INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA MECÂNICA




Estudo e implementacao do Regulamento Maquinas no contexto da automacao industrial

GONÇALO MARTINS PINHO
julho de 2026

POLITÉCNICO
DO PORTO

ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

Estudo e Implementação do Regulamento Máquinas no Contexto da Automação Industrial

Gonçalo Martins Pinho

Dissertação para obtenção do Grau de Mestre em Engenharia Mecânica Área de Especialização em Construções Mecânicas

Orientador: Adriano Manuel de Almeida Santos, Doutor, ISEP

Co-orientador: Filipe Alexandre de Sousa Pereira, Doutor, ISEP

Júri:

Presidente:

Armando Vilaça Campos, Professor Adjunto, ISEP

Arguente:

António Manuel Ferreira Mendes Lopes, Professor Catedrático, FEUP

Porto, junho 2026

Dedicatória

Aos meus pais, à minha irmã e à minha namorada, pelo apoio, pela compreensão e pela presença constante ao longo desta jornada académica.

Agradecimentos

Ao Engenheiro Adriano Santos e ao Engenheiro Filipe Pereira, expresso o meu agradecimento pela orientação, pela disponibilidade e pela dedicação demonstradas ao longo do desenvolvimento deste trabalho. O apoio e interesse foram fundamentais para a concretização desta dissertação.

Aos meus pais, à minha irmã e à minha namorada, agradeço o apoio, a força e o incentivo incondicionais em todo o meu percurso académico.

Aos meus amigos, deixo também uma palavra de agradecimento por me terem acompanhado ao longo deste percurso e pelos momentos de apoio e motivação.

A todos, o meu sincero obrigado!

Resumo

O Regulamento (UE) 2023/1230, publicado em junho de 2023 e aplicável a partir de 20 de janeiro de 2027, substitui a Diretiva 2006/42/CE e representa uma alteração profunda no quadro jurídico europeu de segurança de máquinas, ao introduzir requisitos específicos para software de segurança, cibersegurança, sistemas de aprendizagem autónoma e robótica colaborativa. A presente dissertação tem como objetivo estudar e aplicar este novo regulamento no contexto da automação industrial, analisar de forma estruturada os seus requisitos e traduzir em critérios concretos de conceção, integração e validação de sistemas. A metodologia adotada articula a análise regulamentar e normativa com o desenvolvimento de dois casos de estudo representativos de filosofias de segurança distintas: uma célula robotizada segregada, baseada em segregação física e controlo de acessos, e uma célula robotizada colaborativa, onde operador e robô partilham o mesmo espaço de trabalho em condições controladas. Para cada caso são identificados os limites do sistema, os modos de operação, os perigos, o nível de desempenho requerido das funções de segurança e a arquitetura de controlo correspondente. Os resultados demonstram que ambas as abordagens permitem atingir conformidade com o novo regulamento, embora com exigências técnicas e documentais distintas. A análise comparativa evidencia que a robótica colaborativa introduz maior complexidade na definição e validação das funções de segurança, o que exige uma integração mais rigorosa entre sensores, lógica de comando e comportamento do robô.

Palavras-chave: Segurança de máquinas, Regulamento Máquinas, Automação industrial, Robótica colaborativa, Segurança funcional, Avaliação de risco

Abstract

European Union Regulation 2023/1230, published in June 2023 and applicable from 20 January 2027, replaces Directive 2006/42/EC and represents a fundamental shift in the European legal framework for machinery safety, introducing specific requirements for safety software, cybersecurity, autonomous learning systems and collaborative robotics. The main objective of this dissertation is to study and apply this new regulation in the context of industrial automation, systematically analysing its requirements and translating them into concrete design, integration and validation criteria for robotic systems. The methodology combines regulatory and normative analysis with the development of two case studies representing distinct safety philosophies: a segregated robotic cell, based on physical separation and access control, and a collaborative robotic cell, where operator and robot share the same workspace under controlled conditions. For each case, the system boundaries, operating modes, hazards, required performance level and corresponding safety control architecture are identified. The results demonstrate that both approaches can achieve compliance with the new regulation, albeit with different technical and documentary requirements. The comparative analysis shows that collaborative robotics introduces greater complexity in defining and validating safety functions, requiring more rigorous integration between sensors, control logic and robot behaviour.

KEYWORDS: Machine safety, Machinery Regulation, Industrial automation, Collaborative robotics, Functional safety, Risk assessment

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos e Símbolos

Lista de Acrónimos

CAD	*Computer Aided Design* (*Desenho assistido por computador*)
CAM	Fabrico assistido por computador
CIM	Fabrico integrado por computador
CE	Conformidade europeia
CEN	Comité Europeu de Normalização
CENELEC	Comité Europeu de Normalização Eletrotécnica
CPS	Sistemas ciberfísicos
E-Stop	Paragem de Emergência
ETSI	Instituto Europeu de Normas de Telecomunicações
FS	Função de Segurança
HMI	Interface Homem–Máquina
HRC	Colaboração Humano–Robô
IA	Inteligência Artificial
IoT	Internet das Coisas
ISEP	Instituto Superior de Engenharia do Porto
ISO	Organização Internacional de Normalização
M2M	Comunicação máquina-para-máquina
PFL	Limitação de potência e força
PL	Nível de desempenho
PLC	Controlador Lógico Programável
P.Porto	Instituto Politécnico do Porto
REFIT	Avaliação Regulamentar da Comissão Europeia
RESS	Requisitos Essenciais de Saúde e Segurança
SCADA	Supervisão, controlo e aquisição de dados
SSM	Monitorização de Velocidade e Distância
UE	União Europeia
VPN	Rede privada virtual

1. Introdução

1.1. Contextualização

A automação industrial assumiu um papel central na modernização dos sistemas produtivos, e traz consigo ganhos de produtividade, repetibilidade, qualidade e flexibilidade. Neste contexto, a integração de sistemas robotizados em operações de manipulação, montagem, inspeção e paletização tornou-se uma solução recorrente em diversos setores industriais. Contudo, o aumento da complexidade funcional e da conectividade destes sistemas tem reforçado a necessidade de garantir níveis elevados de segurança na sua conceção, integração e exploração.

A segurança de máquinas assume, por isso, um papel determinante no desenvolvimento de células robotizadas, particularmente em contextos em que coexistem movimentos automáticos, intervenção humana e funções de comando com impacto direto na redução do risco. Esta exigência tornou-se ainda mais relevante com a evolução do enquadramento regulamentar europeu. O Regulamento (UE) 2023/1230 veio substituir a Diretiva 2006/42/CE, e estabeleceu um quadro jurídico mais exigente e mais adequado às atuais realidades tecnológicas, o que inclui sistemas de comando programáveis, sistemas autoevolutivos, robótica avançada, conectividade digital e acesso remoto.

Para responder às exigências da indústria, a evolução da robótica industrial conduziu ao aparecimento de soluções colaborativas, nas quais operador e robô podem partilhar o mesmo espaço de trabalho em condições controladas. Esta transição de modelos baseados em segregação física para modelos de colaboração segura introduz novos desafios de conceção, validação e demonstração da conformidade.

Neste contexto, é relevante estudar de forma comparativa diferentes arquiteturas de segurança aplicáveis a células robotizadas, de modo a avaliar a forma como os princípios regulamentares e normativos podem ser materializados em soluções concretas de automação industrial.

1.2. Objetivos

O trabalho procura enquadrar os principais requisitos regulamentares e normativos aplicáveis à segurança de máquinas, no contexto da automação industrial e da indústria 4.0 e 5.0, presentes no Regulamento (UE) 2023/1230. Pretende-se analisar a articulação entre a apreciação do risco, as funções de segurança, a arquitetura de controlo e o desempenho

requerido das partes relacionadas com a segurança, bem como desenvolver dois casos de estudo representativos de filosofias distintas de segurança, um baseado na segregação física e outro na colaboração homem–robô. Pretende-se ainda identificar, para cada caso, os perigos, os modos de operação, os limites do sistema e as situações perigosas relevantes, definir e justificar as funções de segurança, determinar o respetivo PLr e estruturar a arquitetura de segurança e controlo. É realizada uma análise comparativa às vantagens, limitações e implicações regulamentares das duas abordagens.

1.3. Metodologia

A metodologia adotada nesta dissertação assenta numa abordagem técnico-normativa, estruturada a partir da análise do Regulamento (UE) 2023/1230 e das principais normas harmonizadas aplicáveis à segurança de máquinas e de sistemas robotizados. O trabalho articula a revisão do enquadramento regulamentar com a aplicação prática dos seus princípios a dois casos de estudo desenvolvidos no contexto da automação industrial.

Numa primeira fase, procede-se ao enquadramento do novo Regulamento Máquinas e das normas relevantes para a apreciação do risco, para a definição de funções de segurança e para a conceção das arquiteturas de comando relacionadas com a segurança. Numa segunda fase, são desenvolvidos dois casos de estudo: o primeiro relativo a uma célula robotizada segregada e o segundo relativo a uma célula robotizada colaborativa. Em ambos os casos, são definidos os limites do sistema, os modos de operação, os perigos, a avaliação de risco, as funções de segurança, o PLr e a arquitetura de segurança e controlo.

A validação adotada é de natureza metodológica e arquitetural, sem implementação física, simulação dinâmica ou medição experimental de parâmetros, incidindo sobre a coerência entre perigos, medidas de redução do risco, funções de segurança, comportamento funcional esperado e conformidade normativa.

1.4. Estrutura

A presente dissertação encontra-se organizada em cinco capítulos.

No Capítulo 1 apresenta-se o enquadramento do tema, os objetivos do trabalho, a metodologia adotada e a estrutura do documento.

O Capítulo 2 é dedicado ao enquadramento regulamentar e normativo e ao estudo do estado da arte, que incide sobre o Regulamento (UE) 2023/1230 e sobre as principais normas aplicáveis à segurança de máquinas, segurança funcional e robótica colaborativa.

No Capítulo 3 desenvolvem-se os casos de estudo, correspondentes a duas células robotizadas com filosofias de segurança distintas, uma célula segregada e uma célula colaborativa. Para cada caso são definidos os limites do sistema, os modos de operação, os perigos, a avaliação de risco, as funções de segurança, o PLr e a arquitetura de controlo.

O Capítulo 4 apresenta os resultados e a discussão, incluindo a validação conceptual, funcional, normativa e arquitetural de cada caso de estudo, bem como uma análise crítica comparativa entre as duas abordagens.

Por fim, o Capítulo 5 apresenta as conclusões finais da dissertação, identificando as principais limitações do trabalho e apontando possíveis desenvolvimentos futuros.

2. Estado da arte

O presente capítulo estabelece o enquadramento teórico e o estado da arte necessários para a compreensão dos desafios atuais na segurança de máquinas industriais.

A análise inicia-se com uma contextualização histórica da evolução da automação, desde a mecanização inicial até aos paradigmas da Indústria 4.0 e 5.0, identificando as tecnologias que transformaram os processos produtivos. Posteriormente, é explorada a evolução do quadro regulamentar europeu, com foco na transição da Diretiva 2006/42/CE para o novo Regulamento (UE) 2023/1230, analisando como o legislador procura responder aos riscos emergentes da digitalização, inteligência artificial e conectividade.

2.1. Evolução da automação industrial

Ao longo de toda a história, a humanidade reinventou-se e, em simultâneo, aperfeiçoou a sua capacidade industrial, impulsionada pelo aparecimento de novos recursos e tecnologias. O desenvolvimento da automação e das técnicas de controlo desempenham um papel crucial neste processo, contribuindo para a criação de um mundo mais estável e eficiente [1].

As revoluções industriais trouxeram consigo melhorias na qualidade de vida das sociedades, e alterações na sua estrutura. Para isso, a humanidade tem de se adaptar para tirar o máximo partido dos avanços tecnológicos [2].

A evolução da automação industrial está diretamente ligada às revoluções industriais, em que cada uma se caracteriza por saltos tecnológicos que levaram a mudanças de paradigma nos sistemas produtivos. A primeira revolução industrial ficou marcada pela mecanização, a segunda pela utilização intensiva da energia elétrica e pela produção em massa, e a terceira pela digitalização e automação baseada em eletrónica [3].

A terceira revolução industrial marcou o início da era da automação. A introdução de controladores lógicos programáveis (PLC) e computadores industriais permitiu que as máquinas executassem tarefas complexas sem a intervenção humana direta, aumentando a produtividade, e transformando partes críticas dos processos em tarefas mais eficientes e seguras. O forte investimento em investigação e desenvolvimento, por parte de governos e universidades, inicialmente com objetivos militares, permitiu o desenvolvimento de muitas tecnologias que foram aplicadas à indústria, como a produção integrada por computador (CIM), o desenho assistido por computador (CAD), a manufatura assistida por computador (CAM). Estas ferramentas tornaram-se vitais entre as décadas de 1970 e 1980, quando as crises

económicas e energéticas exigiram às empresas um aumento drástico da eficiência para a redução de custos operacionais. Com os avanços eletrónicos e tecnologias de informação da indústria, os sistemas automatizados evoluíram de forma significativa, tornando-se cada vez mais precisos, eficientes, e em alguns casos, tornando-se totalmente autónomos sem a necessidade de intervenção humana. Contudo, estas evoluções, surgiram novos desafios, relacionados com a integração e comunicação entre máquinas, sistemas e pessoas, pois as tecnologias da época eram baseadas em controlos isolados e redes locais e, dessa forma, ainda não permitiam uma visão global e em tempo real dos processos produtivos [4].

2.2. A transição para a indústria 4.0 e 5.0

A recente evolução da automação industrial não se limita a um incremento da eficiência, mas representa uma mudança estrutural na forma como os sistemas produtivos são concebidos e operados. Esta transição é marcada por dois paradigmas complementares: a indústria 4.0 focada na digitalização e interconectividade, e a indústria 5.0, que reorienta o foco tecnológico para a sustentabilidade, resiliência e centralidade humana.

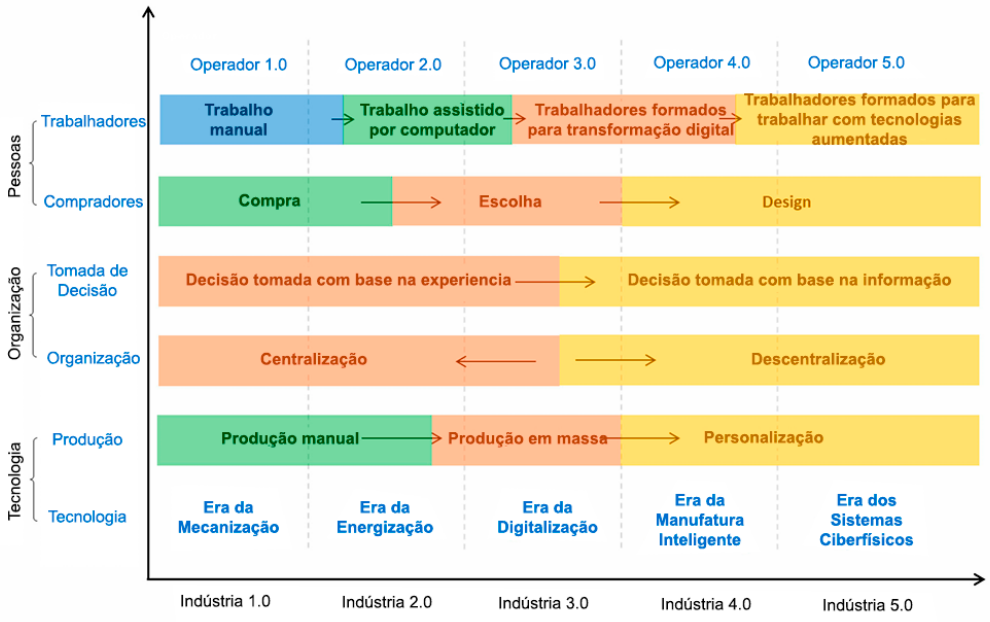


Figura 1 - Evolução da Indústria (adaptado de:[5])

A Figura 1 ilustra esta evolução dos paradigmas industriais sob três perspetivas fundamentais: as pessoas, a organização e a tecnologia. Observa-se uma transição clara do papel do operador, que evolui de um executor de tarefas manuais ou assistidas para um trabalhador aumentado e colaborativo na era dos sistemas ciberfísicos (CPS).

Como destacado por Zizic et al. [5], enquanto a Indústria 4.0 se centrou na fábrica inteligente e na conectividade técnica para descentralizar a decisão com base em informação, a Indústria 5.0 surge como uma evolução necessária para reintegrar o fator humano no processo. Neste novo contexto, a tecnologia deixa de ser apenas uma ferramenta de automação para se tornar um

elemento de colaboração, onde trabalhadores qualificados operam lado a lado com sistemas autónomos e tecnologias aumentadas, exigindo uma nova abordagem à segurança que vá além da simples segregação física.

2.2.1. A indústria 4.0

Introduzido inicialmente em 2011, na Alemanha, no âmbito da iniciativa *High Technology Strategy 2020,* o conceito de indústria 4.0 surge com o objetivo de aumentar a competitividade na indústria transformadora através da integração de tecnologias digitais nos sistemas físicos. O objetivo central é a transformação das fábricas convencionais em fábricas inteligentes, onde os sistemas ciberfísicos (CPS), a internet das coisas (IoT) e a comunicação máquina para máquina (M2M), convergem para criar ambientes de produção autónomos e flexíveis [6]. As fábricas inteligentes adotam uma abordagem completamente nova à produção e processos de fabrico, em que as máquinas, produtos, e sistemas logísticos estão interligados, tornando os produtos mais inteligentes, para lidar com os requisitos funcionais e com os clientes cada vez mais exigentes.

Os Sistemas Ciberfísicos

Os CPS são um dos pilares da Indústria 4.0. Trata-se de sistemas onde os componentes mecânicos e eletrónicos são indissociavelmente ligados a algoritmos computacionais e redes de comunicação. Através de sensores e atuadores, os CPS monitorizam processos físicos, criam uma copia virtual do mundo físico (gémeo digital) e tomam decisões descentralizadas. Esta arquitetura permite funcionalidades avançadas como a manutenção preditiva, a auto otimização da produção e a rastreabilidade total de produtos, resultando numa redução significativa de tempos de paragem e de desperdícios, e um aumento da segurança através da deteção antecipada de anomalias [7]. Estes sistemas, dada a sua natureza híbrida, possibilitam a validação e verificação do modelo de controlo através da simulação do modelo conceptual baseado no modelo real [8].

A Internet das coisas

A IoT no contexto industrial fornece a infraestrutura de conectividade que permite aos CPS comunicarem entre si e com os sistemas de gestão. Ao interligar máquinas, produtos e pessoas numa rede global, a IoT quebra os silos de informação tradicional, permitindo uma recolha massiva de dados qua alimentam algoritmos de análise para dar suporte à decisão em tempo real [9].

A Comunicação Máquina para Máquina

A comunicação M2M consiste na troca direta de informação entre dispositivos, através de redes com ou sem fios, sem a necessidade de intervenção humana. Esta tecnologia permite que sensores, atuadores, controladores e sistemas informáticos comuniquem, a enviar e receber dados para monitorizar, controlar e gerir os processos produtivos. O seu papel estende-se à criação de redes inteligentes e descentralizadas, onde as máquinas podem detetar eventos, trocar informações e executar tarefas de forma automática, contribuindo para a maior eficiência operacional, uma maior flexibilidade, controlo de qualidade e consequente redução

de custos. A comunicação M2M complementa a IoT e os CPS, ao assegurar a comunicação direta entre os equipamentos e o suporte à tomada de decisão em tempo real, sendo assim, um pilar fundamental da automação inteligente [10].

A Robótica colaborativa

A indústria 4.0 caracteriza-se por sistemas produtivos altamente flexíveis, capazes de responder rapidamente a mudanças na procura e a requisitos de personalização crescentes [3]. Neste contexto, a robótica tradicional baseada em células isoladas e programação complexa, apresenta limitações significativas, como os elevados custos de implementação, longos tempos de reconfiguração e a impossibilidade de combinar as capacidades humanas e robóticas [11].

Para responder a estas limitações surgiram os robôs colaborativos (cobots), que se destacam pela segurança, facilidade de uso e colaboração com os humanos, promovendo uma maior flexibilidade e eficiência produtiva. Os cobots destacam-se dos robôs tradicionais ao serem mais leves, mais fáceis de programar e de rápida implementação. Por outro lado, enfrentam restrições técnicas como menor velocidade e capacidade de carga, limitando a sua aplicação em determinados contextos industriais [11].

Os cobots possibilitam diferentes formas de colaboração humano-robô (HRC), onde o operador partilha o seu espaço de trabalho com o robô criando um ambiente dinâmico. A HRC pode assumir diferentes níveis, desde a coexistência no mesmo espaço sem interação direta até à colaboração plena, caracterizada por ações interdependentes e simultâneas entre o robô e o operador. A relação entre o operador humano e o robô também pode variar no que diz respeito aos modos de liderança e cooperação, determinadas pelo grau de autonomia do sistema. Para que esta interação seja eficaz, princípios como a atividade partilhada, interação conjunta e ação orientada por objetivos são essenciais para criar um ambiente ciber-físico verdadeiramente cooperativo, onde as competências do humano e do robô se complementam para resolver tarefas complexas de forma adaptável e previsível [12].

A integração de robôs colaborativos na indústria introduz desafios multidimensionais que devem ser considerados na implementação destes sistemas.

Do ponto de vista da segurança, a partilha do espaço de trabalho sem barreiras físicas exige sistemas robustos de deteção e previsão do movimento humano, a validação experimental de limites de força e pressão, e gestão de situações imprevisíveis resultantes da variabilidade do comportamento humano [13]. Estes aspetos, são regulamentados por normas, como a ISO/TS 15066.

A conectividade característica dos sistemas I4.0 expõe os cobots a ameaças de cibersegurança incluindo acessos não autorizados, manipulação de parâmetros operacionais e ataques para bloqueio de serviço [14]. O Regulamento (UE) 2023/1230 reconhece este risco e introduz requisitos específicos neste domínio, reforçando a necessidade de arquiteturas seguras e protocolos de autenticação robustos [15, Anexo III].

2.2.2. A indústria 5.0

O conceito de Indústria 5.0 surge na literatura académica e em conceitos estratégicos europeus como uma evolução e complemento da indústria 4.0. Esta abordagem propõe uma visão mais humana, sustentável e resiliente, ao reconhecer o papel da indústria na promoção de objetivos sociais e ambientais, colocando o bem-estar do trabalhador no centro do processo produtivo e incentivar o respeito pelos limites do planeta. Este novo paradigma vem completar a digitalização da Indústria 4.0 ao adotar uma abordagem sistemática e centrada nas pessoas, em que a inovação e a tecnologia são orientadas para a criação de valor sustentável. Este novo conceito surge ainda como resposta a desafios recentes, como a necessidade de tornar as cadeias de abastecimento mais resilientes, adotar modelos de economia circular e reduzir a dependência de recursos não renováveis, estando alinhado com o Pacto Ecológico Europeu e as lições da pandemia da Covid-19 [16].

A Comissão Europeia [17], define oficialmente este paradigma e identifica três pilares fundamentais (Figura 2) sendo eles a centralidade do homem, a sustentabilidade e a resiliência.

Figura 2 - Pilares da Indústria 5.0 (adaptado de: [17])

Primeiro Pilar: Centralidade do Homem

O primeiro pilar posiciona o trabalhador humano no centro dos sistemas produtivos, contrastando com abordagens que priorizam exclusivamente a eficiência e a produtividade. Esta perspetiva reconhece características humanas únicas, como a criatividade, capacidade de adaptação, tomada de decisão em situações complexas e competências sociais, características que as máquinas não conseguem replicar [16], [18].

A tecnologia deve, assim, potenciar estas capacidades em vez de as substituir, e promover ambientes de trabalho mais seguros, ergonómicos e satisfatórios [19].

Este pilar sustenta a transição de sistemas totalmente automatizados para sistemas colaborativos, onde os robôs executam as tarefas repetitivas, fisicamente exigentes ou perigosas, enquanto os humanos se concentram em atividades que requerem destreza, perceção e decisão [18].

Segundo Pilar: Sustentabilidade

O segundo pilar enfatiza a responsabilidade ambiental da indústria, ao incorporar princípios de economia circular, eficiência energética e minimização de resíduos nos processos produtivos. Assim, a indústria 5.0 propõe que a otimização industrial não considere apenas métricas económicas, mas também o impacto ambiental ao longo de todo o ciclo de vida dos produtos [16],[19].Tecnologias como os gémeos digitais, inteligência artificial e CPS, já presentes na indústria 4.0, são reorientadas para responder aos objetivos da sustentabilidade, com a otimização do consumo energético, a previsão de falhas que permite prolongar a vida útil dos equipamentos e a personalização de produtos para evitar sobreproduções [19].

Terceiro Pilar: Resiliência

O terceiro pilar refere-se à capacidade das organizações se adaptarem a disrupções, sejam crises económicas, pandemias, roturas na cadeia de abastecimento ou eventos climáticos extremos. Sistemas resilientes combinam a flexibilidade dos sistemas com a capacidade humana de resolução criativa de problemas [16], [17].

Os sistemas de colaboração homem-robô (HRC) contribuem para a resiliência das organizações ao permitir a rápida adaptação dos processos produtivos ao nível dos volumes e produtos a produzir, mantendo o operador humano como elemento decisor central em situações de incerteza [11].

A evolução da Indústria 4.0 para a Indústria 5.0 reflete uma mudança de prioridades, de uma otimização puramente tecnológica para uma visão que integra objetivos sociais, ambientais e económicos.

Implicações Regulamentares

Esta mudança de paradigma tem implicações diretas no enquadramento regulamentar europeu, principalmente na diretiva-máquinas. O novo Regulamento (UE) 2023/1230 materializa esta visão ao introduzir e reforçar requisitos específicos de segurança que protegem não apenas a integridade física, mas também o bem-estar psicológico e cognitivo dos operadores em ambientes colaborativos, alinhando a lei com os princípios da Indústria 5.0 [15].

2.3. Importância do regulamento máquinas

A evolução tecnológica da Indústria 4.0 e os pilares da Indústria 5.0 têm implicações diretas no enquadramento regulamentar que rege a conceção, fabrico e comercialização de máquinas no mercado europeu. As características centrais da Indústria 4.0, a digitalização, a conectividade e a autonomia dos sistemas levantam novos desafios de segurança que a legislação deve prever. Em simultâneo, a visão da centralidade no homem da Indústria 5.0 reforça a importância de a legislação garantir que a automação avançada preserve o bem-estar e a segurança dos trabalhadores.

A transformação digital da indústria coloca novos desafios à regulamentação de segurança de máquinas. Os sistemas ciberfísicos, a conectividade entre equipamentos e a inteligência artificial introduzem riscos que os quadros legislativos já estabelecidos não preveem.

Neste contexto, a União Europeia tem vindo a atualizar o quadro legislativo aplicável a máquinas, a fim de equilibrar a promoção da inovação tecnológica com a proteção eficaz dos seus utilizadores. O presente capítulo analisa a evolução regulamentar, com particular foco nos requisitos aplicáveis a sistemas de comando e segurança em ambientes de automação industrial.

2.3.1. Evolução da legislação máquinas na União Europeia

O regulamento europeu de segurança de máquinas teve origem na década de 1980, quando foi adotada a estratégia que foi denominada de “Nova abordagem”, que estabeleceu princípios inovadores para a harmonização técnica no mercado europeu [20].

Esta abordagem introduziu um modelo de harmonização técnica que é caracterizado por três princípios fundamentais, detalhados no *Blue Guide* da Comissão Europeia [21]:

1. **Requisitos Essenciais:** A legislação harmonizada define apenas os requisitos essenciais de segurança e saúde (RESS), os quais são formulados por objetivos a alcançar, sem definir soluções técnicas específicas. Esta abordagem confere flexibilidade para acomodar diferentes tecnologias e permite inovação sem a necessidade de revisões legislativas constantes.
2. **Normas Harmonizadas:** Delegam as especificações técnicas detalhadas em normas europeias harmonizadas, desenvolvidas por organismos de normalização (CEN, CENELEC, ETSI). A aplicação destas normas é voluntária e ajudam a presumir que os requisitos estão a ser cumpridos, simplificando o processo de avaliação.
3. **Avaliação de Conformidade:** Estabelece os procedimentos de avaliação de conformidade proporcionais ao risco. Quando esses procedimentos são concluídos com sucesso, o produto recebe a marcação CE, que permite a sua livre circulação e comercialização dentro do mercado europeu.

A primeira Diretiva Máquinas (89/392/CEE), publicada a 14 de junho de 1989, estabeleceu pela primeira vez um quadro regulamentar harmonizado para máquinas à escala europeia. Esta

diretiva definiu requisitos de segurança essenciais, aplicáveis à conceção e fabrico de máquinas, ao introduzir conceitos como a obrigatoriedade da avaliação de riscos, a hierarquia de medidas de proteção e os procedimentos de conformidade com a marcação CE.

A Diretiva 98/37/CE, que entrou em vigor em 1995, consolidou a diretiva original, ao alargar o âmbito de aplicação e clarificar definições. Esta diretiva introduziu requisitos mais explícitos para equipamentos de elevação, componentes de segurança e máquinas com riscos específicos.

A Diretiva 2006/42/CE, em vigor desde 2009, representou uma alteração significativa em relação às anteriores, ao clarificar o âmbito de aplicação, introduzir o conceito de "quasi-máquina", reforçar os procedimentos de avaliação para máquinas de elevado risco e atualizar os requisitos face à evolução tecnológica da década de 1990 [22]. Esta manteve-se em vigor durante 15 anos, período onde a indústria sofreu transformações profundas associadas à Indústria 4.0.

A avaliação REFIT da Comissão Europeia (2018-2019) conclui que, com as evoluções tecnológicas dos últimos anos, os objetivos e princípios da diretiva ainda continuavam válidos, mas passaram a existir lacunas no que diz respeito à digitalização e software, conectividade e cibersegurança, inteligência artificial e autonomia [23]. Esta avaliação motivou a adoção do Regulamento (UE) 2023/1230, que foi publicado em junho de 2023 entrou em vigor em 2023 e será aplicável a partir de 20 de janeiro de 2027 [15].

A transição da Diretiva para Regulamento representa uma mudança de instrumento legislativo em que os Regulamentos são diretamente aplicáveis a todos os estados-membros sem transposições nacionais, garantindo uma uniformidade total na sua aplicação.

2.3.2. Novos desafios

A transição para a indústria 4.0 expôs limitações significativas no quadro regulamentar de máquinas, concebido numa era em que as máquinas eram predominantemente sistemas mecânicos e eletromecânicos.

Software e sistemas programáveis

A crescente dependência de software para funções essenciais de segurança representa uma mudança de paradigma. Os Computadores Lógicos programáveis (PLC), os sistemas embebidos, as interfaces homem-máquina (HMI) e os sistemas SCADA executam funções que interferem diretamente na segurança dos utilizadores. A Diretiva 2006/42/CE apenas menciona os sistemas programáveis de forma genérica, sem estabelecer requisitos específicos para desenvolvimento, validação e atualização dos softwares de segurança [22].

Embora normas harmonizadas como a EN ISO 13849-1 e a EN IEC 62061 incluam requisitos para software de segurança, a sua aplicação não é obrigatória sob a diretiva. A avaliação REFIT identificou esta lacuna como área prioritária para revisão [23].

Conectividade e cibersegurança

A integração de máquinas em redes industriais e a conectividade à internet introduzem novos meios de ataque que são inexistentes em máquinas convencionais. Humayed et al., numa

revisão abrangente sobre segurança nos sistemas ciberfísicos, identificam vulnerabilidades específicas em ambientes industriais, sendo elas os protocolos de comunicação industrial sem mecanismos de autenticação robusta, a utilização de sistemas obsoletos concebidos numa época pré-conectividade e sem capacidade de receber atualizações de segurança, e a crescente convergência entre as redes de tecnologia de campo e as redes de tecnologia de informação, que são utilizadas para funções corporativas e que expõe os sistemas a ameaças [24].

A revisão de Yaacoub et al. sobre a segurança dos sistemas ciberfísicos documenta que, os ataques a sistemas de controlo industrial podem ter consequências físicas diretas, transcendendo o domínio tradicional da cibersegurança e afetando diretamente a segurança das pessoas e dos equipamentos. Entre os diferentes tipos de ataques, destaca-se o *spoofing*, que consiste no atacante mascarar a identidade de sensores ou controladores e enviar dados falsos, causando a manipulação ou destruição física dos componentes que foram expostos e, muitas vezes, a interrupção de atividades críticas. Outro ataque comum consiste na disrupção de serviço, que resulta da alteração física ou digital de dispositivos que originam paragens operacionais. Os autores descrevem ainda ataques de *tracking*, que exploram o acesso físico a dispositivos para os seguir ou adulterar. Estes tipos de ataques demonstram como a fronteira entre o digital e o físico se torna cada vez mais ténue, ampliando significativamente a superfície de risco dos sistemas ciberfísicos. [14]

A Diretiva 2006/42/CE não contempla os riscos da cibersegurança, refletindo uma era em que as máquinas operavam isoladamente ou em redes proprietárias fechadas. Esta lacuna foi identificada explicitamente na avaliação REFIT como área prioritária a ser revista [23].

Inteligência artificial e autonomia

A integração de sistemas de inteligência artificial (IA) e a utilização de algoritmos de aprendizagem automática em máquinas industriais representam um dos desafios mais complexos para o quadro regulamentar existente. Ao contrário dos sistemas programáveis tradicionais, cujo comportamento é determinístico e previsível, os sistemas baseados em IA podem modificar autonomamente os seus parâmetros operacionais, introduzindo comportamentos adaptativos que não serão totalmente previsíveis no momento da avaliação de conformidade.

Wang et al., numa revisão sistemática sobre a IA em sistemas de segurança crítica identificam a opacidade dos algoritmos como uma barreira fundamental à certificação. A impossibilidade de prever todos os estados possíveis de um sistema que evolui com novos dados compromete a capacidade de garantir conformidade contínua após a colocação no mercado [25].

Robótica Colaborativa

A robótica colaborativa introduz uma mudança de paradigma na segurança industrial, ao transitar da segregação física para a gestão da interação. Esta proximidade elimina as barreiras de proteção tradicionais, expondo o operador a novos riscos de contacto mecânico que exigem uma validação rigorosa.

A literatura científica identifica a gestão de colisões como o desafio central da segurança colaborativa. Estudos sobre o controlo seguro de robôs enfatizam a necessidade de sistemas

de controlo em tempo real, capazes de limitar a energia cinética e a força de impacto a níveis suportáveis pelo corpo humano, conforme definido tecnicamente na especificação ISO/TS 15066. Contudo, como notam investigações sobre a implementação desta norma, a variabilidade do comportamento humano torna difícil modelar todas as interações possíveis, exigindo sistemas de perceção avançados que não só detetem a presença, mas prevejam a intenção de movimento do operador para evitar contactos acidentais [26].

2.4. Do quadro atual ao novo Regulamento

A transição da Diretiva 2006/42/CE para o novo Regulamento (UE) 2023/1230 não representa apenas uma atualização técnica, mas uma alteração profunda na filosofia de fiscalização e conformidade. As secções seguintes detalham como a arquitetura legislativa foi reconfigurada para abranger as novas tecnologias digitais, analisando as implicações práticas para os fabricantes e as novas exigências de certificação que redefinirão o acesso ao mercado a partir de 2027.

2.4.1. A Diretiva 2006/42/CE

A Diretiva 2006/42/CE, aplicável desde 2009 estabelece os requisitos essenciais de segurança e saúde aplicáveis à conceção e fabrico de máquinas, aos componentes de segurança, acessórios de elevação e componentes de transmissão, equipamentos amovíveis de transmissão mecânica e quasi-máquinas [22].

O modelo baseado em requisitos essenciais genéricos, complementados por normas harmonizadas técnicas, são um contributo importante na redução do número de acidentes. Numa vertente socioeconómica, máquinas mais seguras são fundamentais na redução do custo social de acidentes e danos para a saúde [27].

Os princípios técnicos estabelecidos no Anexo I da Diretiva, nomeadamente os requisitos relativos à fiabilidade dos sistemas de comando, aos dispositivos de paragem de emergência e à prioridade das funções de segurança sobre as funções operacionais, permanecem concetualmente válidos e formam a base da engenharia de segurança atual [21, Anexo I,II].

Face às evoluções tecnológicas da Indústria 4.0, a diretiva apresenta limitações. A avaliação REFIT da comissão europeia, confirmou que, embora a estrutura da Diretiva permanecesse adequada para os riscos mecânicos tradicionais, existiam lacunas críticas na resposta aos riscos emergentes. A indefinição jurídica sobre o estatuto do software de segurança, a ausência de requisitos explícitos para a cibersegurança e a dificuldade em enquadrar sistemas de comportamento autónomo, foram identificadas como barreiras à inovação e potenciais riscos para os utilizadores, motivando a necessidade de uma revisão legislativa [23].

2.4.2. O Regulamento (UE) 2023/1230

O Regulamento (UE) 2023/1230, publicado em 2023, entrou em vigor em 2023 e será aplicável a partir de 20 de janeiro de 2027, representa a resposta europeia aos desafios já identificados [15].

A alteração de diretiva para regulamento visa garantir que, a aplicação é uniforme em todos os estados-membros, ao eliminar as variabilidades resultantes da transposição da diretiva para normas nacionais.

O novo regulamento mantém a estrutura e a filosofia da “nova abordagem”, mas introduz novas disposições para as matérias que foram identificadas como lacunas.

No domínio do software, o regulamento introduz uma alteração estrutural ao classificar explicitamente o software que desempenha funções de segurança como um "componente de segurança" [15, Anexo I]. Isto significa que, o código informático passa a estar sujeito aos mesmos requisitos de avaliação de conformidade e marcação CE que os componentes físicos, devendo ser desenvolvido segundo o estado da arte em segurança funcional.

Relativamente à cibersegurança, o novo requisito essencial 1.1.9 “Proteção contra a corrupção” do Anexo III preenche o vazio legislativo anterior. Este requisito obriga os fabricantes a desenhar as máquinas de forma que a ligação a outros dispositivos ou redes não comprometa as funções de segurança. Torna-se imperativo implementar medidas que previnam o acesso não autorizado e que garantam que qualquer intrusão ou corrupção de dados, acidental ou intencional, não resulte em situações perigosas [15, Anexo III].

Para sistemas com comportamento total ou parcialmente autoevolutivo, o regulamento estabelece que, os dados relativos às tomadas de decisões de funções de segurança devem ser conservados por um período de um ano após a sua recolha, exclusivamente para efeitos de demonstração de conformidade perante as autoridades competentes [15, Anexo III].

2.4.3. Análise comparativa

A transição da Diretiva 2006/42/CE para o Regulamento (UE) 2023/1230 introduz alterações significativas que vão além da sua forma jurídica. De modo a compreender o impacto pratico desta mudança legislativa, é apresentada de seguida uma comparação detalhada, estruturada em seis pontos essenciais: a arquitetura legal, as definições, os requisitos técnicos, a avaliação de conformidade, a marcação CE e o relatório de conformidade.

1. **Arquitetura legislativa**

A diretiva 2006/42/CE é constituída por 29 artigos, complementados por 12 anexos técnicos. Os artigos iniciais delimitam o âmbito e as definições, enquanto o núcleo regulatório estabelece as obrigações fundamentais de colocação no mercado [22].

Os anexos I a III contêm os requisitos essenciais de segurança e saúde para a conceção e fabrico de máquinas, e os anexos III a XI definem a marcação CE, os procedimentos de avaliação de conformidade e os requisitos para os organismos notificados [22].

Ao contrário da diretiva, que era principalmente focada no fabricante, o regulamento define responsabilidades específicas e distintas para importadores [15, Artigo 13º] e distribuidores [15, Artigo 14º].

Uma inovação estrutural relevante é a introdução de mecanismos de atualização dinâmica através de atos delegados e de execução. Este mecanismo confere à comissão europeia a capacidade de adaptar requisitos técnicos específicos sem a necessidade de uma revisão legislativa completa [15, Artigo 47º].

Âmbito de aplicação

A diretiva 2006/42/CE aplica-se a máquinas, equipamentos intermutáveis, componentes de segurança, acessórios de elevação, correntes, cabos, correias, dispositivos amovíveis de transmissão mecânica e quasi-máquinas. O artigo primeiro e segundo excluem do seu âmbito diversas categorias de produtos que já são abrangidos por legislação setorial específica [22].

O regulamento (UE) 2023/1230 mantém o mesmo âmbito de aplicação, preservando as exclusões principais da diretiva. Contudo, o regulamento vem clarificar situações de fronteira que geravam interpretações divergentes entre os estados-membros. Ao considerar o software de segurança como um produto sujeito a marcação CE, e ao integrar explicitamente máquinas com mobilidade autónoma e conectividade, o regulamento elimina as dúvidas interpretativas que existiam entre os Estados-Membros sobre a aplicabilidade da lei a estas novas tecnologias [15].

2. Definições fundamentais

A definição de máquina permanece conceptualmente idêntica em ambos os instrumentos legislativos. A diretiva define máquina como sendo um “conjunto equipado ou destinado a ser equipado com um sistema de acionamento que não seja a força humana ou animal diretamente aplicada, sendo o conjunto composto por peças ou componentes ligados entre si, dos quais pelo menos um é movel” [22]. No regulamento (UE) 2023/1230 esta definição é preservada, assegurando que as interpretações já consolidadas se mantêm [15].

O conceito de quasi-máquina, permanece igualmente inalterado, como sendo um “conjunto que constitui quase uma máquina, mas que por si só, não pode assegurar uma aplicação definida” [15].

A definição de componente de segurança também se mantém, como “componente que não seja um equipamento intermutável” [15], em que o seu fabricante o coloca no mercado com o objetivo de desempenhar uma função de segurança durante a sua utilização, e cuja falha ou funcionamento deficiente põe em perigo a segurança dos utilizadores.

Alteração Substancial

O regulamento introduz uma nova definição legal para “alteração substancial” [15, Artigo 3º]. Na Diretiva, a modificação de máquinas existentes gerava incerteza jurídica sobre se a máquina modificada deveria ser considerada nova e sujeita a uma nova marcação CE. Com esta nova definição, o regulamento vem clarificar que uma alteração é substancial quando cria perigos ou leva a um aumento dos riscos existentes, afetando a segurança, levando a que sejam

necessárias novas medidas de proteção, obrigando o modificador a assumir as obrigações de fabricante [15].

Software de segurança

O regulamento introduz pela primeira vez a definição explicita de "software que desempenha função de segurança", designando o software cujo funcionamento ou falha pode afetar diretamente a segurança das pessoas expostas aos riscos da máquina. Esta formalização responde à ambiguidade detetada na Diretiva 2006/42/CE, onde apenas existiam referencias genéricas a "suporte lógico (programação)" [22], sem estabelecer critérios claros de identificação ou requisitos específicos.

A introdução desta definição terá implicações práticas, ao estabelecer a obrigatoriedade de identificar explicitamente o software de segurança na documentação técnica e, em simultâneo, impõe que o software seja desenvolvido segundo o estado da arte.

Sistemas de aprendizagem autónoma

O regulamento define "aprendizagem automática" como sendo um sistema que, com base em análise de dados durante a operação, pode modificar autonomamente os seus parâmetros de funcionamento ou comportamento [15].

Esta definição é crucial, ao adicionar os novos requisitos de monitorização e limites de decisão, obriga a que a evolução da inteligência da máquina nunca ultrapasse os limites de segurança validados inicialmente.

Proteção contra a corrupção e cibersegurança

O regulamento não introduz uma definição formal de cibersegurança, mas incorpora nos seus artigos e anexos conceitos relacionados com a proteção contra a corrupção acidental ou intencional de funções de segurança. Esta terminologia, ausente da Diretiva, e introduzida no regulamento, reflete a necessidade de abordar as vulnerabilidades introduzidas pela conectividade das máquinas às redes industriais.

Implicações práticas

A introdução de definições especificas para software de segurança, proteção contra a corrupção e sistemas de aprendizagem autónoma, terá impacto direto nos fabricantes, ao introduzir a obrigatoriedade de identificação explícita destes elementos na documentação técnica. Este processo exige mais rigor na fase de conceção, ao haver a necessidade de distinguir claramente o *software* que desempenha funções de segurança de software auxiliar sem impacto na segurança.

Para os sistemas de aprendizagem autónoma, a definição agora imposta no regulamento cria os requisitos necessários para a validação dos dados de treino do modelo e monitorização pós-colocação no mercado [15].

3. Requisitos essenciais de segurança e saúde

Os requisitos essenciais de segurança e saúde (RESS) estabelecidos na Diretiva 2006/42/Ce permanecem conceptualmente inalterados no Regulamento (UE) 2023/1230 [15, 21].

A metodologia de 3 etapas para a redução de riscos, de igual forma, não apresenta alterações, mantendo a sua validade como princípio orientador de conceção segura. Os requisitos para sistemas de comando, proteções e dispositivos de proteção, e outros riscos específicos, preservam a sua estrutura e conteúdo essencial.

3.1. Inovações nos requisitos gerais

Cibersegurança e integridade – requisito 1.1.9

O Regulamento (UE) 2023/1230 introduz um novo requisito essencial no ponto 1.1.9 do anexo III, dedicado à proteção de máquinas contra a corrupção acidental ou intencional das suas funções de segurança [15, Anexo III].

Este requisito estabelece que as máquinas devem ser concebidas e fabricadas de modo que [15]:

- O acesso a funções de segurança seja protegido contra acessos não autorizados;
- As interfaces de comunicação não comprometam a integridade das funções de segurança;
- Ser possível recolher dados quando ocorre uma "intervenção legitima ou ilegítima" de ligação ou acesso a software.

O requisito 1.1.9 vem estabelecer pela primeira vez a obrigatoriedade de consideração da cibersegurança como parte integrante da segurança das máquinas.

Software de segurança - Requisitos específicos

A diretiva 2006/42/CE não estabelecia requisitos específicos para software de segurança, referindo apenas, no Anexo I ponto 1.2.1, que uma falha no "suporte lógico (programação)" não poderia originar "situações perigosas", sem especificar metodologias para o desenvolvimento, validação ou gestão de software [21, Anexo I]. O regulamento vem introduzir requisitos específicos para o software de segurança, presentes no anexo III do regulamento [15, Anexo III].

Sistemas de aprendizagem autónoma

O regulamento veio estabelecer requisitos específicos para máquinas equipadas com sistemas de aprendizagem autónoma que tenham impacto em funções de segurança. O requisito 1.1.6 do anexo III impõe que o comportamento da máquina deve ser previsível, quando atuado por sistemas autoevolutivos [15, Anexo III]. O novo regulamento classifica estas máquinas de alto risco, exigindo que a sua validação seja feita por organismos notificados.

Interação homem-máquina

O regulamento traz uma mudança de paradigma face à diretiva relativamente à interação homem-máquina. A Diretiva focava-se em impedir o acesso a zonas de perigo, enquanto o regulamento reconhece a interação-homem máquina e a necessidade de adaptar a prevenção de riscos, sem que dependam totalmente do isolamento físico, desde que a segurança seja garantida [15, Anexo III].

O requisito 1.1.6 do Anexo III do regulamento [15] inclui a prevenção de tensão psíquica que pode resultar da interação homem-máquina e de sistemas autónomos ou parcialmente autónomos. Este requisito obriga o fabricante a considerar na avaliação de risco a considerar não apenas o dano físico, mas também o stress cognitivo e a ansiedade que a proximidade de uma máquina autónoma pode causar ao operador humano.

O regulamento introduz requisitos específicos para máquinas móveis autónomas, ao estabelecer que estas máquinas devem cumprir as funções de deslocação de forma segura, exigindo capacidade técnica para detetar pessoas ou obstáculos na sua trajetória e imobilizar-se autonomamente para evitar colisões [15].

4. Procedimentos para a avaliação de conformidade

Uma vez definidos os requisitos essenciais de saúde e segurança que as máquinas devem cumprir, é necessário estabelecer o processo de demonstração e validação de conformidade antes das máquinas serem colocadas no mercado. Na Diretiva, a escolha de um procedimento de avaliação dependia essencialmente de a máquina constar ou não na lista de equipamentos perigosos do Anexo IV e da aplicação de normas harmonizadas [22]. O regulamento altera esta lógica no artigo 25º, ao introduzir novos critérios de classificação de risco mais rigorosos e ao limitar a autonomia dos fabricantes na validação da conformidade [15].

O artigo 25º estabelece um sistema escalonado de avaliação de conformidade, estruturado em função da nova divisão das máquinas de alto risco, listadas no Anexo I, que se encontra separado em duas partes distintas, A e B.

Para a categoria de máquinas listadas na Parte A do Anexo I, onde são incluídos os novos sistemas de aprendizagem automática, o regulamento determina que o risco associado é demasiado elevado para permitir o processo de autoavaliação. Assim, é imposta a intervenção de um organismo notificado, em que o fabricante deve optar por um dos seguintes procedimentos [15]:

- “Exame UE de tipo (módulo B) estabelecido no anexo VII, seguido de conformidade com o tipo baseada no controlo interno da produção (módulo C) previsto no anexo VIII;”
- “Conformidade baseada na garantia de qualidade total (módulo H) prevista no anexo IX;”
- “Conformidade baseada na verificação por unidade (módulo G) prevista no anexo X.”

Para as máquinas listadas na Parte B do Anexo I, o regulamento mantém a via flexível de seguir as normas harmonizadas, ao realizar o controlo interno de produção, Modulo A. Se a máquina ou produto não tiver sido desenvolvida e fabricada seguindo essas normas, ou estas não abranjam todos os requisitos essenciais, o fabricante deve optar por um dos seguintes procedimentos [15]:

- “Exame UE de tipo (módulo B) previsto no anexo VII, seguido de conformidade com o tipo baseada no controlo interno da produção (módulo C) previsto no anexo VIII;”
- “Conformidade baseada na garantia de qualidade total (módulo H) previsto no anexo IX;”

- "Conformidade baseada na verificação por unidade (módulo G) previsto no anexo X."

Para todas as máquinas não listadas no Anexo I, o fabricante mantém a possibilidade de aplicar o controlo interno de produção Módulo A, assumindo a total responsabilidade pela conformidade [15].

Comparação Diretiva-Regulamento

Quando comparada a Diretiva [21, Artigo 12º] com o Regulamento [15, Artigo 25º], é possível verificar um mais rígido controlo sobre a conformidade.

A maior diferença apresenta-se no tratamento das máquinas de maior risco, enunciadas na parte A do anexo I do regulamento. A Diretiva permitia que um fabricante de uma máquina que estivesse listada no Anexo IV evitasse a intervenção de um Organismo Notificado desde que concebesse a máquina em total conformidade com as normas harmonizadas, permitindo assim a autoavaliação para qualquer máquina [22]. O Regulamento põe fim a esta possibilidade para as máquinas listadas na Parte A do Anexo I, ao determinar legislativamente que certos riscos exigem validação externa independente, mesmo que existam normas harmonizadas [15].

5. Marcação CE

A marcação CE, definida no regulamento como "marcação através da qual o fabricante indica que uma máquina ou um produto conexo cumpre os requisitos aplicáveis estabelecidos na legislação de harmonização da União que prevê a sua aposição" [15], e representa o passo final da avaliação de conformidade ao sinalizar visualmente ao mercado e às autoridades que são cumpridos integralmente os requisitos.

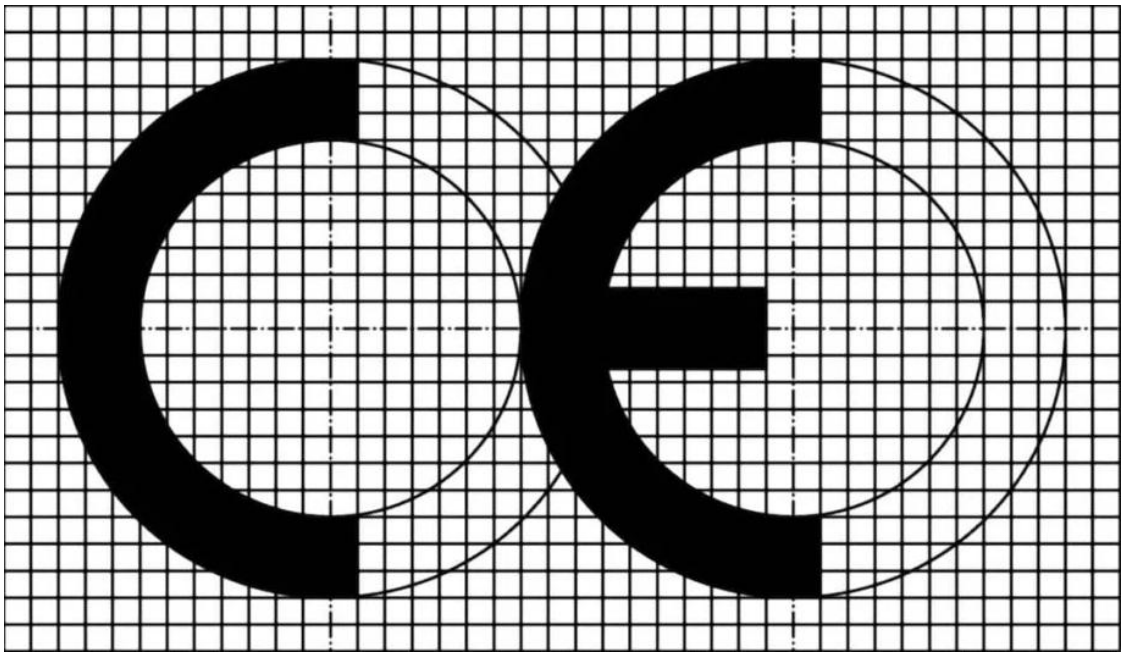


Figura 3 - Marcação CE [27, Anexo III]

A marcação CE (Figura 3) segue os princípios gerais estabelecidos no Regulamento (CE) nº 756/2008. O grafismo da marcação mantem-se inalterado, devendo a marca ser colocada na

máquina de forma "visível, legível e indelével", próximo ao nome do fabricante. Na Figura 3 encontra-se a simbologia representativa da Marcação CE.

Para que seja colocada a Marcação CE numa máquina, é necessária a elaboração de documentação técnica. A Parte "A" do Anexo IV do Regulamento, impõe que o processo técnico deverá conter, pelo menos, os seguintes elementos que se encontram resumidos na Tabela 1 [15]:

Tabela 1 - Elementos para a Marcação CE

Categoria	Finalidade na conformidade	Exemplos de evidência
Identificação do equipamento e âmbito	Clarificar o que foi avaliado e para que utilização foi concebido	Descrição funcional, limites operacionais, variantes/modelos, utilização prevista e usos razoavelmente previsíveis
Demonstração de gestão do risco	Evidenciar que os perigos foram identificados e reduzidos de forma justificada	Registo do processo de avaliação de risco; medidas de redução de risco; justificação de risco residual
Dossier de engenharia (arquitetura e conceção)	Permitir compreender a solução técnica e como as funções se articulam	Desenhos de conjunto; diagramas elétricos/pneumáticos; arquitetura do sistema de comando; descrição de funcionamento
Referenciais técnicos usados	Mostrar como se suportou tecnicamente a conformidade (com ou sem normas harmonizadas)	Lista de normas aplicadas e partes relevantes; requisitos internos; critérios de aceitação; especificações alternativas
Evidência de verificação/validação	Comprovar que a solução funciona e cumpre requisitos de segurança	Relatórios de ensaios; inspeções; resultados de cálculos; registos de validação de requisitos de segurança
Controlo de fabrico e repetibilidade	Garantir que a produção mantém o nível de conformidade da conceção	Plano de controlo; procedimentos de fabrico/inspeção; rastreabilidade; gestão de alterações
Informação ao utilizador e declarações	Assegurar instalação/uso/manutenção segura e a documentação declarativa aplicável	Manual; avisos; instruções de montagem; declarações UE aplicáveis (quando existam)
Software e funcionalidades avançadas (quando aplicável)	Permitir auditoria técnica quando a segurança depende de software/dados/sensores	Gestão de versões; descrição da lógica de segurança; evidência de testes; elementos técnicos a disponibilizar à autoridade quando necessário

6. Relatório de conformidade

O artigo 21º do Regulamento, "Declaração UE de conformidade" [15], vem substituir a antiga "Declaração CE de conformidade" [22]. Esta alteração não é apenas semântica, representa uma simplificação administrativa, ao possibilitar que quando uma máquina está sujeita a múltiplos atos da união Europeia, o fabricante pode emitir um único documento que agrega todas as conformidades, reduzindo a dispersão documental.

Segundo o Anexo V, a declaração UE de conformidade deve conter as informações que se encontram resumidas na Tabela 2 [15].

Tabela 2 - Declaração UE de Conformidade

Informação Necessária	Conteúdo a incluir
Identificação e rastreabilidade	Identificação inequívoca da máquina/produto conexo (tipo/modelo e identificadores como lote/n.º de série), incluindo casos de alteração substancial quando aplicável.
Entidade responsável	Nome e endereço do fabricante e, quando exista, do mandatário.
Local de instalação	Para determinadas máquinas de elevação instaladas permanentemente, indicação do local onde são montadas/instaladas.
Declaração de responsabilidade	Declaração de que a conformidade é assumida sob responsabilidade do fabricante.
Base legal de conformidade	Identificação da legislação de harmonização da União com a qual se declara conformidade.
Referenciais técnicos usados	Referência às normas harmonizadas e/ou especificações comuns utilizadas (incluindo datas de publicação relevantes) e, se aplicável, indicação de aplicação parcial.
Avaliação de conformidade (quando aplicável)	Identificação do organismo notificado (nome/número) e do(s) módulo(s) aplicados, quando a via de avaliação de conformidade o exigir.
Formalidades finais	Local e data de emissão, identificação de quem assina (nome/cargo) e assinatura.

7. Síntese

A transição da Diretiva 2006/42/CE para o Regulamento (UE) 2023/1230 vem responder às ambiguidades anteriormente identificadas, ao contemplar os novos riscos associados à dimensão digital.

A Tabela 3, resume as principais alterações estruturais e técnicas identificadas ao longo deste capítulo.

Tabela 3 - Comparação Diretiva Regulamento

Aspeto	Diretiva 2006/42/CE	Regulamento (UE) 2023/1230
Natureza Jurídica	Exige transposição para lei nacional de cada Estado Membro, podendo gerar divergências interpretativas.	Aplicação direta e imediata em todos os Estados-Membros, garantindo uniformidade total no mercado único
Máquinas de Alto risco	Anexo IV: Permite a autoavaliação para todas as máquinas, desde que fossem cumpridas as normas harmonizadas.	Anexo I (Parte A): Torna obrigatória a certificação por organismo certificado para máquinas críticas
Cibersegurança	Não abordada explicitamente, focando-se apenas na segurança funcional.	O Requisito Essencial 1.1.9 introduz a proteção contra a “corrupção” (acidental ou intencional) do software.
Inteligência artificial	Sem referência explicita	Tratada como “sistemas autoevolutivos", com regras específicas para quando desempenham funções de segurança, exigindo monitorização.
Software de segurança	Considerado como parte integrante do sistema de comando, sem estatuto de produto independente.	Definido como componente de segurança no Anexo II.
Documentação	Exigida em formato de papel	Instruções e Declarações permitidas em formato digital. Exigência do código fonte ou lógica programada no dossier técnico.
Alteração Substancial	Conceito não definido legalmente	Definição legal no Art. 3º, clarificando quando é que uma modificação obriga a uma nova marcação CE
Operadores Económicos	Foco quase exclusivo nas obrigações do fabricante	Define obrigações claras e distintas para importadores e distribuidores.

2.5. Tecnologias de segurança

A implementação de funções de segurança em sistemas automatizados exige um conjunto de equipamentos base que assegurem a deteção de condições perigosas, o processamento da lógica de segurança e a atuação sobre o sistema que está a ser controlado. Neste grupo incluem-se dispositivos como botões de paragem de emergência, relés e controladores de segurança, módulos de entradas e saídas seguras, interbloqueios, sensores de proteção e interfaces homem-máquina.

2.5.1. Tecnologias somuns

Independentemente do tipo de aplicação industrial, a implementação de funções de segurança exige a integração de dispositivos de deteção, lógica de controlo e elementos de atuação destinados a colocar a máquina ou o sistema robotizado num estado seguro sempre que seja detetada uma condição perigosa [29].

Neste contexto, destacam-se como tecnologias de segurança comuns a paragem de emergência, o rearme após atuação de funções de segurança, os relés e PLCs de segurança, os dispositivos de interbloqueio, as cortinas de luz e os tapetes de segurança.

Entre os dispositivos mais elementares e difundidos destaca-se a paragem de emergência (E-Stop), cuja função consiste em permitir a interrupção rápida de um movimento perigoso ou de uma situação de risco quando ocorre uma anomalia ou emergência. A sua função não substitui outras medidas de proteção, mas constitui uma medida complementar que deve estar acessível, ser claramente identificável e exigir reposição manual após atuação, conforme os princípios definidos pela EN ISO 13850 [30].

No domínio da lógica de comando, os relés de segurança e os PLC de segurança desempenham um papel central na implementação das funções de segurança. Os relés de segurança são habitualmente utilizados em arquiteturas simples e dedicadas, como circuitos de paragem de emergência ou monitorização de portas com interbloqueio, enquanto os PLC de segurança oferecem maior flexibilidade, capacidade de diagnóstico, tratamento de múltiplas entradas e escalabilidade para células com maior complexidade funcional. Esta distinção é particularmente relevante na engenharia de segurança, uma vez que a evolução para sistemas mais integrados e reconfiguráveis tem vindo a favorecer a utilização de controladores de segurança programáveis. A importância destes dispositivos deve ser entendida no enquadramento mais amplo das partes dos sistemas de comando relacionadas com a segurança, cujo desempenho deve ser concebido e validado de acordo com princípios de fiabilidade, comportamento em caso de falha e nível de desempenho requerido. A ISO 13849-1 estabelece precisamente os requisitos para a conceção e integração dessas partes do sistema de comando, incluindo hardware e software, constituindo uma referência essencial para a validação de funções de segurança em máquinas [29].

Outro grupo de tecnologias amplamente utilizado corresponde aos interbloqueios de segurança, que impedem o funcionamento da máquina quando uma porta, resguardo ou acesso de proteção se encontra aberto ou numa condição insegura. Estes dispositivos são

particularmente importantes porque asseguram que o acesso à zona perigosa fica condicionado ao estado seguro da máquina, integrando-se frequentemente com relés ou PLC de segurança para monitorização do circuito e gestão da reposição [31].

As cortinas de luz de segurança constituem igualmente uma solução de uso transversal na proteção de acessos perigosos, permitindo a deteção de intrusão sem necessidade de barreira física permanente. A sua principal vantagem reside na proteção de zonas de acesso frequente, preservando simultaneamente a produtividade e a ergonomia da operação, embora a sua seleção dependa sempre da avaliação de risco, da distância de segurança e do nível de desempenho exigido para a função [32].

Em complemento, os tapetes de segurança e os botões de reset desempenham funções específicas dentro da arquitetura de proteção. Os tapetes permitem detetar a presença de uma pessoa numa zona perigosa através da atuação por pressão, enquanto os botões de reset asseguram que o rearme de uma função de segurança só ocorre após verificação deliberada das condições de segurança pelo operador, evitando reinícios inesperados. Embora sejam tecnologias conceptualmente simples, a sua eficácia depende da correta integração no circuito de segurança e da coerência com a estratégia global de redução de risco [29, 33].

Por fim, as interfaces HMI podem desempenhar um papel complementar na segurança, sobretudo ao nível da visualização de estados, alarmes, diagnósticos e seleção de modos de funcionamento. Ainda que a HMI não constitua, em regra, uma função de segurança autónoma, a sua conceção influência a interação homem-máquina e pode contribuir para reduzir erros operacionais, melhorar a rastreabilidade de eventos e apoiar o restabelecimento seguro da operação após uma paragem ou falha. [29]

2.5.2. Tecnologias para robótica industrial

Na robótica industrial convencional, a estratégia de segurança assenta maioritariamente na separação física entre o operador e a zona de trabalho do robô, recorrendo a barreiras, dispositivos de deteção e funções de comando relacionadas com a segurança, em conformidade com os princípios estabelecidos pelas normas ISO 10218 e ISO 13849. Ao contrário da robótica colaborativa, o funcionamento normal destas células pressupõe, em regra, que o acesso humano à área perigosa é impedido ou rigidamente controlado durante a execução automática do ciclo [34].

Entre as medidas mais comuns destaca-se a vedação física da célula robotizada, composta por resguardos fixos, painéis perimetrais e portas de acesso, cuja função é impedir o contacto com movimentos perigosos, zonas de esmagamento ou elementos em deslocação rápida. Esta solução continua a ser uma das formas mais robustas de redução do risco em aplicações industriais de elevada energia, sobretudo quando a velocidade, a força e a imprevisibilidade do movimento inviabilizam a partilha direta do espaço com o operador [32].

As portas com interbloqueio e os sistemas de interbloqueio com bloqueio desempenham um papel central no controlo de acessos a células robotizadas. Estes dispositivos garantem que a abertura de um acesso protegido provoca a paragem da máquina ou impede o arranque,

enquanto o bloqueio adicional assegura que a porta permanece fechada até cessar o movimento perigoso ou até estarem reunidas condições seguras para a entrada. Em contexto robotizado, esta solução é particularmente relevante quando existem tempos de paragem significativos, riscos residuais após comando de stop ou movimentos com elevada inércia [31].

As cortinas de luz de segurança constituem outra tecnologia amplamente utilizada em robótica industrial, sobretudo em zonas onde existe necessidade de acesso frequente a materiais, ferramentas ou postos de operação. A sua principal vantagem reside na deteção sem contacto da intrusão numa área protegida, permitindo salvaguardar a segurança sem recorrer necessariamente a uma barreira física contínua. A seleção entre diferentes tipos ou classes de cortinas deve, contudo, resultar da avaliação de risco, atendendo ao nível de integridade exigido, ao tempo de resposta do sistema e à distância mínima de segurança [35].

Em operações manuais específicas, como alimentação de prensas, dispositivos de corte ou determinados ciclos semiautomáticos integrados em células robotizadas, podem ainda ser utilizados comandos bimanuais. O princípio funcional desta solução assenta na necessidade de atuação simultânea com ambas as mãos, reduzindo a probabilidade de o operador colocar os membros superiores na zona perigosa durante o arranque ou a execução de um movimento crítico [36].

Nas células robotizadas é também frequente a utilização de chaves seletoras de modo, que permitem distinguir entre modos de funcionamento como automático, manual, ajuste, ensino ou manutenção. Esta separação é essencial para garantir que as condições de segurança aplicáveis variam de acordo com a operação em curso, limitando, por exemplo, velocidades, movimentos ou permissões de arranque durante tarefas de intervenção técnica. Em articulação com estes modos, surgem frequentemente os dispositivos enabling de três posições, que permitem ao operador manter o controlo do movimento apenas enquanto o dispositivo é pressionado na posição intermédia, provocando paragem se for libertado ou pressionado em excesso [37].

Do ponto de vista funcional, estas tecnologias não devem ser entendidas como elementos isolados, mas como componentes de uma arquitetura integrada de segurança. A eficácia da célula robotizada depende da correta combinação entre proteção física, deteção de acesso, lógica de segurança e definição adequada dos modos de operação, em função dos riscos específicos da aplicação. Assim, a robótica industrial continua a basear-se num paradigma de segurança assente na segregação e no controlo rigoroso do acesso, ainda que progressivamente complementado por sistemas de monitorização e comando mais inteligentes [37].

2.5.3. Tecnologias para robótica colaborativa

A robótica colaborativa distingue-se da robótica industrial convencional por admitir a partilha controlada do espaço de trabalho entre pessoa e robô, o que desloca o foco da segurança da simples segregação física para a monitorização contínua da interação. A literatura recente mostra que esta transição exige a integração de sensores, funções seguras no sistema de comando e mecanismos de limitação dinâmica do comportamento do robô [38].

O enquadramento técnico desta interação é normalmente descrito a partir dos modos de operação colaborativa previstos na ISO/TS 15066, nomeadamente *safety-rated monitored stop*, *hand guiding*, *speed and separation monitoring* e *power and force limiting*. Estes modos não constituem tecnologias isoladas, mas antes arquiteturas funcionais que combinam perceção, controlo e resposta segura em função da tarefa e do risco associado [38].

Uma das componentes centrais da segurança colaborativa reside nas funções de segurança integradas nos cobots, que permitem supervisionar velocidade, posição, binário, distância de paragem e outros parâmetros operacionais com impacto direto na segurança. A revisão de Scholz et al. mostra que a segurança em colaboração homem-robô depende crescentemente da articulação entre essas funções internas e sistemas sensoriais distribuídos, instalados no robô, no espaço envolvente ou no próprio operador. Assim, a noção de "robô colaborativo" não resulta apenas da morfologia do manipulador, mas da capacidade do sistema completo para detetar presença humana, ajustar o comportamento e manter a operação dentro de limites validados [38].

O modo de *safety-rated monitored stop* é utilizado quando o robô deve parar de forma controlada assim que uma pessoa entra na zona colaborativa, retomando a operação apenas quando as condições seguras forem restabelecidas. Esta abordagem continua a ser relevante em aplicações em que existe partilha sequencial do espaço, mas não contacto físico simultâneo entre operador e robô [38].

O *hand guiding* permite que o operador conduza diretamente o robô em tarefas de ensino, ajuste ou posicionamento, sendo normalmente combinado com limitação de velocidade e dispositivos de validação da intenção humana. A literatura identifica este modo como particularmente útil em ambientes flexíveis e operações de programação intuitiva, mas sublinha que a sua segurança depende da correta configuração do sistema e da validação da interface física de guiamento [38].

Entre as tecnologias mais relevantes na prática colaborativa destaca-se o *speed and separation monitoring* (SSM), que ajusta a velocidade do robô em função da distância relativamente ao operador. Segundo a revisão sistemática de Scholz et al., este é o modo de operação mais frequentemente identificado nos sistemas sensorizados de segurança para colaboração homem-robô. O mesmo estudo mostra ainda que, na última década, se verificou um crescimento claro de soluções baseadas em sensores como LiDAR, câmaras stereo /profundidade, sensores capacitivos, laser scanners e combinações multissensoriais [38].

No plano tecnológico, os scanners laser de segurança e os sensores LiDAR assumem particular relevância porque permitem detetar a aproximação humana e definir zonas de aviso e de perigo configuráveis em torno do robô. A literatura mais recente sobre sensores externos para deteção humana em ambientes colaborativos confirma que estes dispositivos continuam a ser dos mais utilizados para suportar estratégias de SSM, devido à sua maturidade industrial e à facilidade de integração em células robotizadas. Contudo, os mesmos trabalhos também salientam limitações importantes, como zonas de sombra, sensibilidade à geometria do espaço, necessidade de calibração cuidada e dificuldade em lidar com cenários muito dinâmicos ou com múltiplos operadores [38].

As tecnologias de visão, incluindo câmaras RGB-D, stereo e sistemas de perceção baseados em profundidade, têm igualmente ganho relevância por permitirem uma interpretação mais rica da postura e do movimento humano. A revisão sobre sistemas de segurança baseados em visão para colaboração homem-robô mostra que estas soluções oferecem maior informação contextual do que sensores binários de presença, sendo adequadas para estimar trajetórias, prever aproximações e suportar estratégias adaptativas de segurança. No entanto, a literatura também identifica fragilidades ao nível da robustez a oclusões, iluminação variável, complexidade computacional e validação em tempo real para funções críticas de segurança [39].

Outra tecnologia essencial é o power and force limiting (PFL), cuja lógica consiste em garantir que, mesmo em caso de contacto, a energia transferida pelo robô se mantém dentro de limites aceitáveis para o corpo humano. A literatura científica sublinha, porém, que esta estratégia não pode ser reduzida à simples escolha de um cobot intrinsecamente seguro, uma vez que o risco final depende também da ferramenta, da peça manipulada, da massa em movimento, da rigidez do sistema e da região anatómica exposta. Por essa razão, a validação do contacto seguro permanece um dos domínios mais exigentes da segurança colaborativa [40].

A investigação mais recente aponta ainda para uma tendência de integração multissensorial, ao combinar LiDAR com câmaras stereo, LiDAR com sensores capacitivos, ou laser scanners com outras formas de perceção de proximidade. Esta evolução é relevante porque procura ultrapassar as limitações de cada sensor individual e aumentar a fiabilidade da deteção humana em ambientes industriais reais [41].

3. Métodos e Aplicação

O presente capítulo descreve a metodologia adotada para traduzir os requisitos do novo Regulamento Máquinas em critérios de conceção, integração e validação no contexto da automação industrial, com aplicação em células robóticas industriais e colaborativas. O capítulo apresenta a definição do método de desenvolvimento e conformidade, bem como a análise de risco e a implementação das funções de segurança.

Numa primeira fase, estabelece-se a base metodológica que orienta a identificação de perigos, a definição das funções de segurança e a seleção das tecnologias de proteção mais adequadas a cada caso. Esta abordagem é aplicada a dois casos de estudo, um de robótica industrial tradicional e um de robótica colaborativa, que compara as exigências técnicas, funcionais e documentais associadas à conformidade.

3.1. Metodologia de desenvolvimento e conformidade

A metodologia adotada nesta dissertação estabelece a ligação entre o enquadramento jurídico do Regulamento Máquinas, os referenciais normativos aplicáveis à segurança funcional e à implementação prática de medidas de proteção em células robotizadas. A abordagem segue uma sequência sistemática que permite passar da identificação dos perigos à definição, implementação, verificação e validação das funções de segurança aplicáveis a cada arquitetura.

Esta metodologia assenta em três princípios fundamentais. O primeiro consiste na delimitação clara do sistema em análise, incluindo os seus modos de operação, fronteiras físicas, interfaces com o operador e condições previsíveis de utilização, manutenção, ajuste e intervenção. O segundo corresponde à identificação estruturada dos perigos e das situações perigosas, tendo em conta o funcionamento automático normal, e os modos de paragem, recuperação, rearme, setup, formação e acesso a zonas perigosas. O terceiro traduz-se na seleção de medidas de redução do risco de acordo com uma lógica hierárquica, privilegiando a conceção intrinsecamente segura, seguida das proteções técnicas e, por fim, da informação para utilização.

Em termos operacionais, a metodologia organiza-se em seis etapas interligadas. A primeira corresponde ao enquadramento regulamentar e normativo aplicável ao sistema. A segunda incide na definição dos limites da célula robotizada. A terceira consiste na identificação dos perigos e na apreciação do risco. A quarta traduz-se na derivação das funções de segurança necessárias. A quinta incide na seleção de tecnologias e arquiteturas adequadas para a

implementação das funções de segurança. A sexta corresponde à verificação e validação das soluções adotadas.

3.2. Avaliação de risco

A avaliação de risco constitui a base metodológica para a definição das medidas de prevenção e proteção aplicáveis a máquinas e células robotizadas. Nesta dissertação, o processo segue a estrutura definida pela ISO 12100, compreendendo a delimitação do sistema, a identificação de perigos, a estimativa e a avaliação dos riscos associados e determinação das medidas necessárias [42].

A delimitação do sistema inclui a função da célula, os modos de operação, as interfaces com o operador, os acessos previsíveis, as condições de utilização normal e as situações de intervenção, ajuste, manutenção e rearme. Esta etapa é essencial para que a apreciação de risco abranja o funcionamento automático, os estados transitórios e as situações de utilização indevida razoavelmente previsíveis [15,42].

A identificação dos perigos abrange, no contexto desta dissertação, os perigos mecânicos, elétricos, funcionais, ergonómicos e os decorrentes da interação homem-máquina. Os cenários com maior relevância são o acesso a zonas perigosas, a intervenção manual, a falha de sensores, o rearme do sistema e a transição entre modos de operação [42].

A estimativa do risco associado a cada situação perigosa tem em conta a severidade potencial do dano, a frequência e duração da exposição e a possibilidade de evitar o perigo ou limitar as suas consequências. Esta análise estabelece uma hierarquia de criticidade entre cenários, e fundamenta tecnicamente a seleção das medidas de redução do risco [42].

Quando o risco estimado não é aceitável, a sua redução segue uma lógica hierárquica. A redução privilegia, em primeiro lugar, as soluções de conceção intrinsecamente segura, em seguida as medidas técnicas de proteção e, por fim, a informação para utilização. Esta hierarquia constitui um princípio central da abordagem normativa à segurança de máquinas [15,42].

O resultado deste processo é um conjunto de requisitos de segurança que servem de base à derivação das funções de segurança a implementar, e assegurar a rastreabilidade entre os perigos identificados e as soluções técnicas

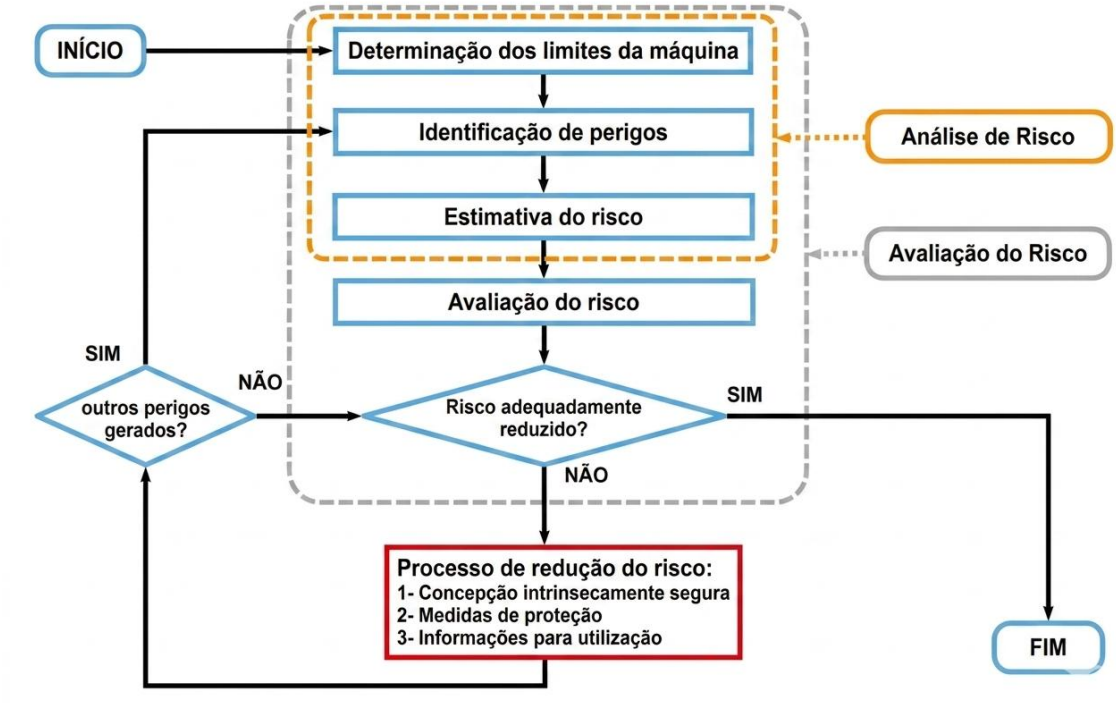


Figura 4 - Avaliação e estimativa risco (adaptado de: [43])

A Figura 4 apresenta o processo para a análise de risco e a avaliação de risco, segundo a ISO 12100.

Para garantir a interpretação uniforme da apreciação de risco, foi adotada uma tabela de classificação (Tabela 4) baseada em critérios qualitativos de severidade, exposição, probabilidade de ocorrência e possibilidade de evitar o perigo. A combinação destes critérios determina o nível de risco inicial e constitui a base para a posterior determinação do PLr das funções de segurança, segundo a ISO 13849-1 [29].

Tabela 4 - Tabela de critérios qualitativos de severidade

Parâmetro	Classe	Descrição
Severidade do dano	S1	Lesão ligeira ou reversível.
	S2	Lesão grave, irreversível ou morte.
Frequência/duração da exposição	F1	Exposição rara ou de curta duração.
	F2	Exposição frequente ou prolongada.
Probabilidade de ocorrência do evento perigoso	O1	Evento perigoso pouco provável.
	O2	Evento perigoso plausível ou expectável.
Possibilidade de evitar o perigo	A1	Possível de evitar em condições favoráveis.
	A2	Dificilmente possível de evitar.

3.3. Implementação de funções de segurança

A implementação de funções de segurança corresponde à fase em que os requisitos de redução de risco, são convertidos em respostas técnicas concretas do sistema. Nesta dissertação, entende-se por função de segurança uma função do sistema de comando ou de um dispositivo associado que atua para impedir a ocorrência de uma situação perigosa ou conduzir a máquina a um estado seguro perante uma condição anómala ou um evento de risco [29].

A definição de cada função de segurança começa pela associação entre perigo identificado, a situação perigosa, a condição de ativação e a resposta esperada do sistema. Para cada função, é necessário explicitar o objetivo de segurança, o estado seguro associado, os elementos que desencadeiam a atuação e o comportamento esperado em condições normais e de falha [29].

Com base nesta definição funcional, determina-se o PLr em função do risco que essa função deve controlar. O PLr constitui um critério de projeto que orienta a seleção da arquitetura, dos componentes e das estratégias de diagnóstico necessárias para garantir um comportamento seguro do sistema. Distingue-se, assim, entre o PLr, definido a partir da apreciação de risco, e o nível de desempenho efetivamente alcançado pela solução implementada [29].

A determinação do PLr segue o procedimento da EN ISO 13849-1, com base nos parâmetros de severidade da lesão (S), frequência e/ou duração da exposição (F) e possibilidade de evitar o perigo ou limitar o dano (P). Para assegurar coerência na aplicação do método, adota-se a classificação apresentada na Tabela 5, que serve de suporte metodológico à seleção do PLr em cada função de segurança [29].

Tabela 5 - Classificação para determinação do PLr [29]

Parâmetro	Classe	Descrição
Severidade da lesão	S1	Lesão ligeira, normalmente reversível.
	S2	Lesão grave, normalmente irreversível, incluindo amputação ou morte.
Frequência e/ou tempo de exposição	F1	Exposição rara a pouco frequente e/ou tempo de exposição curto.
	F2	Exposição frequente a contínua e/ou tempo de exposição longo.
Possibilidade de evitar o perigo ou limitar o dano	P1	Possível sob condições específicas.
	P2	Quase impossível.

A implementação técnica das funções de segurança implica a seleção e integração de dispositivos adequados, a conformidade da solução depende da conformidade individual dos componentes, da coerência funcional da arquitetura adotada e da sua capacidade para manter o estado seguro perante falhas previsíveis. Por esse motivo, a seleção da arquitetura considera interação entre canais, o grau de diagnóstico, a tolerância a falhas e o efeito da falha de um subsistema sobre a resposta segura do conjunto [29].

Depois de definida a solução técnica, procede-se à verificação da correspondência entre os perigos identificados, as funções de segurança especificadas e os meios adotados para a sua implementação. Esta etapa confirma se a função selecionada responde ao risco que pretende controlar e se a arquitetura definida é consistente com os requisitos de desempenho, fiabilidade e comportamento seguro estabelecidos [29].

No âmbito desta dissertação, este enquadramento metodológico serve de base à implementação das funções de segurança nos dois casos de estudo analisados.

3.4. Caso de estudo 1: célula robotizada industrial

O caso de estudo 1 desenvolvido baseia-se numa aplicação de paletização robotizada de fim de linha, composta pelas etapas de alimentação, manipulação, inspeção periódica, e paletização de caixas. A conceção da célula assenta na segregação física entre o operador e os movimentos perigosos do robô.

O fluxo de produto inicia-se com a chegada das caixas através de um transportador até à zona de recolha do robô. O robô, equipado com uma ferramenta de vácuo adequada à manipulação das caixas, recolhe cada caixa e executa o ciclo de paletização. Em funcionamento normal, as caixas são posicionadas diretamente na palete de acordo com o padrão de empilhamento previamente definido no sistema de comando.

Em intervalos periódicos, definidos por parametrização no sistema de operação da célula, uma caixa é colocada pelo robô numa estação intermédia de inspeção. Nesta estação, o operador procede à inspeção visual do estado exterior da embalagem, da integridade do produto e da correta identificação da caixa. Após a inspeção, a caixa é novamente recolhida pelo robô e integrada no ciclo normal, e é depositada na palete de acordo com o padrão em curso. Caso a caixa seja considerada não conforme, o operador retira-a do fluxo e a célula retoma o ciclo.

A palete é posicionada manualmente pelo operador antes do arranque do ciclo. Quando a palete atinge a capacidade prevista, o ciclo é interrompido, o operador remove a palete completa e posiciona uma nova palete vazia, o ciclo é retomado após confirmação das condições necessárias ao arranque.

Para além dos elementos associados à manipulação e paletização, o sistema possui a capacidade de diagnóstico e assistência remota para supervisão, análise de falhas e apoio à manutenção. Embora estas funções não alterem a lógica principal do processo produtivo, introduzem requisitos adicionais de segurança associados à conectividade, os quais devem ser considerados no âmbito do novo Regulamento Máquinas.

3.4.1. Arquitetura e componentes

A célula industrial robotizada é constituída por um conjunto de subsistemas funcionais que asseguram, de forma integrada, a alimentação do produto, a manipulação robotizada, a inspeção periódica por parte do operador e a paletização das caixas. A descrição seguinte identifica os principais componentes da célula e apresenta as características técnicas mais

relevantes para a análise de segurança e implementação das funções de segurança desenvolvidas nas secções subsequentes.

O elemento central da célula é um robô industrial articulado de seis eixos, responsável pela execução de todos os movimentos de recolha, transferência e deposição das caixas ao longo do ciclo automático. Para esta aplicação, considera-se um robô com carga útil compatível com a massa máxima das caixas, e com alcance suficiente para cobrir simultaneamente a zona de recolha, a estação intermédia de inspeção e a zona de paletização.

O robô é comandado pelo seu próprio controlador dedicado, responsável pela gestão das trajetórias, das velocidades e comandos da ferramenta. Este controlador comunica com o PLC da célula, que coordena a lógica global de operação, que inclui o transportador de alimentação, a estação de inspeção e os modos de funcionamento, e comunica com o sistrema de segurança, responsável pela gestão das funções de segurança da célula.

A ferramenta adotada para a manipulação das caixas é uma garra de vácuo, cujo princípio de funcionamento se baseia em gerar pressão negativa através de ventosas em contacto com a face superior de cada caixa. A monitorização do estado de um elemento relevante para a deteção de perda de aderência da carga e para a prevenção de situações suscetíveis de comprometer a segurança e a fiabilidade do ciclo.

A alimentação do produto é assegurada por um transportador de correia, que encaminha as caixas provenientes da linha de produção até à posição de recolha do robô. A interface entre o transportador e o robô é estabelecida por um sensor de presença, que sinaliza a disponibilidade de uma nova caixa na zona de recolha.

Lateralmente à trajetória principal de paletização, foi prevista uma estação intermédia de inspeção visual, acessível ao operador e destinada à sua intervenção periódica. Nesta posição, a caixa é colocada temporariamente pelo robô sempre que o programa determina a realização da inspeção, e é posteriormente reintegrada no ciclo normal ou retirada do processo, consoante o resultado da verificação. A estação é posicionada e dimensionada de forma a garantir uma postura ergonómica adequada ao operador e encontra-se integrada na lógica de controlo da célula, garantindo que a intervenção humana ocorre apenas em condições de segurança previamente definidas.

A zona de paletização corresponde ao espaço onde o robô coloca as caixas na palete, seguindo um padrão de empilhamento previamente definido no sistema de comando. Esta zona apresenta relevância particular do ponto de vista da segurança, em virtude da coexistência entre movimentos do robô, variação geométrica da carga empilhada e necessidade periódica de intervenção humana para substituição da palete.

A contenção de zonas perigosas é assegurada por resguardos perimetrais fixos e por acessos controlados por dispositivos com interbloqueio, destinados a impedir o acesso a zonas de risco enquanto subsistirem movimentos perigosos.

O sistema de comando é constituído pela parte funcional, responsável pela lógica do processo produtivo, e pela parte de segurança, responsável pela monitorização e execução das funções de segurança. Considera-se ainda que o sistema de comando dispõe de capacidade de

diagnostico, supervisão, análise de falhas e apoio à manutenção. Esta funcionalidade introduz uma dimensão de conectividade que deve ser considerada do ponto de vista da segurança, em particular na proteção contra acessos não autorizados, conforme contemplado no novo Regulamento (UE) 2023/1230.

A disposição espacial dos componentes e a implementação das medidas de proteção encontram-se representadas na Figura 5. O layout é meramente ilustrativo, pelo que, as barreiras de proteção físicas seriam em formato de rede, para impedir o acesso de qualquer parte do corpo ao interior da célula.

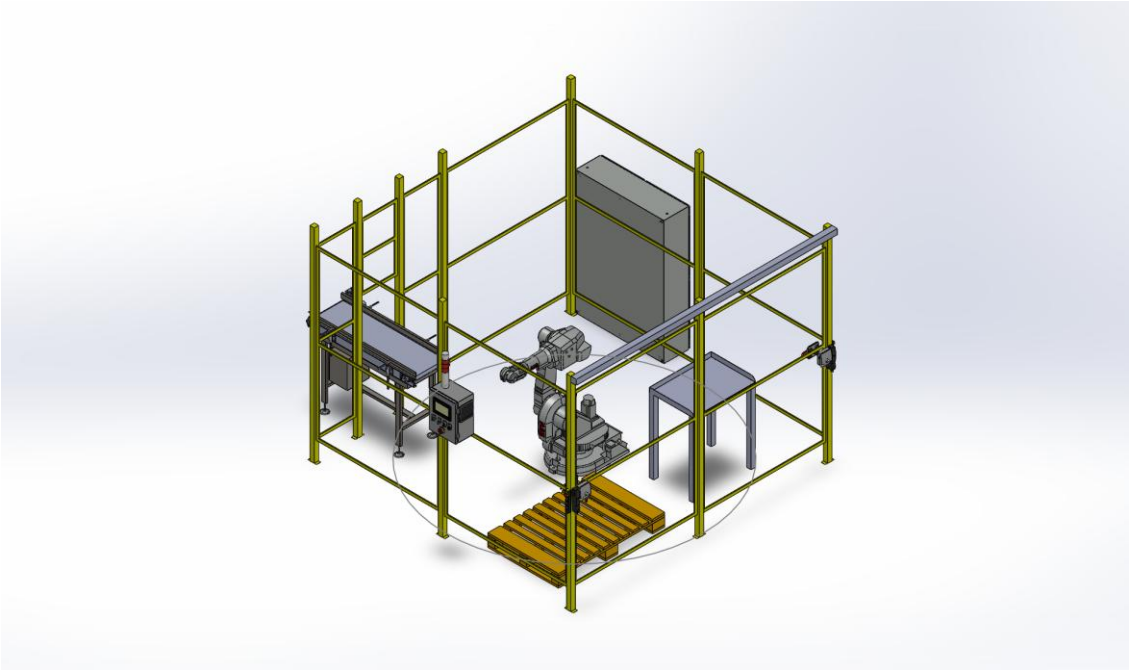


Figura 5 - Layout caso de estudo 1

No Apendice A encontra-se o layout detalhado com dimensões e legenda técnica.

3.4.2. Limites do sistema e zonas perigosas

A definição dos limites do sistema constitui uma etapa essencial da apreciação do risco, uma vez que permite delimitar o âmbito da célula em análise, as condições de utilização consideradas e os contextos em que o operador pode ficar exposto a perigos associados ao funcionamento do sistema. De acordo com a ISO 12100, esta delimitação deve considerar a utilização prevista da máquina, o uso indevido razoavelmente previsível e as diferentes fases do seu ciclo de vida.

No presente caso de estudo, os limites funcionais da célula abrangem o robô industrial, o respetivo controlador, o PLC da célula, o sistema de comando de segurança, a ferramenta de vácuo do robô, o troço do transportador de alimentação associado à entrega da caixa, a estação

intermédia de inspeção, a zona de paletização, a palete e os dispositivos de proteção e acesso. Excluem-se do âmbito os processos a montante da entrega da caixa à célula e as operações logísticas posteriores à remoção da palete, uma vez que esses elementos não interferem diretamente com a arquitetura funcional e de segurança aqui analisada.

Do ponto de vista espacial, os limites da célula correspondem ao perímetro físico definido pelos resguardos perimetrais, pelos acessos controlados e pelo volume de trabalho associado ao robô, à ferramenta e à carga movimentada. Para efeitos de análise de risco deve considerar-se relevante o alcance total do robô na aplicação real, incluindo a ferramenta e a carga.

Do ponto de vista temporal e operacional, os limites da célula incluem o arranque, a produção automática, as paragens normais, as paragens por anomalia, a reposição após falha, as operações de ajuste, a manutenção e as intervenções de limpeza compatíveis com o caso de estudo.

Do ponto de vista da utilização, consideram-se o funcionamento automático da célula, as intervenções periódicas do operador na estação intermédia de inspeção, a remoção manual de caixas não conformes, a substituição da palete completa por uma palete vazia e ainda as situações de programação, ajuste, recuperação e manutenção. Em conformidade com a ISO 12100, estes limites de utilização devem abranger também situações de uso indevido razoavelmente previsíveis, como a tentativa de acesso ao interior da célula para remoção de uma caixa, ou a retoma do funcionamento sem a reposição integral das condições de segurança.

A identificação das zonas perigosas decorre diretamente desta delimitação. A célula é assim divida em zonas e domínios de análise que permitem localizar com maior precisão os perigos associados ao transportador, à recolha da caixa, ao movimento do robô, à estação de inspeção, à zona da palete, ao acesso do operador e ao acesso remoto ou alteração de parâmetros.

Em síntese, a célula em estudo é delimitada por fronteiras funcionais, espaciais, operacionais e lógicas que permitem identificar os contextos em que o operador pode ficar exposto a movimentos perigosos e a situações suscetíveis de originar lesão. A explicitação destes limites constitui a base para a identificação dos perigos, para a estimativa do risco e para a definição das funções de segurança aplicadas à célula.

3.4.3. Modos de operação e interação com o operador

O funcionamento da célula do caso de estudo é descrito a partir dos seus modos de operação e das situações em que ocorre interação com o operador. Para o presente caso de estudo, consideram-se o modo automático, o modo manual ou de setup, o modo de manutenção ou recuperação e a condição de acesso remoto para supervisão e assistência técnica.

No modo automático, a célula executa o ciclo normal de produção, constituído pela alimentação das caixas, pela sua recolha pelo robô e deposição na zona de paletização ou, quando aplicável, na estação intermédia de inspeção. Neste modo, o sistema opera com base no programa previamente definido e o acesso do operador à zona protegida da célula não é permitida enquanto existirem movimentos perigosos. A interação com o operador ocorre sempre a partir do exterior da célula.

O modo manual destina-se a operações de ajuste, ensaio, programação, recuperação de falhas e verificação do comportamento da célula. A utilização deste modo impõe restrições acrescidas, nomeadamente a redução segura da velocidade, e exige que o movimento do robô ocorra apenas através de dispositivos de comando por ação continuada, utilizados por pessoal autorizado.

O modo de manutenção ou recuperação foca-se na resolução de anomalias, reposição de condições operacionais e execução de intervenções técnicas específicas. A sua consideração autónoma é útil para a análise de risco, uma vez que concentra tarefas menos frequentes, mas potencialmente críticas, em que o operador ou técnico pode ficar exposto a zonas perigosas em condições distintas das do funcionamento automático.

Para além destes modos, a célula permite acesso remoto associado a funções de supervisão, diagnostico e apoio à manutenção. Esta capacidade permite ao fabricante aceder ao sistema para analisar falhas ou atualizar parâmetros funcionais. No entanto, o acesso remoto introduz perigos específicos de cibersegurança que devem ser previstos na avaliação de risco, e exige controlo de autenticação, segregação de permissões e protecção da integridade das funções de segurança da máquina.

No caso em estudo, a interação do operador com a célula ocorre em quatro momentos principais:

1. A remoção da palete completa e inserção da palete vazia;
2. A solicitação de acesso à estação intermédia para inspeção visual periódica;
3. A remoção de caixas não conformes;
4. As ações de reposição e rearme do sistema após uma paragem ou anomalia.

Do ponto de vista operacional, estas interações possuem naturezas distintas. A inspeção visual e a substituição de paletes fazem parte do funcionamento previsto do sistema. Em contrapartida, as intervenções de ajuste, programação, recuperação ou manutenção, ocorrem apenas em condições ocasionais e implicam a transição para modos de funcionamento específicos.

A caracterização dos modos de operação e das formas de interação com o operador constitui uma base necessária para a definição dos limites da célula e para a identificação das situações em que pode ocorrer exposição a perigos mecânicos, funcionais ou operacionais. Está distinção será utilizada na secção seguinte para delimitar as zonas perigosas de operação, os acessos e os contextos de intervenção humana.

3.4.4. Identificação de perigos

A identificação de perigos constitui uma etapa central da apreciação de risco, uma vez que permite reconhecer, de forma sistemática, as fontes de potencial dano associadas à utilização da célula robotiza, às suas condições de operação e às intervenções humanas previsíveis ao longo do ciclo de vida. De acordo com a ISO 12100, esta etapa deve ser realizada após a definição dos limites do sistema e deve abranger não apenas a utilização prevista, mas também

situações de uso indevido razoavelmente previsível, incluindo comportamentos humanos expectáveis em contexto industrial.

No presente caso de estudo, a identificação dos perigos incide sobre as condições de funcionamento automático, as intervenções periódicas de inspeção, as operações de reposição, as trocas de palete e as atividades de ajuste e manutenção, bem como a existência de conectividade remota.

Os perigos foram estruturados em função das oito zonas físicas e lógicas da célula, o que permite associar de forma direta as fontes de perigo (mecânicas, elétricas, de comando ou de cibersegurança) aos contextos exatos de exposição do operador.

Na zona do transportador e na zona de recolha, predominam os perigos de natureza mecânica, nomeadamente o arrastamento, o pinçamento e o entalamento nos elementos móveis e na interface de recolha. A zona de movimento do robô concentra os perigos de impacto e esmagamento mais severos, bem como o perigo de queda de carga provocado por perda de vácuo ou falha na ferramenta durante a trajetória.

As zonas de maior interação humana, como a estação de inspeção e a zona da palete, partilham perigos críticos associados à presença intencional do operador no interior do espaço protegido. Nesses contextos, a exposição prolongada, combinada com o risco de arranque inesperado ou de retoma do funcionamento sem confirmação visual do exterior, assume elevada gravidade. A zona de acesso do operador está diretamente ligada aos perigos de falha de contenção e falha do sistema de comando na libertação do interbloqueio antes da paragem total.

Ao nível das infraestruturas de suporte, o quadro elétrico introduz perigos de choque elétrico e eletrocussão durante intervenções de diagnóstico e manutenção. O sistema de comando global acarreta perigos funcionais devido a eventuais falhas lógicas, perda de comunicação ou perdas de sincronização entre o PLC e o controlador do robô.

Por fim, a zona lógica de acesso remoto introduz perigos associados à conectividade nomeadamente a alteração indevida de parâmetros, a modificação indevida de software de segurança ou uma atuação incompatível com o estado físico da célula constituem perigos críticos no âmbito da cibersegurança industrial.

A Tabela 6 sintetiza os principais perigos e situações perigosas identificadas para o caso de estudo 1, constituindo a base para a etapa seguinte de estimativa e avaliação de risco.

Tabela 6 - Zonas perigosas caso de estudo 1

Zona / Elemento	Perigo	Situação perigosa	Possível consequência	Observações
Zona do transportador	Arrastamento / pinçamento	Aproximação à correia em movimento contínuo	Lesão nos membros	Acesso ao tapete sem inibição de marcha
Zona de recolha (Pick)	Entalamento	Intervenção manual para soltar caixa bloqueada na interface transportador-robô	Lesão grave	Risco associado ao movimento da garra e à recolha da carga
Zona de movimento do robô	Impacto / esmagamento	Presença humana no interior da célula durante o ciclo automático	Lesão muito grave ou fatal	Decorrente de falha de hardware ou de acesso indevido por cima da vedação
Zona de movimento do robô	Queda de carga	Perda de vácuo durante a trajetória com a caixa suspensa	Impacto contuso e perturbação do ciclo	A gravidade depende da massa da embalagem e da velocidade
Estação de inspeção	Exposição a movimento perigoso	Abertura da porta de acesso à estação sem a confirmação de paragem segura total	Impacto ou aprisionamento	Requer interbloqueio com retenção
Estação de inspeção	Exposição por permanência	Permanência do operador junto à estação enquanto ocorre tentativa externa de retoma de ciclo	Lesão muito grave ou fatal	A retoma exige rearme com visibilidade do exterior
Zona de paletização	Esmagamento / impacto	Intervenção para troca de palete com arranque inesperado por reset inadequado	Lesão muito grave ou fatal	Associado a comandos imprevistos ou lógicas erradas
Zona de paletização	Perigo ergonómico	Movimentação, remoção e colocação da palete vazia em posturas incorretas	Perturbações musculoesqueléticas	Perigo de caráter não mecânico da máquina

Tabela 6 - Zonas perigosas caso de estudo 1 (cont.)

Zona / Elemento	Perigo	Situação perigosa	Possível consequência	Observações
Zona de acesso (Vedação / Porta)	Falha de contenção	Acesso inadvertido por porta interbloqueada em falha	Exposição imediata ao perigo contínuo	A segregação física deve manter-se eficaz em todas as condições previsíveis
Acesso remoto (Cibersegurança)	Alteração indevida de software	Modificação remota do F-program (software de segurança) ou de parâmetros sem controlo local	Comportamento imprevisível; anulação de funções de proteção	Risco mitigado por autenticação robusta e controlo de permissões
Acesso remoto (Cibersegurança)	Perda de integridade da comunicação	Interrupção ou manipulação da ligação remota durante intervenção activa no sistema	Ausência de rastreabilidade; estado indeterminado do sistema	Requer registo auditável de todas as intervenções remotas
Infraestrutura (Comando)	Movimento não previsto	Comando manual local (modo de setup) com visibilidade incompleta ou excesso de velocidade	Impacto e esmagamento	Requer restrições de movimento e dispositivo de ação continuada
Infraestrutura (Quadro elétrico)	Choque elétrico	Intervenção técnica no quadro elétrico não isolado	Eletrocussão	Requer procedimento LOTO

3.4.5. Avaliação de risco

Com base nos perigos identificados e na delimitação funcional e espacial da célula, a Tabela 7 apresenta a avaliação de risco inicial para o caso de estudo 1, com base nos parâmetros definidos na Tabela 4, assumindo a ausência de medidas de segurança dedicadas. Está classificação constitui a base para a definição das medidas de redução de risco e para a determinação do PLr das funções de segurança.

Tabela 7 - Avaliação de risco caso de estudo 1

Ref.	Zona	Situação Perigosa	S	F	O	A	Risco Inicial	Justificação
R1	Zona do transportador	Aproximação a elementos móveis na interface de alimentação contínua	S1	F1	O1	A1	Médio	O acesso tangencial acarreta risco de pinçamento
R2	Zona de movimento	Perda de vácuo e queda da carga durante a trajetória rápida do robô	S1	F1	O1	A1	Médio	Risco concentrado junto aos limites da vedação.
R3	Estação de inspeção	Entrada do operador para inspeção sem paragem segura plenamente estabelecida	S2	F2	O2	A2	Muito elevado	A exposição aos eixos do robô em movimento rápido gera risco iminente de impacto grave.
R4	Estação de inspeção	Permanência do operador no interior durante tentativa externa de retoma de ciclo	S2	F1	O2	A2	Muito elevado	A prevenção de rearranque inesperado é crítica quando o operador perde a visibilidade global.
R5	Zona de paletização	Intervenção manual para substituição de palete com arranque ou movimento inesperado	S2	F1	O2	A2	Elevado	O manuseamento de carga pesada com o robô em prontidão gera risco de esmagamento.
R6	Zona de acesso	Abertura da porta interbloqueada antes da imobilização completa do sistema	S2	F1	O2	A2	Muito elevado	O encravamento físico deve garantir a segregação total até dissipação da energia cinética.
R7	Zona de acesso	Rearme de segurança efetuado sem confirmação da ausência de pessoas no interior	S2	F1	O2	A2	Muito elevado	O rearme manual tem de ocorrer a partir de uma posição exterior segura com visibilidade total.
R8	Acesso remoto	Alteração remota indevida de parâmetros ou software de segurança	S2	F1	O1	A2	Elevado	Pode anular funções críticas sem o conhecimento da equipa local; exige rastreabilidade e chave física.

3.4.6. Funções de segurança implementadas

As funções de segurança implementadas no caso de estudo 1 resultam diretamente da avaliação de risco anteriormente desenvolvida e visam reduzir os riscos identificados, em conformidade com a lógica de redução do risco preconizada pela ISO 12100.

A Tabela 8 sintetiza a relação entre as situações perigosas avaliadas (R1 a R8) e as medidas e funções de segurança adotadas para a sua mitigação.

A análise da Tabela 8 evidencia que a redução do risco assenta numa combinação entre medidas físicas de segregação, funções de segurança ativas no sistema de comando e medidas complementares de utilização. Com base nesta sistematização, descrevem-se de seguida as funções de segurança implementadas, indicando-se para cada uma o seu objetivo, a condição de ativação e a ação de segurança esperada e as condições de rearme e arranque.

Tabela 8 - Situações perigosas e medidas adotadas

Referencia de Risco	Solução adotada / Medida de redução do risco	Função de segurança adotada
R3, R6	Vedação perimetral fixa e acesso exclusivo por porta com interbloqueio.	FS2 – Interbloqueio da porta de acesso FS5 – Paragem segura associada ao acesso
R4, R5, R7	Lógica de bloqueio de rearranque no interior e rearme manual no exterior, fora da zona perigosa.	FS3 – Prevenção de arranque inesperado FS4 – Rearme seguro
R2	Monitorização de pressão do sistema pneumático de vácuo	FS7 – Monitorização do estado de vácuo
R1	Barreiras físicas tangenciais e paragem do tapete em caso de perda da condição de segurança.	FS8 – Paragem segura do transportador
R3, R5	O ciclo apenas avança se as lógicas de proteção estiverem integralmente verificadas.	FS6 – Permissão de arranque seguro
Geral	Botões de paragem de emergência em posições de rápido alcance na periferia e na HMI.	FS1 – Paragem de emergência
R8	Controlo estrito de acesso à rede de automação mediante autenticação e bloqueio físico local (chave).	Medida de segregação e Controlo de Acesso Remoto
Geral	Isolamento e bloqueio de fontes de energia.	Medida complementar (Procedimento LOTO)

FS1 – Paragem de emergência

A função de paragem de emergência tem como objetivo interromper de forma imediata o funcionamento do sistema perante uma situação de perigo identificada pelo operador ou por outro interveniente. No caso de estudo, a atuação desta função deve provocar a paragem imediata de todos os movimentos perigosos da célula.

Do ponto de vista da implementação, atuação da paragem de emergência provoca a desabilitação segura do binário do robô e a paragem segura do transportador. Esta função

possui prioridade absoluta sobre todos os comandos restantes, e o simples desbloqueio mecânico do atuador não pode originar o reinício automático do sistema.

A Figura 6 ilustra a sequência de atuação da FS1, em que, após o acionamento da paragem de emergência, é removida a energia do robô e do transportador, e o sistema apenas retoma o funcionamento após o rearme manual.

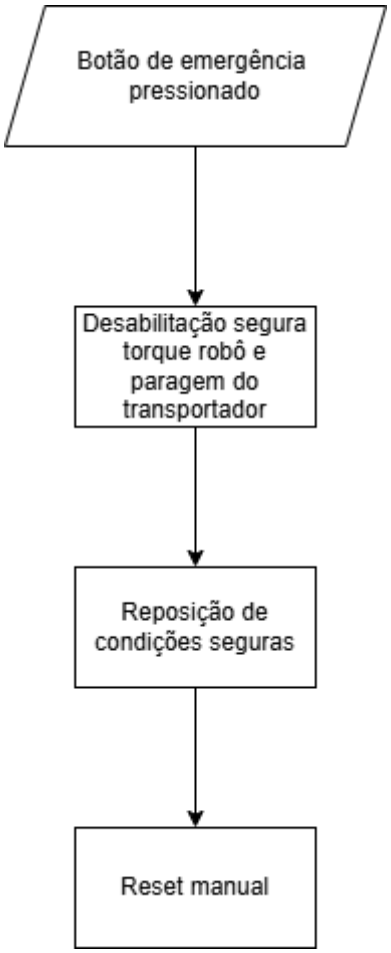


Figura 6 - Fluxograma atuação FS1

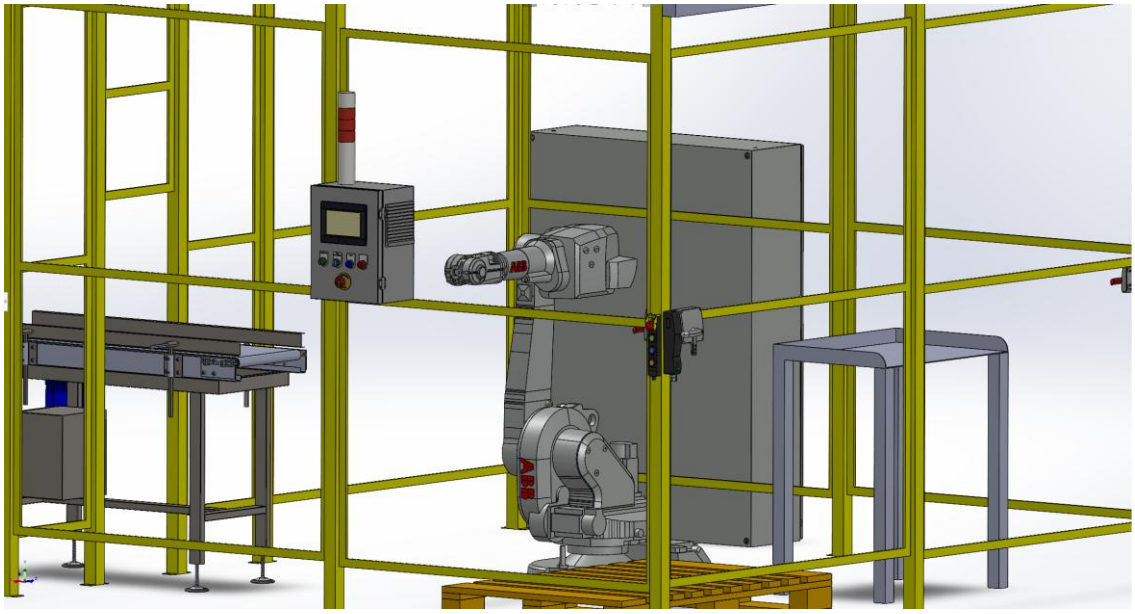


Figura 7 - Localização FS1 – Quadro de controlo

O sistema possui uma botoneira de emergência no painel de controlo e nos comandos de pedido de acesso ao interior da célula, junto de cada porta (Figura 7 e Figura 8)

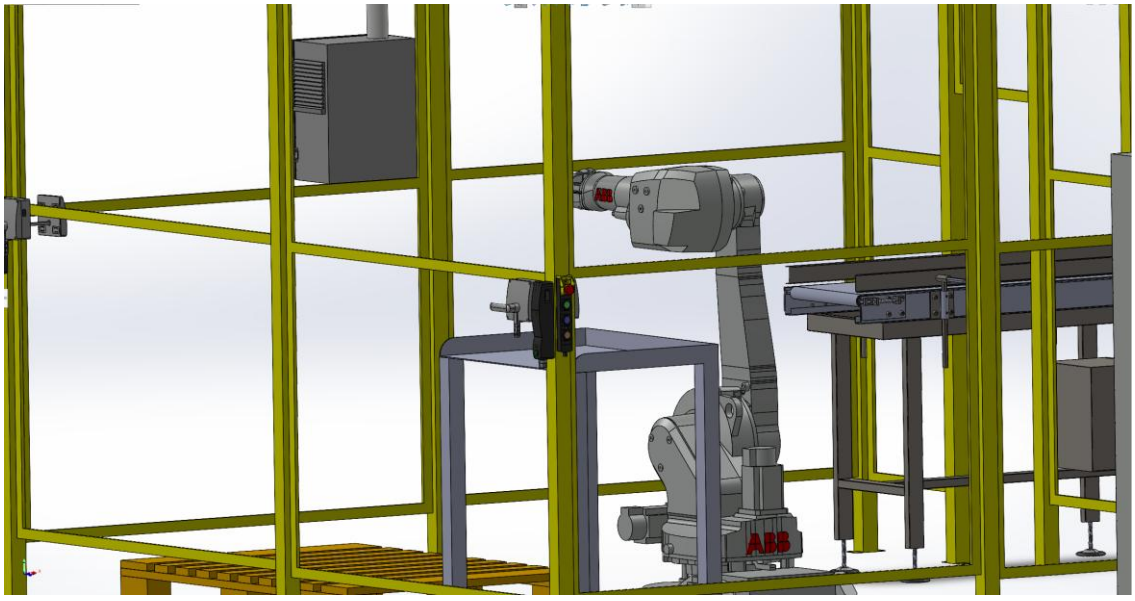


Figura 8 - Localização FS1 – Junto ao interbloqueio

FS2 – Interbloqueio da porta de acesso

O interbloqueio da porta de acesso destina-se a impedir a abertura da porta enquanto existirem movimentos perigosos no interior da célula. Durante o ciclo, o acesso permanece bloqueado. Quando o operador solicita o acesso, a porta apenas é destrancada após a paragem confirmada

e segura de todos os atuadores, de modo a garantir que o acesso à estação de inspeção ou à zona da palete ocorre sem risco.

A Figura 9 ilustra a sequência de atuação da FS2, em que, após o pedido de abertura de porta, o sistema verifica a existência de movimentos por parte do robô, remove a energia perigosa do robô e do transportador, e apenas quando isto é garantido, destranca a porta.

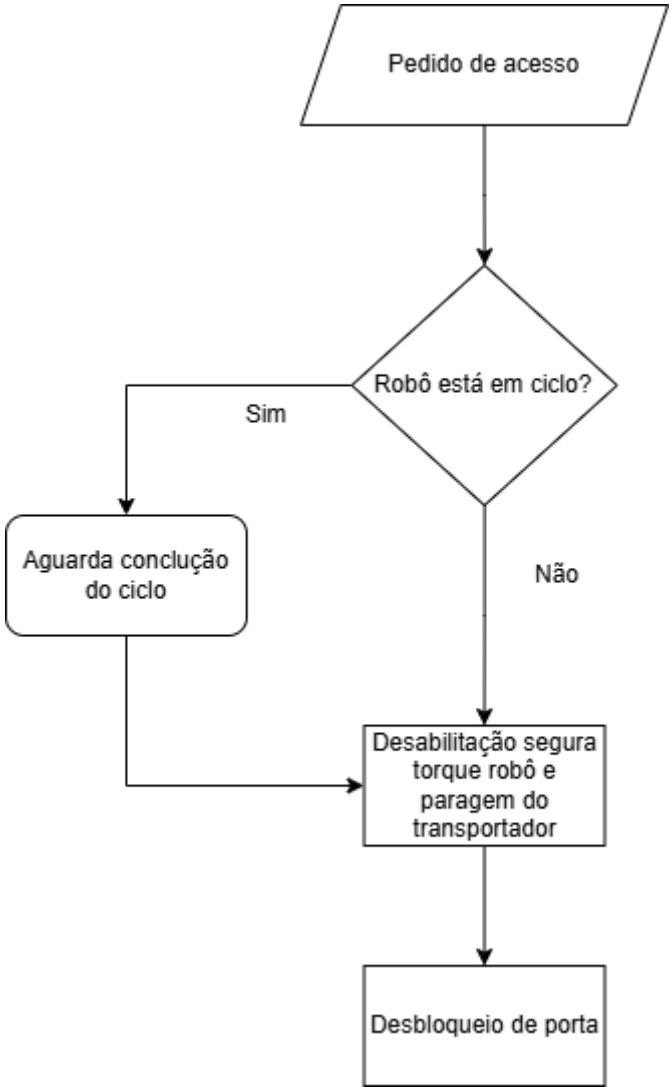


Figura 9 - Fluxograma de atuação FS2

A Figura 10 representa o interbloqueio presente em ambas as portas, bem como o botão de pedido de acesso, representado a laranja.

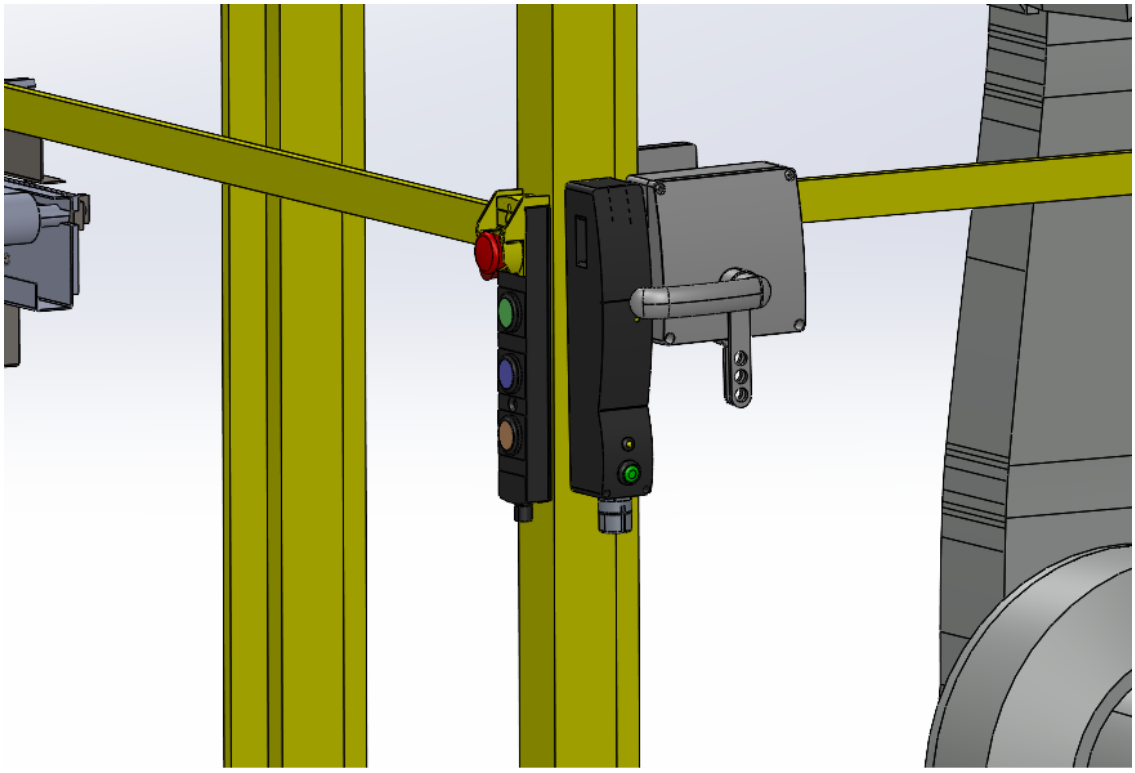


Figura 10 - Localização FS2

FS3 – Prevenção de arranque inesperado

A prevenção de arranque inesperado tem como objetivo impedir que a célula retome de forma automática o funcionamento após uma paragem de segurança, abertura de porta ou o restabelecimento da alimentação. O sistema mantém o ciclo inibido mesmo após a normalização dos sinais físicos dos sensores, ao exigir uma ação deliberada de rearme seguida de um comando de arranque.

FS4 – Rearme Seguro

O rearme seguro assegura que o rearme da célula após uma paragem de segurança ocorre de forma manual, intencional e segura. O botão de rearme encontra-se localizado no exterior da célula, com visibilidade para o interior. A sua ativação apenas valida que o sistema de segurança está pronto. O arranque do processo fica dependente de um comando distinto.

O sistema possui um botão de rearme no painel central de controlo e um botão de rearme no comando de controlo de cada porta de acesso, representados a azul (Figura 10 e Figura 11).

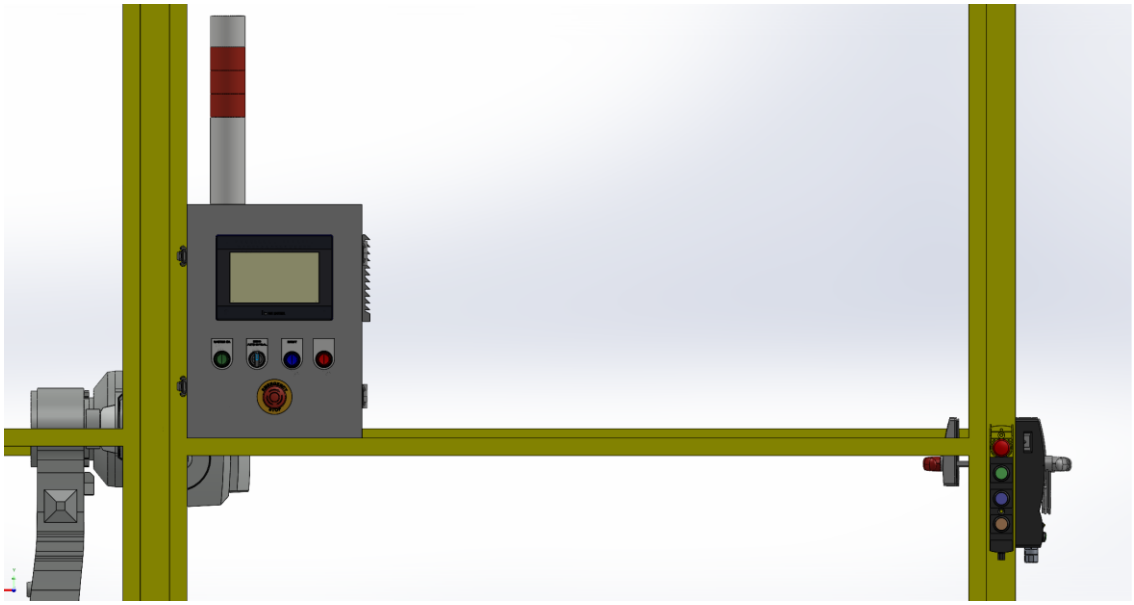


Figura 11 - Localização FS4

FS5 – Paragem segura associada ao acesso

A paragem segura associada ao acesso atua em coordenação com a FS2. Sempre que ocorre um pedido formal de acesso ou a abertura forçada de uma proteção interbloqueada, a FS5 coloca o sistema num estado seguro. No controlador do robô, esta função é materializada através das funções de paragem segura, que garantem a travagem controlada e a remoção segura do binário dos motores.

FS6 – Permissão de arranque seguro

A permissão de arranque seguro assegura que o ciclo automático apenas se pode iniciar ou retomar quando todas as condições de segurança estiverem satisfeitas. Esta função atua como verificação integradora do estado global da célula. Na prática, impede que o PLC autorize a sequencia automática enquanto qualquer condição de segurança se mantenha inválida. A existência desta função de segurança permite estruturar o comportamento global da célula em torno de permissões claras e rastreáveis, e evitar ambiguidades entre “máquina pronta” e “máquina segura para arrancar”.

FS7 – Monitorização do estado de vácuo

A monitorização do estado de vácuo está associada ao risco de perda de vácuo e consequente queda de carga durante o transporte da caixa pelo robô. Quando ocorre, o sistema deve inibir a continuação da trajetória, gerar um alarme e colocar o processo em estado seguro ou controlado.

FS8 – Paragem segura do transportador

A paragem segura do transportador visa eliminar o movimento perigoso do transportador de alimentação sempre que as condições de segurança da célula deixem de estar asseguradas. O

seu rearranque deve ficar condicionado às mesmas regras gerais aplicáveis à célula, nomeadamente reposição das condições de segurança e validação pelo sistema.

Medidas complementares de manutenção

Para além das medidas apresentadas anteriormente, o caso de estudo considera a necessidade de medidas específicas para manutenção, assistência técnica e outras intervenções prolongadas no interior da célula. Nestes contextos, a paragem segura assegurada pelo sistema de comando não substitui a necessidade de isolamento e bloqueio das fontes de energia perigosas. Assim, deve ser prevista a existência de procedimentos de LOTO aplicáveis à alimentação elétrica.

3.4.7. Determinação do PLr

Após a definição das funções de segurança, procede-se à determinação do PLr para cada uma das funções, de acordo com o gráfico de risco, previsto na ISO 13849-1. Os parâmetros de classificação utilizados nesta etapa encontram-se na Tabela 5.

A Tabela 9 sintetiza o PLr atribuído a cada função de segurança, mantendo-se a numeração e designação funcional, de modo a assegurar a rastreabilidade entre a avaliação de risco, a definição funcional das medidas de segurança e a subsequente conceção da arquitetura de segurança e controlo.

Tabela 9 - Determinação PLr caso de estudo 1

FS	Designação da função de segurança	S	F	P	PLr	Justificação
FS1	Paragem de emergência	S2	F1	P2	d	A função destina-se a reagir a situações de perigo iminente com potencial de lesão grave ou fatal (S2). A sua atuação é solicitada apenas em situações excecionais de emergência, pelo que a exposição é pouco frequente (F1). Perante um evento de emergência com o sistema em movimento, a capacidade de evitar o dano sem a atuação desta função é praticamente nula (P2). A combinação S2/F1/P2 determina o PLr d.
FS2	Interbloqueio da porta de acesso	S2	F1	P2	d	O acesso expõe o operador ao espaço de movimento do robô, com elevada severidade e reduzida possibilidade de evitamento caso subsistam movimentos perigosos (S2). O acesso ocorre de forma pontual (F1). Uma vez no interior com o robô em movimento, a velocidade e inércia do manipulador tornam o evitamento do contacto dificilmente possível (P2). A combinação S2/F1/P2 determina o PLr d.

Tabela 9 - Determinação PLr caso de estudo 1 (cont.)

FS	Designação da função de segurança	S	F	P	PLr	Justificação
FS3	Prevenção de arranque inesperado	S2	F1	P2	d	Um arranque inesperado com o operador no interior da célula pode originar lesão grave ou fatal (S2). O evento é pouco frequente, ocorrendo apenas após paragem de segurança, abertura de porta ou restabelecimento de alimentação (F1). Perante um arranque súbito e não sinalizado, o operador não dispõe de tempo de reacção suficiente para se afastar da zona perigosa (P2). A combinação S2/F1/P2 determina o PLr d.
FS4	Rearme Seguro	S2	F1	P2	d	Um rearme inadequado pode conduzir a retoma do funcionamento em condições perigosas (S2). O evento é pouco frequente, ocorre apenas após paragem de segurança, abertura de porta ou restabelecimento de alimentação (F1). Perante um arranque súbito, o operador não dispõe de tempo de reação suficiente para se afastar da zona perigosa (P2). A combinação S2/F1/P2 determina o PLr d.
FS5	Paragem segura associada ao acesso	S2	F1	P2	d	Esta função está diretamente associada à proteção do operador durante o acesso ao interior da célula, onde a falha pode resultar em contacto com movimentos perigosos e lesão grave ou fatal (S2). A exposição ocorre de forma pontual, em cada operação de acesso (F1). Com o robô em movimento no interior da célula, é difícil de evitar o contacto (P2). A combinação S2/F1/P2 determina o PLr d.
FS6	Permissão de arranque seguro	S2	F1	P2	d	O arranque só pode ocorrer quando todas as condições de segurança estiverem validadas. Uma falha nesta função pode originar movimento perigoso com presença humana e consequências graves ou fatais (S2). A função atua em cada ciclo de arranque, mas a exposição a condições perigosas é pouco frequente (F1). Se o ciclo se iniciar com uma condição de segurança inválida não detetada, o operador não tem meios de antecipar ou evitar o perigo (P2). A combinação S2/F1/P2 determina o PLr d.
FS7	Monitorização do estado de vácuo	S1	F1	P1	b	A função destina-se a mitigar o risco associado à perda de vácuo e eventual queda de carga, num cenário de severidade moderada com lesão ligeira ou reversível (S1). A ocorrência é pouco frequente, dependente de falha do sistema pneumático (F1). A queda de carga ocorre ao longo de uma trajetória definida dentro da zona limitada (P1). A combinação S1/F1/P1 determina o PLr b.

Tabela 9 - Determinação PLr caso de estudo 1 (cont.)

FS	Designação da função de segurança	S	F	P	PLr	Justificação
FS8	Paragem segura do transportado	S1	F1	P1	b	O risco principal está associado a entalamento ou arrastamento localizado na interface do transportador, com potencial de lesão ligeira ou moderada (S1). A exposição ocorre de forma pouco frequente, em situações de intervenção técnica junto ao transportador (F1). A velocidade reduzida do transportador e a visibilidade da zona permitem ao operador, em condições normais, afastar-se antes de ocorrer contacto (P1)

Da análise da Tabela 9 conclui-se que as funções de segurança centrais para a proteção contra os perigos mecânicos da célula segregada, nomeadamente FS2 a FS6, requerem um PLr d. Por outro lado, as funções associadas à interface de transporte (FS8) e à falha da ferramenta (FS7) mitigam riscos consideravelmente inferiores, necessitando apenas de um PLr b. Desta forma, a arquitetura de segurança do caso de estudo 1 assenta numa topologia redundante e devidamente monitorizada, estabelecido pela ISO 13849-1 para o PLr d, de modo a garantir a execução fiável das funções de interbloqueio, paragem e prevenção de arranque inesperado.

3.4.8. Arquitetura de segurança e controlo

A arquitetura de segurança e controlo da célula tem como objetivo materializar as sequencias operacionais e as funções de segurança previamente definidas, de modo a assegurar a segregação adequada entre a lógica de processo e a lógica de segurança. De modo a atender à exigência de PLr d para as funções críticas, e em conformidade com a EN ISO 13849-1, a conceção desta arquitetura adota uma topologia baseada na redundância de canais e na monitorização continua de diagnóstico.

A arquitetura baseia-se num sistema de controlo integrado, composto por um PLC integrado de segurança do tipo S7-1200F. Internamente, o PLC possui uma arquitetura que assegura a execução segregada do programa funcional e do programa de segurança, em partições de memória independentes e com ciclos de varrimento isolados.

O sistema divide-se em quatro blocos principais: entradas funcionais, entradas de segurança, lógica de controlo e saídas funcionais e seguras. Esta separação permite distinguir claramente os sinais associados ao processo produtivo daqueles que intervêm diretamente na redução do risco.

O PLC é o núcleo de processamento do sistema e comunica com os módulos periféricos e com o controlador do robô através de um barramento industrial de campo partilhado, Profinet. Para assegurar a integridade dos sinais de segurança trocados entre os equipamentos, utiliza-se um protocolo de comunicação segura, ProfiSafe, sobrejacente à rede primária. O controlador do robô processa internamente as trajetórias e o movimento, mas encontra-se subordinado às

permissões emitidas pelo PLC, bem como pelo estado global do sistema pelo estado global do sistema definido pela lógica funcional.

O HMI e o módulo de acesso remoto comunicam com o PLC de controlo, para efeitos de parametrização, diagnostico e consulta de estados. O acesso remoto é condicionado por um seletor de chave física, de modo a garantir que a habilitação do acesso apenas ocorre em condições locais autorizadas e sem risco de movimentos inesperados.

As entradas funcionais, como os sensores de presença de caixas no transportador ou de confirmação de palete, são ligadas diretamente aos módulos de entradas e saídas standard do PLC. As entradas de segurança incluem os botões de paragem de emergência, os interbloqueios das portas de acesso e os botões de rearme manual, sendo avaliadas em duplo canal para permitir a deteção de falhas.

As saídas funcionais comandam os sinalizadores luminosos, o funcionamento do transportador e da ferramenta de vácuo. As saídas de segurança, controladas pela parte de segurança do PLC garantem o estado seguro da máquina perante uma falha ou pedido de acesso.

O router de acesso remoto encontra-se fisicamente ligado ao switch da rede de controlo, permitindo aos técnicos aceder à programação do PLC. A lógica de segurança impede que sinais forçados via rede anulem o estado das portas ou das paragens de emergência, de modo a garantir que o sistema não inicia movimentos sem supervisão local.

A Figura 12 apresenta de forma esquemática a arquitetura de segurança e controlo.

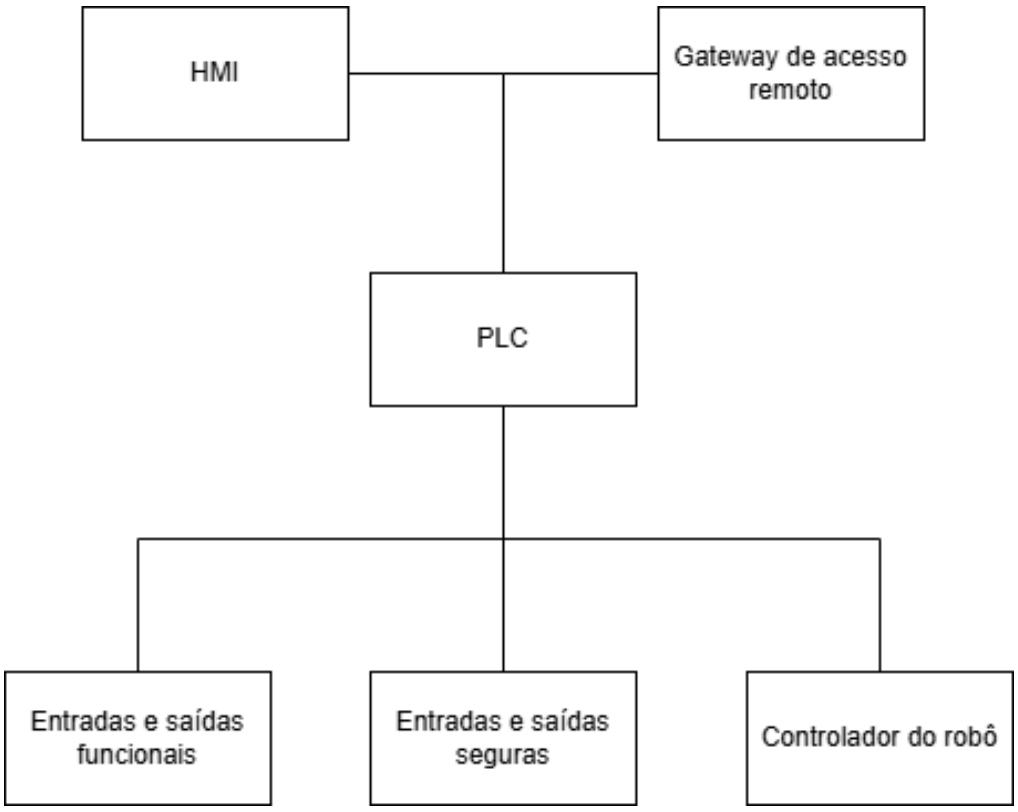


Figura 12 - Arquitetura de segurança e controlo

A Tabela 10 apresenta a matriz de causa–efeito das funções de segurança da célula. O seu objetivo é sintetizar, de forma clara e rastreável, a relação entre os sinais de entrada com impacto na segurança e a resposta segura esperada do sistema de comando.

Tabela 10 - Matriz causa-efeito caso de estudo 1

Causa	Robô (corte de binário)	Transportador (corte do comando de marcha)	Inibição do modo automático	Sinalização de falha (alarme)	Ação necessária para retomar
Botoneira de emergência ativada	●	●	●	●	Desbloqueio e rearme
Porta inertbloqueada aberta	●	●	●	●	Fechar a porta e rearme
Perda do estado de vácuo	Paragem controlada		●	●	Rearme

3.4.9. Implementação funcional do sistema de controlo

A implementação funcional do sistema de controlo da célula assenta na definição estruturada dos sinais de entrada e saída necessários ao processamento da sequência automática, à supervisão de estados do sistema, à interação com o robô e à implementação das funções de segurança. Em coerência com a arquitetura anterior, os sinais são organizados em dois grupos, os sinais funcionais, associados à lógica de processo, e os sinais de segurança, associados às funções de segurança. Esta separação permite distinguir de forma clara a lógica responsável pela execução da produção da lógica responsável pela prevenção de situações perigosas, assegurando que o comportamento da célula permanece previsível, rastreável e compatível com os requisitos de segurança estabelecidos.

A Tabela 11 apresenta os principais sinais de controlo.

Tabela 11 - Sinais de controlo caso de estudo 1

Endereço	Tipo	Sinal	Descrição
I0.0	Entrada digital	Sensor de caixa em posição de recolha	Confirma que a caixa está disponível para recolha pelo robô
I0.1	Entrada digital	Sensor de presença de palete	Confirma a presença da palete na posição de trabalho
I0.2	Entrada digital	Robô pronto	Indica disponibilidade do robô para executar a sequência
I0.3	Entrada digital	Robô em ciclo	Indica que o robô está em execução
I0.4	Entrada digital	Robô em falha	Indica ocorrência de falha no controlador do robô
I0.5	Entrada digital	Ciclo robô concluído	Confirma a conclusão da tarefa solicitada
I0.6	Entrada digital	Modo automático	Seletor modo automático
I0.7	Entrada digital	Modo manual	Seletor modo manual
I1.0	Entrada digital	Estado de vácuo	Monitorização do estado de vácuo
I1.1	Entrada digital	Botão de Start	Comando de arranque do modo automático
I1.2	Entrada digital	Botão de Stop	Comando de paragem do modo automático
I1.3	Entrada digital	Botão de pedido de acesso à célula	Comando de pedido de acesso ao interior da célula
M10.0	Bit Interno	Confirmação operador — caixa OK	Regista, via HMI, que a caixa foi aprovada após inspeção
M10.1	Bit interno	Confirmação operador — caixa NOK	Regista, via HMI, que a caixa foi rejeitada após inspeção
Q0.0	Saída digital	Marcha do transportador	Comanda o funcionamento do transportador
Q0.1	Saída digital	Pedido de pick ao robô	Solicita recolha da caixa
Q0.2	Saída digital	Pedido de deposição em palete	Solicita deposição da caixa na palete
Q0.3	Saída digital	Pedido de deposição na estação intermédia	Solicita deposição da caixa na estação de inspeção
Q0.4	Saída digital	Pedido de recolha da estação intermédia	Solicita recolha da caixa após inspeção
Q0.5	Saída digital	Comando de vácuo	Ativa/desativa a ferramenta de preensão
Q0.6	Saída digital	Torre luminosa verde	Indica funcionamento normal
Q0.7	Saída digital	Torre luminosa amarela	Indica espera por intervenção / inspeção
Q1.0	Saída digital	Torre luminosa vermelha / alarme	Indica falha ou paragem

A Tabela 12 apresenta os sinais de segurança.

Tabela 12 - Sinais de segurança caso de estudo 1

Endereço	Tipo	Sinal	Função associada
F-I1.0	Entrada segura	E-stop canal A	FS1 — Paragem de emergência
F-I1.1	Entrada segura	E-stop canal B	FS1 — Paragem de emergência
F-I1.2	Entrada segura	Interbloqueio porta canal A	FS2 — Interbloqueio da porta (palete)
F-I1.3	Entrada segura	Interbloqueio porta canal B	FS2 — Interbloqueio da porta (palete)
F-I1.4	Entrada segura	Interbloqueio porta canal A	FS2 — Interbloqueio da porta (estação de inspeção)
F-I1.5	Entrada segura	Interbloqueio porta canal B	FS2 — Interbloqueio da porta (estação de inspeção)
F-I1.6	Entrada segura	Botão de reset manual	FS4 — Reset seguro
F-Q1.0	Saída segura	Desabilitação segura do torque do robô	Paragem segura do robô
F-Q1.1	Saída segura	Corte de energia do transportador	Paragem segura do transportador

Máquina de estados

A lógica sequencial de processo é controlada pelo PLC através de uma máquina de estados de alto nível, estruturada em torno dos modos de funcionamento da célula. Esta organização garante que as transições operacionais ocorrem de forma rigorosa e que o arranque, a produção, as paragens e a recuperação de falhas obedecem a regras claramente definidas.

A máquina de estados divide-se em 5 macro estados, conforme ilustrado na Figura 13.

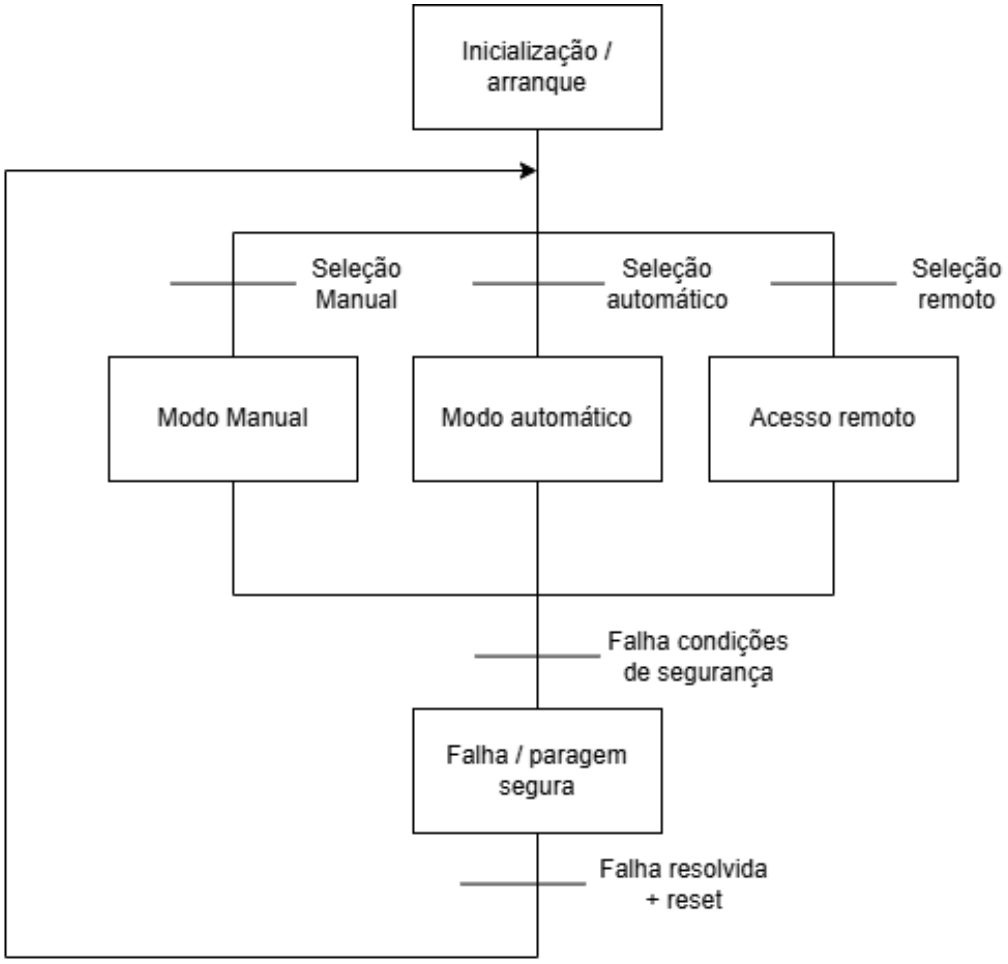


Figura 13 - Máquina de estados caso de estudo 1

O estado de arranque e rearme corresponde à fase de preparação da máquina após energização ou após uma paragem de segurança. Nesta fase, o PLC verifica a ausência de alarmes de processo, a integridade das funções de segurança e o estado dos atuadores. A máquina permanece bloqueada até que o operador efetue o reconhecimento das falhas e valide o rearme manual. Após a validação, o sistema autoriza a seleção de um modo operacional.

O estado automático representa o funcionamento contínuo e autónomo da célula. A entrada neste estado requer a validação de todas as condições iniciais, incluindo a presença de palete, a disponibilidade do robô, a inexistência de falhas ativas e a confirmação do estado seguro da célula. Dentro deste estado, a lógica funcional executa 3 sequencias cíclicas.

Na sequência de alimentação, o transportador é ativado para encaminhar as caixas até à zona de recolha do robô. Quando o sensor de presença deteta uma caixa disponível, o PLC emite o pedido de recolha ao robô.

Na sequência de transferência e paletização, o robô recolhe a caixa, mantém a preensão com base na confirmação do vácuo e deposita-a na palete, ou na estação intermédia, quando determinado pela lógica de inspeção.

Na sequência de inspeção intermédia, ativada periodicamente com base num temporizador definido previamente pelo operador no HMI, o PLC ordena ao robô que deposite a caixa na estação de inspeção. Após a intervenção do operador, este regista o resultado da inspeção através da confirmação OK ou NOK. Em caso de OK, o PLC ordena a recolha da caixa e a sua reintegração no ciclo normal. Em caso de NOK, o operador remove a caixa manualmente e o PLC regista a sua exclusão do fluxo de produção.

O estado manual destina-se a operações de ajuste, manutenção, formação ou recuperação de falhas. Neste estado, a execução automática encontra-se inibida e o operador assume o controlo individual dos atuadores através da HMI. O PLC garante que as ações manuais permanecem subordinadas às restrições de segurança.

O estado de acesso remoto é ativado exclusivamente mediante a comutação de um seletor de chave física no quadro elétrico, o qual autoriza o acesso e comando na interface remota. Neste estado, os técnicos conseguem forçar parâmetros, alterar cadências ou realizar diagnósticos aprofundados. A lógica de segurança bloqueia, contudo, ordens remotas que tentem contornar funções de proteção.

O estado de falha constitui o estado hierarquicamente superior da máquina. A quebra de qualquer condição de segurança, ou a deteção de um alarme crítico de processo força a saída imediata de qualquer um dos estados anteriores. O PLC revoga os pedidos de movimento e a célula transita para paragem segura, e exige nova passagem pelo estado de arranque e rearme.

A transição entre estados obedece à lógica representada na Figura 14.

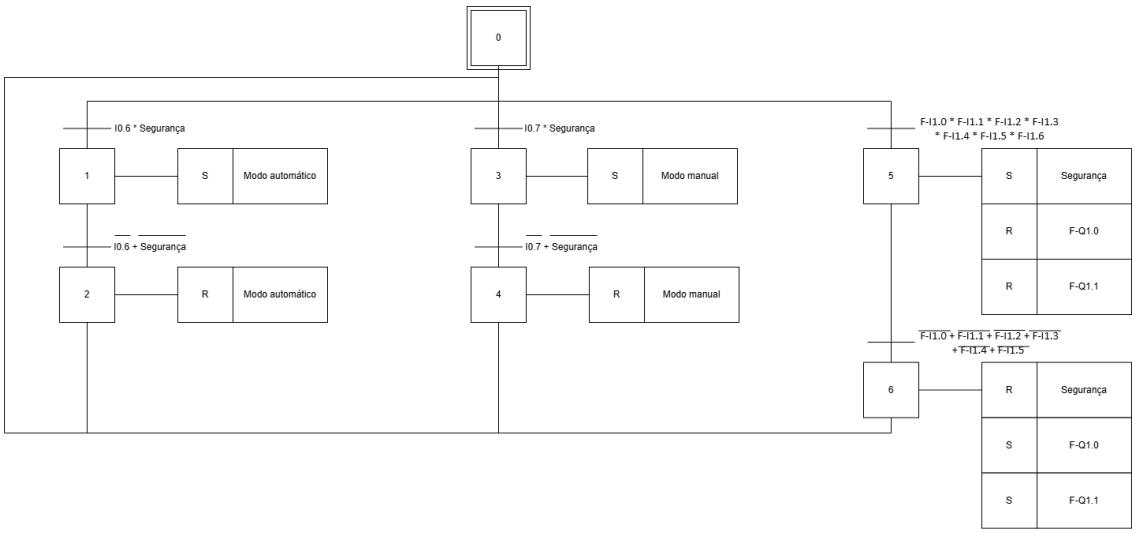


Figura 14 - Grafcet principal caso de estudo 1

O ciclo de produção, executado no modo automático, obedece a uma lógica sequencial descrita através da norma GRAFCET, conforme ilustrado na Figura 15.

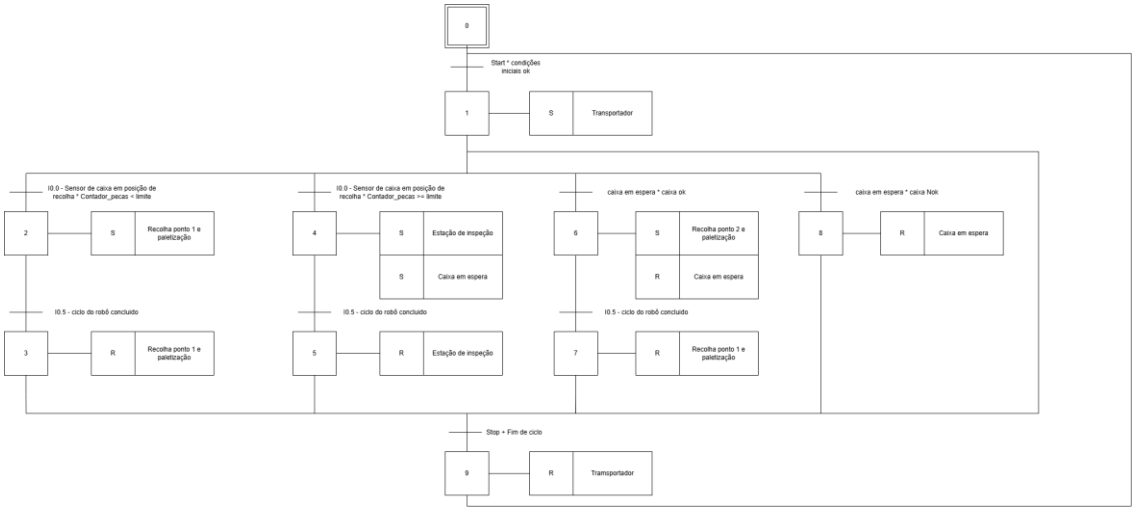


Figura 15 -Grafcet modo automático caso de estudo 1

A sequencia, inicia-se na etapa 0 (repouso). Mediante o comando de arranque e a validação das condições iniciais, o sistema avança para a etapa 1, em que é ativo o transportador de alimentação. Com o transportador em funcionamento, o GRAFCET apresenta uma estrutura de bifurcação lógica, onde o PLC avalia um conjunto de condições exclusivas para determinar o caminho a seguir.

Interação com o robô

A integração entre o PLC e o controlador do robô baseia-se numa arquitetura de mestre-escravo, na qual o PLC assume a função de mestre. A comunicação entre ambos é realizada através de Profinet, que assegura a troca em tempo real de comandos, permissões e estados operacionais. Esta arquitetura garante que o robô apenas atua quando recebe uma ordem explícita do PLC e quando as condições de segurança e de processo se encontram satisfeitas. Os sinais trocados entre os sistemas dividem-se em comandos de execução e estados de confirmação, e permite sincronizar a lógica de processo com a posição real do robô no ciclo.

Interface Homem-Máquina

A navegação HMI foi estruturada num modelo hierárquico simplificado, divido em três níveis principais de acesso e detalhe, com funcionalidades geridas a partir de utilizadores com diferentes níveis de acesso.

A página principal (Figura 16) dá acesso a todas as subpáginas necessárias, bem como a visão geral do estado atual da célula. Na parte superior do HMI é possível ver o modo de operação atual do sistema. Na caixa de texto inferior, irá aparecer um breve texto em caso de haver algum alarme ativo, e do lado direito, há um botão virtual que dá acesso à página com a lista de todos os alarmes ativos e histórico de alarmes (Figura 17). Dentro dessa página é ainda possível aceder ao histórico de alarmes.

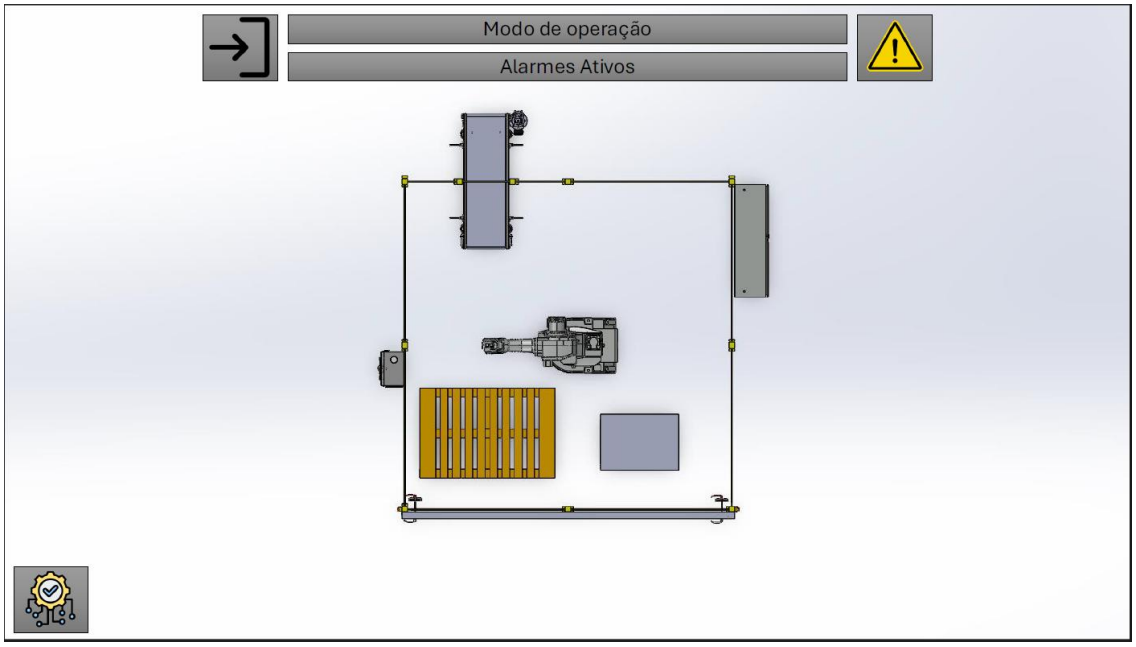


Figura 16 - HMI Principal

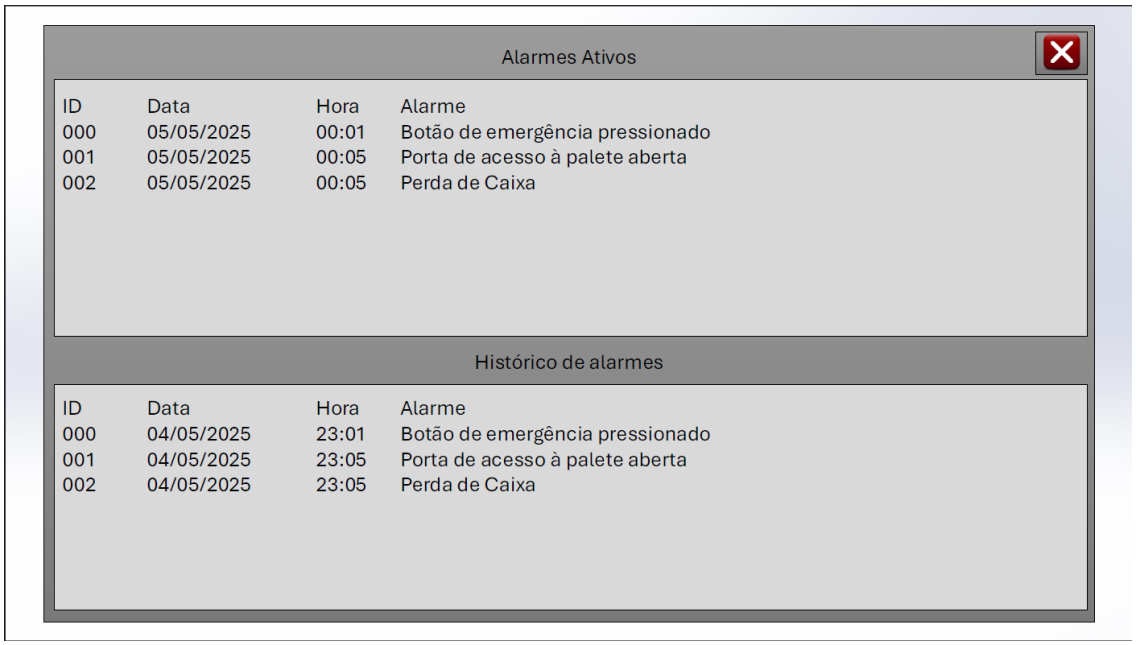


Figura 17 - HMI Alarmes

Na página principal, no canto superior esquerdo, há um botão virtual que permite fazer o login no utilizador pretendido (Figura 18). O nível de acesso 0, destinado aos operadores, apenas permite a operação da célula em modo automático. O nível de acesso 1, destinado a operadores especializados, permite a operação da célula em modo manual. O nível de acesso 2, destinado a técnicos especializados, permite a alteração de parâmetros do sistema.

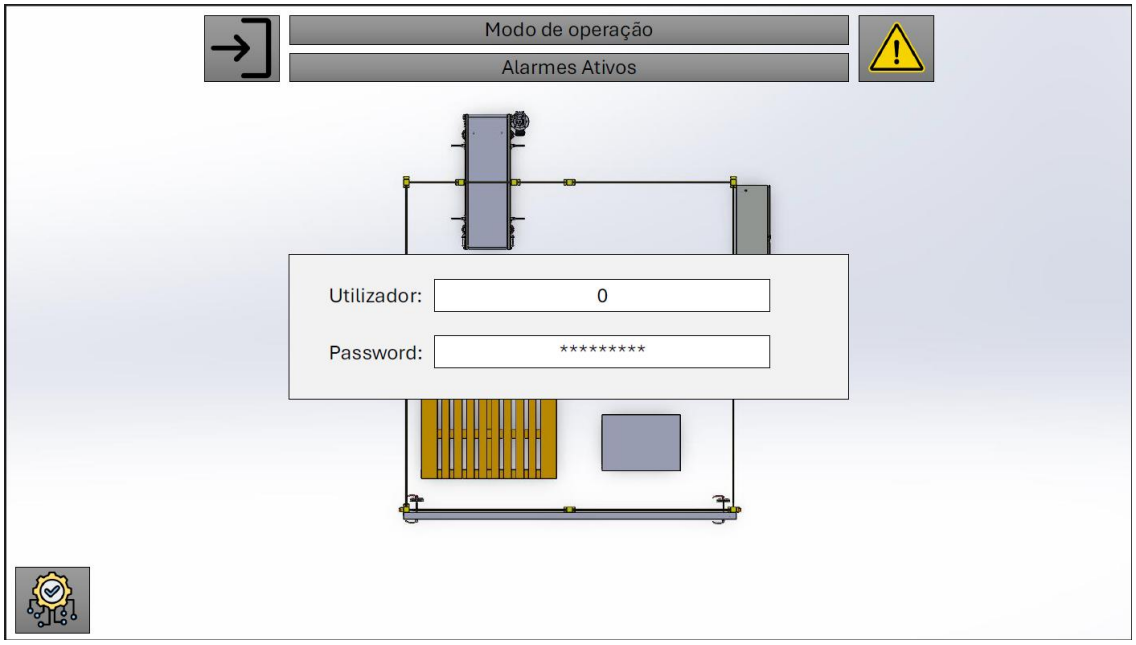


Figura 18 - Login HMI

Na página principal, ao clicar em cima dos equipamentos, é possível ver o seu estado, com o nível de acesso 0, ou operar manualmente, com o nível de acesso 1 (Figura 18). No canto inferior esquerdo, com o nível de acesso 2 é possível aceder à página de parâmetros do sistema e alterar os mesmos (Figura 19).

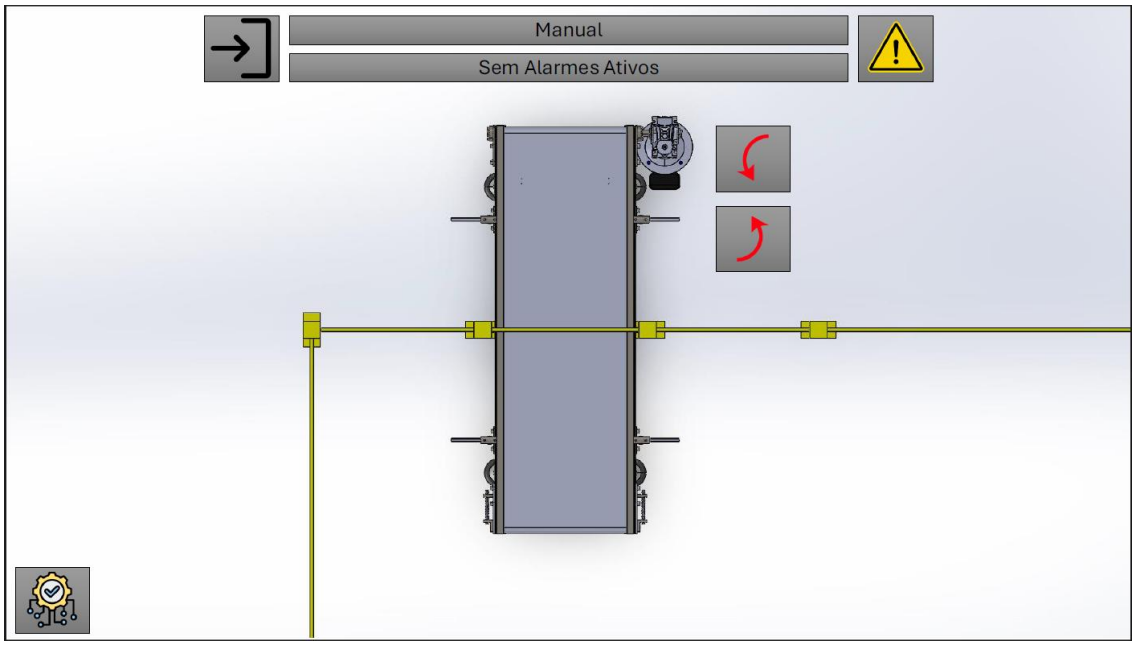


Figura 19 - Modo Manual HMI

Com a célula em funcionamento automático, quando uma caixa for depositada na estação de inspeção, irá aparecer uma janela no HMI a pedir para validar ou rejeitar a caixa (Figura 20).

Figura 20 - Validar Inspeção HMI

3.4.10. Estratégia de acesso remoto

A célula robótica contempla uma arquitetura de acesso remoto para efeitos de diagnóstico e manutenção. A integração desta conectividade obriga ao cumprimento estrito do Regulamento (UE) 2023/1230, que reforça a necessidade de considerar, na conceção da máquina, os riscos associados a acessos não autorizados, a alterações indevidas de software e a comprometimentos da integridade funcional dos sistemas de comando.

A estratégia de acesso remoto utilizada assenta na utilização de um router industrial com suporte para redes privadas virtuais (VPN), o que permite encriptar a comunicação entre o técnico remoto e o PLC, reduzindo o risco de interceção ou acesso indevido durante a transmissão de dados. Contudo, a VPN não constitui, por si só, uma medida de proteção suficiente. Por esse motivo, a arquitetura proposta inclui mecanismos complementares de autenticação, validação local, segregação de acessos e registo de eventos, que garantem que a conectividade remota permanece subordinada às condições de segurança da célula e não interfere com as funções de proteção locais.

O acesso remoto encontra-se inibido por defeito e apenas pode ser ativado mediante validação local explícita por parte de um técnico autorizado, através de um seletor de chave física instalado no quadro elétrico. Esta solução assegura que a sessão remota depende sempre de autorização presencial na instalação e impede a ativação autónoma do acesso a partir do exterior.

A chave física gera um sinal de permissão local que é lido pelo PLC como uma entrada digital. Na ausência desta permissão, o router industrial mantém a porta VPN desativada e não aceita ligações externas. Quando a chave é colocada na posição de autorização, o PLC emite o sinal de permissão que irá habilitar o serviço de acesso remoto.

O acesso remoto permite a monitorização em tempo real de variáveis, a consulta de estados e o apoio ao diagnostico. Pode igualmente ser utilizado para parametrização de variáveis do processo ou a transferência de novas versões do programa. As permissões de acesso são estruturadas por perfil de utilizador. O perfil de diagnóstico apenas permite a leitura de variáveis e estados. O perfil de parametrização permite alterar receitas e temporizadores de processo. O acesso à lógica de segurança exige um terceiro perfil.

Para proteger o acesso direto ao controlador, recorre-se aos mecanismos de proteção nativos do PLC de autenticação dedicada e gestão de permissões. As variáveis e blocos associados às funções de segurança operam numa partição dedicada do PLC. O acesso a essa partição exige um utilizador específico, e sempre que é autenticado e existe uma mordicação de parâmetros ou blocos do sistema, o sistema gera um registo de alteração com identificação, data, hora e alteração efetuada.

A conectividade remota implementa um mecanismo de registo histórico e de auditoria. Todas as tentativas de acesso remoto, as sessões autorizadas, as transferências de blocos de blocos e as alterações aos parâmetros são registadas em memória não volátil do sistema-

A Tabela 13 sintetiza as medidas implementadas, o mecanismo de implementação e o comportamento esperado do sistema em cada cenário de acesso remoto.

Tabela 13 - Medidas acesso remoto

Medida	Implementação	Comportamento esperado
Inibição por defeito	Chave física gera permissão de ligação	Sem permição, router recusa qualquer ligação externa
Autenticação	Perfis de utilizador com palavra-passe dedicada por nível	Acesso recusado sem credenciais válidas e tentativa registada
Limitação funcional	Permissões por perfil e segregação funcional/segurança	Ações fora do perfil são recusadas e registadas
Proteção do programa de segurança	Partição dedicada	Registo automático
Registo e auditoria	Registo auditável em memória não volátil	Toda a atividade remota é rastreável e auditável
Verificação de integridade	Comparação entre versão ativa e versão aprovada	Divergências são sinalizadas e auditáveis

3.5. Caso de estudo 2: célula robotizada colaborativa

O caso de estudo 2 desenvolve-se com base numa aplicação robótica colaborativa de fim de linha, constituída pelas mesmas etapas funcionais do caso de estudo 1, a alimentação de caixas através de um transportador, a inspeção periódica e a paletização. A diferença fundamental face ao primeiro caso de estudo reside na filosofia de segurança adotada. Em vez da segregação física entre o operador e os movimentos perigosos, a célula colaborativa assenta na coexistência controlada entre o operador e o robô. Esta abordagem permite que ambos

partilhem o mesmo espaço de trabalho em condições devidamente monitorizadas e geridas pelo sistema de controlo.

O elemento central da célula é um robô colaborativo, projetado para operar em proximidade com pessoas sem recurso a resguardos perimetrais fixos. Este robô integra mecanismos de monitorização contínua de força, que deteta possíveis colisões. A ferramenta adotada é uma garra de vácuo com características semelhantes à adotada no caso de estudo 1. A monitorização do vácuo mantém relevância operacional no presente caso.

À semelhança ao primeiro caso de estudo, o fluxo de produto mantém-se. O produto chega por um transportador de alimentação, que conduz as caixas à zona de paletização, e o robô deposita as mesmas na palete. Em intervalos periódicos, determinados por parametrização no sistema de controlo, uma caixa é depositada pelo robô na estação intermédia de inspeção. Nesse momento, o operador intervém para realizar o controlo de qualidade.

A diferença crítica face ao caso de estudo 1 reside no facto de esta intervenção ocorrer sem separação física entre o operador e o robô. A segurança do operador durante a inspeção não é garantida por uma porta interbloqueada, mas sim pela gestão dinâmica do comportamento do robô. O robô deve detetar a presença humana, reduzir a velocidade e, se necessário, parar de forma controlada antes de qualquer aproximação indevida.

3.5.1. Arquitetura e componentes

A célula colaborativa é constituída por um conjunto de subsistemas que asseguram, de forma integrada, a alimentação do produto, a manipulação robotizada, a inspeção periódica e a paletização das caixas. A descrição seguinte identifica os principais componentes e as características técnicas mais relevantes para a análise de segurança.

O elemento central da célula é um robô colaborativo, com carga útil e alcance compatíveis com a manipulação das caixas. O robô permite a cobertura simultânea da zona de recolha, de paletização e de inspeção. Ao contrário de um robô industrial convencional, o robô colaborativo integra, no seu sistema de controlo nativo, funções de monitorização de força e velocidade que permitem detetar contacto inesperado com o operador e reagir de forma segura. O robô é comandado pelo seu próprio controlador dedicado, que comunica com o PLC da célula através de Profinet, subordinando a execução dos movimentos às permissões e estados emitidos pelo sistema de controlo global.

A ferramenta de manipulação é uma garra de vácuo, funcionalmente equivalente à descrita no caso de estudo 1. A monitorização do estado de vácuo mantém-se relevante, uma vez que a perda de aderência da carga durante a trajetória pode gerar uma situação perigosa, agravada pelo facto de o operador poder estar presente na célula durante o ciclo.

A alimentação do produto é assegurada por um transportador de correia, que encaminha as caixas até à posição de recolha do robô. A interface entre o transportador e o robô é estabelecida por um sensor de presença, que sinaliza a disponibilidade de uma nova caixa na zona de recolha.

A estação intermédia de inspeção está posicionada de forma acessível ao operador, no espaço partilhado da célula. A sua localização e dimensionamento devem garantir uma postura ergonómica adequada e permitir que o operador realize a inspeção sem necessidade de se aproximar das zonas de maior risco de impacto ou esmagamento. Esta estação é o ponto central da interação homem-robô na célula colaborativa e, por isso, constitui o elemento mais crítico do ponto de vista da segurança funcional.

A zona de paletização corresponde ao espaço onde o robô deposita as caixas na palete. Esta zona pode ser partilhada com o operador durante a troca de paletes, e exige que o sistema de controlo garanta a paragem segura do robô antes de qualquer intervenção nesse espaço.

A Figura 21 representa o layout da célula

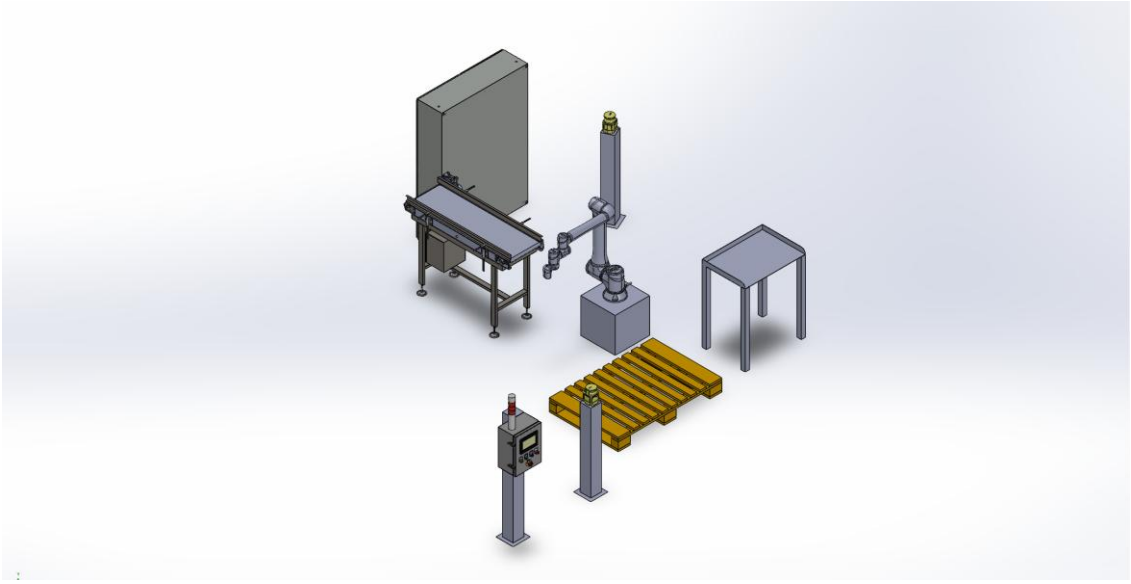


Figura 21 - Layout caso de estudo 2

No Apêndice B encontra-se o layout detalhado com dimensões e legenda técnica.

3.5.2. Limites do sistema e zonas perigosas

No presente caso de estudo, os limites funcionais da célula abrangem o robô colaborativo, o respetivo controlador, o PLC da célula, o sistema de comando de segurança, a ferramenta de vácuo, o troço do transportador de alimentação associado à entrega da caixa, a estação intermédia de inspeção, a zona de paletização, a palete e os dispositivos de monitorização da presença humana no espaço colaborativo. Excluem-se do âmbito os processos a montante da entrega da caixa à célula e as operações logísticas posteriores à remoção da palete, por não interferirem diretamente com a arquitetura funcional e de segurança analisada.

Do ponto de vista espacial, os limites da célula correspondem ao volume de trabalho do robô, à zona de alimentação, à estação intermédia de inspeção, à zona de paletização e às áreas

adjacentes onde o operador pode circular ou intervir durante a operação. Ao contrário do caso de estudo 1, a delimitação do sistema não assenta na existência de uma segregação física rígida, mas sim na definição de um espaço de trabalho partilhado, no qual a presença do operador é permitida em condições controladas.

Para efeitos de análise de risco, a célula pode ser dividida em cinco zonas funcionais principais. A primeira corresponde à zona do transportador, onde subsistem riscos de contacto com elementos móveis. A segunda é a zona de recolha da caixa, onde o robô recebe o produto e inicia o movimento de manipulação. A terceira corresponde à zona colaborativa, centrada na estação intermédia de inspeção, onde o operador interage com a caixa e pode partilhar temporariamente o espaço com o robô. A quarta é a zona de paletização, onde o robô deposita as caixas segundo o padrão definido. A quinta corresponde à zona de transição e circulação do operador, onde se torna relevante a monitorização da aproximação humana ao espaço de trabalho do robô.

Do ponto de vista operacional, os limites da célula incluem o arranque, a produção automática, a operação colaborativa na estação de inspeção, as paragens normais, as paragens por falha, as operações de ajuste, a recuperação após anomalia e as intervenções de manutenção compatíveis com o caso de estudo. Esta definição é particularmente importante numa aplicação colaborativa, uma vez que o risco depende a segurança depende da adaptação do comportamento do robô à presença humana no espaço partilhado.

3.5.3. Modos de operação e interação com o operador

Relativamente aos modos de operação, consideram-se relevantes o modo automático, o modo colaborativo, o modo manual ou setup, o modo de manutenção e o estado de falha ou paragem segura.

No modo automático, a célula executa o ciclo normal de alimentação, recolha e paletização das caixas, incluindo a deposição periódica de uma unidade na estação intermédia de inspeção. Neste modo, o robô opera segundo a sequência de produção definida, mantendo-se a lógica de segurança ativa e pronta a reagir à entrada ou aproximação do operador na zona colaborativa.

O modo colaborativo corresponde à condição em que o sistema ajusta automaticamente o comportamento do robô em função da presença humana na zona de trabalho partilhada. Quando o sistema de monitorização deteta a aproximação do operador à zona colaborativa, nomeadamente à estação intermédia de inspeção, o robô transita de forma automática e sem intervenção do operador para um regime de operação compatível com a coexistência humana. Desta forma, o operador não necessita de executar qualquer ação deliberada para aceder à zona colaborativa, uma vez que a segurança resulta da resposta autónoma do sistema à sua presença. Quando o operador abandona a zona monitorizada, o sistema deteta a sua saída e o robô pode retomar o regime de operação normal, desde que as condições de segurança o permitam.

O modo manual ou setup destina-se a operações de ajuste, ensino de pontos, recuperação de falhas e verificação funcional. Neste modo, a execução automática encontra-se inibida e

qualquer movimento do robô deve ocorrer com limitações adicionais de velocidade e sob condições de comando controladas.

O modo de manutenção aplica-se a intervenções técnicas de maior profundidade. Nestas intervenções, a colaboração normal deixa de ser relevante e o sistema deve ser colocado em condição segura, podendo exigir isolamento de energia e aplicação de procedimentos complementares, como LOTO.

O estado de falha ou paragem segura constitui o estado hierarquicamente superior. A célula deve transitar para este estado sempre que uma condição de segurança deixe de estar assegurada.

Para além destes modos, a célula permite acesso remoto associado a funções de supervisão, diagnostico e apoio à manutenção. Esta capacidade permite ao fabricante aceder ao sistema para analisar falhas ou atualizar parâmetros funcionais.

No caso em estudo, a interação do operador com a célula ocorre em quatro momentos principais:

1. A remoção da palete completa e inserção da palete vazia;
2. A solicitação de acesso à estação intermédia para inspeção visual periódica;
3. A remoção de caixas não conformes;
4. As ações de reposição e rearme do sistema após uma paragem ou anomalia.

A definição dos limites do sistema e dos modos de operação no caso de estudo 2 evidencia que a segurança da célula colaborativa não assenta na segregação física entre operador e robô, mas na gestão segura da coexistência entre ambos no mesmo espaço de trabalho.

3.5.4. Identificação dos perigos

No presente caso de estudo, a identificação dos perigos incide sobre o modo automático, o modo colaborativo, o modo manual, as operações de manutenção e as situações de falha ou paragem segura. Ao contrário do Caso 1, o operador pode permanecer na zona de trabalho durante parte do ciclo, o que altera de forma significativa o tipo de risco associado ao robô e à ferramenta de vácuo.

Os perigos podem ser agrupados em seis grandes categorias, que são os perigos mecânicos, os perigos associados à interação Homem-robô, os perigos funcionais e de controlo, os perigos de transição de modo, os perigos associados ao uso indevido e falhas humanas e os perigos associados ao acesso remoto.

A principal fonte de perigos mecânicos na célula resulta do movimento do robô em proximidade com o operador. Apesar de o robô ser colaborativo, subsistem riscos de impacto e esmagamento, particularmente em caso de erro de posicionamento, atraso na deteção da presença humana ou comportamento inesperado do robô. A perda de carga pode ainda originar impacto com o operador, perturbações do ciclo produtivo ou movimentos bruscos.

Os perigos associados à interação Homem-robô decorrem sobretudo da intervenção periódica na estação intermédia de inspeção. Esta interação situações de proximidade entre a pessoa e o robô, o que torna crítica a correta transição entre o regime automático e o regime colaborativo.

Para além dos perigos puramente mecânicos, a célula apresenta perigos associados ao controlo funcional do sistema. Uma falha de sincronização entre o PLC e o controlador do robô, uma perda de comunicação ou um erro de lógica podem conduzir a movimentos não previstos ou a transições incorretas entre estados operacionais.

A transição entre modos de operação constitui um momento crítico da célula colaborativa. O risco aumenta sempre que o sistema passa do modo automático para o modo colaborativo, do modo colaborativo para o modo manual, ou do modo manual para o modo de manutenção. A retoma do funcionamento após uma pausa ou após a saída do operador da zona colaborativa também requer atenção especial. Se o sistema retomar o movimento antes de a zona estar efetivamente livre ou antes de a condição de segurança estar confirmada, pode ocorrer uma colisão ou um aprisionamento.

Como em qualquer aplicação industrial, devem ser considerados usos indevidos razoavelmente previsíveis. No presente caso, estes incluem a permanência do operador demasiado próximo do robô, a colocação de objetos na zona de trabalho sem autorização do sistema, a tentativa de acelerar o ciclo sem validação das condições de segurança ou a intervenção manual sem respeito pelos procedimentos definidos.

Os perigos associados ao acesso remoto incluem o acesso não autorizado ao controlador, a alteração indevida de parâmetros ou de software, a perda de integridade da comunicação entre sistemas e a ausência de rastreabilidade das intervenções remotas.

A Tabela 14 sintetiza os principais perigos e situações perigosas identificadas para o caso de estudo 2.

Tabela 14 - Zonas perigosas caso de estudo 2

Zona / Elemento	Perigo	Situação perigosa	Possível consequência	Observações
Zona de movimento do robô	Impacto / esmagamento	Presença humana na zona de trabalho durante o ciclo automático	Lesão muito grave ou fatal	Risco aumentado face ao Caso 1 pela ausência de resguardos físicos permanentes
Zona de movimento do robô	Queda de carga	Perda de vácuo durante a trajetória com caixa suspensa na proximidade do operador	Impacto e perturbação do ciclo	A gravidade depende da massa da embalagem, da velocidade e da posição do operador
Estação de inspeção	Exposição a movimento perigoso	Transição incorreta do modo automático para o modo colaborativo	Impacto ou aprisionamento	Requer transição precisa de modo

Tabela 14 - Zonas perigosas caso de estudo 2 (cont.)

Zona / Elemento	Perigo	Situação perigosa	Possível consequência	Observações
Zona de paletização	Esmagamento / impacto	Intervenção do operador durante a troca de palete com retoma inesperada do ciclo por rearme inadequado	Lesão muito grave ou fatal	Associado a comandos imprevistos ou ausência de confirmação de zona livre
Zona de paletização	Perigo ergonómico	Movimentação, remoção e colocação da palete vazia em posturas incorretas	Perturbações musculoesqueléticas	Perigo de caráter não mecânico da máquina
Zona colaborativa (geral)	Contacto não previsto homem-robô	Permanência do operador demasiado próximo do robô durante o modo colaborativo com falha de limitação de velocidade	Lesão moderada a grave	A monitorização de força nativa do robô constitui a última linha de proteção
Zona colaborativa (geral)	Colisão por zona cega dos LiDAR	Postura de evitamento ou obstáculo que mascare parcialmente a deteção pelos scanners LiDAR	Lesão moderada a grave	A cobertura cruzada dos dois LiDAR minimiza, mas não elimina, o risco de zona cega
Transição de modos	Movimento não previsto	Transição do modo colaborativo para manual ou de manual para manutenção sem inibição total dos movimentos	Impacto e esmagamento	Requer restrições de movimento e validação explícita a cada transição
Transição de modos	Arranque inesperado	Retoma do movimento após pausa antes de a zona colaborativa estar efectivamente livre	Colisão ou aprisionamento	A permissão de arranque deve exigir confirmação explícita e zona livre confirmada pelos LiDAR
Infraestrutura (Comando / PLC)	Movimento não previsto	Falha de sincronização entre o PLC e o controlador do robô ou perda de comunicação PROFIsafe	Comportamento imprevisível do robô	Requer monitorização de integridade da comunicação com paragem segura por falha

Tabela 14 - Zonas perigosas caso de estudo 2 (cont.)

Infraestrutura (Comando / PLC)	Erro de lógica	Transição incorreta entre estados operacionais por falha lógica no GRAFCET ou na máquina de estados	Exposição a movimento perigoso em condições não previstas	Mitigado por PLC de segurança com diagnóstico e duplo canal
Uso indevido	Aceleração do ciclo sem validação	Tentativa de antecipar o arranque sem validação das condições de segurança pelo operador	Colisão com robô em movimento	Uso indevido razoavelmente previsível conforme ISO 12100
Uso indevido	Colocação de objectos na zona de trabalho	Introdução de objectos na zona sem autorização do sistema, interferindo com a deteção LiDAR	Falha de deteção; colisão com robô	Pode mascarar a presença humana ou gerar falsos negativos nos scanners
Acesso remoto (Cibersegurança)	Alteração indevida de parâmetros	Modificação remota de parâmetros de velocidade, força ou software de segurança sem controlo local	Comportamento imprevisível; anulação de funções de proteção	Risco mitigado por autenticação e controlo de permições
Acesso remoto (Cibersegurança)	Perda de integridade da comunicação	Interrupção ou manipulação da ligação remota durante intervenção activa no sistema	Ausência de rastreabilidade; estado indeterminado do sistema	Requer registo auditável de todas as intervenções remotas
Infraestrutura (Comando)	Movimento não previsto	Comando manual local (modo de setup) com visibilidade incompleta ou excesso de velocidade	Impacto e esmagamento	Requer restrições de movimento e dispositivo de ação continuada
Infraestrutura (Quadro elétrico)	Choque elétrico	Intervenção técnica no quadro elétrico não isolado	Eletrocussão	Requer procediment o LOTO

3.5.5. Avaliação de risco

Após a identificação estruturada dos perigos, procede-se à avaliação de risco com o objetivo de estimar a gravidade potencial do dano e a probabilidade da sua ocorrência em cada cenário relevante de utilização da célula colaborativa.

No presente caso de estudo, a avaliação de risco incide sobre os perigos associados ao movimento do robô em proximidade com o operador, à manipulação da carga por vácuo, à transição entre modos de operação, à coerência da lógica de controlo e aos riscos introduzidos pela conectividade remota. Ao contrário do caso de estudo 1, a presença do operador no espaço de trabalho durante determinadas fases do ciclo integra o funcionamento previsto da célula, o que aumenta a importância relativa dos parâmetros de exposição e de evitamento.

À semelhança do caso de estudo anterior, a avaliação de risco baseia-se nos três parâmetros qualitativos apresentado na Tabela 4.

A Tabela 15 sintetiza a avaliação de risco inicial para os principais cenários identificados no caso de estudo 2, considerando a célula antes da aplicação das funções de segurança dedicadas.

Tabela 15 - Avaliação de risco caso de estudo 2

Referencia	Zona / contexto	Situação perigosa	S	F	O	A	Risco inicial	Justificação
R1	Zona da estação de inspeção	Aproximação do operador ao robô durante movimento em direção à estação	S2	F2	O2	A2	Muito elevado	Existe contacto previsível em contexto de operação normal. A colisão pode originar lesão grave e o evitamento pode ser difícil se a resposta do sistema não for imediata.
R2	Zona de paletização	Presença do operador durante deposição da caixa pelo robô	S2	F1	O2	A2	Muito elevado	A exposição é menos frequente do que na inspeção, mas o risco de impacto ou esmagamento mantém severidade elevada.
R3	Ferramenta de vácuo / trajetória	Perda de vácuo e queda da carga em proximidade do operador	S1	F1	O1	A1	Elevado	A criticidade depende da massa da caixa, da altura de queda e da posição do operador relativamente à trajetória.

Tabela 15 - Avaliação de risco caso de estudo 2 (cont.)

Referencia	Zona / contexto	Situação perigosa	S	F	O	A	Risco inicial	Justificação
R4	Transição entre modos	Retoma do movimento após saída parcial ou indevidamente detetada do operador	S2	F1	O2	A2	Muito elevado	O risco resulta da incoerência entre estado real da célula e estado assumido pelo sistema.
R5	Lógica de controlo	Falha de monitorização da presença humana ou erro de parametrização de zonas	S2	F1	O1	A2	Elevado	Uma deteção incorreta pode anular a base de segurança da operação colaborativa.
R6	Acesso remoto	Alteração indevida de parâmetros ou lógica de segurança	S2	F1	O1	A2	Elevado	Pode comprometer a resposta segura do robô sem perceção imediata pelo operador local.

Da análise qualitativa efetuada resulta que os riscos mais críticos do caso de estudo 2 concentram-se nas situações de proximidade previsível entre o operador e o robô, nas transições entre modos de operação e nas falhas que comprometam a monitorização segura do espaço colaborativo.

3.5.6. Funções de segurança

As funções de segurança implementadas no caso de estudo 2 resultam diretamente da avaliação de risco anteriormente desenvolvida. O objetivo destas funções é reduzir os riscos identificados para níveis aceitáveis, em conformidade com a lógica de redução do risco preconizada pela ISO 12100. No contexto de uma célula colaborativa, estas privilegiam monitorização da presença humana, a limitação do comportamento do robô e a gestão controlada das transições entre modos de operação.

A Tabela 16 sistematiza a relação entre as situações perigosas previamente avaliadas e as respetivas medidas e funções de segurança adotadas para a sua mitigação.

Tabela 16 - Situações perigosas e medidas adotadas

Referência de risco	Solução adotada / medida de redução do risco	Função de segurança adotada
R1, R2	Monitorização da presença humana na zona colaborativa e adaptação automática do comportamento do robô.	FS2 — Monitorização da proximidade / presença humana. FS4 — Limitação segura do movimento.
R3	Supervisão contínua do estado da ferramenta e inibição da continuação do ciclo em caso de perda de vácuo.	FS7 — Monitorização do estado de vácuo.
R4, R5	Lógica de transição segura entre modos e validação das condições antes da retoma do ciclo.	FS5 — Permissão de arranque seguro. FS6 — Rearme seguro.
R6	Segregação lógica entre acesso remoto, controlo funcional e lógica de segurança.	FS8 — Proteção face a alterações remotas indevidas.
Geral	Paragem imediata perante perigo iminente ou falha crítica.	FS1 — Paragem de emergência.
Geral	Paragem segura quando a presença humana é detetada em condição incompatível com a trajetória em curso.	FS3 — Paragem monitorizada por presença humana.
Geral	Isolamento e bloqueio de fontes de energia.	Medida complementar (Procedimento LOTO)

FS1 – Paragem de emergência

A função de paragem de emergência tem como objetivo interromper de forma imediata o funcionamento da célula perante uma situação de perigo iminente identificada pelo operador. No caso de estudo 2, esta função deve atuar sobre todos os movimentos perigosos do robô e do transportador, impondo a paragem segura do sistema.

A Figura 22 - Fluxograma de atuação FS1Figura 22 ilustra a sequência de atuação da FS1, em que, após o acionamento da paragem de emergência, é removida a energia do robô e do transportador, e o sistema só retoma o funcionamento após o rearme manual.

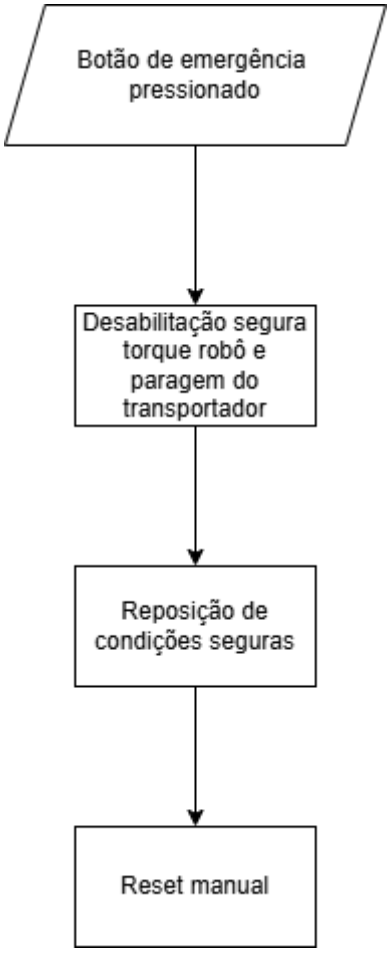


Figura 22 - Fluxograma de atuação FS1

O sistema possui um botão de paragem de emergência no quadro de controlo da linha (Figura 23)

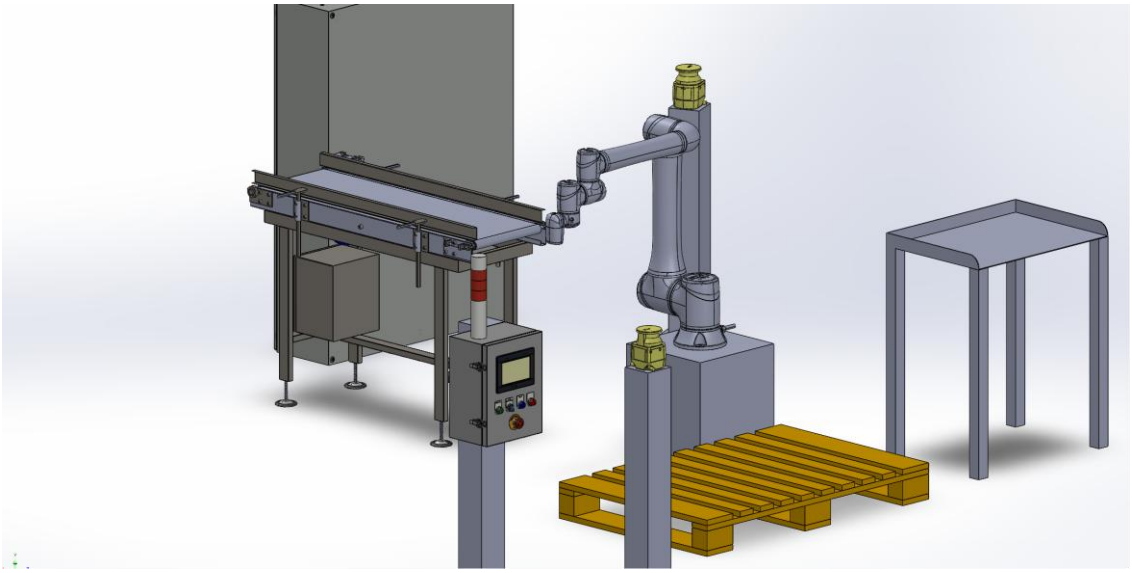


Figura 23 - Localização FS1

FS2 — Monitorização da presença humana

A monitorização da presença humana tem como objetivo detetar a aproximação ou permanência do operador na zona colaborativa, em particular na estação intermédia de inspeção e nas áreas adjacentes onde a interação homem-robô ocorre de forma prevista. Esta função é central na filosofia de segurança da célula colaborativa, pois permite que o sistema adapte o comportamento do robô à presença do operador sem necessidade de segregação física permanente.

Quando a presença humana é detetada na zona monitorizada, o sistema deve reconhecer essa condição e ajustar a operação do robô em conformidade. O ajuste inclui a redução de velocidade, restrição da trajetória ou condução da célula a uma condição de paragem segura, consoante a configuração adotada. A retoma do movimento normal apenas deve ocorrer após a saída do operador da zona monitorizada e após validação das condições de retoma.

FS3 — Paragem monitorizada por presença humana

A paragem monitorizada por presença humana tem como objetivo colocar o robô num estado seguro quando a presença do operador é detetada em situação incompatível com o movimento em curso. Esta função atua quando os sensores LiDAR detetam a entrada de uma pessoa nas zonas de intrusão definidas.

O sistema executa uma paragem segura do robô e a célula mantém o estado bloqueado até rearme manual. A presença na zona de aviso conduz à redução do desempenho do sistema, sem comprometer a continuidade controlada da operação.

O fluxograma da Figura 24 representa o comportamento esperado dos sensores LiDAR.

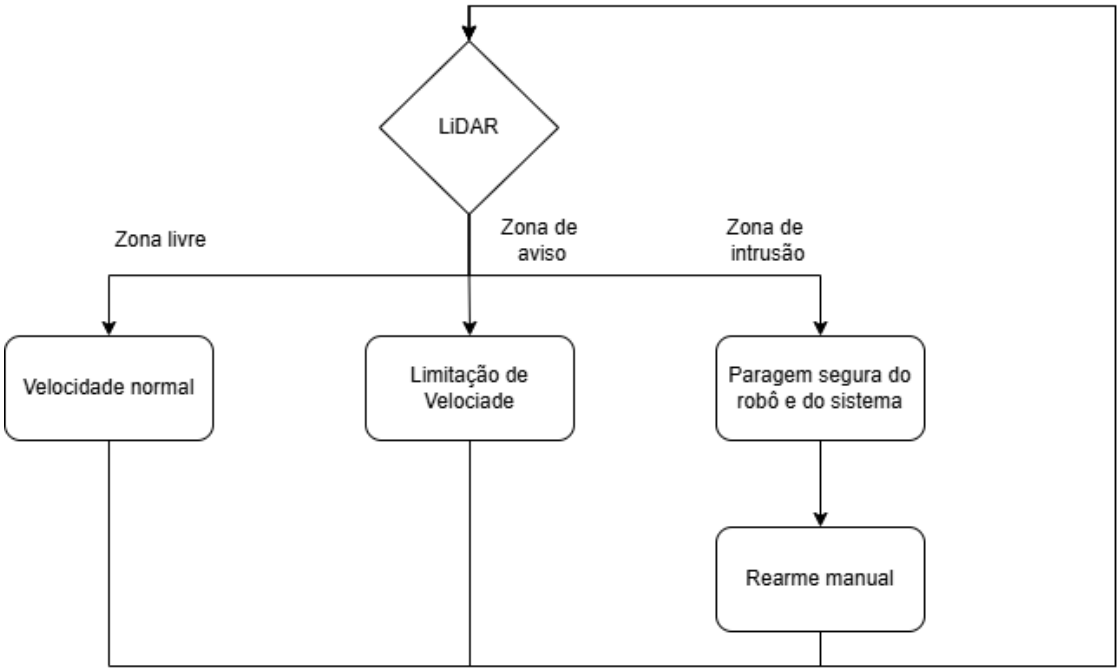


Figura 24 - Fluxograma de atuação FS2

O sistema possui dois sensores LiDAR (Figura 25) de modo a cobrir toda a área de trabalho do robô.

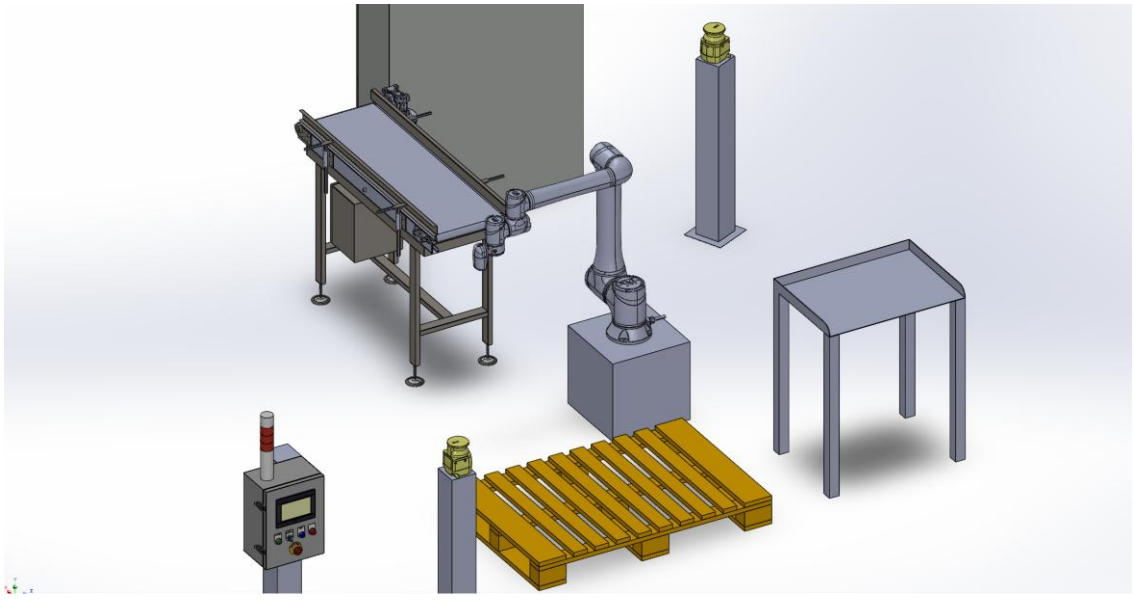


Figura 25 - Localização FS2

FS4 — Limitação segura do movimento

Esta função assegura que o robô deteta contacto inesperado com pessoas ou objectos e execute paragem segura automaticamente. Quando uma pessoa toca no robô, o sensor de força interno deteta o aumento de carga. O robô comunica imediatamente esta condição ao PLC, e o PLC executa paragem segura e bloqueia o rearranque até confirmação de rearme manual.

FS5 — Permissão de arranque seguro

A permissão de arranque seguro assegura que o ciclo automático apenas se pode iniciar ou retomar quando todas as condições de segurança estiverem satisfeitas. Esta função atua como uma verificação integradora do estado global da célula. A função impede que o PLC autorize a sequência automática enquanto qualquer condição de segurança se mantenha inválida.

No contexto da célula colaborativa, esta função verifica, entre outros aspetos, a ausência de falhas ativas, a validação da zona colaborativa, o estado correto dos sensores de presença humana e a compatibilidade entre o modo selecionado e a operação pretendida. Assim, o sistema não retoma o movimento em condições em que o operador ainda se encontre em zona de risco ou em que a lógica de segurança não esteja plenamente assegurada.

FS6 — Rearme seguro

O rearme seguro assegura que o restabelecimento do funcionamento após uma paragem de segurança ocorre de forma manual, intencional e controlada. O botão de rearme deve estar localizado num ponto acessível, mas fora da zona de risco, e o seu acionamento não pode iniciar qualquer movimento por si só.

Esta função limita-se a validar que o sistema de segurança está pronto para autorizar nova sequência operacional. O arranque ou a retoma do ciclo dependem sempre de um comando distinto e da verificação posterior das condições de segurança. Desta forma, o rearranque inesperado da célula após uma interrupção provocada por falha, presença humana ou outra condição de paragem segura é evitado.

O sistema possui um botão de rearme na consola de controlo da célula (Figura 26).

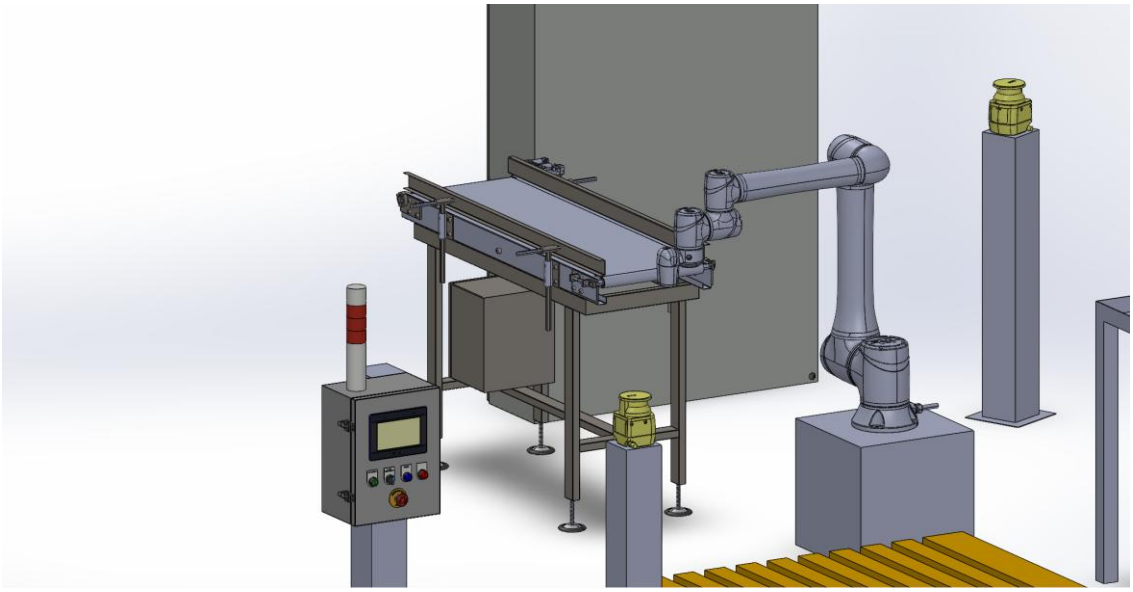


Figura 26 - Localização FS6

FS7 — Monitorização do estado de vácuo

A monitorização do estado de vácuo está associada ao risco de perda da caixa durante o transporte pelo robô. Quando ocorre uma queda de pressão ou perda de vácuo, o sistema inibe a continuação da trajetória e conduz o processo a um estado controlado ou seguro.

FS8 — Proteção face a alterações remotas indevidas

A proteção face a alterações remotas indevidas tem como objetivo impedir que uma ligação externa possa contornar ou modificar indevidamente funções de segurança, parâmetros críticos ou a lógica de operação da célula.

A função assegura que a lógica de segurança permanece segregada da lógica funcional e que qualquer tentativa de alteração não autorizada é bloqueada e registada. O sistema não pode permitir que uma intervenção remota altere o estado de segurança da célula, force movimentos perigosos.

Para além das medidas apresentadas anteriormente, o caso de estudo considera a necessidade de medidas específicas para manutenção, assistência técnica e outras intervenções prolongadas no interior da célula. Nestes contextos, a paragem segura assegurada pelo sistema de comando não substitui a necessidade de isolamento e bloqueio das fontes de energia perigosas. Assim, deve ser prevista a existência de procedimentos de LOTO aplicáveis à alimentação elétrica.

3.5.7. Determinação do nível de PLr

Após a definição das funções de segurança a implementar, procede-se à determinação do PLr para cada uma das funções, com base nos parâmetros definidos na Tabela 5.

A determinação do PLr para cada função de segurança do caso de estudo 2 encontra-se sistematizada na Tabela 17. A tabela mantém a numeração e designação funcional adotada na

secção anterior, de modo a assegurar a rastreabilidade entre a avaliação de risco, as funções de segurança e a arquitetura de controlo.

Tabela 17 - Determinação PLr caso de estudo 2

FS	Designação	S	F	P	PLr	Justificação
FS1	Paragem de emergência	S2	F1	P2	d	Destina-se a reagir a situações de perigo iminente com potencial de lesão grave ou fatal (S2). A sua atuação é solicitada apenas em situações excecionais de emergência, pelo que a exposição é pouco frequente (F1). Perante um evento de emergência com o sistema em movimento, a capacidade de evitar o dano sem a atuação desta função é praticamente nula (P2). A combinação S2/F1/P2 determina o PLr d.
FS2	Monitorização da presença humana	S2	F2	P2	d	A interação homem-robô é frequente e prevista (S2). A exposição ocorre com elevada frequência, uma vez que a partilha do espaço de trabalho é inerente à filosofia colaborativa (F2). A falha desta função expõe o operador a movimentos perigosos sem qualquer reação do sistema, o que torna difícil evitar o dano (P2). A combinação S2/F2/P2 determina o PLr d.
FS3	Paragem monitorizada por presença humana	S2	F2	P2	d	A paragem monitorizada é a resposta direta à deteção de presença na zona de risco, cuja falha pode resultar em colisão com o operador durante a operação colaborativa, com potencial de lesão grave ou fatal (S2). A ativação desta função é frequente, dado que a presença humana na zona colaborativa ocorre regularmente durante o ciclo produtivo (F2). Perante uma falha na resposta do sistema, a velocidade e inércia do robô tornam o evitamento do contacto dificilmente possível (P2). A combinação S2/F2/P2 determina o PLr d.
FS4	Limitação segura do movimento	S2	F2	P2	d	A limitação de velocidade e força é uma das principais barreiras de segurança da célula colaborativa, cuja falha pode originar contacto com energia cinética incompatível com a presença humana e causar lesão grave ou fatal (S2). A função atua continuamente durante o modo colaborativo, em que a proximidade entre operador e robô é frequente e prevista (F2). Em caso de falha, a resposta do robô torna-se imprevisível e o operador não dispõe de tempo de reação suficiente para evitar o contacto (P2). A combinação S2/F2/P2 determina o PLr d.

Tabela 17 - Determinação PLr caso de estudo 2 (cont.)

FS	Designação	S	F	P	PLr	Justificação
FS5	Permissão de arranque seguro	S2	F1	P2	d	O arranque com o operador na zona de risco pode originar lesão grave ou fatal, e uma falha nesta função anula a lógica de proteção global da célula (S2). A função atua em cada ciclo de arranque, mas a exposição a condições perigosas é pouco frequente (F1). Se o ciclo se iniciar com uma condição de segurança inválida não detetada, o operador não tem meios de antecipar ou evitar o perigo (P2). A combinação S2/F1/P2 determina o PLr d.
FS6	Rearme seguro	S2	F1	P2	d	Um rearme inadequado pode conduzir a rearranque inesperado com o operador na proximidade do robô, com potencial de lesão grave ou fatal (S2). A operação de rearme ocorre apenas após paragens de segurança, pelo que a exposição é pouco frequente (F1). Se o rearme não exigir ação deliberada e verificação das condições, o operador pode não ter consciência do iminente rearranque do sistema (P2). A combinação S2/F1/P2 determina o PLr d.
FS7	Monitorização do estado de vácuo	S1	F1	P1	b	O risco associado à queda de carga é moderado, com potencial de lesão ligeira ou reversível dependente da posição do operador no momento da ocorrência (S1). A falha é pouco frequente, dependente de uma anomalia no sistema pneumático (F1). A trajetória do robô é definida e conhecida, pelo que o operador tem alguma capacidade de se afastar da zona de risco (P1). A combinação S1/F1/P1 determina o PLr b.
FS8	Proteção face a alterações remotas indevidas	S2	F1	P2	d	Uma alteração remota não autorizada pode comprometer qualquer função de segurança da célula sem que o operador local seja imediatamente informado, com potencial de lesão grave ou fatal (S2). O evento é pouco frequente, associado a tentativas de acesso indevido ou falha nos mecanismos de autenticação (F1). Se uma função de segurança for comprometida remotamente, o operador não tem meios de detetar a alteração nem de evitar as consequências do comportamento imprevisível do sistema (P2). A combinação S2/F1/P2 determina o PLr d.

Da análise da tabela conclui-se que as funções de segurança críticas do caso de estudo 2, nomeadamente FS1 a FS6 e FS8, requerem PLr d. Em contraste, a função FS7, associada à monitorização do estado de vácuo, requer PLr b. Assim, a arquitetura de segurança do caso de estudo 2 deve assentar numa topologia capaz de suportar PLr d para as funções críticas, com redundância de canais e diagnóstico contínuo, em conformidade com os requisitos da EN ISO 13849-1.

3.5.8. Arquitetura de segurança e controlo

A arquitetura de segurança e controlo da célula colaborativa tem como finalidade materializar as sequências operacionais previamente definidas, e assegurar, em simultâneo, a coexistência segura entre operador e robô. Em conformidade com as exigências de PLr d para as funções críticas, a arquitetura adota um PLC integrado de segurança, do tipo S7-1200F, responsável pela execução da lógica funcional e da lógica de segurança, bem como pela supervisão dos sinais provenientes dos dispositivos de segurança e dos sensores de presença humana.

Ao contrário do caso de estudo 1, a segurança da célula colaborativa não assenta na segregação física do operador face ao robô. A proteção resulta da capacidade do sistema em detetar a presença humana e adaptar automaticamente o comportamento do robô em função dessa condição. Assim, a arquitetura deve separar claramente a lógica funcional, responsável pela execução do processo, da lógica de segurança, responsável pela monitorização da interação homem-robô.

A monitorização da zona colaborativa é realizada por dois scanners LiDAR de segurança, posicionados em lados opostos da célula, de modo a garantir cobertura cruzada e a reduzir zonas cegas. O primeiro LiDAR é colocado na zona do transportador e da recolha, enquanto o segundo é colocado na zona da estação intermédia de inspeção e da palete. Esta distribuição permite vigiar a área de trabalho do robô, o corredor de aproximação do operador e as zonas onde ocorre a interação direta

A principal diferença face ao caso de estudo 1 é que, reside no facto de a segurança não depender da exclusão do operador do espaço de trabalho, mas da capacidade do sistema reconhecer a sua presença e adaptar o comportamento do robô em conformidade. A arquitetura deve, por isso, ser concebida para suportar a colaboração segura, e garantir que a proximidade entre humano e robô não conduz a níveis de energia incompatíveis com a presença humana.

A Tabela 18 apresenta a matriz de causa–efeito das funções de segurança da célula. O seu objetivo é sintetizar, de forma clara e rastreável, a relação entre os sinais de entrada com impacto na segurança e a resposta segura esperada do sistema de comando.

Tabela 18 - Matriz causa-efeito caso de estudo 2

Causa / Efeito	Paragem robô (F-Q0.0)	Limitação velocidade (F-Q0.1)	Paragem transportador (F-Q0.3)	Sinalização falha (F-Q0.4)	Bloqueio rearranque (F-Q0.5)	Ação necessária para retomar
E-stop activo (F-I0.0)	●	●	●	●	●	Desbloqueio e rearme
LiDAR 1 — zona de aviso (F-I0.2)		●				Libertar zona
LiDAR 1 — zona de intrusão (F-I0.3)	●	●		●	●	Libertar zona e rearme
LiDAR 2 — zona de aviso (F-I0.5)		●				Libertar zona
LiDAR 2 — zona de intrusão (F-I0.6)	●	●		●	●	Libertar zona e rearme
Falha de vácuo (I1.3)			●	●		Reposição e rearme
Falha do robô (I1.2)	●	●	●	●	●	Reposição e rearme
Falha de comunicação	●	●	●	●	●	Reposição e rearme

3.5.9. Implementação funcional do sistema de comando

A implementação funcional do sistema de controlo da célula colaborativa assenta num PLC integrado de segurança, do tipo S7-1200F ou equivalente. O PLC é responsável pela coordenação global da sequência produtiva e pela supervisão das condições de segurança associadas à presença do operador na célula. Esta implementação articula a lógica de produção com a lógica de segurança e garante que o robô colaborativo apenas executa movimentos compatíveis com o estado da célula e com a posição do operador no espaço de trabalho partilhado.

A sequência funcional inicia-se com a chegada da caixa ao transportador de alimentação. Após a deteção de presença, o PLC autoriza o robô a recolher a caixa e a executa a etapa de paletização. O robô deposita a caixa na palete de acordo com o padrão previamente definido. Em intervalos parametrizados, o sistema desvia uma caixa para a estação intermédia de inspeção, onde o operador realiza o controlo visual e funcional do produto. Esta etapa constitui o núcleo colaborativo da aplicação, uma vez que a intervenção humana ocorre em coexistência com o funcionamento do robô, embora sob supervisão contínua da lógica de segurança.

Após a inspeção, o operador confirma o resultado através da interface de operação. Em caso de OK, o robô reintegra a caixa no fluxo normal. Em caso de NOK, o sistema bloqueia a reintegração da caixa no processo e permite que o operador a remova manualmente da estação de inspeção.

A implementação funcional deve refletir esta sequência através de uma máquina de estados estruturada em torno dos modos de funcionamento da célula, com os estados de inibição, pronto, automático, colaborativo, paragem monitorizada, falha e rearme. Em estado automático, o robô executa a paletização e a deposição periódica de caixas na estação de inspeção. Quando o sistema deteta a presença humana na zona colaborativa, a máquina de estados transita para o modo colaborativo, no qual o robô reduz a sua velocidade e mantém um comportamento compatível com a aproximação do operador. Se o LiDAR deteta uma intrusão numa zona incompatível com a trajetória em curso, o sistema comanda uma paragem monitorizada ou uma paragem segura, consoante a criticidade da situação. Esta lógica sequencial garante que o arranque, a produção, as paragens e a recuperação de falhas obedecem a regras claramente definidas.

A implementação funcional da célula exige a definição clara dos sinais de entrada e de saída associados à lógica de processo e à lógica de segurança. A Tabela 19 apresenta as entradas do sistema de comando, que inclui os sinais funcionais provenientes dos sensores de processo e os sinais de segurança associados à botoneira de emergência, aos sensores LiDAR e ao estado seguro do robô.

Tabela 19 - Entradas sistema

Sinal	Tipo	Descrição
I0.0	Digital	Sensor de presença de caixa no transportador
I0.1	Digital	Confirmação de palete presente
I0.2	Digital	Seletor de modo automático
I0.3	Digital	Seletor de modo manual
I0.4	Digital	Botão de start
I0.5	Digital	Botão de stop
M10.0	Bit interno	Confirmação de inspeção OK pelo operador
M10.1	Bit interno	Confirmação de inspeção NOK pelo operador
I0.6	Digital	Estado do robô pronto
I0.7	Digital	Estado do robô em ciclo
I1.0	Digital	Estado de falha do robô
I1.1	Digital	Confirmação de vácuo
I1.2	Digital	Confirmação de ciclo concluido
F-I0.0	Digital de segurança	Botoneira de emergência canal A
F-I0.1	Digital de segurança	Botoneira de emergência canal B
F-I0.2	Digital de segurança	LiDAR 1 — zona livre
F-I0.3	Digital de segurança	LiDAR 1 — zona de aviso
F-I0.4	Digital de segurança	LiDAR 1 — zona de intrusão

Tabela 19 - Entradas sistema (cont.)

Sinal	Tipo	Descrição
F-I0.5	Digital de segurança	LiDAR 2 — zona livre
F-I0.6	Digital de segurança	LiDAR 2 — zona de aviso
F-I0.7	Digital de segurança	LiDAR 2 — zona de intrusão
F-I1.0	Digital de segurança	Estado seguro do robô
F-I1.1	Digital de segurança	Permissão de acesso remoto

Tabela 20 - Saídas sistema

Sinal	Tipo	Descrição
Q0.0	Digital	Comando do transportador
Q0.1	Digital	Pedido de pick ao robô
Q0.2	Digital	Pedido de deposição na palete
Q0.3	Digital	Pedido de deposição na estação de inspeção
Q0.4	Digital	Comando da ferramenta de vácuo
Q0.5	Digital	Indicador de célula pronta
Q0.6	Digital	Indicador de célula em ciclo
Q0.7	Digital	Indicador de célula em falha
F-Q0.0	Digital de segurança	Paragem segura do robô
F-Q0.1	Digital de segurança	Limitação de velocidade do robô
F-Q0.2	Digital de segurança	Limitação de força do robô
F-Q0.3	Digital de segurança	Paragem do transportador
F-Q0.4	Digital de segurança	Sinalização de intrusão
F-Q0.5	Digital de segurança	Bloqueio de rearranque
F-Q0.6	Digital de segurança	Velocidade nominal do robô

A seleção do modo de funcionamento da célula pode ser representada pelo grafcet da Figura 27.

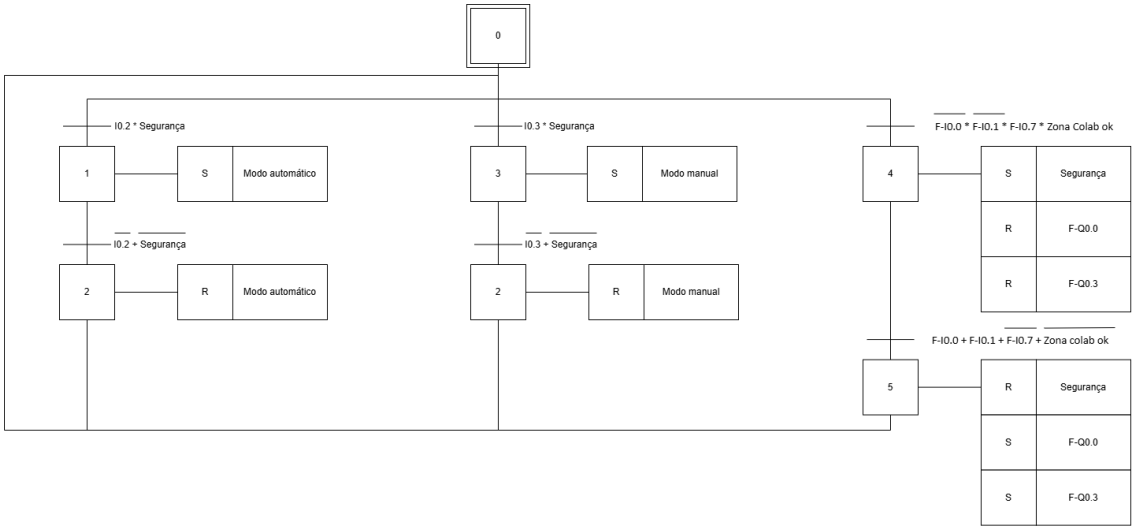


Figura 27 - Grafcet principal caso de estudo 2

O funcionamento do modo automático da célula pode ser representado pelo grafcet da Figura 28.

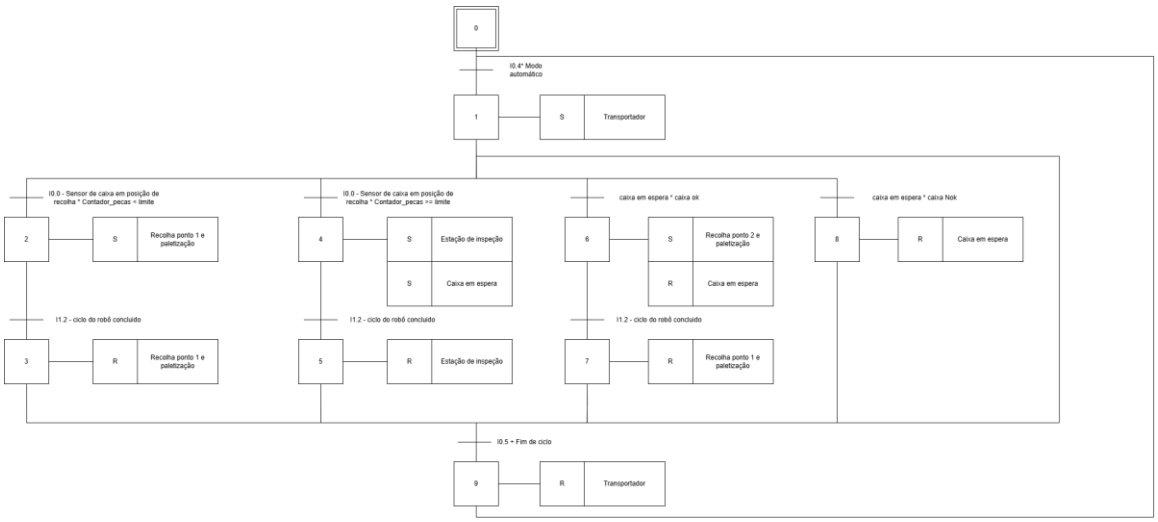


Figura 28 - Grafcet modo automático caso de estudo 2

Integração com o robô

À semelhança do caso de estudo 1, o robô é controlado pelo controlador próprio e encontra-se subordinado às ordens de movimentação do PLC e às permissões de segurança. O controlador do robô comunica com a parte de segurança do sistema, para validar as funções de segurança presentes no robô, como o controlo de força.

Mediante a deteção de pessoas pelos sensores LiDAR, o PLC determina se o robô colaborativo pode movimentar-se à velocidade nominal, com velocidade limitada ou se deve suspender a

trajetória. Esta lógica assegura que o comportamento do robô se mantém compatível com a presença humana na zona colaborativa (Figura 29).

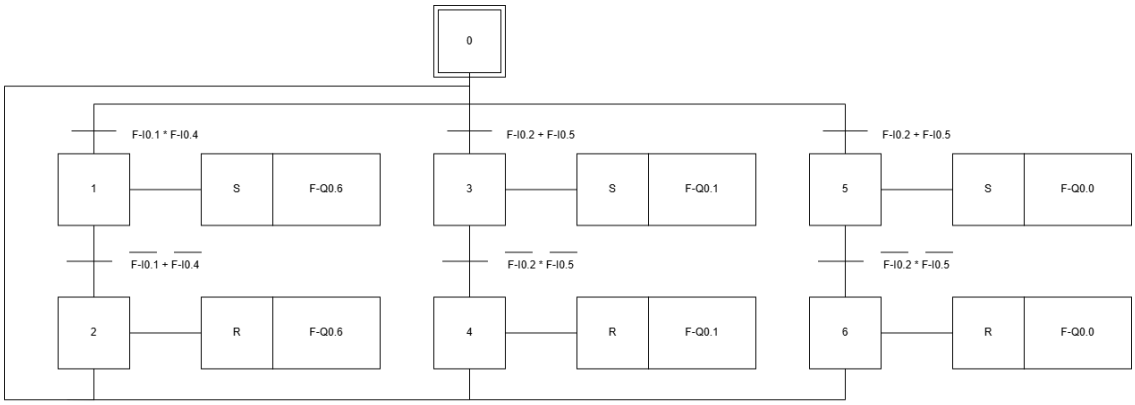


Figura 29 - Grafcet controlo LiDAR

Interface Homem-Máquina

À semelhança do caso de estudo 1, os HMI's permitem a visualização do modo de operação selecionado, do estado do robô, do estado da palete, da presença de caixa, dos avisos de segurança e da confirmação de inspeção. Assim, o operador dispõe de informação suficiente para interagir com a célula de forma segura e para tomar a decisão de destino da caixa após o controlo de qualidade (Figura 30).

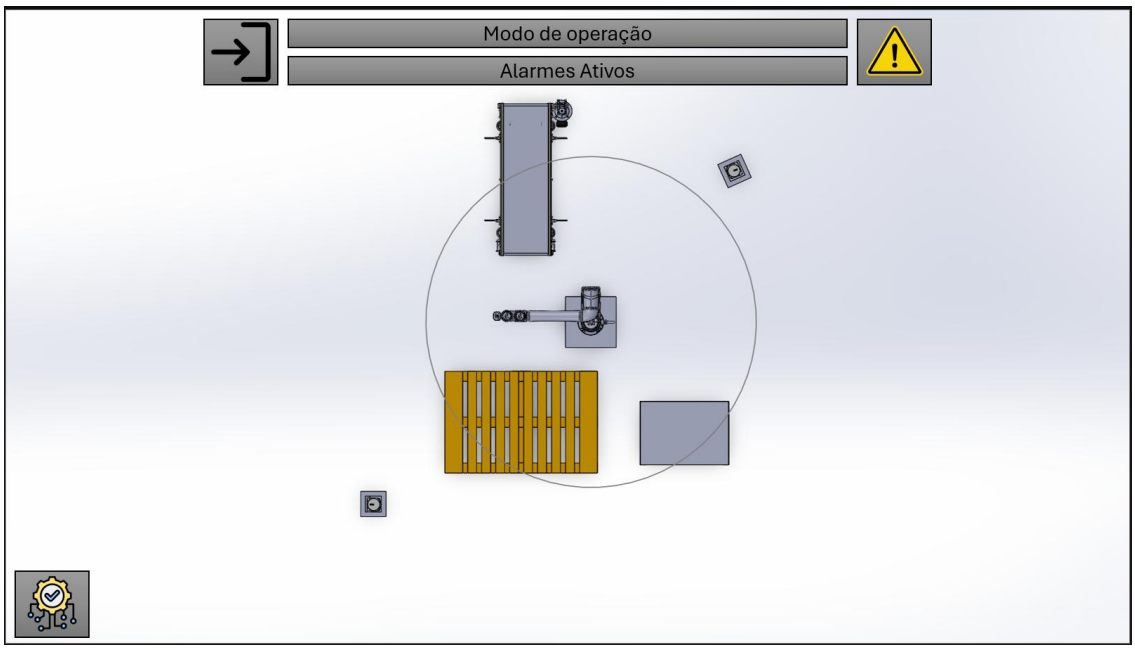


Figura 30 - HMI principal caso de estudo 2

Estratégia de acesso remoto

No caso de estudo 2, a estratégia de acesso remoto é equivalente à adotada no caso de estudo 1. O acesso remoto permanece condicionado por autorização local, autenticação dedicada e registo histórico de acesso e alteração, e está limitado a diagnóstico, supervisão e parametrização autorizada.

4. Resultados e Discussão

A validação apresentada neste capítulo é de natureza conceptual e metodológica. As afirmações de conformidade devem ser interpretadas como compatibilidade normativa da solução proposta, e não como conformidade demonstrada experimentalmente.

A validação estrutura-se em quatro níveis complementares. O nível conceptual avalia a coerência entre os perigos identificados, as funções de segurança definidas e as medidas implementadas. O nível funcional analisa o comportamento esperado do sistema, a matriz causa-efeito e as máquinas de estados. O nível normativo verifica a conformidade com o Regulamento (UE) 2023/1230 e as normas ISO 13849-1, ISO/TS 15066 e IEC 62061. O nível arquitetural avalia a adequação da topologia de controlo, a categoria e o PLr atingível.

Esta estrutura permite validar cada caso de estudo de forma independente, e assegura que as soluções propostas cumprem os Requisitos Essenciais de Saúde e Segurança previstos na legislação.

4.1. Validação caso 1

4.1.1. Validação conceptual

A estratégia de segurança do Caso 1 baseia-se na segregação física completa entre o operador e a célula robotizada, através da utilização de resguardos fixos e portas com interbloqueio. Esta abordagem elimina a possibilidade de interação acidental durante o modo automático, no qual o acesso humano é tratado como uma condição de exceção.

A coerência conceptual verifica-se pela correspondência direta entre os perigos identificados, as funções de segurança implementadas e as medidas de proteção adotadas. Os principais riscos mecânicos e de esmagamento no interior da célula são mitigados por resguardos físicos, interbloqueio das portas de acesso, paragem monitorizada e rearme seguro. Os resguardos fixos implementam a norma ISO 14120 e o interbloqueio segue a ISO 14119. Não se identificam incoerências entre a análise de risco inicial e as medidas propostas.

4.1.2. Validação funcional

As funções de segurança definidas respondem conforme o previsto face às causas de ativação. A paragem de emergência, ao ser ativada pela botoneira, provoca a paragem do robô e do transportador e bloqueia o rearranque. O interbloqueio de porta, ao detetar um pedido de abertura de porta durante, provoca a paragem segura e bloqueia o arranque até à reposição das condições de segurança e rearme manual. O rearme seguro habilita o arranque apenas após confirmação de que a zona está segura, e o arranque só acontece após ordem deliberada.

O PLr d determinado para as funções críticas é atingível com a arquitetura proposta, que inclui PLC S7-1200F, duplo canal nos elementos de segurança e diagnóstico de falhas, conforme a ISO 13849-1.

4.1.3. Validação normativa

A solução proposta apresenta coerência com os RESS do Regulamento (UE) 2023/1230. Os resguardos fixos atendem ao RESS 1.4.1 e 1.4.2 A porta com interbloqueio e bloqueio de abertura atende ao RESS 1.4.2. A arquitetura de duplo canal atinge Categoria 3 e PLr d conforme ISO 13849-1. O interbloqueio com bloqueio cumpre a ISO 14119 e os resguardos fixos cumprem a ISO 14120.

A avaliação de risco baseada nos parâmetros de severidade, frequência de exposição e possibilidade de evitamento, encontra-se alinhada com o Anexo I do Regulamento (UE) 2023/1230 e com a ISO 12100. O PLr d atribuído é adequado aos riscos de severidade média a alta identificados para o caso 1.

4.1.4. Validação arquitetural

A arquitetura de controlo utiliza um PLC de segurança integrado S7-1200F com módulos de entradas e saídas distintos entre funcional e de segurança, com os elementos de segurança a trabalhar em duplo canal. Esta configuração garante a Categoria 3 conforme ISO 13849-1, o que significa que uma única falha não detetada não conduz à perda da função de segurança.

A plataforma de segurança inclui diagnóstico interno para deteção de curtos-circuitos, cruzamento de canais e falhas relevantes. A comunicação segura com o robô via Profinet e PROFIsafe garante integridade dos sinais de paragem e permissão de arranque.

A Tabela 21 sintetiza, para cada função de segurança definida, o perigo mitigado, o requisito normativo aplicável, o nível de desempenho requerido, a evidência de validação disponível e as limitações identificadas, o que consolida os resultados dos quatro níveis de validação aplicados.

Tabela 21 - Validação caso 1

Função de segurança	Perigo mitigado	Norma / Requisito	PLr	Evidência de validação	Limitação
FS1 — Paragem de emergência	Exposição a movimento perigoso por falha operacional	Regulamento (UE) 2023/1230, ISO 13850	d	Botoneira de duplo canal; matriz causa-efeito define paragem robô, transportador e robô	Tempo de paragem real não verificado experimentalmente
FS2 — Interbloqueio de porta	Acesso indevido à célula durante ciclo automático	Regulamento (UE) 2023/1230, ISO 14119	d	Interbloqueio com bloqueio; paragem segura confirmada na máquina de estados	Eficácia do bloqueio mecânico não validada
FS3 — Prevenção de arranque inesperado	Retoma automática do ciclo após paragem de segurança, abertura de porta ou restabelecimento de alimentação	Regulamento (UE) 2023/1230, ISO 13849-1	d	Sistema mantém ciclo inibido após normalização dos sinais físicos, rearme manual obrigatório seguido de comando de arranque distinto	Não testado com múltiplos cenários de falha simultânea
FS4 — Rearme seguro	Reposição do sistema sem verificação deliberada das condições de segurança	Regulamento (UE) 2023/1230, ISO 13849-1	d	Botão de rearme no exterior da célula com visibilidade para o interior, rearme apenas valida prontidão do sistema de segurança, arranque dependente de comando distinto;	Visibilidade efetiva para o interior da célula não verificada em contexto físico real

Tabela 21 - Validação caso 1 (cont.)

Função de segurança	Perigo mitigado	Norma / Requisito	PLr	Evidência de validação	Limitação
FS5 — Paragem segura associada ao acesso	Presença humana no interior com movimentos perigosos residuais	Regulamento (UE) 2023/1230, ISO 13849-1, ISO 13850	d	Atuação em coordenação com FS2, paragem segura no controlador do robô com travagem controlada e remoção segura do binário dos motores	Tempo de travagem e distância de paragem residual não medidos experimentalmente
FS6 — Permissão de arranque seguro	Arranque inesperado após falha ou acesso	Regulamento (UE) 2023/1230 — RESS 1.2.3	d	Ciclo automático condicionado à validação de todas as condições de segurança pelo PLC	Não testado com cenários de condição de segurança inválida não detetada
FS7 — Monitorização do estado de vácuo	Queda de carga durante trajetória por perda de vácuo na ferramenta	Regulamento (UE) 2023/1230	b	Supervisão contínua da pressão da garra, inibição da trajetória	Limiar de pressão crítica e tempo de resposta não testado
FS8 — Paragem segura do transportador	Movimento perigoso do transportador com condições de segurança da célula não asseguradas	Regulamento (UE) 2023/1230, ISO 13849-1	d	Paragem do transportador condicionada às mesmas regras da célula, rearranque dependente de reposição de condições de segurança e validação pelo sistema	Tempo de paragem do transportador não verificado

4.2. Validação do caso de estudo 2

4.2.1. Validação conceptual

A filosofia de segurança do caso 2 assenta na coexistência controlada entre o operador e o robô, mediante a monitorização contínua por sensores LiDAR. Ao contrário do caso 1, não existem resguardos físicos permanentes. A segurança é garantida por funções ativas de monitorização contínua de presença humana pelos sensores LiDAR.

A coerência conceptual verifica-se pela correspondência entre os perigos identificados, as funções de segurança implementadas e as medidas de proteção adotadas. Os riscos de interação homem-robô e de esmagamento são mitigados pelas funções de monitorização de presença, paragem por intrusão, limitação de movimento e limitação de velocidade. Os dois LiDAR com zonas de aviso, intrusão e livre, combinados com o robô com monitorização de força integrada, materializam a estratégia de colaboração segura baseada na limitação de velocidade e na paragem controlada, em conformidade com a ISO/TS 15066.

4.2.2. Validação funcional

As funções de segurança definidas respondem conforme o previsto face às causas de ativação. A paragem de emergência, ativada pela botoneira de duplo canal, provoca a paragem do robô e do transportador e bloqueia o rearranque automático.

A monitorização da presença humana recorre aos dois scanners LiDAR de segurança, que controlam de forma contínua as zonas de aviso e intrusão definidas. Quando um LiDAR deteta a violação da zona de aviso, o sistema limita a velocidade do robô. Quando deteta a violação da zona de intrusão, executa paragem segura do robô e bloqueia o rearranque.

A limitação segura do movimento inclui a capacidade intrínseca do robô colaborativo para detetar contacto inesperado com uma pessoa ou obstáculo. Nessa situação, o robô interrompe o movimento, comunica o evento ao sistema de comando e a célula transita para um estado seguro que exige rearme manual antes da retoma da operação.

A permissão de arranque seguro impede o arranque do robô se o modo de operação tiver sido alterado. O arranque só é habilitado após confirmação de que as condições de segurança se encontram satisfeitas e após ordem explícita de arranque. O rearme seguro exige atuação manual após paragem por intrusão ou falha de segurança. O rearranque apenas é habilitado após confirmação de que a zona está livre e todas as condições de segurança foram restauradas, e rearme manual por parte do operador

A monitorização do estado de vácuo supervisiona a pressão da garra de vácuo. Quando deteta falha de pressão, provoca paragem do ciclo.

A proteção face a alterações remotas indevidas bloqueia alterações não autorizadas ao sistema de comando através de acesso remoto e regista todas as operações. O acesso requer autenticação por chave física e VPN segura.

4.2.3. Validação normativa

A solução proposta apresenta coerência com os RESS do Regulamento (UE) 2023/1230. Os dispositivos de deteção de presença implementados por LiDAR atendem ao RESS 1.4.3 e são conformes com IEC 61496-1 e IEC 61496-2. Os controlos de arranque e rearranque atendem ao RESS 1.2.1, uma vez que o rearme manual é obrigatório após intrusão. A colaboração por monitorização de distância, com duas zonas de resposta diferenciada, atende à ISO/TS 15066. A velocidade reduzida em zona de aviso e paragem em intrusão respeitam os limites de velocidade e força da ISO/TS 15066. A arquitetura suportada por diagnóstico e redundância atinge Categoria 3 e PLr d conforme ISO 13849-1. A comunicação PROFIsafe suporta a integridade funcional da troca de sinais de segurança na arquitetura proposta.

A avaliação de risco considera os parâmetros de severidade, frequência de exposição e possibilidade de evitamento conforme ISO 12100, com especial atenção aos riscos de interação homem-robô. Os limites de força e velocidade adotados cumprem com a ISO/TS 15066. A confirmação de inspeção pelo operador é obrigatória e não automática, alinhada com RESS 1.2.5 sobre controlos de confirmação.

4.2.4. Validação arquitetural

A arquitetura de controlo integra PLC de segurança S7-1200F como controlador central, dois scanners LiDAR de segurança posicionados em cobertura cruzada com três zonas cada, comunicação Profinet e PROFIsafe entre PLC e robô colaborativo, HMI para confirmação de inspeção, seleção de modos e visualização de alarmes, e acesso remoto seguro via VPN com router industrial, autenticação por chave física e registo de acesso e alterações auditável.

A cobertura cruzada dos LiDAR minimiza zonas cegas e garante deteção confiável mesmo em posturas de evitamento. A comunicação PROFIsafe assegura integridade dos sinais de segurança, incluindo deteção de perda de quadro, repetição e atraso. A integração com o robô colaborativo de monitorização de força nativa é compatível com a arquitetura proposta. O HMI, embora não detalhado em implementação, está conceptualmente definido para os ecrãs principais de operação, inspeção, alarmes e seleção de modos.

A Tabela 22 sintetiza, para cada função de segurança definida, o perigo mitigado, o requisito normativo aplicável, o nível de desempenho requerido, a evidência de validação disponível e as limitações identificadas, o que consolida os resultados dos quatro níveis de validação aplicados.

Tabela 22 - Validação caso 2

Função de segurança	Perigo mitigado	Norma / Requisito	PLr	Evidência de validação	Limitação
FS1 — Paragem de emergência	Exposição a movimento perigoso por falha operacional	Regulamento (UE) 2023/1230, ISO 13850	d	Botoneira duplo canal; matriz causa-efeito define paragem total, bloqueio, sinalização	Tempo de paragem real não verificado experimentalmente
FS2 — Monitorização de presença humana	Entrada do operador em zona de trabalho activa	Regulamento (UE) 2023/1230, IEC 61496-1/2, ISO/TS 15066	d	Dois LiDAR com cobertura cruzada e diferentes zonas de monitorização	Eficácia em condições reais de poeira, reflexos e múltiplos operadores não validada
FS3 — Paragem monitorizada por presença humana	Colisão e situações de interação perigosa	ISO 13849-1, ISO/TS 15066, ISO 14119	d	Definido comportamento de transição de modos por grafcet	Cenários de transição rápida de modo não simulados
FS4 — Limitação segura do movimento	Contacto inesperado com operador ou obstáculo	ISO/TS 15066	d	Robô com monitorização de força nativa, célula transita para estado seguro	Limites de força e pressão por zona corporal não validados experimentalmente conforme ISO/TS 15066
FS5 — Permissão de arranque seguro	Arranque sem confirmação de condições de segurança	Regulamento (UE) 2023/1230	d	Arranque condicionado a confirmação explícita	Não testado com cenários de condição de segurança inválida não detetada
FS6 — Rearme seguro	Retoma do ciclo após intrusão sem verificação	Regulamento (UE) 2023/1230, ISO 14119	d	Rearme manual obrigatório após paragem de segurança	Visibilidade e confirmação efetiva da zona livre não testadas em contexto real
FS7 — Monitorização do estado de vácuo	Queda de carga durante trajetória por falha de vácuo	Regulamento (UE) 2023/1230 — RESS 1.3.2	b	Supervisão contínua da pressão da garra, inibição da trajetória	Limiar de pressão crítica e tempo de resposta não testado
FS8 — Proteção face a alterações remotas	Modificação indevida de parâmetros ou software de segurança por acesso remoto	Regulamento (UE) 2023/1230	d	VPN, autenticação por diferentes níveis de permissão e registo de alterações	Proteção não testada experimentalmente

4.3. Análise critica global

A análise crítica dos dois casos de estudo evidencia que, embora ambas as soluções respondam ao mesmo objetivo funcional, assentam em filosofias de segurança distintas. No caso de estudo 1, a redução do risco resulta da segregação física entre o operador e a célula robotizada, enquanto no caso de estudo 2 assenta na coexistência controlada entre operador e robô colaborativo, suportada por monitorização ativa da presença humana e por funções intrínsecas de limitação e paragem.

Do ponto de vista conceptual, o caso de estudo 1 apresenta maior simplicidade e maior clareza na delimitação da zona perigosa, uma vez que a segregação física torna inequívoca a separação entre o operador e os movimentos perigosos. No caso de estudo 2, a delimitação funcional é mais complexa, pois a segurança depende da deteção fiável da presença humana, da limitação dinâmica do comportamento do robô e da coerência entre sensores, controlador e lógica de segurança.

A comparação (Tabela 23) mostra que a célula segregada privilegia robustez e clareza de delimitação do risco, à custa de menor flexibilidade operacional. A célula colaborativa oferece maior adaptabilidade a processos com intervenção humana periódica, mas aumenta a complexidade da validação e a dependência da fiabilidade dos sistemas de monitorização e controlo. Esta diferença é particularmente relevante no enquadramento do Regulamento (UE) 2023/1230, uma vez que a conformidade da solução colaborativa depende de demonstrar que a combinação entre deteção, limitação de movimento e paragem controlada assegura um nível de proteção equivalente ao da segregação física.

Tabela 23 - Comparação casos de estudo

Dimensão	Caso de estudo 1 — Célula segregada	Caso de estudo 2 — Célula colaborativa
Estratégia de segurança	Segregação física completa com resguardos fixos e porta com interbloqueio.	Coexistência controlada com monitorização contínua da presença humana e funções intrínsecas do robô colaborativo.
Separação homem–máquina	Separação física permanente; o acesso ao interior da célula só é permitido com paragem segura.	Separação funcional dinâmica; o operador pode aproximar-se ou interagir em condições controladas pelo sistema de segurança.
Sensores e dispositivos principais	Botoneira de emergência e interbloqueio da porta de acesso.	Dois scanners LiDAR de segurança, botoneira de emergência e monitorização nativa de força no robô colaborativo.
Resposta à aproximação do operador	Não existe resposta dinâmica durante o funcionamento automático, porque o acesso é impedido pelos resguardos físicos.	O sistema reduz a velocidade do robô quando o operador entra na zona de aviso definida pelos LiDAR.

Tabela 23 - Comparação casos de estudo (cont.)

Dimensão	Caso de estudo 1 — Célula segregada	Caso de estudo 2 — Célula colaborativa
Resposta à entrada indevida	A abertura da porta interbloqueada provoca paragem segura e bloqueio do rearranque até rearme manual.	A entrada na zona de intrusão provoca paragem segura, sinalização de alarme e bloqueio do rearranque até rearme manual.
Modos de operação	Automático, manual ou setup, manutenção e falha ou paragem segura.	Automático, colaborativo, manual ou setup, manutenção e falha ou paragem segura.
Vantagens	Solução robusta, madura, de interpretação normativa mais direta e com menor complexidade de integração.	Solução mais flexível, mais adaptada a tarefas com intervenção humana periódica e mais compatível com contextos de partilha controlada de espaço.
Limitações	Menor flexibilidade operacional e necessidade de paragem total para qualquer acesso ao interior da célula.	Maior complexidade arquitetural, maior dependência da fiabilidade dos sensores e necessidade de validação mais exigente da interação homem–robô.
Implicações no Regulamento (UE) 2023/1230	A conformidade demonstra-se sobretudo através de resguardos, interbloqueios e prevenção de acesso ao perigo.	A conformidade exige demonstrar que a deteção de presença, a monitorização de distância e a limitação de força asseguram um nível de proteção equivalente.
Acesso remoto	Garantir integridade do sistema, proteção contra alterações indevidas e rastreabilidade de acessos e alterações	Garantir integridade do sistema, proteção contra alterações indevidas e rastreabilidade de acessos e alterações

As limitações da validação são comuns aos dois casos. A análise realizada é metodológica e arquitetural, não experimental, pelo que não foram verificados tempos de resposta reais, tempos de paragem, comportamento em ambiente físico nem taxa efetiva de falhas. Também não foi desenvolvido um protótipo funcional da HMI nem executada simulação operacional dos GRAFCETs. No caso de estudo 2, esta limitação é ainda mais sensível, dado que a eficácia da arquitetura depende da interação segura entre operador, sensores LiDAR e robô colaborativo.

Apesar destas limitações, a solução proposta revela coerência interna e fiabilidade teórica compatível com os níveis de desempenho requeridos. A utilização de PLC de segurança, comunicação Profinet/PROFIsafe e mecanismos de acesso remoto controlado constitui uma base tecnológica consistente com práticas industriais consolidadas e com as exigências atuais de segurança funcional e cibersegurança industrial.

Em síntese, as soluções propostas demonstram coerência conceptual, funcional e normativa com os requisitos do Regulamento (UE) 2023/1230 e das normas aplicáveis. A transição para conformidade plena exigiria a realização de ensaios experimentais, a medição de tempos de resposta e paragem, a validação em ambiente físico e a verificação da taxa de falhas ao longo da vida útil dos componentes.

5. Conclusão

5.1. Conclusões finais

O presente trabalho teve como objetivo estudar e implementar uma abordagem de conceção e validação de segurança para células robotizadas no contexto da automação industrial, com base no Regulamento (UE) 2023/1230 e as principais normas técnicas aplicáveis à segurança de máquinas. A análise desenvolvida permitiu demonstrar que a segurança funcional de uma célula robotizada depende não apenas da seleção adequada de componentes e dispositivos de proteção, mas também da coerência entre a avaliação de risco, as funções de segurança, a arquitetura de controlo e a lógica operacional do sistema.

No caso de estudo 1, correspondente à célula segregada, verificou-se que a estratégia baseada em resguardos fixos, portas com interbloqueio e funções de paragem e rearme seguros constitui uma solução robusta, de interpretação normativa direta. Esta abordagem assegura uma clara separação entre o operador e a zona perigosa, o que reduz de forma significativa a exposição ao risco durante o funcionamento automático. A validação efetuada confirmou a consistência entre os perigos identificados, as medidas de redução do risco adotadas e os níveis de desempenho requerido definidos para as funções de segurança críticas.

No caso de estudo 2, correspondente à célula robotizada colaborativa, concluiu-se que a segurança pode ser assegurada sem segregação física permanente, desde que exista uma arquitetura de controlo capaz de monitorizar de forma fiável a presença humana e de adaptar o comportamento do robô em função dessa presença. A utilização de sensores LiDAR, em conjunto com funções de limitação de velocidade, paragem monitorizada, rearme seguro e controlo de arranque, permitiu estruturar uma solução tecnicamente coerente com os princípios da colaboração segura. Este caso evidenciou, contudo, uma maior exigência de validação funcional e arquitetural, dado que a proteção do operador depende da interação dinâmica entre sensores, controlador e robô colaborativo.

A comparação entre os dois casos de estudo mostrou que a opção entre segregação física e colaboração controlada não deve ser entendida como uma mera escolha de tecnologia, mas como uma decisão de engenharia que envolve compromissos entre segurança, flexibilidade operacional, complexidade de integração e esforço de validação. A célula segregada oferece maior simplicidade conceptual e regulamentar, enquanto a célula colaborativa proporciona maior adaptabilidade a processos com intervenção humana periódica, embora com maior exigência em termos de conceção e justificação técnica.

Em ambos os casos, a arquitetura proposta revelou-se compatível com os níveis de desempenho requerido estabelecidos a partir da avaliação de risco. A integração entre PLC de segurança, dispositivos de proteção, funções intrínsecas do robô e mecanismos de supervisão permitiu construir soluções coerentes com os RESS aplicáveis. Adicionalmente, o estudo evidenciou a importância de considerar, desde a fase de conceção, não só a segurança funcional, mas também os aspetos de acessibilidade, manutenção, retorno à operação e, no caso da célula colaborativa, a segurança do acesso remoto.

5.2. Limitações e trabalhos futuros

A presente dissertação apresenta uma validação de natureza metodológica e arquitetural, não experimental. Assim, uma das principais limitações do trabalho reside na ausência de implementação física integral dos casos de estudo, o que impede a verificação empírica de parâmetros como tempos de paragem, tempos de resposta, robustez real dos dispositivos de segurança e comportamento do sistema em ambiente industrial. Do mesmo modo, não foi desenvolvida uma campanha de ensaios laboratoriais que permitisse confirmar, em condições reais, a eficácia das funções de segurança definidas.

Outra limitação relevante prende-se com a inexistência de um protótipo funcional completo da interface homem-máquina e da lógica de controlo em ambiente de simulação ou execução industrial. Embora a arquitetura proposta seja coerente do ponto de vista conceptual e normativo, a ausência de validação em plataforma de simulação impede a análise detalhada de estados transitórios, falhas intermitentes, comportamentos não previstos e interações dinâmicas entre PLC, robô, sensores e dispositivos de segurança. No caso da célula colaborativa, esta limitação é ainda mais significativa, dada a dependência da solução relativamente à fiabilidade dos sensores LiDAR e à resposta do robô em contextos de coexistência com o operador.

Acresce que o trabalho não considerou, de forma experimental, fatores ambientais e operacionais que podem influenciar o desempenho real da solução, como variações de iluminação, poeiras, vibrações, tolerâncias mecânicas, desgaste de componentes e perturbações na comunicação industrial. Também não foi analisada em profundidade a cibersegurança da arquitetura de acesso remoto, para além da definição conceptual das medidas de autenticação, segregação e registo de atividade. Estes fatores poderão condicionar o desempenho global da solução em aplicação industrial real.

No que respeita a trabalhos futuros, recomenda-se a implementação de um protótipo funcional das duas células em ambiente de simulação e, sempre que possível, em bancada experimental, com recurso a plataformas de programação e validação industrial. Essa implementação permitiria avaliar o comportamento dos GRAFCETs, a lógica de máquina de estados, os tempos de resposta das funções de segurança e a coerência entre a arquitetura proposta e o funcionamento real do sistema. No caso da célula colaborativa, seria particularmente útil validar em condições práticas a deteção de presença humana, a adaptação dinâmica da velocidade do robô e a eficácia dos estados de paragem monitorizada.

Em síntese, as limitações identificadas não comprometem a validade conceptual do estudo, mas indicam claramente o caminho para uma futura fase de implementação, teste e otimização da solução proposta.

Referências

[[1] P. P. Groumpos, “A Critical Historical and Scientific Overview of all Industrial Revolutions,” *IFAC-PapersOnLine*, vol. 54, no. 13, pp. 464–471, 2021, doi: 10.1016/j.ifacol.2021.10.492.

[2] K. Schwab, *The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016.

[3] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, “Industry 4.0,” *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, Aug. 2014, doi: 10.1007/s12599-014-0334-4.

[4] A. Sharma and B. J. Singh, “Evolution of Industrial Revolutions: A Review,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 11, pp. 66–73, Sep. 2020, doi: 10.35940/ijitee.I7144.0991120.

[5] M. C. Zizic, M. Mladineo, N. Gjeldum, and L. Celent, “From Industry 4.0 towards Industry 5.0: A Review and Analysis of Paradigm Shift for the People, Organization and Technology,” *Energies*, vol. 15, no. 14, p. 5221, Jul. 2022, doi: 10.3390/en15145221.

[6] M. K. Habib and C. Chimsom, “Industry 4.0: Sustainability and Design Principles,” in *2019 20th International Conference on Research and Education in Mechatronics (REM)*, IEEE, May 2019, pp. 1–8. doi: 10.1109/REM.2019.8744120.

[7] N. Jazdi, “Cyber physical systems in the context of Industry 4.0,” in *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, IEEE, May 2014, pp. 1–4. doi: 10.1109/AQTR.2014.6857843.

[8] A. A. Santos, A. F. da Silva, and F. Pereira, “Simulation of Cyber-Physical Intelligent Mechatronic Component Behavior Using Timed Automata Approach,” J. Machado, F. Soares, J. Trojanowska, S. Yildirim, J. Vojtěšek, P. Rea, B. Gramescu, and O. O. Hrybiuk, Eds., Cham: Springer International Publishing, 2022, pp. 72–85. doi: 10.1007/978-3-031-09385-2_7.

[9] G. Lampropoulos, K. Siakas, and T. Anastasiadis, “Internet of Things in the Context of Industry 4.0: An Overview,” *Int. J. Entrep. Knowl.*, vol. 7, no. 1, pp. 4–19, Jun. 2019, doi: 10.2478/ijek-2019-0001.

[10] E. Oztemel and S. Gursev, “Literature review of Industry 4.0 and related technologies,” *J. Intell. Manuf.*, vol. 31, no. 1, pp. 127–182, Jan. 2020, doi: 10.1007/s10845-018-1433-8.

[11] L. Liu, F. Guo, Z. Zou, and V. G. Duffy, “Application, Development and Future Opportunities of Collaborative Robots (Cobots) in Manufacturing: A Literature Review,” *Int. J. Human–Computer Interact.*, vol. 40, no. 4, pp. 915–932, Feb. 2024, doi: 10.1080/10447318.2022.2041907.

[12] E. Matheson, R. Minto, E. G. G. Zampieri, M. Faccio, and G. Rosati, “Human–Robot

Collaboration in Manufacturing Applications: A Review," *Robotics*, vol. 8, no. 4, p. 100, Dec. 2019, doi: 10.3390/robotics8040100.

[13] S. Robla-Gomez, V. M. Becerra, J. R. Llata, E. Gonzalez-Sarabia, C. Torre-Ferrero, and J. Perez-Oria, "Working Together: A Review on Safe Human-Robot Collaboration in Industrial Environments," *IEEE Access*, vol. 5, pp. 26754–26773, 2017, doi: 10.1109/ACCESS.2017.2773127.

[14] J. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess. Microsyst.*, vol. 77, p. 103201, Sep. 2020, doi: 10.1016/j.micpro.2020.103201.

[15] European Parliament and Council of the European Union, "Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC," *Off. J. Eur. Union*, vol. L165, pp. 1–102, 2023.

[16] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and Industry 5.0—Inception, conception and perception," *J. Manuf. Syst.*, vol. 61, no. October, pp. 530–535, Oct. 2021, doi: 10.1016/j.jmsy.2021.10.006.

[17] Directorate-General for Research and Innovation, "Industry 5.0 - Towards a sustainable, human-centric and resilient European industry," 2021. doi: doi/10.2777/308407.

[18] S. Nahavandi, "Industry 5.0—A Human-Centric Solution," *Sustainability*, vol. 11, no. 16, p. 4371, Aug. 2019, doi: 10.3390/su11164371.

[19] P. K. R. Maddikunta *et al.*, "Industry 5.0: A survey on enabling technologies and potential applications," *J. Ind. Inf. Integr.*, vol. 26, no. July, p. 100257, Mar. 2022, doi: 10.1016/j.jii.2021.100257.

[20] Council of the European Communities, *Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards*. Official Journal of the European Communities, 1985.

[21] European Commission, "The 'Blue Guide' on the implementation of EU product rules 2022," 2022.

[22] European Parliament and Council of the European Union, "Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC," *Off. J. Eur. Union*, vol. L157, pp. 24–86, 2006.

[23] European Commission, "Evaluation of the Machinery Directive 2006/42/EC," 2018.

[24] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[25] Y. Wang and S. H. Chung, "Artificial intelligence in safety-critical systems: a systematic review," *Ind. Manag. Data Syst.*, vol. 122, no. 2, pp. 442–470, Feb. 2022, doi: 10.1108/IMDS-07-2021-0419.

[26] P. Chemweno, L. Pintelon, and W. Decre, "Orienting safety assurance with outcomes of hazard analysis and risk assessment: A review of the ISO 15066 standard for collaborative robot systems," *Saf. Sci.*, vol. 129, no. February, p. 104832, Sep. 2020, doi: 10.1016/j.ssci.2020.104832.

[27] European Commission, “Guide to application of the Machinery Directive 2006/42/EC,” 2024.

[28] European Commission, “REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,” *Off. J. Eur. Union*, vol. L218, 2008.

[29] International Organization for Standardization, “ISO 13849-1:2023 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design,” 2023.

[30] International Organization for Standardization, “ISO 13850:2015 Safety of machinery — Emergency stop function — Principles for design,” 2015.

[31] International Organization for Standardization, “ISO 14119:2024 Safety of machinery — Interlocking devices associated with guards — Principles for design and selection,” 2024.

[32] International Organization for Standardization, “ISO 14120:2015 Safety of machinery — Guards — General requirements for the design and construction of fixed and movable guards,” 2015.

[33] International Organization for Standardization, “ISO 13856-1:2013 Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for the design and testing of pressure-sensitive mats and pressure-sensitive floors,” 2013.

[34] International Organization for Standardization, “ISO 10218-2:2011 Safety requirements for industrial robots — Part 2: Robot systems and integration,” 2011.

[35] International Electrotechnical Commission, “IEC 61496-2 Safety of machinery — Electro-sensitive protective equipment — Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs),” 2020.

[36] International Organization for Standardization, “ISO 13851:2019 Safety of machinery — Two-hand control devices — Principles for design and selection,” 2019.

[37] International Organization for Standardization, “ISO 10218-1:2011 Safety requirements for industrial robots — Part 1: Robot,” 2011.

[38] C. Scholz *et al.*, “Sensor-Enabled Safety Systems for Human – Robot Collaboration : A Review,” *IEEE Sens. J.*, vol. 25, no. 1, pp. 65–88, 2025, doi: 10.1109/JSEN.2024.3496905.

[39] R.-J. Halme, M. Lanz, J. Kämäräinen, R. Pieters, J. Latokartano, and A. Hietanen, “Review of vision-based safety systems for human-robot collaboration,” *Procedia CIRP*, vol. 72, pp. 111–116, 2018, doi: https://doi.org/10.1016/j.procir.2018.03.043.

[40] S. S. M. B. P. B., M. Valori, G. Legnani, and I. Fassi, “Assessing Safety in Physical Human–Robot Interaction in Industrial Settings: A Systematic Review of Contact Modelling and Impact Measuring Methods,” 2025. doi: 10.3390/robotics14030027.

[41] Z. Saleem, F. Gustafsson, E. Furey, M. Mcafee, and S. Huq, “A review of external sensors for human detection in a human robot collaborative environment,” *J. Intell. Manuf.*, vol. 36, no. 4, pp. 2255–2279, 2025, doi: 10.1007/s10845-024-02341-2.

[42] International Organization for Standardization, “ISO 12100:2010 Safety of machinery — General principles for design — Risk assessment and risk reduction,” 2010.

[43] O. Görnemann and S. A. G. Waldkirch, “EN ISO 12100 and its relation to the Machinery

Directive," 2019. [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/Areas of Work/CENELEC sectors/Mechanical and Machines/Documents/Quicklinks/eniso12100relationmachinerydirective.pdf

Declaração de Integridade

Declaro ter conduzido este trabalho académico com integridade. Não plagiei ou apliquei qualquer forma de uso indevido de informações ou falsificação de resultados ao longo do processo que levou à sua elaboração.

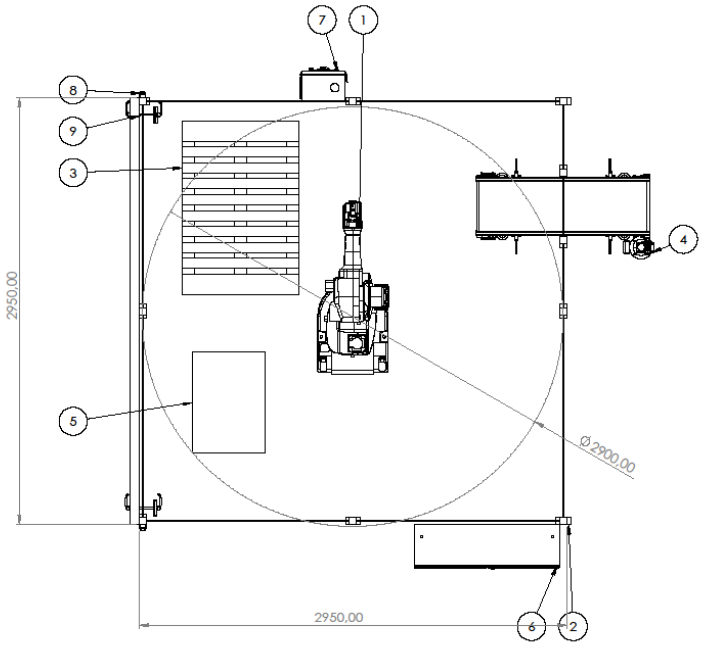
Declaro que o trabalho apresentado neste documento é original e de minha autoria, não tendo sido utilizado anteriormente para nenhum outro fim.

Declaro ainda que tenho pleno conhecimento do Código de Conduta Ética do P.PORTO.

NOME: Gonçalo Martins Pinho

ISEP, Porto, 12 de junho de 2026

Apêndice A



ITEM NO.	PART NUMBER	QTY.
1	Robô	1
2	Vedação	1
3	Palete	1
4	Transportador de alimentação	1
5	Estação de Inspeção	1
6	Quadro elétrico	1
7	HMI	1
8	Botoneira	2
9	Interbloqueio - FS2	2

UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:

FINISH:

DEBURR AND BREAK SHARP EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

TITLE:

MATERIAL:

WEIGHT:

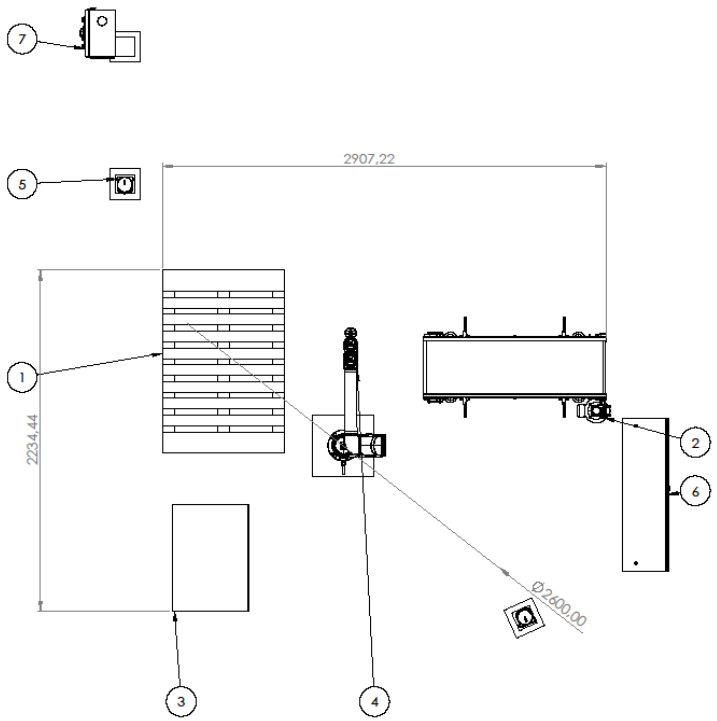
DWG NO. caso 1

A2

SCALE:1:50

SHEET 1 OF 1

Apêndice B



ITEM NO.	Descrição	QTY.
1	Palete	1
2	Transportador de alimentação	1
3	Estação de Inspeção	1
4	Robô colaborativo	1
5	LiDAR	2
6	Quadro elétrico	1
7	Consola	1

UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBURR AND BREAK SHARP EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

TITLE:

MATERIAL:

DWG NO. caso 2

A2

WEIGHT:

SCALE:1:20

SHEET 1 OF 1