mensagens de camada de aplicação, no nível 7 do modelo *Open Systems Interconnection* (OSI). Este fornece uma comunicação cliente/servidor entre dispositivos ligados em diferentes tipos de bus ou redes. O Modbus TCP significa que o protocolo Modbus é utilizado em cima de Ethernet TCP/IP. Este protocolo baseia-se numa transmissão de pedido/resposta que oferece serviços específicos por códigos de função. Fornece um conjunto de funções para ler e gravar dados nos dispositivos de campo.

O desempenho de uma rede Modbus TCP é altamente dependente do tipo e da conceção da rede Ethernet que é usada e do desempenho dos processadores nas interfaces de comunicação dos respetivos dispositivos [65].

Caraterísticas:

- **Tipo de rede:** Baseada em Ethernet TCP/IP;
- **Tipologia:** Pode ser implementada qualquer tipologia;
- **Velocidade de transmissão:** 10, 100, 1000 Mbits/s;
- **Número máximo de estações:** Praticamente ilimitado.

4.2.2 Protocolo de Comunicação Selecionado

Neste subcapítulo é selecionado o protocolo de comunicação aplicável ao projeto, tendo em conta alguns dos pontos e critérios mais importantes para a sua seleção. Posteriormente é descrito este protocolo identificando algumas das suas vantagens e caraterísticas.

Critérios de Seleção

Proximamente são apresentados e explicados os principais pontos que contribuíram para a escolha do Protocolo de comunicação aplicável.

- **Velocidade de transmissão**. O protocolo deve permitir velocidades de transmissão rápidas;
- A **Correção de erros** é importante para garantir envio de dados, entre os diferentes nós da rede sem que estes sejam comprometidos;
- **Compatibilidade de equipamentos**. Neste caso foi tido em conta um protocolo que fosse possível de utilizar no controlador da Phoenix selecionado;
- **Controlo de sequência de pacotes**, que acrescente fiabilidade de entrega de pacotes na sequência correta;
- **A Facilidade de uso**, é um fator importante na medida em que a configuração do protocolo deve ser intuitiva e fácil de implementar;
- **Número elevado de estação**. Um número de estações é fundamental para garantir que é possível estabelecer a comunicação com o número de equipamentos pretendidos;
- **Tipologia**. Deve poder ser implementado em qualquer tipologia.

Uma vez analisados os seguintes pontos, a escolha decaiu sobre o protocolo **Modbus TCP**, já usado pela Efacec noutros projetos.

Descrição do Protocolo de Comunicação Escolhido

Este protocolo é uma variante do protocolo Modbus, que cobre o uso de mensagens Modbus num ambiente "Intranet" ou "Internet", usando protocolos TCP/IP. O uso mais comum deste protocolo é para a ligação Ethernet de PLCs, módulos de entradas e saídas e para outros barramentos de campos simples.

O protocolo Modbus é um dos protocolo mais utilizados a nível de automação industrial, devido à sua simplicidade e facilidade de implementação, podendo ser utilizado em diversos padrões de meio físico, como: RS-232, RS-485 ou Ethernet.

A transmissão de informação é feita através de redes Ethernet e utiliza o modelo Cliente/Servidor. Este modelo consiste num ciclo de pedido e resposta entre o Servidor e o Cliente através de um pacote de dados que engloba o endereço do dispositivo, o código da função, os dados, a comprovação de erros, entre outros. Nestes dados, pode estar contida informação de escrita e/ou leitura de dados para ambos o Servidor ou Cliente, esquematizado na Figura 4.19.

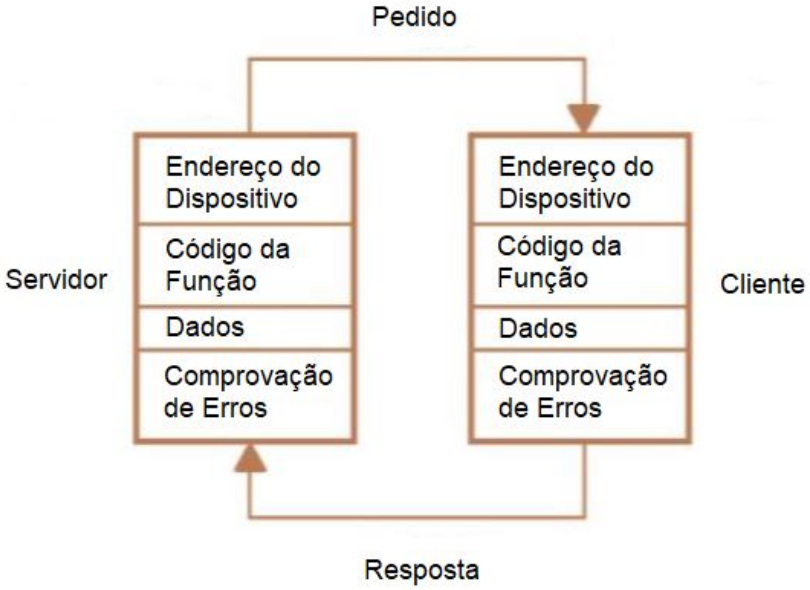


Figura 4.19: Quadro de mensagens Modbus TCP [71]

4.3 Conclusão

Na primeira parte do capítulo é feito um levantamento das principais caraterísticas de alguns PLCs de segurança significativos para o projeto e disponíveis no mercado. É proposta uma arquitetura de um PLC aplicável, tendo por base alguns critérios de seleção relevantes. Seguidamente é feita uma análise e comparação com o cumprimento dos requisitos propostos pela Efacec e, por fim, é apresentado o custo deste PLC. Na segunda parte do capítulo, são listados os protocolos de comunicação mais utilizados no âmbito de automação e de seguida é escolhido o mais aplicável ao projeto, apresentando as principais razões da sua escolha e o seu funcionamento básico. No próximo capítulo, será implementada e desenvolvida a solução escolhida.

Capítulo 5

Implementação da Solução

Neste capítulo é desenvolvida a solução do problema analisado anteriormente, descrevendo os pontos e os passos que se deram relativamente à implementação do código de software no PLC escolhido, até se chegar à solução final e funcional. É também descrita a configuração do protocolo de comunicação utilizado.

5.1 Desenvolvimento das Funções do Sistema

Uma vez selecionado o controlador a ser usado, prossegue-se com a programação do mesmo numa plataforma de software disponibilizada pela empresa Phoenix Contact no seu site oficial, que pode ser descarregada e utilizada por qualquer pessoa gratuitamente [72].

Esta plataforma de software de engenharia para controladores de automação, desenvolvida pela Phoenix Contact, é compatível com a norma IEC 61131-3. Permite três tipos de linguagens de programação, ST, Linguagem Ladder e FBD. Dentro da plataforma é possível selecionar o modelo de PLC que se vai utilizar, assim como selecionar a lista das entradas e saídas.

É também possível testar o programa desenvolvido no software através de uma interface homem-máquina (HMI), onde é possível simular o funcionamento do sistema, ou até dar-lhe comandos diretos.

A interface de ligação entre o PLC e a máquina de programação com o programa instalado, pode ser feita através de um cabo Ethernet (RJ-45).

Uma vez instalado o software com a última versão do aplicativo, neste caso a versão 2021.0.2, começa-se por desenvolver a solução em função dos requisitos pré-definidos pela empresa que tinham relação direta com o controlador da barreira, apresentados no subcapítulo 3.3.6, através do desenvolvimento lógico destes requisitos.

Inicialmente foram selecionados as seguintes entradas e saídas a serem implementadas no controlador:

As entradas do sistema são:

- **"Sinal Abrir Barreira"**, esta entrada está ligada a um botão no interior da caixa que, segundo a lógica do programa, permite abrir a barreira, se se cumprir as condições necessárias. Este sinal é ligado a um dos pontos de entrada de canal duplo de um dos módulos de entradas;
- **"Sinal Fechar Barreira"**, esta entrada está ligada a um botão no interior da caixa que, segundo a lógica do programa, permite fechar a barreira, se se cumprir as condições necessárias. Este sinal é ligado a um dos pontos de entrada de canal duplo de um dos módulos de entradas;
- **"Sinal Barreira Aberta"**, esta entrada do controlador está ligada a um sensor no interior do mecanismo, que permite saber quando a barreira atingiu uma posição de 90º. Este sinal é ligado a um dos pontos de entrada de canal duplo de um dos módulos de entradas;
- **"Sinal Barreira Fechada"**, esta entrada do controlador está ligada a um sensor no interior do mecanismo, que permite saber quando a barreira atingiu uma posição de 0º. Este sinal é ligado a um dos pontos de entrada de canal duplo de um dos módulos de entradas;
- **"Sinal Barreira Metade"**, esta entrada do controlador está ligada a um sensor no interior do mecanismo, que ativa um sinal lógico de "1", cada vez que a barreira se encontra entre a posição de 45° e 90°. Este sinal é ligado a um dos pontos de entrada de canal duplo de um dos módulos de entradas;
- **"Sinal Caixa Fechada"**, este sinal é normalmente fechado, dando a indicação lógica "1", cada vez que a porta da caixa se encontra fechada, e quando essa

porta é aberta, interrompe-se o sinal, passando para o estado lógico "0". Este sinal é ligado a um dos pontos de entrada de canal único de um dos módulos de entradas;

- **"Modo Automático"** é um sinal normalmente fechado ("1") que permite uma execução automática da barreira controlada pelo PLC que dá sinais ao motor de subida ou descida da barreira. Por sua vez, quando é acionando a engrenagem que permite acoplar a manivela para fazer o movimento da barreira manual, este sinal é interrompido, passando para o estado lógico de aberto ("0"). Desta maneira, qualquer tentativa do motor acionar a barreira é impedida. Este sinal é ligado a um dos pontos de entrada de canal duplo de um dos módulos de entradas.

As saídas do sistema são:

- **"Abrir Ligar Motor"**, esta saída permite dar um sinal ao motor, por meio de contactores, para iniciar um movimento rotativo no mecanismo de rodas dentadas, que por sua vez permite subir a barreira. Este sinal é ligado a um dos pontos de saída de canal duplo de um dos módulos de saídas;
- **"Fechar Ligar Motor"**, esta saída permite dar um sinal ao motor, por meio de contactores, para iniciar um movimento rotativo no mecanismo de rodas dentadas, que por sua vez permite descer a barreira. Este sinal é ligado a um dos pontos de saída de canal duplo de um dos módulos de saídas;
- **"Luz Haste Exterior"**, saída que permite, quando cumpridas as condições necessárias, ativar uma luz que está situada na parte superior da barreira no ponto mais afastado da caixa. Este sinal é ligado a um dos pontos de saída de canal duplo de um dos módulos de saídas;
- **"Luz Haste Interior"**, saída que permite, quando cumpridas as condições necessárias, ativar um conjunto de luzes situadas na parte superior ao longo da barreira, de forma intermitente. Este sinal é ligado a um dos pontos de saída de canal duplo de um dos módulos de saídas;
- **"Iluminação Interior"**, saída que permite fazer a ligação de um conjunto de luzes localizadas no interior da caixa da barreira, uma vez que a porta da caixa é aberta. Este sinal é ligado a um dos pontos de saída de canal único de um dos módulos de saídas;
- **"Barreira Aberta Confirmação"**, saída que dá um sinal à rede uma vez que a entrada "Sinal Barreira Aberta" se encontra ativada. Este sinal é ligado a um dos pontos de saída de canal duplo de um dos módulos de saídas;

- **"Barreira Fechada Confirmação"**, saída que dá um sinal à rede uma vez que a entrada "Sinal Barreira Fechada" se encontra ativada. Este sinal é ligado a um dos pontos de saída de canal duplo de um dos módulos de saídas.

Uma vez definidas as entradas e saídas do sistema foram desenvolvidas conforme os requisitos funcionais apresentados no subcapítulo 3.3.6.

1- O controlador tem de estar apto para dar o comando ao motor de abrir a barreira.

2- O controlador tem de estar apto para dar o comando ao motor de fechar a barreira.

Para cumprir com estes dois requisitos utiliza-se um sinal de saída ligado desde o PLC até ao motor, por intermédio de um contactor. Assim, o controlador foi programado para estar apto para dar comando ao motor de abrir e de fechar.

Foram projetadas as seguintes lógicas de segurança que devem ser cumpridas para que a ação de subir a barreira possa ser executada.

- Ter a confirmação que o "Sinal Abrir Barreira" está ativado;
- O modo tentativas deve estar desativado;
- Não pode haver um sinal a confirmar que a barreira está aberta;
- O PLC não pode dar nenhum comando ao motor de fechar a barreira;
- O sinal que dá indicação à barreira de se fechar não pode estar ativado, ou seja, o comando oposto;
- O mecanismo não pode ter o modo manual ativado, pelo que deve permanecer no modo automático.

Da mesma maneira foram projetadas as seguintes condições para o caso da ação de descer:

- Ter a confirmação que o "Sinal Fechar Barreira" está ativado;
- O modo de tentativas tem de estar desligado;
- Não pode existir o sinal a confirmar que a barreira já esta fechada;
- O PLC não pode dar nenhum comando ao motor de abrir a barreira;

- O sinal que dá indicação à barreira de se abrir não pode estar ativado, ou seja, o comando oposto;
- O mecanismo não pode ter o modo manual ativado, pelo que deve permanecer no modo automático.

3- Cada movimento ativo deve ter um comando independente do controlador da passagem de nível.

Este requisito é conseguido através da própria implementação do controlador no próprio mecanismo de barreira, ao serem ligados os sinais de entrada e saída directamente nos sensores ou atuadores do mecanismo de barreira.

4- Se a posição para a qual o mecanismo é comandado não for atingida após um tempo limite configurável, o controlador deve parar de alimentar o motor.

5- O tempo limite deve ser configurado para entre 5 e 60 segundos.

6- Quando o controlador parar a barreira após um tempo limite, se a posição para a qual o mecanismo é comandado não for alcançada, o controlador deverá efetuar outra tentativa de mandar sinal após um determinado período de tempo.

7- Esse tempo deve ser configurado para entre 5 a 60 segundos.

8- O número máximo de tentativas deve ser configurado de entre 0 a 10.

Para estes objetivos foi implementado um sistema chamado de "Modo de tentativas", que forma parte do sistema principal de "Abertura e fecho de barreira".

Este modo de tentativas permite ao mecanismo desligar o motor e apenas é acionado caso a localização da barreira não esteja na posição pretendida (aberta ou fechada), passado um determinado tempo (configurável entre 5 a 60 segundos), após ter sido ativado o comando correspondente.

Passado um determinado período de tempo programado (configurado para entre 5 a 60 segundos), é dado outra vez um comando ao motor para iniciar de novo o movimento da barreira para a posição pretendida. Se novamente a sua posição não for a pretendida, após um determinado tempo, este volta a fazer o mesmo processo de desligar o motor e voltar a dar um comando para a posição em questão. Além disso foi implementado um sistema que limita o número de tentativas de reinício do motor e consequente tentativa de atingir a posição final. Foi programada uma opção

para que seja o utilizador que selecione o número de tentativas que serão efetuadas. Este valor pode ser configurado entre 0 e 10.

Em termos de programação foram criados 2 ciclos, uma para abrir a barreira e outro para fechar.

No caso do ciclo de abrir, o sistema apenas passa para o modo de tentativas, se passado um determinado período de tempo pré-programado não se receber uma confirmação do sensor que a barreira está aberta. Nesse caso, o motor desliga-se passando o sistema a estar no 'modo tentativas'.

Uma vez ativado o "Modo tentativas" é iniciado um contador que aumenta o seu valor, cada vez que se desliga o motor, sendo assim programado para apenas executar a ação de reiniciar o motor até um determinado número de vezes.

Caso este contador não tenha chegado ao número máximo de vezes, o sistema ativa uma contagem temporal, que quando terminada, permite ligar o motor e iniciar de novo o comando de acionar o motor para abrir a barreira, se todos os outros requisitos referidos anteriormente se cumprirem.

Passado um determinado período de tempo, se a barreira não atingir a posição pretendida, o ciclo volta a começar desligando o motor. O "Modo Tentativas" apenas é desativado, caso a barreira dê sinal que já se encontra aberta, ou caso se dê um comando ao motor de fechar a barreira.

O mesmo ciclo se aplica para o caso de fechar a barreira.

9- Quando a barreira está em modo manual, o controlador não pode dar nenhum comando de movimento ao motor.

Quando se desativa o sinal de entrada do "Modo automático", o sistema passa a estar no modo manual e são impostas uma série de condições no programa que impedem o controlador de dar qualquer sinal ao motor de movimento.

10- A barreira só se pode mover quando lhe for ordenado fazê-lo.

Para este requisito foi implementada uma lógica no programa que impede a barreira de fazer movimentos indesejados em condições específicas. Além disso, nenhum dos movimentos da barreira se deve à ação da gravidade.

11- A ativação da indicação "prova que está fechado" quando a barreira estiver num estado diferente, devido a uma falha de componentes (mecânicos, elétricos, etc.), deve apresentar uma taxa de falha máxima de 1. e-9, h-1.

Este requisito é alcançado através da seleção do controlador de segurança da Phoenix, que permite ter uma taxa de falha máxima de $1.e^{-9}.h^{-1}$., explicada no 4.

12- As ligações elétricas das luzes devem permitir a ligação independente de dois grupos de luzes.

13- Para permitir, por exemplo, a iluminação independente da luz da ponta das demais.

Para cumprir estes pontos foram programados dois tipos de grupos de luz. A luz exterior e a luz interior.

As luzes interiores devem permanecer intermitentes e a luz exterior deve permanecer fixa e acesa cada vez que a barreira não se encontra na posição "aberta". Além disso, cada um destes grupos de luzes está ligado a saídas diferentes do PLC.

Por outro lado, este sinal de ligação destas luzes será efetuado se:

- a barreira está na posição fechada;
- a barreira se encontra a subir;
- a barreira está a descer.

Para a ativação destes grupos de luzes, deve ser ligada uma saída desde o PLC a cada um dos grupos de luzes individualmente. Desta maneira, a luz exterior tem um tipo de iluminação independente das restantes luzes interiores.

14- A abertura da caixa do mecanismo de barreira deve cortar a energia do mecanismo.

Este requisito pretende dizer que se a caixa do mecanismo for aberta, deve ser impedido qualquer sinal externo de dar uma instrução de movimento, mas o PLC da barreira pode continuar a executar funções de abrir e fechar a barreira sempre que forem ativados os botões de "Sinal Abrir Barreira" e "Sinal Fechar Barreira" e quando se cumprirem as condições necessárias.

Atualmente, o mecanismo não foi configurado para receber sinais externos de comandos, pelo que neste momento ainda não é possível a comunicação externa, a não ser com o testes de comunicação feitos no 6.

Foi ainda desenvolvida uma função lógica que permite desativar todos os movimentos ativos do mecanismo de barreira, cada vez que a caixa do mecanismo é aberta, ou seja, se o sinal lógico da "Caixa fechada" passar de "1" a "0". A seguir a esta comutação pode ser retomado o movimento, se for dada novamente uma instrução para o fazer, ou seja, depois da caixa ter sido aberta.

15- Um painel de manutenção deve ser equipado com indicações para sinalizar o status de operação do mecanismo de barreira.

16- A operação deste painel de manutenção deve inibir o modo de operação automática.

Este painel de manutenção ainda não está fisicamente presente no sistema, pelo que estes dois requisitos ainda não foram implementados.

O status de operação e as indicações dos sinais são possíveis de ser comprovadas na interface gráfica HMI, desenvolvida no subcapítulo 6.1.4.

17- Os comandos e indicações devem estar prontos para interface com um painel externo, com as mesmas funcionalidades.

18- O controlador deve permitir a configuração do tempo de abertura.

19- O controlador deve permitir a configuração do tempo de fecho.

20- O valor mínimo para o tempo de abertura deve ser, no máximo, 6 segundos.

21- O valor máximo para o tempo de abertura deve ser, no mínimo, 12 segundos.

22- O valor mínimo para o tempo de fecho deve ser, no máximo, 6 segundos.

23- O valor máximo para o tempo de fecho deve ser, no mínimo, 12 segundos.

Estes requisitos são conseguidos através da sua configuração na interface HMI do weberver, desenvolvido no 6.1.4.

24- O controlador deve comandar a luz interna do mecanismo.

O controlador permite a ativação da luz interna do mecanismo, sempre que o sinal de "caixa fechada" se encontra no estado lógico 0, ou seja, sempre que a caixa está aberta, a luz interna do mecanismo presente dentro da caixa deste é ativada.

25- O controlador deve ter uma entrada para receber a informação de que a barreira está na posição aberta.

26- O controlador deve ter uma entrada para receber a informação de que a barreira está na posição fechada.

27- O controlador deve ter uma entrada para receber a informação de que a posição da barreira está acima do meio.

No interior da caixa do mecanismo de barreira, existem 3 sensores que estão ligados a 3 entradas do PLC, que permitem saber se a barreira se encontra na posição, "Sinal Barreira Aberta", "Sinal Barreira Metade", ou "Sinal Barreira Fechada".

28- O controlador deve ter entradas para receber as informações sobre a abertura das portas do mecanismo.

Como referido anteriormente, existe uma entrada que é ativada através de um sensor, normalmente fechado, uma vez que a porta do mecanismo é aberta.

29- O controlador dever ter uma entrada para receber a informação de que o mecanismo foi mudado para operação manual.

Como mencionado anteriormente, existe uma entrada que é ativada através de um sensor localizado na ativação da manivela que permite o acionamento manual da barreira, passando assim a dar indicação que está no modo manual.

5.1.1 Grafcets Representativos do Programa

Neste subcapitulo são apresentados alguns grafcets que representam a lógica implementada em algumas das funções principais do mecanismo de barreira.

O grafcet da Figura 5.1 representa o funcionamento do sistema de subida e descida da barreira.

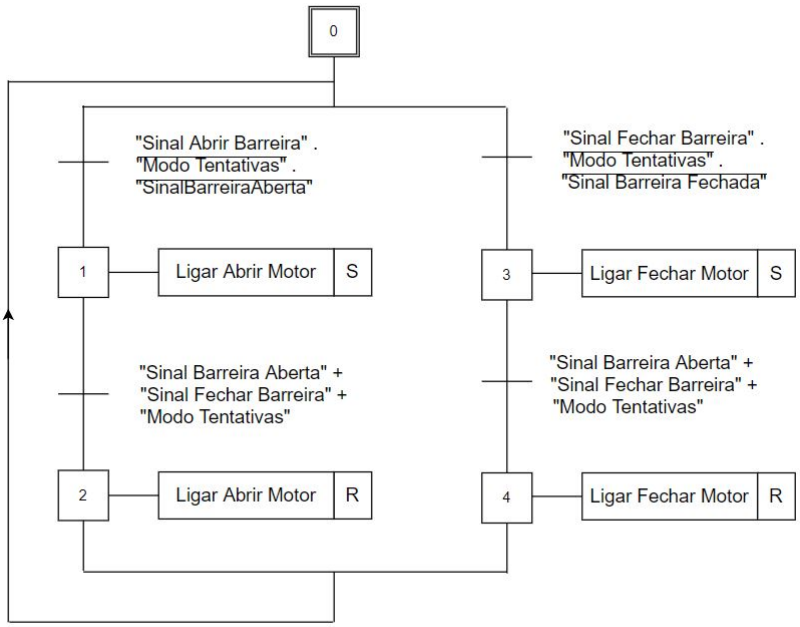


Figura 5.1: Grafcet de "Subida e descida da barreira"

O grafcet da Figura 5.2 representa o ciclo de funcionamento da barreira quando se encontra no “Modo Tentativas Abrir”.

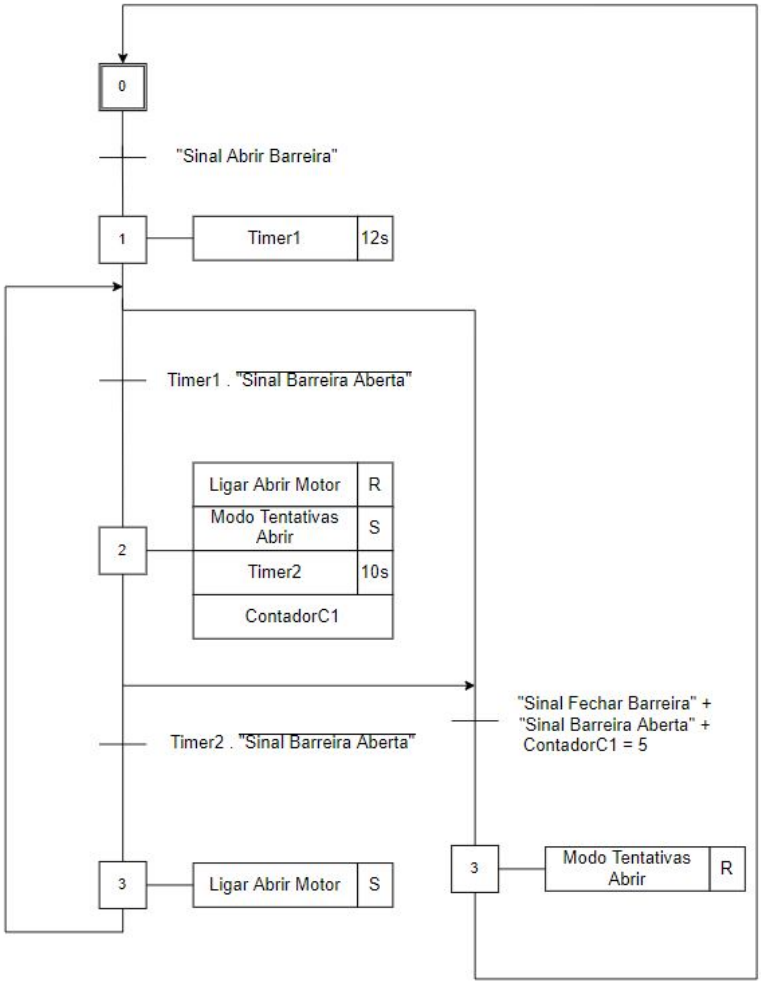


Figura 5.2: Grafcet do funcionamento do "Modo Tentativas Abrir"

O grafcet da Figura 5.3 representa o ciclo de funcionamento da barreira quando se encontra no “Modo Tentativas Fechar”.

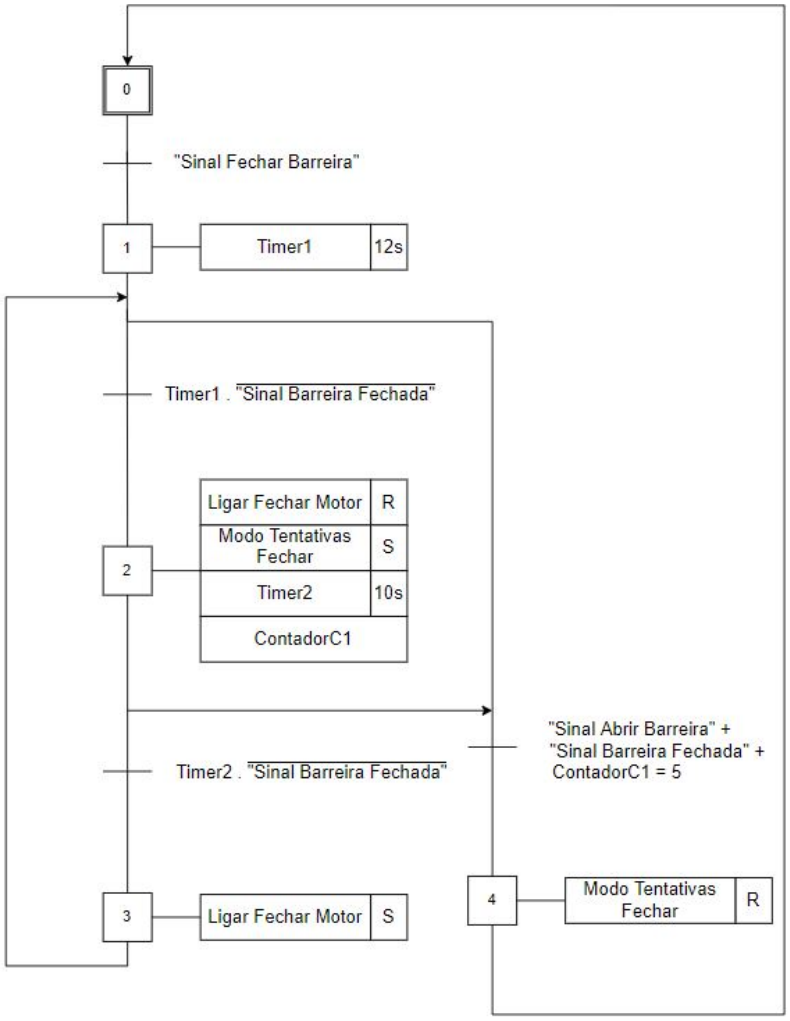


Figura 5.3: Grafcet do funcionamento do "Modo Tentativas Fechar"

Os grafcets da Figura 5.4 e da Figura 5.5 representa uma funcionalidade adicionada ao sistema para testar o correto funcionamento da barreira, que permite a constante abertura e fecho desta até se dar um sinal para acabar com este processo.

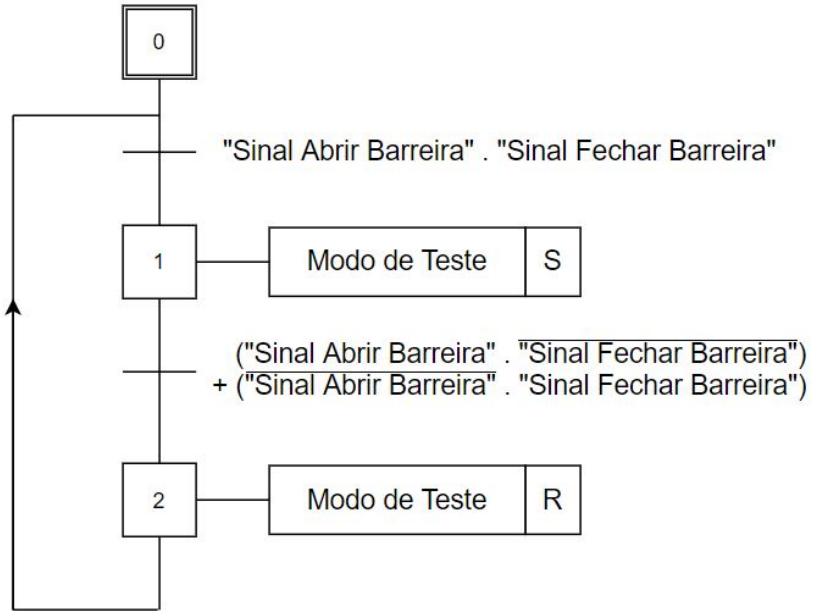


Figura 5.4: Grafcet de ativação do "Modo Teste"

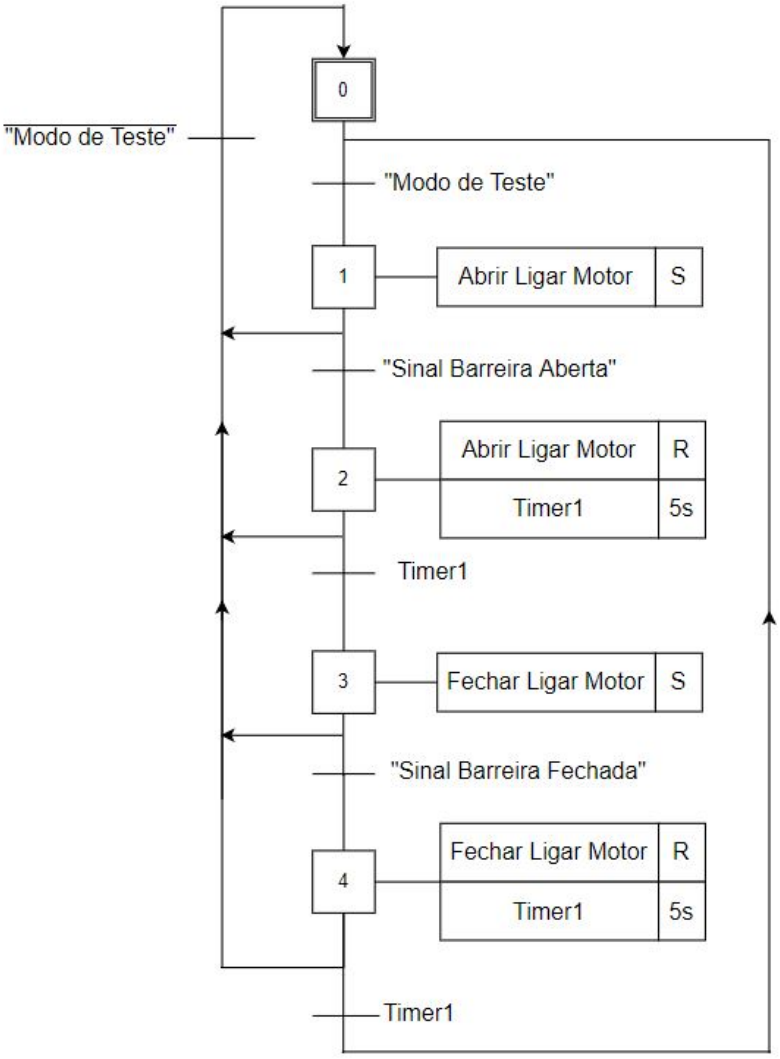


Figura 5.5: Grafcet do funcionamento do "Modo Teste"

5.2 Configuração do Protocolo de Comunicação

Para pôr em prática e verificar a valência do protocolo de comunicação escolhido no 4.2.2, recorre-se à utilização de dois módulos de CPU da Phoenix, ACX F 2152, e posteriormente procedeu-se a configuração de cada um deles.

O primeiro módulo, denominado de PLC da barreira, é configurado para desempenhar a função de PLC Cliente. Este encontra-se incorporado dentro da caixa do mecanismo de barreira de testes, situada no recinto exterior da Efacec, e foi previamente programado com uma série de funções desenvolvidas no subcapítulo 5.1.

O segundo módulo, denominado por PLC de testes, é configurado com a função de PLC Servidor e está localizado no edifício da Efacec, por isso, situa-se fisicamente separado do mecanismo de barreira.

Previamente os PLCs são ligados a uma mesma subrede, pertencente à rede principal da Efacec. De seguida, e para configurar cada um deste PLCs, recorreu-se ao uso do software PLCNext, onde foram programadas anteriormente as funções do PLC da barreira. Foram adicionalmente instaladas as bibliotecas relativas ao protocolo de comunicação Modbus TCP, para proceder à sua configuração.

O primeiro passo consiste na programação do PLC de testes. Foram configurados alguns pontos para o correto funcionamento deste, tais como:

- Capacidade de escrita de uma série de bits na memória do PLC Cliente pertencentes a um vetor do PLC Servidor;
- Capacidade de leitura de dados em relação a cada um dos clientes;
- Activação do modo *Transmission Control Protocol* (TCP) em detrimento do *User Datagram Protocol* (UDP), devido a uma maior fiabilidade;
- Definição do número da porta local associada ao endereço IP do adaptador de Ethernet selecionado, ao qual o socket criado está ligado. O número da porta selecionada é usado pelo servidor TCP para dados de entrada. A porta oficial reservada para este protocolo é a porta 502;
- Determinação de um tempo de atraso entre duas execuções de ligação ao cliente de 50ms para dar tempo ao PLC de executar, no mínimo, um ciclo;
- Configuração de um tempo limite depois de se ter dado um comando de escrita. Após ter sido dado este comando, deve-se esperar a receção de um telegrama de confirmação de escrita dentro de um tempo especificado. Esse tempo é configurado para 100ms, numa fase de teste, podendo ser reduzido.

O PLC da barreira é configurado com uma série de funções:

- Capacidade de escrita de uma série de bits na memória do PLC servidor pertencentes a um vetor do cliente;
- Capacidade de leitura de dados provenientes do servidor;
- Activação do modo TCP em detrimento do UDP, devido a uma maior fiabilidade;

- Definição do número da porta local associada ao endereço IP do adaptador de Ethernet selecionado, ao qual o socket criado está ligado. O número da porta selecionada é usado pelo servidor TCP para dados de entrada. A porta oficial reservada para este protocolo é a porta 502;
- Determinação de um tempo de atraso entre duas execuções de ligação de 50 ms para dar tempo ao PLC de executar, no mínimo, um ciclo;
- Definição de um tempo de espera limite de comunicação. O servidor Modbus deve responder a uma solicitação de ligação dentro do tempo limite especificado, caso contrario, um erro será acionado. Este tempo foi configurado para 200 ms;
- Criação de um vetor de memória com capacidade de armazenamento das informações booleanas de cada uma das entradas e saídas do próprio PLC;
- Indicação da direção destino, neste caso, do servidor.

Através destes parâmetros e configurações do programa, foi estabelecida a comunicação destes dois dispositivos através do protocolo Modbus TCP, com possibilidade de transmissão de dados bidirecional (capacidade de escrita e leitura de ambos os PLCs).

Cada vez que são alteradas informações na memória do PLC da barreira, como pode ser a passagem do estado lógico de "0" para "1" de uma variável de entrada, estas informações são escritas na memória do PLC servidor automaticamente através do protocolo. De maneira contrária, também é possível escrever dados na memória do PLC da barreira, através do PLC de testes. Com esta implementação é possível controlar o mecanismo de barreira mediante o PLC de testes. A correta comunicação entre estes dois dispositivos será demonstrada no capítulo 6.2.

5.3 Conclusão

Com vista ao desenvolvimento das funções do sistema que implementa a solução do controlo da barreira, começa-se por ter em consideração os requisitos previamente definidos pela empresa, determinando os diferentes pontos de ligação às entradas. É com estes pressupostos que são desenvolvidas as funções implementadas no PLC escolhido. É ainda explicada a configuração do protocolo de comunicação do PLC. No próximo capítulo são mostrados os testes feitos que comprovam o correto funcionamento do sistema.

Capítulo 6

Resultados

Neste capítulo são apresentados os resultados obtidos através da análise de testes experimentais realizados depois de ser ter chegado a uma solução final. Estes testes serão o ponto de partida para a verificação de toda a abordagem ao problema, permitindo propor adaptações e melhorias.

6.1 Testes do Controlador da Barreira

Uma vez concluída a fase de programação do código na plataforma de programação do PLC, foram feitos alguns testes para verificar o correto funcionamento da lógica implementada, em função dos requisitos pretendidos. Para estes testes foi utilizado o controlador da Phoenix Contact AXC F 2152, que permite o carregamento e execução do programa lógico que se pretende instalar no PLC de segurança, executando as mesmas funções lógicas que o PLC a ser implementado. Esta fase experimental de resultados e de testes foi dividida em 4 partes:

- Teste teórico no webserver;
- Teste no Simulador;

- Teste Físico da Barreira;
- Aplicação do Webserver.

6.1.1 Teste Teórico no Webserver

A primeira fase consistiu na realização de testes a partir Interface HMI do software da Phoenix, PLCnext Engineer. Esta interface permite simular a lógica do programa através da criação de botões virtuais, sinais de entrada, sinais de saída, entre outras funcionalidades do próprio software, para entender e saber se a lógica criada corresponde ao que se pretende que o programa realize num caso prático.

É possível aceder a esta interface a partir de uma página web (webserver), única de cada controlador, acessível pelo seu endereço IP. Para isso, apenas é necessário ter ligação ao PLC em questão, introduzir o seu IP na barra de pesquisas de um motor de busca e introduzir as respetivas credenciais de acesso, numa janela de pop-up, como a da Figura 6.1.

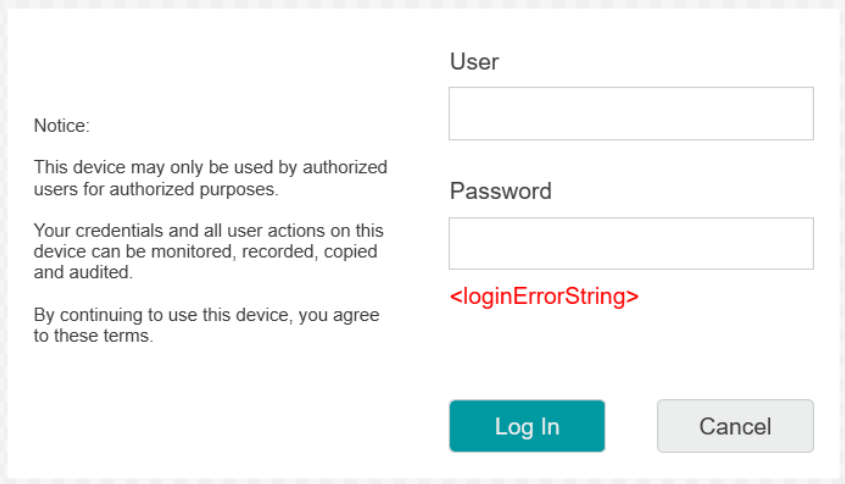


Figura 6.1: Página de LogIn

Uma vez na página do webserver, é possível visualizar a página criada através do software PLCnext. Nesta página foram introduzidos dois botões, um de "Sinal Abrir Barreira" e outro de "Sinal Fechar Barreira", além de outros sinais, que resultam do acionamento destes. Desta maneira, ao pressionar os botões virtuais, é possível comprovar o correto funcionamento da lógica da barreira ao ver as indicações dos sinais virtuais, ou então, testar se ao estar desligado o sinal de "Caixa Fechada", o que na prática significa que a caixa está aberta, ver se o sinal que ativa a iluminação

no interior da caixa foi acionado. Esta página web de testes está representada na Figura 6.2

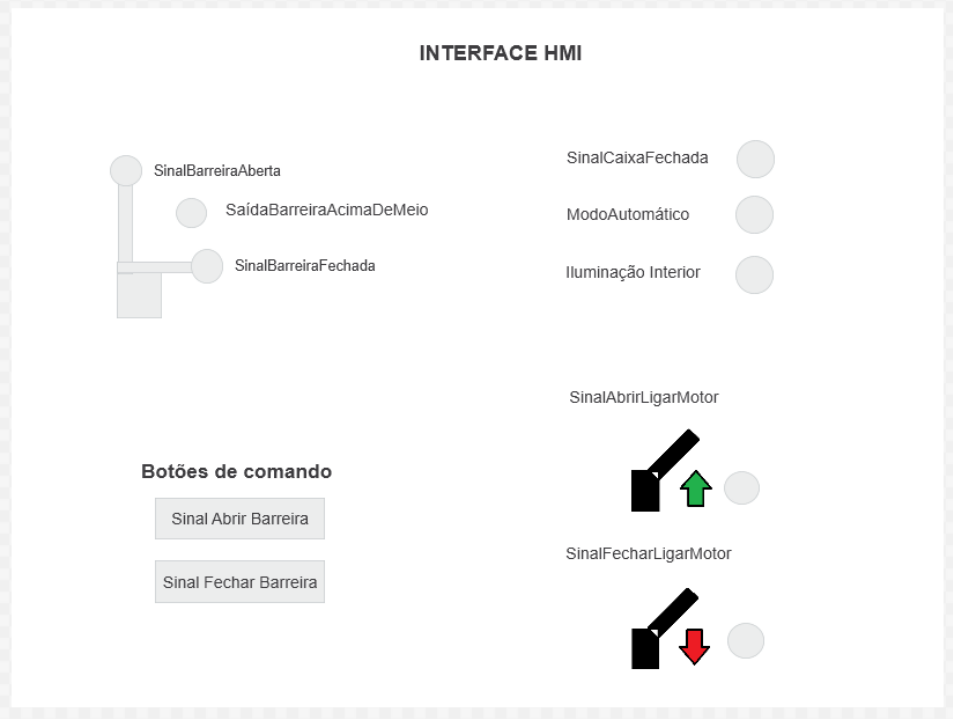


Figura 6.2: Interface HMI

Também é possível forçar os sinais de entrada ou saída no software do PLCNext, como por exemplo, o sinal de "Barreira Aberta" e de "Barreira Fechada" e simular que houve um problema na barreira e que, por isso, nunca se chegou a abrir ou fechar, ativando por isso o "Modo de Tentativas" e através da indicação das saídas "Abrir Ligar Motor" e "Motor Ligar Fechar" é possível testar o correto funcionamento deste ciclo. A Figura 6.2, representa a página do software onde é possível forçar entradas ou saídas do programa. Neste exemplo é forçada a entrada de "Barreira Fechada" para o estado lógico "0", simulando que a barreira nunca se chegou a fechar.

Process data item	Variable (PLC)	Value	Type	Usage	Comment	Init
di-1 / ~DI16	*Select Variable (PLC) here*					
di-1 / IN01	SinalAbrirBarreira	FALSE	BOOL	Global		FALSE
di-1 / IN02	SinalFecharBarreira	FALSE	BOOL	Global		FALSE
di-1 / IN03	SinalBarreiraAberta	FALSE	BOOL	Global		FALSE
di-1 / IN04	SinalBarreiraFechada	FALSE	BOOL	Global		FALSE
di-1 / IN05	SinalBarreiraAcimaDeMeio	FALSE	BOOL	Global		FALSE
di-1 / IN06	SinalCaixaFechada	TRUE	BOOL	Global		FALSE
di-1 / IN07	ModoAutomatico	TRUE	BOOL	Global		FALSE

Figura 6.3: Simulação da variável 'Barreira Fechada' no estado lógico "0"

Nesta fase de testes, ainda não é possível testar o correto funcionamento do mecanismo, ao se tratar de um teste teórico e não se dispor de uma barreira real. Por exemplo, para testar o valor da variável "Sinal Barreira Fechada" ("0" ou "1") é necessário criar um temporizador que simule o tempo de fecho da barreira.

Mas, por outro lado, esta fase é essencial para ficar a entender o funcionamento do programa e corrigir partes do código que dependem da parte lógica, ou do desenvolvimento da lógica.

6.1.2 Teste no Simulador

A segunda fase consiste na utilização de uma pequena caixa de simulação, que permite a simulação das entradas e saídas do código através de interruptores biestáveis e *Light Emitting Diodes* LEDs, que simulam as entradas e saídas. Para isso foram ligados as respetivas entradas e saídas do PLC aos interruptores e LEDs da caixa alimentados a 24V DC.

Uma vez feitas as ligações, é possível acionar as diferentes entradas físicas através da mudança de estados dos interruptores, (aberto ou fechado), podendo assim simular o programa de uma forma mais visual e física.

Com isto, é possível fazer as ligações do PLC à caixa e verificar o correto funcionamento das entradas e saídas, no modelo de teste. Na Figura 6.4 está representada a caixa de simulação utilizada.

Figura 6.4: Caixa de simulação

Esta caixa de simulação continha várias entradas, entre elas, "Modo Automático", "Caixa Fechada", "Abrir Barreira" e "Fechar Barreira". A ativação destas

entradas é confirmada através de um LED acima dos respetivos botões. Na parte da direita da caixa, estão ligadas as saídas de "Barreira Aberta" e "Barreira Fechada", com um botão a controlar a sua ativação, tendo dois possíveis estados, ligado ("1") ou desligado ("0").

Com este teste, é possível ver de uma forma concreta e física o funcionamento do programa, podendo testar a correta ligação de cada um dos sinais de entrada e saída do PLC e a correta atribuição dos endereços aos mesmos.

6.1.3 Teste Físico da Barreira

O terceiro teste consiste na visualização dos movimentos do sistema de barreira, dados pelo PLC acoplado. Este mecanismo de barreira encontra-se nas instalações exteriores da Efacec, para desta maneira se ter um acesso rápido a ele de forma a se poder ver os movimentos ativos em tempo real.

Figura 6.5: Barreira de testes XBarrier 100

De forma a visualizar os movimentos ativos da barreira, são pressionados os botões incorporados na caixa do mecanismo para desta forma se poder observar o seu funcionamento.

Inicialmente o sistema da barreira apresentava um ligeiro *delay* ao dar a informação de "Sinal Barreira Aberta" ou "Sinal Barreira Fechada", uma vez que a barreira subia ou descia alguns graus em excesso.

Inicialmente o sistema da barreira subia ou descia alguns graus em excesso. Graças a este teste pode-se comprovar que existia um ligeiro *delay* desde a fase de receção do "Sinal Barreira Aberta" ou "Sinal Barreira Fechada" no PLC até que

este enviava um sinal ao motor para deter o movimento da barreira. Desta maneira, foi possível diagnosticar um problema de atraso no tempo de ciclo, ou tempo de varrimento do PLC. Este é o tempo que o PLC demora a correr o CPU, a confirmar o estado dos módulos I/O, a confirmar as entradas, a executar o programa e a atualizar as saídas do PLC. Uma vez diagnosticado este problema, foi corrigido e diminuído o tempo de ciclo do programa, até um tempo mínimo que seja possível de executar pelo controlador. Foi então definido um tempo de ciclo de 10ms, o que permitiu uma maior capacidade de reação por parte do sistema.

6.1.4 Aplicação do Webserver

Por último e uma vez feitos os testes práticos na barreira, foi criada uma aplicação de interface HMI.

Para aceder a esta interface o utilizador precisa de estabelecer uma ligação com o PLC via ethernet ou wi-fi e introduzir o endereço IP do PLC na barra de busca de um navegador qualquer. De seguida, é mostrada uma página de login que requer a introdução de um ID e de uma password (afixados no PLC), de maneira a garantir que o utilizador é o proprietário do PLC, ou tem acesso legal ao mesmo.

Uma vez feito o login o utilizador é redirecionado para uma página de início, onde se programou a hiperligação a 3 páginas diferentes à escolha do utilizador.

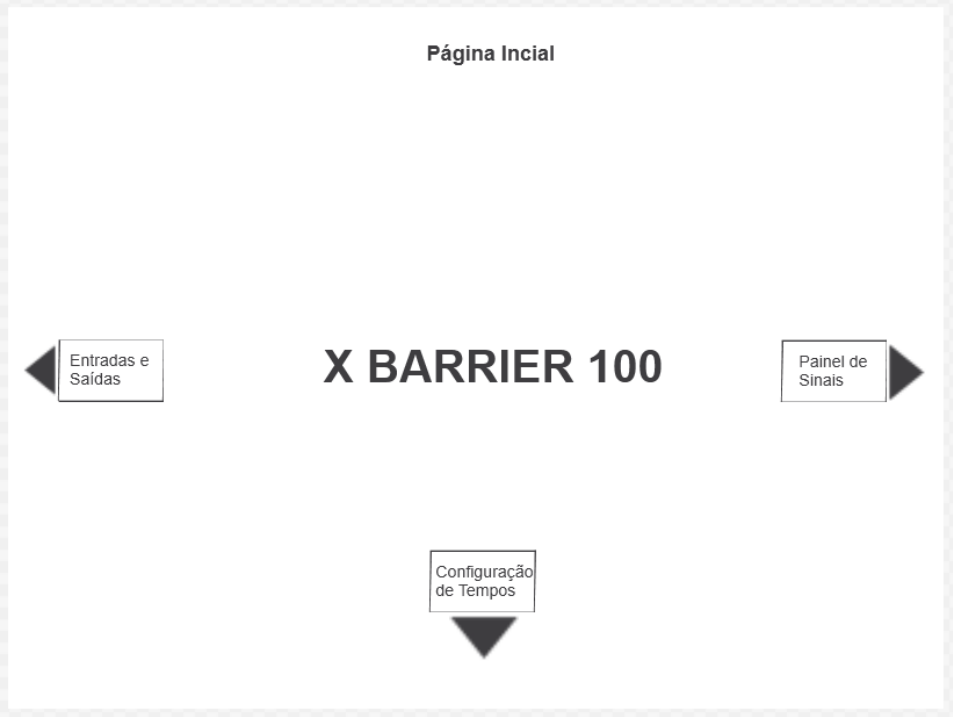


Figura 6.6: Página Inicial

Clicando no botão à direita na página de início, é redireccionado para a página de "Painel de Sinais", com informações sobre todos os sinais e funcionalidades presentes no mecanismo de barreira, representada na Figura 6.7. Para retornar à pagina inicial, é possível carregar no botão à esquerda da página ou no símbolo da casa em cima à direita.

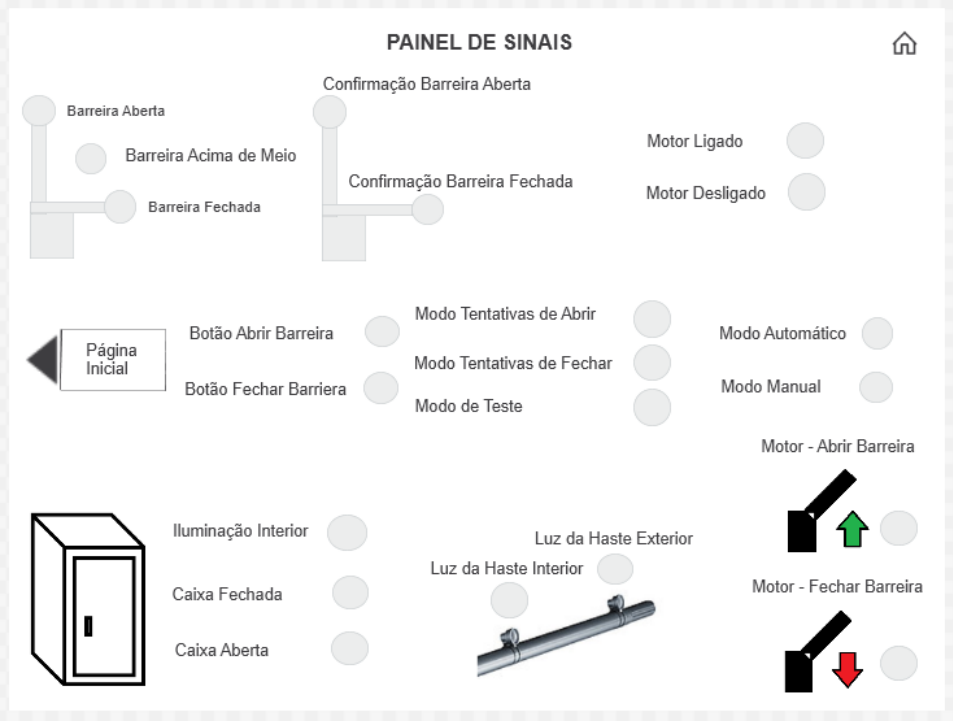


Figura 6.7: Painel de Sinais

Clicando no botão à direita aparece uma página que apresenta as entradas e saídas do sistema. Nesta página também é possível visualizar qual das entradas ou saídas se encontra ativa, assim como ver a que endereço se encontram estas ligadas. Para retornar à pagina inicial, basta carregar no botão à direita na página ou no símbolo da casa em cima à direita.

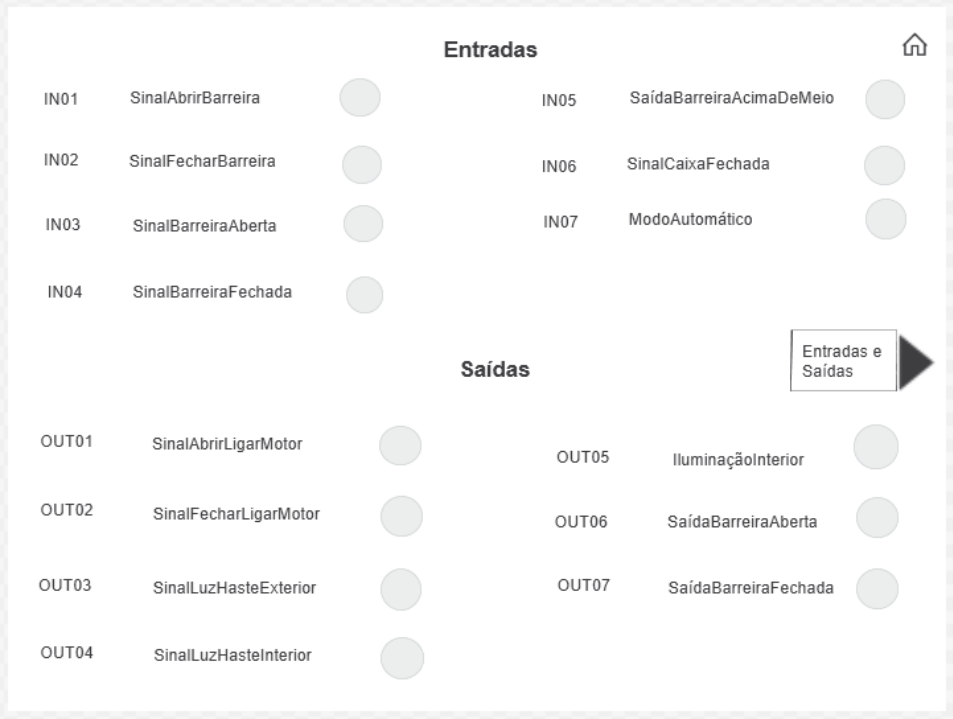


Figura 6.8: Página de Entradas e Saídas

Por fim, a página de configuração de tempos permite ao utilizador configurar alguns dos tempos ou valores programados. Como por exemplo, o tempo que o motor demora a desligar, uma vez que foi comandado para abrir a barreira e esta não chegou à sua posição final, devido a um erro ou falha. Para selecionar os valores, basta introduzir um número no campo onde está indicada a sua função. Para retornar à pagina inicial, é possível com carregar no botão em cima na página ou no símbolo da casa em cima à direita.

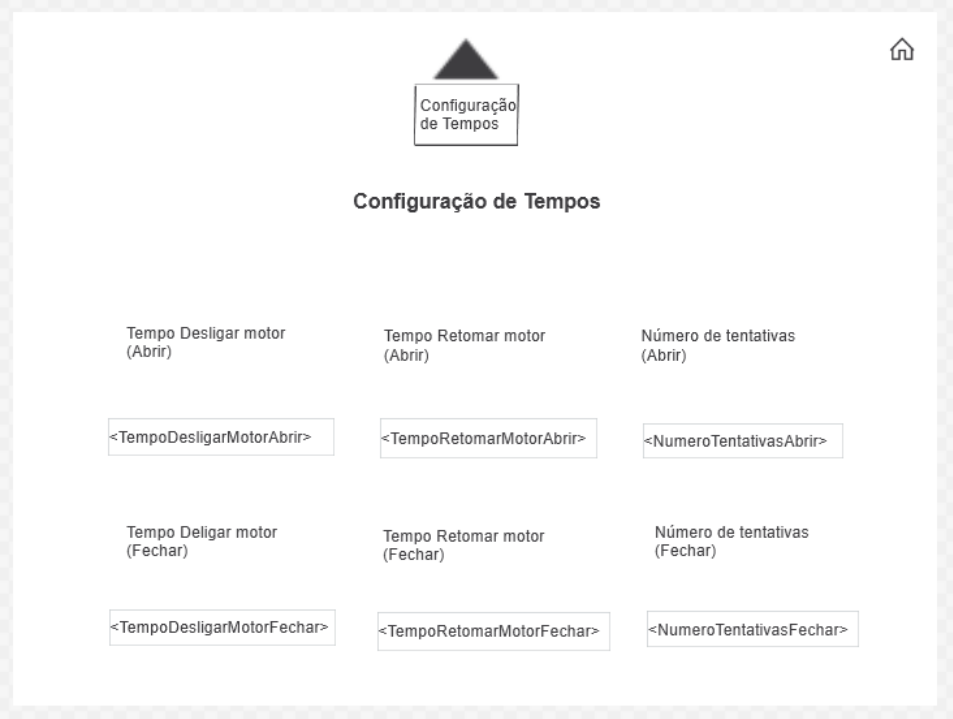


Figura 6.9: Página de Configuração de Tempos

Na Figura 6.10 representa de forma esquemática, a comutação possível entre as diferente páginas web.

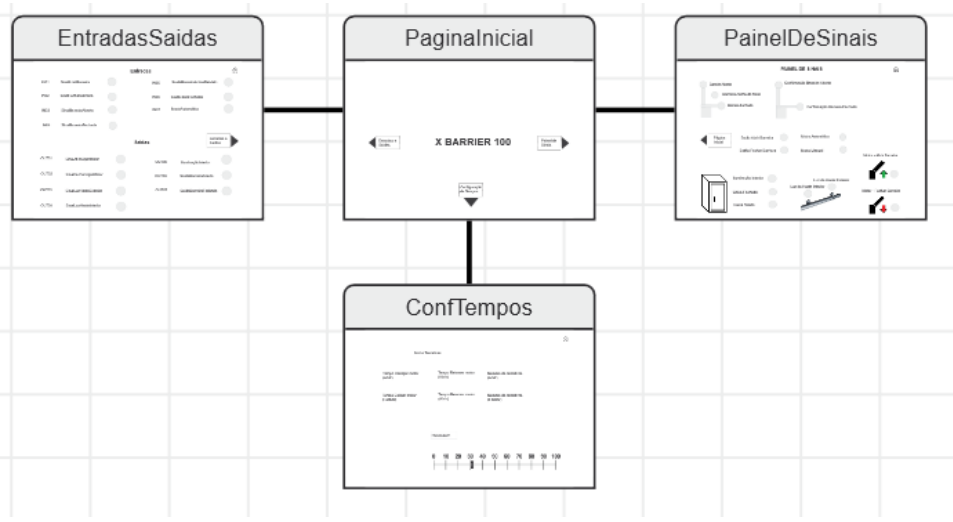


Figura 6.10: Página de Navegação

Este teste permite saber se todos os sinais do PLC estão configurados e associados de forma certa aos sensores e atuadores do sistema de barreira. Por outro lado,

é possível criar uma interface gráfica com algumas funcionalidades de configuração e visualização de sinais em tempo real.

6.2 Teste de Comunicação

Para testar a eficácia do protocolo de comunicação ModBus TCP, cuja configuração foi explicada no subcapítulo 5.2, foi testado um caso prático que consiste no acionamento do comando de "Fechar Barreira" dado pelo PLC de testes, no momento em que a barreira se encontra a abrir, de forma a visualizar a capacidade de comunicação entre os PLCs.

Para isso, acedeu-se à página de programação do PLC de testes no software PLCNext Engineer para observar a comutação de valores dos bits da memória deste PLC. Também foi necessário estar presente no local onde se encontra o mecanismo de barreira para observar o seu comportamento.

Inicialmente, é dada uma indicação ao mecanismo de abertura da barreira através da ativação do botão presente na caixa do mecanismo. Uma vez dado este comando, foi possível observar a leitura do bit correspondente à variável "Abrir Ligar Motor", por parte PLC de testes, como representado na Figura 6.11, que corresponde à ação de abertura da barreira. Desta forma, conclui-se que o PLC da barreira escreveu com sucesso esse bit no PLC de testes. Da mesma maneira, foi possível visualizar a barreira a efetuar um movimento rotativo ascendente.

Figura 6.11: Leitura de dados do PLC de testes

Posteriormente, e enquanto a barreira ainda se encontrava em movimento ascendente, foi dado o comando ao PLC de testes para fechar a barreira. De seguida confirmou-se a passagem da variável ""Fechar Ligar Motor"" para o estado lógico "1" ou *TRUE*, como se visualiza na Figura 6.12.

Figura 6.12: Escrita de dados do PLC de testes

Nesse preciso instante observou-se a mudança na direção do movimento da barreira, passando a ser feita no sentido descendente rotativo. Desta maneira, concluise que o bit correspondente à variável "Fechar Ligar Motor" foi escrita com sucesso pelo PLC de testes ao PLC da barreira e também foi concluído que este último PLC enviou o correspondente sinal ao motor para iniciar a descida da barreira.

Com este teste, foi possível constatar que a comunicação entre estes dois PLCs foi realizada com sucesso.

6.3 Conclusão

Neste capítulo são inicialmente apresentados os testes realizados para confirmar o correto funcionamento do programa implementado no PLC da barreira. Numa primeira fase, são realizadas provas de comprovação da lógica do programa na interface HMI do software PLCNext. O segundo teste consiste na configuração de uma caixa de simulação que permite observar de forma física e real o desempenho das entradas e saídas do sistema. O terceiro passo abrange a aplicação deste programa ao PLC da Barreira e a consequente análise ao comportamento do mecanismo do sistema, para saber se está a funcionar conforme o esperado. O quarto teste do controlador integra a observação do correto funcionamento de uma interface HMI que permite observar os sinais e as alterações de dados do sistema. Por último, são realizados testes experimentais para verificar o correto funcionamento e implementação do protocolo de comunicação escolhido e posteriormente são descritos os resultados observados. Globalmente, os ensaios validaram o correto funcionamento do sistema, permitindo aplicar algumas correções, nomeadamente quanto ao atraso no tempo do ciclo. O conjunto destes testes contribuíram assim para a consistência da solução proposta.

Capítulo 7

Conclusão

7.1 Trabalho Realizado

Ao longo deste trabalho é desenvolvida uma solução de hardware e software de um controlador com caraterísticas de segurança para realizar umas funções específicas no mecanismo de barreira, de acordo com os requisitos propostos pela empresa Efacec. São desenvolvidas estas funções, tendo em conta a segurança do mecanismo e as entradas e saídas selecionadas. Posteriormente, é selecionado um protocolo de comunicação compatível com o controlador escolhido que permita fazer a comunicação entre o PLC e os restantes equipamentos pertencentes à rede do sistema. É estabelecida uma comunicação entre dois PLCs dentro de uma mesma rede através deste protocolo, para testar o correto funcionamento e comunicação.

A solução implementada tem como premissas garantir os requisitos de segurança do sistema, para o qual foram abordadas as seguintes tarefas:

- Análise e escolha de um PLC de SIL3, o qual tem uma taxa de falhas reduzida, em comparação com os PLCs *standard*;
- Desenvolvimento de um programa que apenas permite a realização de certas ações de movimento se previamente são satisfeitas uma série de condições;

- Acoplamento de entradas e saídas de duplo canal aumentando a segurança do sistema;
- Cumprimentos de normas de segurança impostas pelo projeto.

7.2 Trabalho Futuro

O sistema da barreira será sujeito a novas implementações e melhorias, que não foram abordadas neste projeto, e que poderão vir a ser objeto de um trabalho futuro, como é o caso dos seguintes pontos:

- Escolha de um protocolo de comunicação de segurança que se adeque ao PLC selecionado, assim como apropriado para o sistema de barreira e para os dispositivos com os quais se pretende comunicar;
- Configuração deste protocolo de comunicação seguro de forma a permitir a comunicação entre o PLC do controlador e a rede onde estão inseridos outros dispositivos do sistema;
- Escolha e configuração de um *driver* de potência que permita controlar a velocidade de fecho e abertura da barreira;
- Implementação de um codificador rotativo (*encoder* rotativo) que permita saber a posição angular da barreira em tempo real.

.

Referências

[1] Efacec. Available at https://www.efacec.pt/, 2021. (Last accessed in 22/10/2020). [Citado na página 1]

[2] L. Transport, "Passagens de nível em portugal." Available at https://lumotransport.eu/passagens-de-nivel-em-portugal//, Mar. 2021. (Last accessed in 25/06/2021). [Citado na página 2]

[3] RealPars, "Plc." Available at https://realpars.com//, 2021. [Citado na página 7]

[4] Álvaro Roberto Rojas Castrov, "Integración de sistemas erp y mes mediante el estándar ansi/isa-95." Available at http://bibing.us.es/proyectos/abreproy/70822/fichero/TFM+%C3%81lvaro+Rojas+Castro+-+Integraci%C3%B3n+de+sistemas+ERP+y+MES+mediante+el+est%C3%A1ndar+ISA-95.pdf, June 2018. (Last accessed in 2/02/2021). [Citado na página 7]

[5] M. T. Hoske, "Safety plcs." Available at https://www.controleng.com/articles/safety-plcs/, Aug. 2005. (Last accessed in 15/11/2020). [Citado na página 7]

[6] T. Mortenson, "Safety plc." Available at https://realpars.com/safety-plc/, July 2020. (Last accessed in 12/05/2021). [Citado nas páginas 7 e 8]

[7] PLCdesign, "What's a safety plc? - fundamentals and differences." Available at https://plcdesign.xyz/en/whats-safety-plc/, 2021. (Last accessed in 9/11/2020). [Citado nas páginas ix, 8 e 9]

[8] IEC, "Iec61508 functional safety of electrical/electronic/programmable electronic safety-realated systems," 2010. (Last accessed in 04/04/2021). [Citado nas páginas ix, 10, 12 e 15]

[9] H. C. William Goble, ed., *Safety Instrumented Systems Verification: Practical Probabilistic Calculation*. Europe: ISA, apr 2005. [Citado na página 10]

[10] C. Cassiolato, "Sis - sistemas instrumentados de segurança - uma visão prática - parte 3." Available at https://www.smar.com/brasil/artigo-tecnico/

sis-sistemas-instrumentados-de-seguranca-uma-visao-pratica-parte-3, 2003. (Last accessed in 18/11/2020). [Citado na página 10]

[11] W. Goble, "Learn to trust safety plcs." Available at https://www.controleng.com/articles/safety-plcs/, May 2003. (Last accessed in 18/11/2020). [Citado na página 10]

[12] IEC, "Standard for programmable controllers - part 2." Available at https://webstore.iec.ch/publication/31007, 2020. [Citado na página 11]

[13] IEC, "Standard for programmable controllers - part 2." Available at https://www.sis.se/api/document/preview/562828/, 2020. [Citado na página 11]

[14] IEC, "Iec61131-2 programmable controllers – part 2:equipment requirements and tests." Available at https://webstore.iec.ch/preview/info_iec61131-2%7Bed3.0%7Den.pdf, July 2007. [Citado na página 11]

[15] J.-P. Nikko, "Safety plcs–competitor analysis of software usability." Available at https://www.theseus.fi/bitstream/handle/10024/261420/Nikko_Thesis_1_0.pdf?sequence=2&isAllowed=y, 2019. [Citado na página 12]

[16] S. Sommer, "What is a safety intrumented system." Available at https://realpars.com/safety-instrumented-system/, Aug. 2018. [Citado nas páginas 12 e 13]

[17] C. Cassiolato, "Sis - safety instrumented systems - a practical view - part 1." Available at https://www.smar.com/en/technical-article/sis-safety-instrumented-systems-a-practical-view-part-1, 2003. (Last accessed in 18/11/2020). [Citado na página 12]

[18] IEC, "European agency for safety and health at work," 2020. (Last accessed in 13/04/2021). [Citado na página 12]

[19] "Safety instrumented funcion." Available at https://safetyandsis.com/safety-instrumented-function/. (Last accessed in 20/11/2020). [Citado na página 13]

[20] H. Jin, *A contribution to reliability assessment of safety-instrumented systems*. PhD thesis, Norwegian University of Science and Technology, Sept. 2013. [Citado na página 13]

[21] Consiltant, "Qualitative lopa." Available at https://www.consiltant.com/procesveiligheid/lopa/, 2020. [Citado nas páginas ix e 13]

[22] Hastam, "Quantitive lopa." Available at hastam.co.uk/are-you-taking-risks-with-risk-assessment/, 2020. [Citado nas páginas ix e 14]

[23] M. Raza, "System reliability & availability calculations." Available at `https://www.bmc.com/blogs/system-reliability-availability-calculations/`, 2021. (Last accessed in 20/11/2021). [Citado nas páginas 14, 18, 20 e 26]

[24] IEC, "Iec61511 safety instrumented systems for the process industry sector," 2020. (Last accessed in 01/04/2021). [Citado nas páginas ix e 15]

[25] I. technology for safety, "Understanding safety integrity level iec61511." Available at `https://app.box.com/s/szmbycw237qingc113mgey77njm0qloy`, 2012. (Last accessed in 18/03/2021). [Citado nas páginas ix e 15]

[26] S. Sultana, "A new approach of uncertainty treatment in the verification of safety integrity level of safety instrumented system," Master's thesis, University of Stavanger Faculty of Science and Technology, Norway, Stavanger, 2015. [Citado nas páginas ix e 16]

[27] N. Portuguesas, "Np50126 aplicações ferroviárias – especificação e demonstração de fiabilidade, disponibilidade, manutenibilidade e segurança (rams)," 2000. (Last accessed in 18/2/2021). [Citado na página 16]

[28] VALEUKEEP, "O que é o mttr e o mtbf?." Available at `https://valuekeep.com/pt-pt/recursos/e-books-artigos/o-que-e-o-mttr-e-o-mtbf/`, 2021. (Last accessed in 15/2/2021). [Citado na página 17]

[29] Fiix, "What is mean time between failures?." Available at `https://www.fiixsoftware.com/mean-time-between-fail-maintenance/`, 2021. (Last accessed in 20/02/2021). [Citado na página 17]

[30] Fiix, "What is mttr?." Available at `https://www.fiixsoftware.com/mean-time-to-repair-maintenance/`, 2021. (Last accessed in 22/01/2021). [Citado na página 17]

[31] G. Greeff and R. Ghoshal, eds., *Practical E-Manufacturing and Supply Chain Management*. Amsterdão: Elsvier, 2004. [Citado na página 17]

[32] B. Dhillon, ed., *Reliability, Quality, and Safety for Engineers*. Boca Raton: CRC PRESS, 2005. [Citado nas páginas 18 e 21]

[33] Normas Portuguesas, Portugal, *Norma NP EN013306 2007 - Terminologia da Manutenção*, 2007. [Citado nas páginas 18 e 20]

[34] A. K. Pandey, "Rams management for a complex railway system: A case study," Nov. 2014. (Last accessed in 10/10/2020). [Citado nas páginas 18 e 19]

[35] M. M. A. Silva, "Avaliação de fiabilidade de sistemas elétricos e de automação em instalações de frio industrial," Master's thesis, Instituto Superior de Engenharia de Lisboa, Lisboa, 2014. [Citado nas páginas ix e 19]

[36] J. Menčík, ed., *Reliability of Systems*. IntechOpen, 2016. [Citado na página 19]

[37] B. P. E. F. de Almeida, "Estudo da metodologia rams - aplicação a um caso prático," Master's thesis, Universidade técnica de Lisboa, Lisboa, 2011. [Citado na página 20]

[38] J. A. da Silva Sobral, *Utilização da metodologia RAMS na análise de barreiras de segurança de instalações industriais de risco elevado*. PhD thesis, Faculdade de Engenharia do Porto, 2010. [Citado na página 20]

[39] I. O. for Standardization, "Iso13849-1:2015 safety of machinery — safety-related parts of control systems — part 1: General principles for design." Available at `https://www.iso.org/standard/69883.html`, 2015. (Last accessed in 21/03/2021). [Citado nas páginas ix, 21, 23, 25 e 28]

[40] keyence, "The idea of performance level." Available at `https://www.keyence.com/ss/products/safetyknowledge/performance/`, 2021. (Last accessed in 02/03/2021). [Citado nas páginas ix, 22 e 27]

[41] Siemens, "Difference between en/iso 13849 and en/iec 62061," 2014. (Last accessed in 07/03/2021). [Citado na página 22]

[42] ADQ, "Iso 13849 - performance level." Available at `https://adqconsultoria.com/perfil-post/iso-13849---performance-level-/13`, 2020. (Last accessed in 14/11/2020). [Citado nas páginas ix e 24]

[43] A. R.-. (R2009), "Industrial robots and robot systems - safety requirements." Available at `https://webstore.ansi.org/Standards/RIA/ANSIRIAR15061999R2009?gclid=EAIaIQobChMI3NLV5YXC8QIVFPhRCh2xEwsYEAAYASAAEgKPLPD_BwE`, 2009. (Last accessed in 01/04/2021). [Citado na página 24]

[44] C. insight consulting inc, "Machinery safety 101." Available at `https://machinerysafety101.com/2017/02/27/iso-13849-1-analysis-part-5/`, 2017. (Last accessed in 02/03/2021). [Citado nas páginas ix, 25 e 26]

[45] WIKA, "What is meant by diagnostic coverage?." Available at `https://blog.wika.com/knowhow/diagnostic-coverage/`, 2021. (Last accessed in 24/01/2021). [Citado na página 26]

[46] IEC, "Guidance on the application of iso 13849-1 and iec 62061 in the design of safety-related control systems for machinery." Available at `https://webstore.iec.ch/publication/6424`, 2010. [Citado nas páginas ix e 29]

[47] C. Vavra, "Control engineering | protect plcs and pacs from cybersecurity threats." Available at `https://www.controleng.com/articles/`

protect-plcs-and-pacs-from-cybersecurity-threats/, May 2020. (Last accessed in 1/12/2020). [Citado na página 30]

[48] Fortinet, "What is operational technology (ot): An operational technology security primer." Available at https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security. (Last accessed in 1/12/2020). [Citado na página 30]

[49] G. Rigotti, "O que a convergência entre it e ot significa para as indústrias?." Available at https://www.abii.com.br/single-post/o-que-a-converg%C3%AAncia-entre-it-e-ot-significa-para-as-ind%C3%BAstrias. (Last accessed in 1/12/2020). [Citado na página 30]

[50] sumo logic, "What is an attack vector? | sumo logic." Available at https://www.sumologic.com/glossary/attack-vector/. (Last accessed in 07/12/2020). [Citado na página 31]

[51] balbix, "cyber attack vector." Available at https://www.balbix.com/insights/attack-vectors-and-breach-methods/. (Last accessed in 11/01/2021). [Citado na página 31]

[52] C. Engeneering, "Protect plcs and pacs from cybersecurity threats." Available at https://www.controleng.com/articles/protect-plcs-and-pacs-from-cybersecurity-threats/, May 2020. (Last accessed in 4/12/2020). [Citado na página 33]

[53] Reddor, "Level crossing system." Available at https://www.red-dot.org/project/xbarrier-100-51516, 2021. (Last accessed in 22/10/2020). [Citado na página 35]

[54] E. Knapp, ed., *Industrial Network Security*. New York: Syngress, 2011. [Citado nas páginas 41 e 64]

[55] ABB, "Ac500-s safety plc." Available at https://new.abb.com/plc/programmable-logic-controllers-plcs/ac500-s, 2021. (Last accessed in 12/04/2021). [Citado nas páginas x, 48 e 49]

[56] A. Bradley, "Controladores controllogix 5580." Available at https://www.rockwellautomation.com/pt-pt/products/hardware/allen-bradley/programmable-controllers/large-controllers/controllogix/1756controllogix5580.html, 2021. (Last accessed in 12/04/2021). [Citado nas páginas x e 50]

[57] HIMA, "Himatrix." Available at https://www.hima.com/en/products-services/himatrix, 2021. (Last accessed in 12/04/2021). [Citado nas páginas x, 50 e 51]

[58] Mitsubishi, "Safety programmable controller melsec-qs series." Available at https://www.mitsubishielectric.com/fa/products/cnt/plcqsws/pmerit/concept/safetyplc.html, 2021. (Last accessed in 13/04/2021). [Citado nas páginas x, 51 e 52]

[59] Shneider, "Preventa xps mf." Available at https://www.se.com/us/en/product-range/1439-preventa-xps-mf/?parent-subcategory-id=51330#overview, 2021. (Last accessed in 14/04/2021). [Citado nas páginas x, 52 e 53]

[60] PhoenixContact, "Safety module - axl f lpsdo8/3 1f - 2702171." Available at https://www.phoenixcontact.com/online/portal, 2021. (Last accessed in 02/04/2021). [Citado nas páginas x, 53, 54, 57, 58, 60, 61, 62 e 63]

[61] ladder logic world, "Plc hardware: A detailed overview with component examples." Available at https://ladderlogicworld.com/PLC-hardware/, 2021. (Last accessed in 20/05/2021). [Citado na página 57]

[62] eibabo, "eibabo technology store." Available at https://www.eibabo.pt/, 2021. (Last accessed in 01/06/2021). [Citado na página 64]

[63] indusmelec, "Redes de comunicação industrial." Available at http://www.indusmelec.pt/newsletter/21/RedesIndustriais.pdf, June 2016. (Last accessed in 03/06/2021). [Citado na página 64]

[64] AS-Inteface, "As-inteface protocol." Available at https://www.as-interface.net/en/, 2021. (Last accessed in 06/06/2021). [Citado na página 65]

[65] Modbus, "Modbus protocol." Available at https://modbus.org, 2021. (Last accessed in 06/06/2021). [Citado nas páginas 66 e 70]

[66] Profibus, "Profibus protocol." Available at https://www.profibus.com, 2021. (Last accessed in 06/06/2021). [Citado nas páginas 66, 67 e 68]

[67] R. Automation, "Devicenet protocol." Available at https://www.rockwellautomation.com/pt-pt/products/hardware/allen-bradley/network-security-and-infrastructure/devicenet-networks.html, 2021. (Last accessed in 07/06/2021). [Citado na página 67]

[68] CC-Link.org, "Cc-link protocol." Available at https://www.cc-link.org/en/cclink/cclink/index.html, 2021. (Last accessed in 07/06/2021). [Citado na página 68]

[69] ODVA, "Ethernet ip protocol." Available at https://www.odva.org/technology-standards/key-technologies/ethernet-ip, 2021. (Last accessed in 07/06/2021). [Citado na página 69]

[70] EtherCat, "Ethercat protocol." Available at `https://www.ethercat.org/default.htm`, 2021. (Last accessed in 07/06/2021). [Citado na página 69]

[71] Embarcados, "Protocolo modbus: Fundamentos e aplicações." Available at `https://www.embarcados.com.br/protocolo-modbus/`, 2021. (Last accessed in 08/06/2021). [Citado nas páginas x e 72]

[72] P. Contact. Available at `https://www.phoenixcontact.com/online/portal/gb/?uri=pxc-oc-itemdetail:pid=1046008&library=gben&pcck=P&tab=5&selectedCategory=ALL`, 2021. (Last accessed in 022/06/2021). [Citado na página 73]