ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

Sistema de Integração Segura e Análise Automática de CCTV com Câmaras em Redes Não Controladas

Gustavo Caiano

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Engenharia de Software

Orientador: Paulo Baltarejo Sousa
Supervisor: Francisco Loureiro

Porto, 31 de dezembro de 2025

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.

Portanto, 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.

ISEP, Porto, 31 de dezembro de 2025

Dedicatória

The dedicatory is optional. Below is an example of a humorous dedication.

"To my wife Marganit and my children Ella Rose and Daniel Adam without whom this book would have been completed two years earlier."in "An Introduction To Algebraic Topology"by Joseph J. Rotman.

Resumo

O presente trabalho de dissertação propõe o desenvolvimento do Flexible Universal Stream Engine (FUSE), uma plataforma de software inovadora concebida para centralizar e organizar sistemas de videovigilância heterogéneos, geograficamente dispersos e situados em redes não controladas. Esta investigação surge em resposta a desafios críticos identificados na segurança pública e privada, nomeadamente a fragmentação tecnológica, as vulnerabilidades de segurança inerentes às comunicações Peer-to-Peer (P2P) e a ineficiência operacional enfrentada por entidades como os Órgão de Polícia Criminals (OPCs) na análise forense de vídeo.

A arquitetura proposta integra uma camada de abstração de hardware que normaliza a comunicação com câmaras de diversos fabricantes através do protocolo Real Time Streaming Protocol (RTSP), garantindo a interoperabilidade. A segurança das comunicações é assegurada através de túneis Virtual Private Network (VPN) que protegem a integridade e confidencialidade dos dados em redes não controladas, complementada por um modelo de controlo de acessos Action/Attribute Based Access Control (ABAC). Adicionalmente, o sistema incorpora um módulo de visão computacional progressivo, estruturado em três fases: deteção de atividade para filtragem temporal, classificação de objetos (e.g., humanos, veículos) e extração de atributos específicos, visando a automatização da análise forense e a redução significativa da carga de trabalho manual.

A metodologia adotada segue o paradigma de "Design and Creation", com a validação da solução a ser realizada através de um protótipo funcional (Minimum Viable Product (MVP)) em cenários simulados e reais. Os resultados esperados centram-se na demonstração da eficácia da integração segura de dispositivos, na robustez da proteção de dados e na otimização dos processos de investigação criminal, sempre em estrita observância dos princípios éticos e regulamentares, como o EU AI Act.

Palavras-chave: Videovigilância, Integração CCTV, Automatização, Deteção de Objetos, Software Seguro, IoT Communication

Abstract

This dissertation presents the development of FUSE, a software platform designed to unify and secure heterogeneous video surveillance systems dispersed across uncontrolled networks. Addressing the challenges of technological fragmentation and security vulnerabilities in current Closed Circuit Television (CCTV) infrastructures, FUSE provides a centralized solution for entities such as Law Enforcement Agenciess (LEAs)

The proposed architecture features a hardware abstraction layer for normalizing camera communications via RTSP and secures data transmission through VPN tunneling. It implements ABAC as an access control method, and integrates a three-stage computer vision pipeline for automated activity detection, object classification, and attribute extraction. This approach aims to enhance interoperability, data security, and forensic analysis efficiency, adhering to ethical standards like the EU AI Act.

Agradecimentos

The optional Acknowledgment goes here. . . Below is an example of a humorous acknowledgment.

"I'd also like to thank the Van Allen belts for protecting us from the harmful solar wind, and the earth for being just the right distance from the sun for being conducive to life, and for the ability for water atoms to clump so efficiently, for pretty much the same reason. Finally, I'd like to thank every single one of my forebears for surviving long enough in this hostile world to procreate. Without any one of you, this book would not have been possible."in "The Woman Who Died a Lot"by Jasper Fforde.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Contexto

No panorama atual dos sistemas de videovigilância verifica-se uma grande dependência de hardware, como Network Video Recorders (NVRs) para agregar várias câmaras e disponibilizar streaming da sua imagem. A maioria destes dispositivos também possibilita o *playback* e exportação de vídeos gravados, sendo que alguns controlam ainda os acessos de utilizadores. A detecção de movimentos ou objetos é uma *feature* de apenas alguns modelos apesar de que, ultimamente, se têm verificado um grande crescimento e aposta tecnológica nesta área [1]. Assim, os NVRs, embora raramente reúnam individualmente todas estas funcionalidades num dispositivo só [2], são a peça central do processo de videovigilância dentro de uma rede controlada.

O presente trabalho decorre em contexto empresarial, sendo acolhido pela empresa Stability-Bubble, Lda. O Flexible Universal Stream Engine (FUSE) não se configura apenas como um exercício académico teórico, mas sim como a proposta de uma plataforma comercial destinada a responder a lacunas de mercado identificadas pela empresa. Assim, esta dissertação visa conciliar o rigor da investigação científica com os requisitos práticos e operacionais de um produto de software real, tirando partido da infraestrutura e *know-how* da entidade de acolhimento.

1.2 Problema

Em determinados cenários [3], existe a impossibilidade destas câmaras serem inseridas todas numa determinada Local Area Network (LAN) privada. Por este motivo e por estarem numa outra rede não controlada, é necessário aceder via Internet, que origina alguns problemas, tais como:

- Incompatibilidade entre câmaras de diferentes fornecedores, obrigando muitas vezes à utilização de mais do que um software, já que nem todas são totalmente compatíveis com a mesma aplicação.
- Falta de segurança e de privacidade dos dados, uma vez que muitas destas câmaras recorrem a conexões Peer-to-Peer (P2P) quando acedidas fora da LAN. Este mecanismo depende, geralmente, de servidores do fabricante, sobre os quais não existe controlo nem garantia de proteção dos dados [4]. Além disso, a comunicação entre a aplicação e a câmara é frequentemente pouco segura e não encriptada, expondo a stream de vídeo e as credenciais a potenciais ataques.

- Falta de controlo de acessos e gestão de utilizadores, pois a maior parte das aplicações de acesso remoto a Closed Circuit Television (CCTV) são desenvolvidas para cenários onde estas atividades não são a prioridade [5], priorizando o acesso intuitivo e rápido.

Para além destas barreiras técnicas e de segurança, emerge um desafio operacional extremamente relevante, particularmente no contexto da segurança pública. Entidades como os Órgão de Polícia Criminals (OPCs) dependem de videovigilância para a obtenção de provas. O processo atual, contudo, assenta frequentemente na revisão humana através da visualização integral contínua das gravações efetuadas, distribuindo muitas vezes intervalos de tempo por vários agentes para que seja facilitado. Esta informação foi obtida através de um questionário/entrevista, realizado em conjunto com agentes da investigação criminal da Guarda Nacional Republicana (GNR) e da Polícia de Segurança Pública (PSP), no qual o objetivo principal seria a validação da existência deste problema. O mesmo pode ser consultado no Apêndice A. Ainda assim, este processo torna-se demorado e intensivo, recorrendo a uma enorme quantidade de recursos humanos e tempo, que são valiosos e, infelizmente, escassos [6].

Uma vez que estes problemas trazem insegurança e ineficiência, resolvê-los é uma preocupação do encarregado de segurança e CCTV de uma entidade pública ou privada, tal como dos agentes encarregues pela obtenção de prova sob videovigilância dentro das polícias de investigação criminal. É neste contexto de múltiplos desafios que surge a proposta deste trabalho: o desenvolvimento do FUSE. O FUSE é idealizado como uma plataforma de software que centraliza e organiza sistemas de videovigilância heterogéneos e geograficamente dispersos, com um foco integrado na segurança dos dados, na automatização da análise de vídeo, e na manutenção de registos de auditoria e gestão de utilizadores.

1.3 Pergunta de Investigação

A proposta desta plataforma levanta a seguinte pergunta principais de investigação:

RQ1: De que forma pode ser desenhada/projetada uma solução de software que permita aceder seguramente a câmaras CCTV, localizadas em redes externas não controladas, caracterizadas por uma elevada diversidade de arquiteturas, padrões tecnológicos e origem de fabrico?

Decompondo esta pergunta para uma melhor e mais estruturada compreensão, a investigação será guiada pelas seguintes sub-perguntas operacionais:

RQ1.1: Como pode ser desenhada uma camada de abstração de software que normalize as funcionalidades (visualização, controlo, gravação) de câmaras de diferentes interfaces e especificações técnicas distintas, garantindo a extensibilidade futura do sistema?

RQ1.2: Que mecanismos de rede e protocolos de comunicação são mais eficazes para garantir a confidencialidade e integridade da comunicação com câmaras localizadas em redes não fidedignas, sem introduzir vulnerabilidades na rede de destino e agregação das várias streams?

RQ1.3: Em que medida a integração de modelos de visão computacional para a automatização da deteção de eventos pode validar a utilização da plataforma proposta para otimização de processos de investigação criminal?

A resposta à questão central de investigação (RQ1) será materializada através da implementação e validação experimental da plataforma FUSE. Todo o processo encontra-se detalhado

na Seção 1.5 referente à Metodologia. No entanto, para fundamentar as decisões técnicas necessárias na implementação do Minimum Viable Product (MVP) analisar-se-ão as sub-questões operacionais, no Capítulo 2.

1.4 Objetivos

Foram definidos o seguintes objetivos para o desenvolvimento e validação do FUSE:

- Desenvolver uma arquitetura de software extensível que, através de uma camada de abstração, normalize a comunicação com câmaras de diferentes fornecedores. O sistema deverá suportar um protocolo base de streaming como o Real Time Streaming Protocol (RTSP) e centralizar as funcionalidades de visualização em tempo real, gravação, e *playback* numa interface unificada.
- Implementar um modelo de comunicação seguro, Secured By Design, que utilize túneis Virtual Private Network (VPN) para isolar e criptografar a comunicação entre as câmaras externas e o servidor de implementação da aplicação.
- Desenvolver um sistema de controlo de acessos baseado em ações (modelo Action/Attribute Based Access Control (ABAC)) para gerir as permissões de utilizadores de forma granular e garantir a auditoria das ações.
- Integrar um módulo de análise de vídeo para a deteção automatizada de eventos complexos, implementando uma *pipeline* de processamento progressivo em três fases:
  - Fase 1 (Deteção de Atividade): Identificação de movimento e atividade relevante nos streams de vídeo para filtrar segmentos de interesse.
  - Fase 2 (Classificação de Objetos): Análise dos segmentos filtrados para detectar e classificar objetos de categorias pré-definidas (e.g., humanos, veículos, animais).
  - Fase 3 (Extração de Atributos): Análise aprofundada dos objetos classificados para extrair características específicas e customizáveis, como matrículas e cores de veículos, ou atributos de vestuário e acessórios de pessoas, que servirão de base para a pesquisa de eventos complexos.
- Validar a viabilidade da arquitetura através de um protótipo funcional (MVP) que demonstre a integração bem-sucedida de, no mínimo, duas câmaras tecnologicamente diferentes, a segurança da comunicação e a eficácia da deteção de eventos num cenário simulado, pelo menos até à Fase 2 anteriormente mencionada.

Quanto aos principais contributos deste trabalho, espera-se que do ponto de vista técnico-científico surja uma arquitetura referência para integração segura e inteligente de sistemas CCTV distribuídos, principalmente quando há a presença de interoperabilidade entre redes não controladas e controladas. Por outro lado, do ponto de vista social e operacional, tenciona-se validar a ferramenta para que esta possa vir a aumentar significativamente a eficiência e eficácia da investigação criminal dos OPC, otimizando a alocação de recursos e reduzindo o tempo de análise manual do vídeo.

1.5 Metodologia

A metodologia adotada para a realização deste trabalho académico baseia-se no modelo de "Research Process" proposto por B. J. Oates no livro "Researching Information Systems and Computing" [7], ilustrado na Figura 1.1.

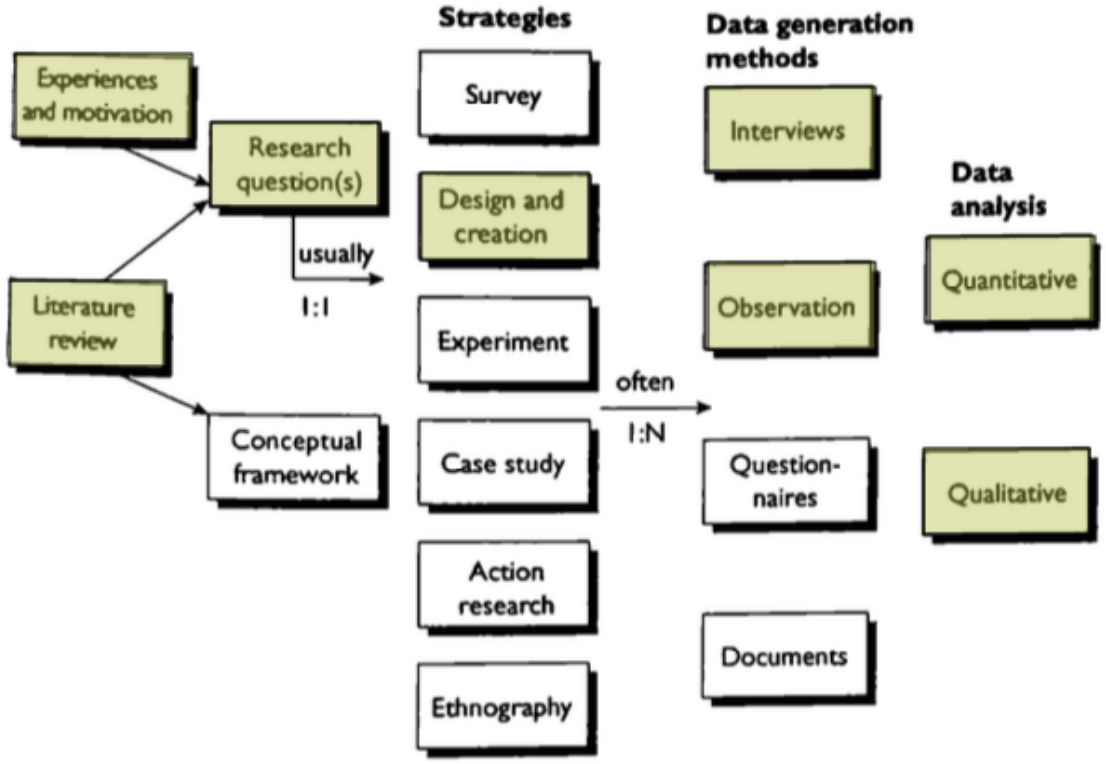

Figura 1.1: Diagrama de "Research Process" de B. J. Oates [7], aplicado ao contexto do projeto.

O ponto de partida da investigação enquadra-se em "**Experiences and motivation**", dado que a génese deste projeto deriva diretamente da observação da ineficiência e limitações técnicas enfrentadas pelos OPCs e gestores de segurança na recolha de imagens de CCTV. Através de feedback adquirido através de questionários e entrevistas com Núcleos (GNR) e Esquadras (PSP) de Investigação Criminal (Apêndice A), estes problemas são confirmados e registrados. Complementarmente, é realizada uma revisão de literatura preliminar para compreender o estado da arte em protocolos de comunicação e visão computacional. Esta análise permitiu identificar a ausência de soluções integradas que garantam simultaneamente segurança em redes não controladas e inteligência analítica avançada. A junção desta necessidade prática (experiência) com a identificação desta lacuna teórica (literatura) resultou na formalização das perguntas de investigação apresentadas anteriormente.

A estratégia central adotada para este trabalho é a de "**Design and Creation**". Esta abordagem é a mais adequada para projetos de Engenharia de Software cujo objetivo primário é o desenvolvimento de um protótipo que visa resolver muitos dos problemas práticos observados e identificados em determinado cenário, como forma de validação de futura implementação ou desenvolvimento de algo mais avançado. Dentro desta estratégia inserem-se quatro principais passos, nomeadamente Design, Desenvolvimento, Testes e Conclusões.

Relativamente aos resultados e à sua avaliação, será usado o método de "**Interviews**" com utilizadores finais, sendo estes OPCs ou encarregados de segurança de uma outra entidade, de modo a recolher feedback e validação do funcionamento do protótipo e respetiva utilidade do mesmo. Em adição, será também usado o método de "**Observation**", onde se poderá obter e quantificar resultados e taxas de correspondência na análise automática de eventos e objetos.

Quanto à análise de dados, optou-se por uma abordagem mista que integra os dois métodos disponíveis: "**Quantitative**" e "**Qualitative**". A análise quantitativa incidirá sobre as métricas técnicas recolhidas durante os testes do protótipo, tais como as taxas de precisão e alerta na deteção e classificação de objetos (Fase 2 e 3 da pipeline), a latência do streaming via túnel VPN, os tempos de processamento da análise de vídeo, entre outros. Já a análise qualitativa será aplicada à interpretação do feedback dos utilizadores e das observações de cenário real, avaliando o impacto operacional da ferramenta, a eficácia percebida na redução do tempo de investigação e a adequação da interface aos processos de trabalho dos OPCs.

1.6 Considerações Éticas

A realização deste trabalho rege-se pelos princípios de integridade, responsabilidade e rigor científico descritos no Código de Boas Práticas e de Conduta do P.PORTO [8].

Do ponto de vista profissional, o trabalho enquadra-se nos princípios estruturantes da engenharia de software, alinhados com referências internacionais como o Software Engineering Code of Ethics and Professional Practice, desenvolvido em conjunto pela Association for Computing Machinery (ACM) e pela IEEE Computer Society (IEEE-CS) [9]. A conformidade com estes princípios garante a qualidade e segurança dos sistemas desenvolvidos, a responsabilidade perante clientes e utilizadores, e a honestidade na comunicação de resultados, limitações e riscos associados às soluções tecnológicas.

O FUSE envolve uma *pipeline* de análise automática aplicada a contextos de videovigilância, potencialmente incidindo sobre a obtenção de dados pessoais identificáveis. Estes dados sensíveis apenas serão obtidos num contexto de validação do MVP em cenário real, que estará sempre salvaguardado por requerimento de despacho judicial para fornecimento de meios técnicos e respetiva autorização de captação de imagem. Ainda assim, a pipeline é desenhada em estrita observância do EU AI Act [10], garantindo que o sistema não incorre em "Unacceptable risks".

O sistema não se destina, nem permite, práticas proibidas tais como:

- *Social scoring* ou manipulação comportamental;
- Recolha indiscriminada (untargeted scraping) de imagens de CCTV para criação de bases de dados de reconhecimento facial;
- Identificação biométrica remota em tempo real em espaços públicos para fins policiais (real-time remote biometric identification).

No âmbito do último ponto, apesar do alvo ser legislar o reconhecimento biométrico em tempo-real, justifica-se a conformidade pela natureza da análise automática, que será realizada sob gravações dos eventos, e não sob o próprio streaming.

A análise focada na "Fase 3" da pipeline de deteção automática restringe-se à classificação de características objetivas (e.g., cor de vestuário, tipo de veículo) para auxiliar a pesquisa

forense, mantendo sempre o princípio da validação humana, onde a decisão final cabe ao agente humano e não ao algoritmo.

1.7 Estrutura do Documento

Este documento está organizado em capítulos que apresentam de forma estruturada o trabalho desenvolvido. O Capítulo 1 (Introdução) apresenta o contexto do problema, as questões de investigação, os objetivos, as considerações éticas, a metodologia adotada e a estrutura do documento.

O Capítulo 2 (Estudo do Estado da Arte) apresenta uma revisão sistemática da literatura sobre arquiteturas de abstração e interoperabilidade de dispositivos Internet of Things (IoT), protocolos de comunicação segura e visão computacional, respondendo às sub-questões de investigação operacionais.

O Capítulo 3 (Planeamento de Trabalho) descreve o âmbito do projeto através de um Work Breakdown Structure (WBS), apresenta o cronograma de execução através de um diagrama de Gantt e identifica os stakeholders e riscos do projeto.

O documento inclui ainda uma secção de Bibliografia com todas as referências utilizadas e o Apêndice A que contém o questionário e entrevistas realizadas junto dos OPCs.

Capítulo 2

Estudo do Estado da Arte

Este capítulo apresenta a revisão de literatura fundamentada no âmbito do projeto, analisando o estado atual das tecnologias críticas para o desenvolvimento do FUSE. O objetivo principal desta revisão é responder às sub-questões operacionais previamente identificadas, nomeadamente a RQ1.1 e a RQ1.2, estabelecendo uma base teórica sólida para as decisões de arquitetura e segurança.

Adicionalmente, e dada a natureza aplicada da RQ1.3, é conduzido um estudo técnico aprofundado sobre os paradigmas atuais de visão computacional. Este estudo visa não apenas identificar o estado da arte, mas também comparar padrões, pipelines de processamento e modelos de Artificial Intelligence (AI) passíveis de integração na plataforma.

2.1 Processo de Investigação

O Processo de investigação foi guiado pelo mapeamento das duas primeiras sub-questões da presente dissertação em questões de pesquisa com foco na revisão literária, conforme descrito na Tabela 2.1.

Tabela 2.1: Questões de Pesquisa Orientadas à Revisão Literária

RQ ID	**LRRQ ID**	**Description**	**Tópicos e Keywords de pesquisa**
RQ1.1	LRRQ1	Quais são as arquiteturas de referência e padrões de design de software descritos na literatura para a abstração e interoperabilidade de dispositivos IoT heterogéneos?	IoT Interoperability, Hardware Abstraction Layer, Middleware patterns, Open Network Video Interface Forum (ONVIF) standardization, Heterogeneous device integration.
RQ1.2	LRRQ2	Qual o estado da arte em protocolos de comunicação segura e VPNs para acesso remoto e *streaming*?	Secure Tunneling Protocols, VPN performance analysis, Streaming encryption, Network Address Translation (NAT) Traversal, Zero Trust Network Access (ZTNA).

Cada questão de pesquisa será enquadrada de acordo com o modelo Population, Intervention, Comparison, Outcomes, Context, Study (PICOCS) [11], garantindo o rigor na seleção

das fontes utilizadas. A informação será depois selecionada seguindo o fluxo Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) [12]. O processo inclui a definição de keywords de pesquisa, a aplicação estrita de critérios de inclusão e exclusão, seguida de uma filtragem em etapas e, finalmente, uma discussão crítica sobre a aplicabilidade dos estudos selecionados para a arquitetura do FUSE.

Como fator inclusivo de seleção, selecionou-se, por exemplo, a data de publicação posterior a 2018. A escolha deste intervalo visa garantir que as arquiteturas, frameworks e algoritmos analisados representam o atual estado da arte, evitando a adoção de paradigmas que, embora válidos no passado, não refletem as necessidades de desempenho e escalabilidade dos sistemas modernos. Foram privilegiados artigos revistos por pares, normas técnicas e literatura técnica amplamente reconhecida. Excluíram-se estudos puramente teóricos sem aplicação prática ao domínio da videovigilância ou da integração de dispositivos, tal como trabalhos relativos a soluções proprietárias fechadas sem documentação técnica pública suficiente.

2.2 LRRQ1 - Arquiteturas de Abstração e Interoperabilidade IoT

Nesta secção, a literatura é revista de forma a responder à questão de investigação "Quais são as arquiteturas de referência e padrões de design de software descritos na literatura para a abstração e interoperabilidade de dispositivos IoT heterogéneos?".

2.2.1 Processo de Pesquisa

A questão de investigação foi estruturada de acordo com o modelo PICOCS apresentado na Tabela 2.2.

Tabela 2.2: Modelo PICOCS para a LRRQ1

PICOCS	Parte da RQ	I/E	Sub string
P	Estudos envolvendo dispositivos IoT heterogéneos e CCTV	I - Estudos que considerem heterogeneidade E - Anteriores a 2018	>=2018; IoT; Heterogeneous; CCTV
I	Arquiteturas de software, Middleware e Camadas de Abstração	I - Estudos sobre padrões de design e abstração E - Soluções proprietárias fechadas	Software Architecture; Middleware; Abstraction Layer; Design Patterns
C	—	—	—
O	Arquiteturas de referência e interoperabilidade	I - Estudos que propõem ou validam arquiteturas	Architecture; Interoperability; Framework
C	Engenharia de Software e Sistemas Distribuídos	I - Académico I - Indústria	Software Engineering; Distributed Systems
S	Estudos de caso e Propostas de Arquitetura	I - Case Studies I - System Proposals E - Opiniões sem validação	Case study; Proposal; Prototype

A tabela inclui os critérios de inclusão e exclusão (I/E) relacionados com cada parte da questão de investigação, bem como as possíveis *sub-strings* utilizadas para conduzir a pesquisa nas bases de dados científicas. Apenas estudos de 2018 em diante que contemplem arquiteturas de software ou middleware para integração de dispositivos heterogéneos foram considerados.

A pesquisa foi conduzida em três bases de dados principais: IEEE Xplore (282 registos), ACM Digital Library (94 registos) e ScienceDirect (59 registos), totalizando 435 registos identificados através de pesquisa sistemática. Adicionalmente, foi identificado 1 registo [13] através de outras fontes, resultando num total de 436 registos na fase de identificação.

Após a remoção de duplicados (1 registo), foram analisados 435 registos na fase de screening através da leitura de títulos e resumos. Desta análise, 412 registos foram excluídos por não cumprirem os critérios de inclusão, nomeadamente por focarem-se puramente em algoritmos de visão computacional sem arquitetura de sistema, abordarem domínios como agricultura ou saúde sem componente de vídeo, ou simplemsmente não se adequar ao tema de integração de dispositivos IoT ou de camadas de abstração em design de software. Os 23 registos restantes foram avaliados em texto completo, dos quais 12 foram excluídos por falta de detalhes de implementação, ausência de diagrama de arquitetura claro, ou por serem propostas teóricas sem validação prática. O processo resultou na inclusão final de 11 estudos na revisão qualitativa, conforme ilustrado na Figura 2.1.

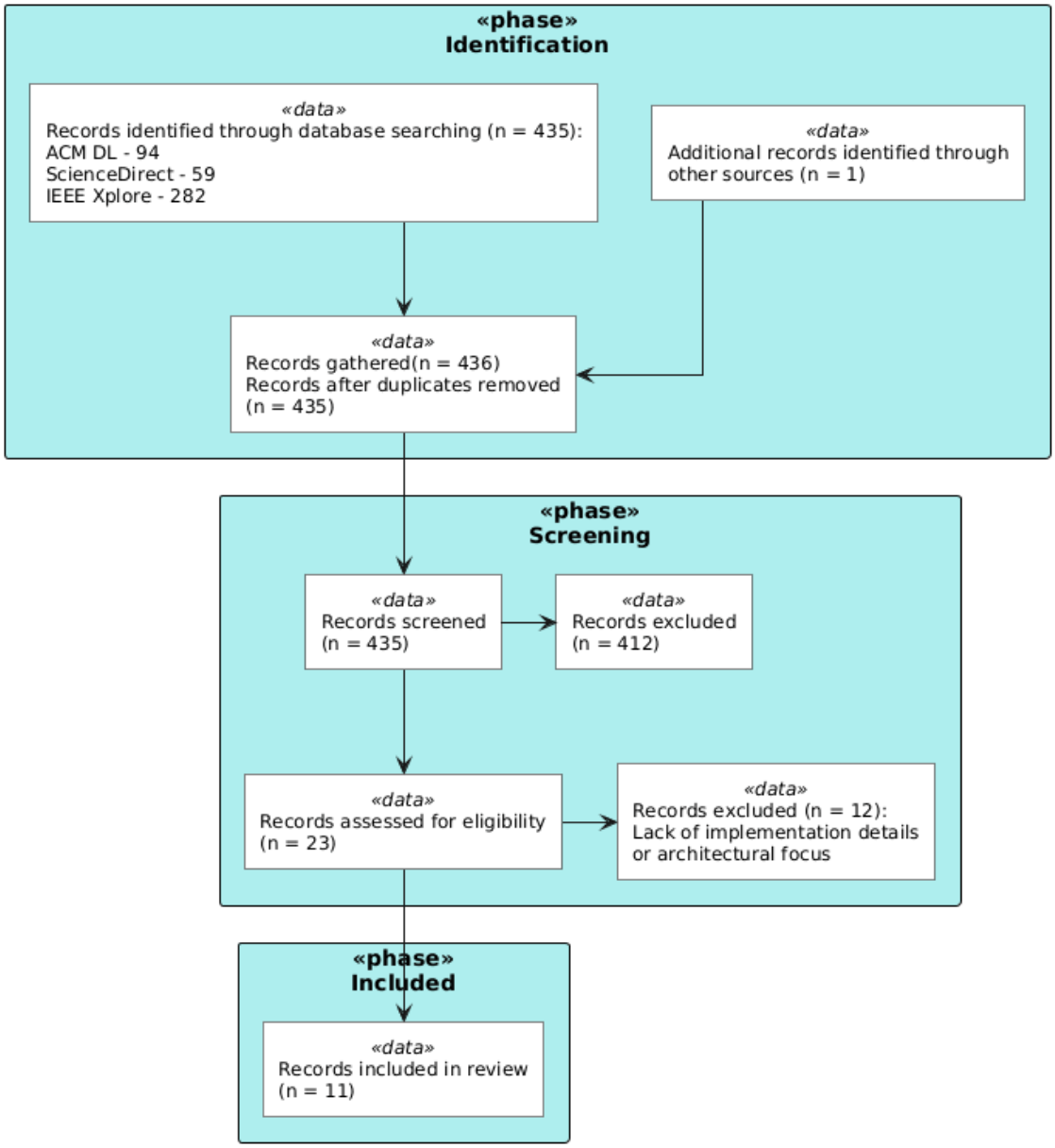

Figura 2.1: Fluxo PRISMA para a LRRQ1

O rigor na filtragem aplicada, reduzindo de 435 para 11 estudos incluídos, garantiu que apenas trabalhos com arquiteturas de sistema relevantes, detalhadas e validadas fossem analisados, assegurando a qualidade e relevância da revisão de literatura para fundamentar as decisões arquiteturais do FUSE.

2.2.2 Discussão

A análise dos 11 estudos incluídos revela uma convergência clara na literatura: a integração direta de dispositivos IoT heterogéneos sem uma camada intermediária resulta em sistemas monolíticos e de difícil manutenção.A diversidade de protocolos (RTSP, Hypertext Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT)), algoritmos de

codificação de vídeo (H.264, H.265, MJPEG) e especificidades de fabricantes exige, invariavelmente a implementação de uma camada de abstração que atue como tradutor universal. Como observa [14], a ausência desta camada força o sistema central a lidar com a complexidade de hardware, violando princípios de desacoplamento. A literatura valida que a solução reside numa arquitetura que isole a lógica de negócio das particularidades dos dispositivos.

Padrões Arquiteturais: De Gateways a Microserviços Agnósticos

A evolução dos padrões arquiteturais na literatura aponta para um distanciamento de *gateways* simples em direção a microserviços inteligentes. Inicialmente, soluções como o IoTM2B [15] e Smart Gateway [14] validaram o uso de um ponto central para tradução de protocolos (ex: converter MQTT/Constrained Application Protocol (CoAP) para HTTP). No entanto, [15] identifica uma limitação crítica: a normalização para HTTP POST, embora eficaz para telemetria escalar (temperatura), introduz um gargalo de desempenho inaceitável para *streaming* de vídeo contínuo.

A resposta a esta limitação encontra-se na adoção de microserviços com o padrão *Mediator*, como proposto por [16]. Esta abordagem introduz uma Camada de Abstração de Dados dedicada que desacopla a lógica de serviço da comunicação com o dispositivo. Mais relevante para o conceito do FUSE é a introdução do padrão "Access Mapper" ou "Digital Twin" por [17]. Neste modelo, a aplicação central interage exclusivamente com um "Dispositivo Virtual" estandardizado, tornando-se completamente agnóstica ao hardware físico. Este é o fundamento teórico para um componente da solução a desenvolver, ou seja, uma camada que encapsula a complexidade do driver proprietário e expõe uma interface limpa e uniforme.

Abstração de Media e Normalização de Streaming

A abstração em sistemas de videovigilância exige também a normalização do próprio fluxo de vídeo. A conexão direta entre uma aplicação web e câmaras de vigilância apresenta desafios técnicos significativos devido à natureza dos fluxos de vídeo brutos e algoritmos de codificação de vídeo utilizados. A literatura, nomeadamente [18], suporta a implementação de uma camada intermédia responsável pela ingestão e gestão destes fluxos, expondo-os posteriormente num formato standardizado e otimizado para consumo web (como HTTP Live Streaming (HLS) ou Web Real-Time Communication (WebRTC)).

Esta abordagem desacopla a aplicação cliente da complexidade de conexão direta às câmaras: o cliente consome sempre um fluxo normalizado a partir da camada de abstração. Embora [18] e [19] discutam também o processamento semântico destes fluxos na Edge (análise de vídeo), este tópico específico de automação e visão computacional será aprofundado na Secção 2.4. Para a LRRQ1, o contributo essencial é a arquitetura que garante a estabilidade e abstração do *streaming*.

Escalabilidade e Adaptabilidade à Rede

A viabilidade futura do sistema depende da sua capacidade de escalar para novos dispositivos e adaptar-se a redes instáveis. [14] demonstra a importância do *ThingDiscovery* automatizado para detetar novas câmaras sem configuração manual, um requisito essencial para a usabilidade. No que toca à rede, [20] introduz o conceito vital de "Latency-Accuracy Trade-off", onde o middleware ajusta dinamicamente parâmetros (como resolução) face à congestão da rede. A validação empírica desta topologia distribuída é fornecida por [21], que

comprova uma redução de latência de até 98% em arquiteturas Edge Computing comparativamente à Cloud pura para serviços críticos. Adicionalmente, [22] demonstra as vantagens de uma arquitetura baseada em cadeias de módulos independentes. Esta modularidade permite que componentes distintos (como a ingestão de vídeo, a transcodificação e a análise) operem de forma independente e encadeada. Para o FUSE, isto significa que é possível atualizar ou substituir módulos individuais sem comprometer a estabilidade do sistema base.

Análise Crítica

Apesar da diversidade de soluções, a revisão identifica lacunas relevantes para o contexto do FUSE. Primeiro, a maioria das arquiteturas foca-se em telemetria (sensores), negligenciando os requisitos específicos de largura de banda do vídeo [15]. Segundo, embora existam padrões sintáticos, [23] alerta para a falta de "Interoperabilidade Pragmática", ou seja, a capacidade dos dispositivos comunicarem a intenção do dado (ex: urgência de um alerta) e não apenas o conteúdo.

O trabalho de [13] valida a viabilidade de usar plataformas open-source como o ZoneMinder para orquestrar estes fluxos em hardware modesto, atuando como um middleware de abstração eficaz. No entanto, o estudo alerta para os limites de performance quando se tenta realizar processamento analítico pesado no mesmo *node*, reforçando a necessidade de uma arquitetura eficiente e distribuída.

Conclusão

A revisão da literatura fundamenta, de forma inequívoca, que a arquitetura do FUSE deve assentar numa **Camada de Abstração Modular localizada**. Esta camada tem como responsabilidades críticas: (1) normalizar a comunicação com dispositivos heterogéneos para uma interface agnóstica [15, 14], (2) abstrair a complexidade do hardware físico através de representações virtuais [17], e (3) garantir a gestão unificada do *streaming* de vídeo [18]. A adoção de uma estrutura modular, em detrimento de uma abordagem monolítica rígida, assegura que o sistema possa acomodar novos protocolos e dispositivos futuramente [16], garantindo que a aplicação central permaneça desacoplada da volatilidade do hardware e assegurando a sua escalabilidade a longo prazo.

2.3 LRRQ2 - Protocolos de Comunicação Segura e VPN

Nesta secção, a literatura é revista de forma a responder à questão de investigação "Qual o estado da arte em protocolos de comunicação segura e VPNs para acesso remoto e *streaming*".

2.3.1 Processo de Pesquisa

A questão de investigação foi estruturada de acordo com o modelo PICOCS apresentado na Tabela 2.3.

Tabela 2.3: Modelo PICOCS para a LRRQ2

PICOCS	Parte da RQ	I/E	Sub string
P	Estudos envolvendo acesso remoto a dispositivos em redes não controladas	I - Estudos que considerem redes não controladas E - Anteriores a 2018	>=2018; Remote access; Uncontrolled networks; Hostile networks
I	Protocolos de comunicação segura, VPNs e mecanismos de túnel	I - Estudos sobre protocolos de segurança e túneis E - Soluções proprietárias fechadas	Secure protocols; VPN; Tunneling; Encryption; Secure communication
C	—	—	—
O	Estado da arte em protocolos e desempenho de VPNs	I - Estudos que analisem ou comparem protocolos I - Análises de desempenho	Protocol comparison; VPN performance; Security analysis; Streaming protocols
C	Comunicações de rede e segurança de sistemas distribuídos	I - Académico I - Indústria	Network security; Distributed systems; Secure streaming
S	Estudos de caso, análises comparativas e propostas de protocolos	I - Case Studies I - Comparative analysis E - Opiniões sem validação	Case study; Comparative study; Protocol proposal; Performance evaluation

A tabela inclui os critérios de inclusão e exclusão (I/E) relacionados com cada parte da questão de investigação, bem como as possíveis *sub-strings* utilizadas para conduzir a pesquisa nas bases de dados científicas. Apenas estudos de 2018 em diante que contemplem protocolos de comunicação segura, VPNs ou mecanismos de túnel para acesso remoto e *streaming* foram considerados.

A pesquisa foi conduzida em três bases de dados principais: IEEE Xplore (62 registos), ACM Digital Library (15 registos) e ScienceDirect (2 registos), totalizando 79 registos identificados através de pesquisa sistemática. Adicionalmente, foi identificado 1 registo através de outras fontes, o mesmo identificado para a outra questão [13], resultando num total de 80 registos na fase de identificação.

Após a verificação de duplicados, não foram encontrados registos duplicados, mantendo-se os 80 registos para análise na fase de screening através da leitura de títulos e resumos. Desta análise, 52 registos foram excluídos por não cumprirem os critérios de inclusão, nomeadamente por serem irrelevantes para o tema de VPNs, protocolos seguros ou por falta de foco em acesso remoto. Os 28 registos restantes foram avaliados em texto completo, dos quais 9 foram excluídos por tecnologia obsoleta, falta de detalhes de implementação ou por estarem fora do âmbito do estudo. O processo resultou na inclusão final de 19 estudos na revisão qualitativa, conforme ilustrado na Figura 2.2.

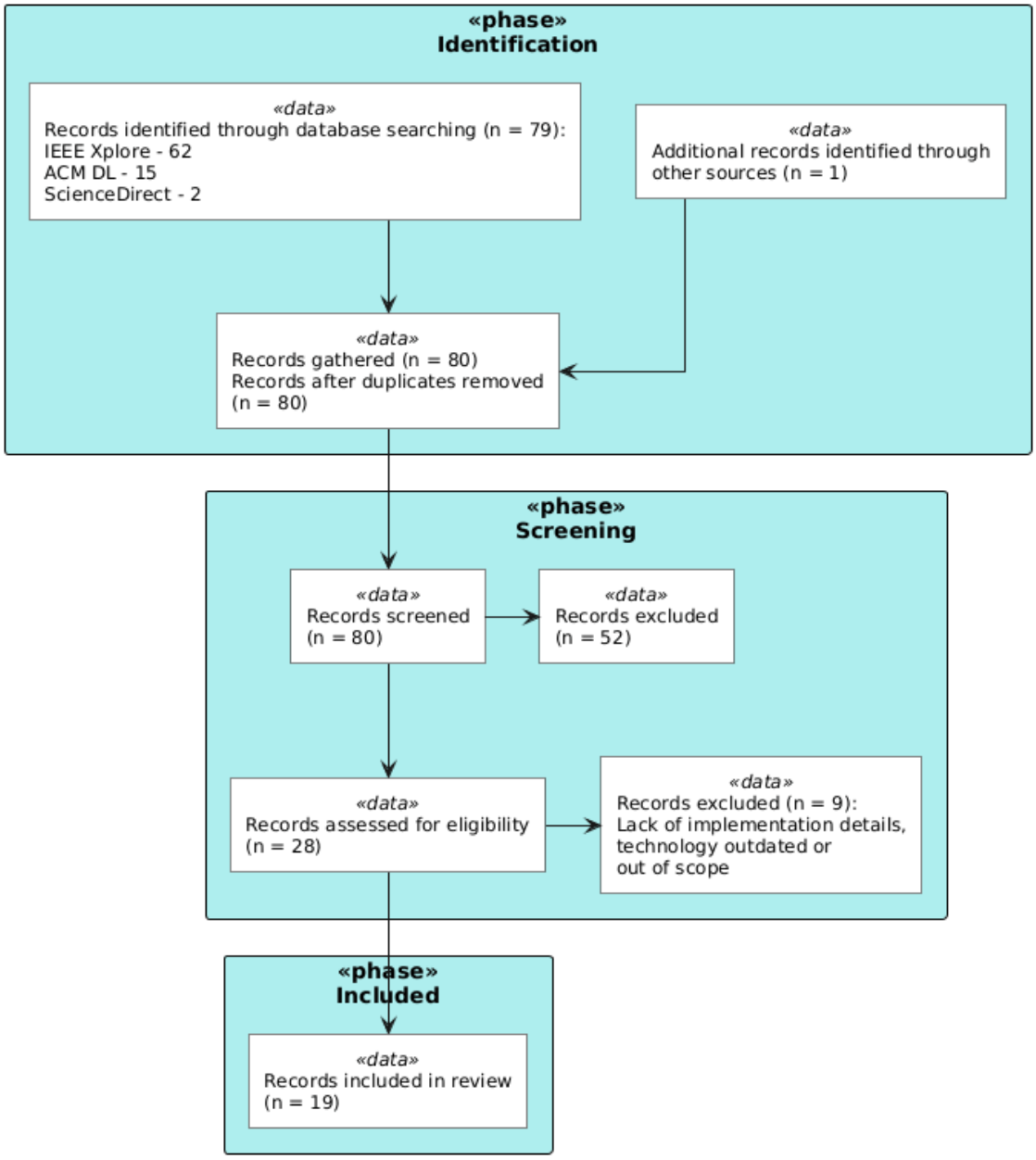

Figura 2.2: Fluxo PRISMA para a LRRQ2

O rigor na filtragem aplicada, reduzindo de 80 para 19 estudos incluídos, garantiu que apenas trabalhos com protocolos de comunicação segura relevantes, detalhados e validadas fossem analisados. Comparativamente à LRRQ1, que identificou 435 registos resultando em 11 estudos incluídos (2,5% de taxa de aproveitamento), a presente questão apresentou uma taxa de aproveitamento significativamente superior (23,8%), indicando que a literatura sobre protocolos de comunicação segura e VPNs apresenta uma maior concentração de artigos com conteúdo interessante e utilizável para fundamentar as decisões de segurança e comunicação do FUSE.

2.3.2 Discussão

A análise dos 19 estudos incluídos permitiu traçar uma evolução clara nas tecnologias de acesso remoto seguro, partindo de soluções *legacy* e centralizadas para arquiteturas modernas, descentralizadas e baseadas em túneis de alta performance. Esta secção sintetiza as descobertas literárias, organizando-as em quatro vetores fundamentais para o desenho da solução FUSE.

O Desafio da Conectividade em Redes Não Controladas

Um consenso transversal na literatura é a impraticabilidade e insegurança da exposição direta de dispositivos IoT à Internet. [24] demonstra que o método tradicional de "Port Forwarding" expõe vulnerabilidades críticas de firmware, defendendo o uso de túneis como única defesa viável. Contudo, a criação destes túneis enfrenta barreiras estruturais nas redes modernas. [25] valida o problema do Carrier-Grade NAT (CGNAT) em redes móveis (4G/5G), onde os Internet Service Providers (ISPs) não alocam endereços IP públicos aos dispositivos, tornando impossível o acesso direto (inbound). A solução validada por [26] reside na inversão do modelo de conexão: é o dispositivo na Edge que deve iniciar o túnel para um ponto de encontro externo, ou utilizar redes P2P (como o Tailscale) para garantir a travessia de NAT sem configurações complexas de firewall.

Limitações dos Protocolos Legacy e Comparação TCP vs. UDP

A literatura estabelece protocolos como OpenVPN e IPSec como referências sólidas para a transmissão de dados de sensores e telemetria de baixo débito [27, 28]. No entanto, a sua aplicação a fluxos de vídeo em tempo real apresenta limitações severas. [29] destaca o problema crítico do "TCP-over-TCP meltdown": o encapsulamento de tráfego de vídeo (que beneficia da natureza *fire-and-forget* do User Datagram Protocol (UDP)) dentro de túneis baseados em Transmission Control Protocol (TCP) (comuns em VPNs baseadas em Secure Sockets Layer (SSL)) provoca um ciclo vicioso de retransmissões redundantes, resultando em latência exponencial sob redes instáveis. Para além da performance, [30] alerta para a vulnerabilidade de segurança: o tráfego OpenVPN possui padrões de dados identificáveis (tamanho de pacotes e tempos de resposta específicos), permitindo que ISPs reconheçam e bloqueiem a conexão, mesmo quando encriptada.

A Ascensão do WireGuard e Túneis de Alta Performance

Como resposta às limitações supracitadas, o protocolo WireGuard emerge na literatura analisada como o novo estado da arte para comunicações seguras em dispositivos com recursos limitados. [32] e [33] fornecem evidência empírica de que o WireGuard introduz uma latência mínima (na ordem dos microsegundos) e um overhead de processamento significativamente inferior aos antecessores. A sua eficiência em hardware *low-cost* (como Raspberry Pi) é validada por [34], tornando-o ideal para a arquitetura Edge do FUSE. Mais relevante ainda, [13] valida integralmente uma stack tecnológica semelhante à proposta para o FUSE: utilização de WireGuard num Single Board Computer (SBC) para possibilitar que um NVR baseado em ZoneMinder aceda de forma segura à câmara. [35] reforça esta abordagem ao demonstrar que arquiteturas descentralizadas, onde a comunicação ocorre diretamente entre o produtor e o consumidor de dados (P2P), são significativamente mais eficientes do que modelos que dependem de um servidor central para o encaminhamento de todo o tráfego, apresentando ganhos de desempenho na ordem de 3x a 5x.

Análise Crítica

A síntese dos estudos permite validar as decisões arquiteturais preliminares do FUSE. A literatura suporta a implementação de um "Secure Gateway" na Edge [36], capaz de gerir não apenas o vídeo, mas também o ciclo de vida e atualizações do sistema de forma segura [37]. Contrariando a intuição de que a encriptação degrada a performance, [38] sugere que o encapsulamento em túneis modernos pode, de facto, melhorar a qualidade de experiência em redes instáveis ao gerir melhor a fragmentação e perda de pacotes.

Importa referir que quatro dos estudos selecionados na filtragem PRISMA não foram aprofundados na discussão principal por apresentarem redundância conceptual ou limitações de âmbito face aos restantes. [39] propõe uma VPN distribuída baseada em *fog computing* e *blockchain*, uma abordagem que, embora inovadora, introduz complexidade excessiva sem vantagens comprovadas para o cenário específico de vídeo ponto-a-ponto do FUSE, já coberto de forma mais eficiente pelas soluções de P2P citadas. [31] discute a otimização de parâmetros em OpenVPN (AdamVPN), focando-se em melhorar um protocolo *legacy* que o presente projeto opta por substituir integralmente por WireGuard. Similarmente, [40] apresenta um sistema de vigilância seguro, mas recorre a arquiteturas centralizadas clássicas (IPSec/DMVPN) cujas limitações já foram extensamente caracterizadas por outros autores. Por fim, [41] valida o uso de OpenVPN para sistemas *legacy* (SCADA), reforçando conclusões já estabelecidas sobre a viabilidade de VPNs para controlo, mas sem acrescentar novidade ao debate sobre *streaming* de vídeo de alta performance.

Conclusão

A resposta à LRRQ2 aponta inequivocamente para a adoção de protocolos baseados em UDP (como Wireguard) e conexões iniciadas na Edge com tecnologia P2P para garantir soberania de dados, baixa latência e resiliência em redes não controladas, rejeitando soluções baseadas em Cloud centralizada ou VPNs TCP *legacy*.

Concretamente, a arquitetura do FUSE materializa-se na disponibilização de cada câmara (ou conjunto de câmaras) em conjunto com um SBC, especificamente um Raspberry Pi. Este dispositivo atuará como um gateway de rede, controlando o tráfego e estabelecendo o encaminhamento através de uma VPN gerida pelo Tailscale. Desta forma, o servidor central consegue agregar e controlar o *streaming* de vídeo de todas as câmaras dispersas, garantindo a segurança sem expor os dispositivos diretamente à rede pública.

2.4 Estado da Arte em Visão Computacional

Relativamente à terceira sub-questão, a RQ1.3, referente à automatização da análise de vídeo, optou-se por uma abordagem de Revisão Narrativa e Exploratória, como descrita por Maria J. Grant e Andrew Booth em [42] como "State-of-the-art review". Esta modalidade metodológica caracteriza-se pela sua flexibilidade na análise crítica da literatura atual, permitindo identificar conceitos-chave, padrões arquiteturais e soluções técnicas emergentes sem a rigidez protocolar de uma revisão sistemática e formal.

Esta opção justifica-se pela vertiginosa evolução dos modelos de AI e pela necessidade de analisar não apenas literatura académica clássica, mas também documentação técnica de modelos recentes e *benchmarks* da indústria. A análise encontra-se segmentada em três domínios fundamentais que correspondem às fases da pipeline de processamento proposta para o FUSE:

1. Deteção de Movimento (Fase 1)
2. Deteção de Objetos (Fase 2)
3. Visual-Language Models - Vision-Language Models (VLMs) (Fase 3)

Apesar da natureza exploratória, esta pesquisa manterá o rigor científico na seleção de fontes, priorizando publicações de menos de 1 ano, dado o exponencial e recente crescimento tecnológico da área, e repositórios open-source com forte validação comunitária. A pesquisa foi orientada pelas seguintes *keywords*, agrupadas por domínio:

- **Fase 1 (Pré-processamento):** Background Subtraction, Motion Detection Algorithms, Frame Differencing efficiency, Video Activity Detection.
- **Fase 2 (Classificação):** Real-time Object Detection, You Only Look Once (YOLO) architecture, One-stage detectors, Convolutional Neural Network (CNN) inference optimization, Edge AI.
- **Fase 3 (Extração de Atributos):** Vision-Language Models (VLMs), Multimodal AI, Zero-Shot Learning, Open-vocabulary detection, Visual Question Answering.

2.4.1 Deteção de Movimento e Filtragem Temporal

2.4.2 Deteção e Classificação de Objetos (Object Detection)

2.4.3 Modelos de Visão-Linguagem (VLMs)

2.5 Identificação da Lacuna Literária

é Necessário este tópico? ou isto era apenas para complementar o extended abstract?

Capítulo 3

Planeamento de Trabalho

Este capítulo descreve o planeamento deste projeto, que foi estruturado para garantir a exequibilidade dos objetivos propostos dentro do prazo académico estipulado. A organização das atividades divide-se entre a fase de preparação (unidade curricular de Preparação para Dissertação (PREPD)) e a fase de execução e escrita da dissertação (unidade curricular de Dissertação do Mestrado em Engenharia Informática (DIMEI)).

3.1 Definição do Âmbito e Entregáveis

O âmbito deste projeto foi decomposto através de um WBS. Pelo mesmo, ilustrado na Figura 3.1, estão organizados os entregáveis previstos por cinco fases principais, sendo estas:

1. **Planeamento e Análise:** Focada na definição do problema e estado da arte. Inclui entregáveis como o Project Charter, o próprio WBS, um Gantt Chart, um questionário e respetivas respostas dos OPCs, este Extended Abstract e a revisão da literatura incluída no mesmo.
2. **Design:** Dedicada à modelação da solução. Os principais entregáveis previstos são a documentação da Arquitetura de Software (Vistas 4+1) e o Modelo de Domínio, assegurando que a estrutura do FUSE é robusta antes da implementação.
3. **Desenvolvimento:** Fase central do projeto, onde será implementado o código da aplicação. Divide-se em três módulos críticos: Comunicações Seguras, Camada de Abstração e Módulo de Análise de Vídeo.
4. **Testes:** Validação da solução através de testes unitários e funcionais, em conjunto com a validação do protótipo em ambiente controlado ou cenário real.
5. **Conclusões:** Considerações finais do projeto, incluindo a redação final da dissertação, a interpretação dos resultados e a apresentação final.

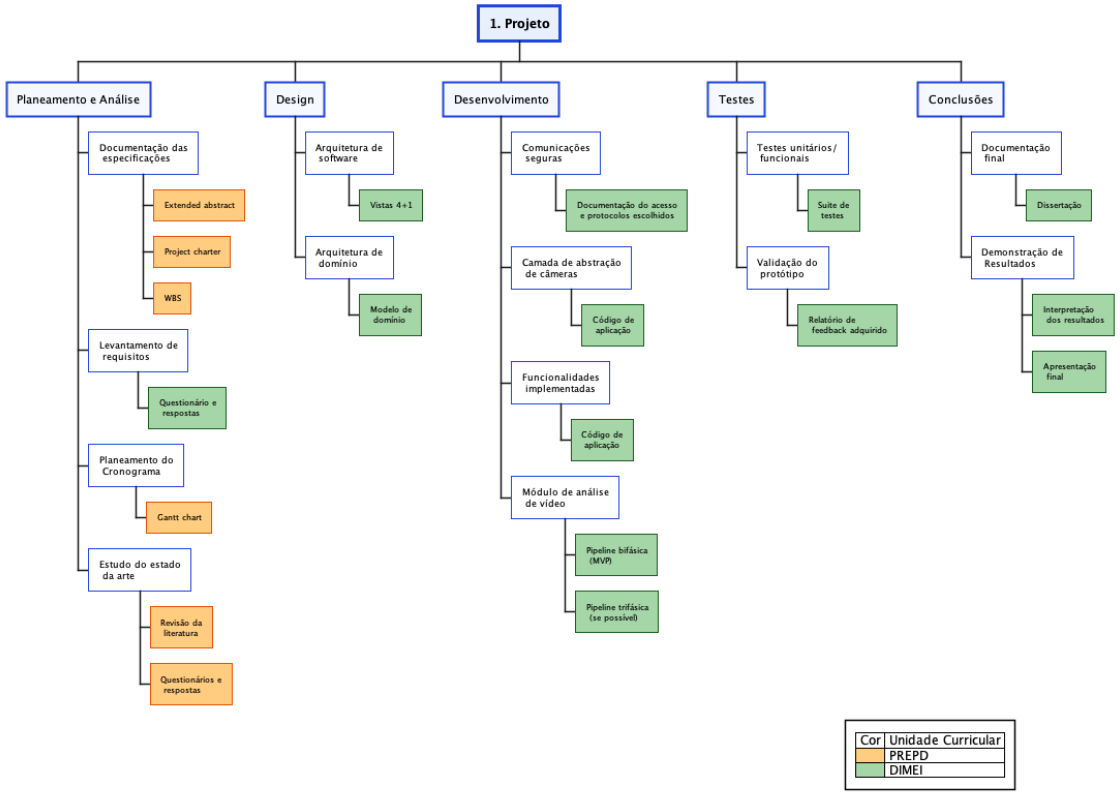

Figura 3.1: WBS do projeto.

3.2 Plano de Trabalho

O objetivo desta secção é ilustrar e descrever a calendarização das entregas dos respetivos entregáveis mencionados anteriormente, garantindo um acompanhamento rigoroso do progresso do projeto. O planeamento temporal encontra-se representado no diagrama de Gantt, Figura 3.2.

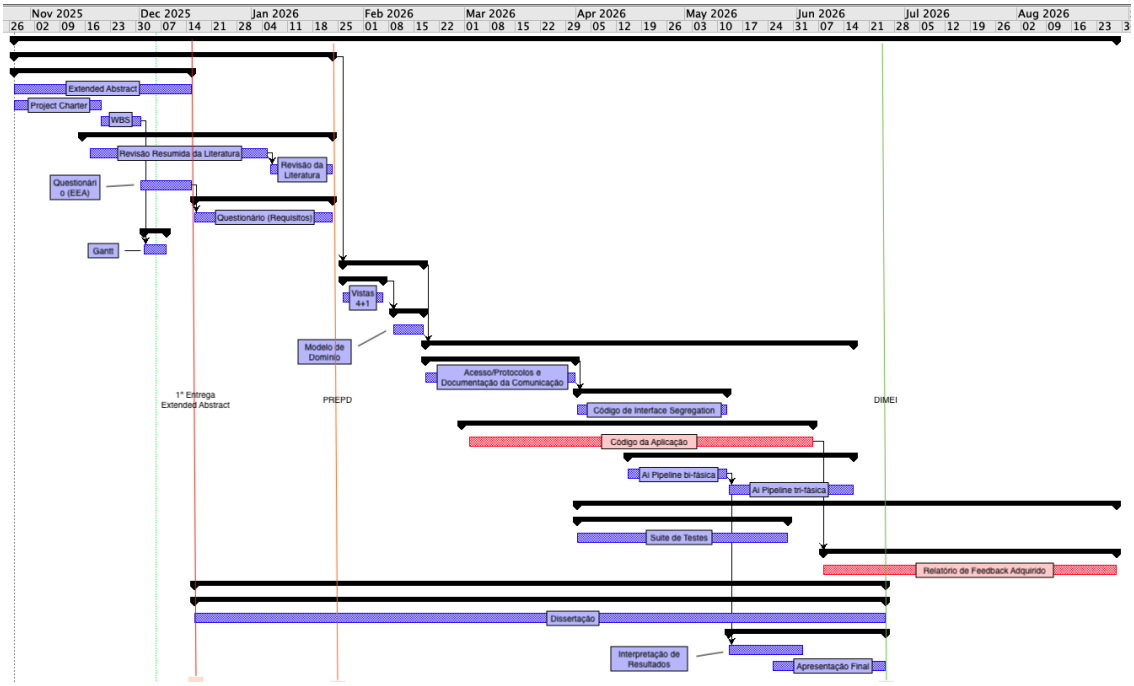

Figura 3.2: Gantt Chart do projeto.

A execução do cronograma inicia-se com um primeiro marco de controlo a 15 de dezembro de 2025. O encerramento da fase de planeamento (PREPD) está estipulado para 22 de janeiro de 2026. O segundo grande bloco temporal, referente à unidade curricular de DIMEI, tem como data-alvo de entrega final o dia 22 de junho de 2026.

O diagrama de Gantt ilustra a distribuição temporal das atividades ao longo de aproximadamente 220 dias úteis, desde o início do projeto em outubro de 2025 até agosto de 2026. A fase de **Planeamento e Análise**, com duração prevista de 65 dias, concentra-se nos primeiros meses do projeto e inclui a elaboração do Extended Abstract, do Project Charter, do WBS, bem como a realização do estudo do estado da arte e a aplicação de questionários junto dos OPCs. Esta fase culmina com a produção do próprio Gantt Chart, que depende da conclusão do WBS.

A fase de **Design**, com duração de 17 dias, inicia-se imediatamente após o término do planeamento, em janeiro de 2026. Esta fase contempla a documentação da Arquitetura de Software através das Vistas 4+1 e a modelação do Domínio, estabelecendo as bases arquiteturais para o desenvolvimento subsequente.

O **Desenvolvimento**, a fase mais extensa com 85 dias de duração, estende-se de fevereiro a junho de 2026. Esta fase estrutura-se em três componentes principais que se desenvolvem de forma parcialmente paralela: as Comunicações Seguras (30 dias), a Camada de Abstração de Câmaras (30 dias) e o Módulo de Análise Automática de Vídeo (45 dias). O módulo de análise de vídeo, por sua vez, divide-se em duas etapas sequenciais: a implementação de uma pipeline bi-fásica (20 dias) seguida da evolução para uma pipeline tri-fásica (25 dias), permitindo uma abordagem incremental na integração das funcionalidades de deteção e classificação.

A fase de **Testes** inicia-se em paralelo com o desenvolvimento, em abril de 2026, e prolonga-se até ao final do projeto. Esta fase compreende a execução de testes unitários e funcionais

durante 43 dias, seguida de um período de validação do protótipo em ambiente real que se estende por 60 dias, permitindo a recolha de feedback dos utilizadores finais e a produção do respetivo relatório.

Como se observa na Figura 3.2, após a data de entrega da unidade curricular de DIMEI a 22 de junho de 2026, ainda existe trabalho planeado que se estende até final de agosto de 2026. Esta extensão temporal deve-se ao facto de a validação do protótipo estar desde já expectada a requerer um período mais alargado do que o estipulado para o término formal da dissertação. Embora o início da fase de validação esteja previsto dentro do prazo académico, a sua conclusão completa poderá estender-se para além da data de entrega da dissertação. O feedback que for possível adquirir durante o período de validação será anexado ao relatório final, permitindo documentar os resultados obtidos e as observações recolhidas junto dos utilizadores finais, mesmo que o processo de validação se prolongue para além do término formal do trabalho académico.

3.3 Project Charter e Gestão de Riscos

O Project Charter constituiu o artefacto inicial deste projeto, servindo como primeiro documento para a formalização da proposta de dissertação junto da empresa acolhedora e da instituição académica. Dada a sua natureza preliminar, este documento apresentou uma visão inicial do problema e dos objetivos que, embora alinhados com a missão do FUSE, se revelaram amplos, tendo sido posteriormente refinados e concretizados no WBS e no plano de trabalhos detalhado anteriormente. As datas e entregáveis originais constantes no Charter foram, por conseguinte, ajustados para refletir um mais correto e detalhado planeamento.

3.3.1 Stakeholder Identification

Apesar dos ajustes realizados, o Project Charter mantém-se como a referência central para a identificação das partes interessadas (Stakeholders). A Tabela 3.1 apresenta o mapeamento atualizado dos Stakeholders, classificando-os quanto ao seu poder de influência e nível de interesse no sucesso do projeto. Destaca-se a inclusão da StabilityBubble, cuja posição estratégica evolui para fornecedor potencial do software pós-desenvolvimento, e a exclusão de entusiastas de Home Automation, inicialmente projetados como possível público-alvo. Esta exclusão dá-se devido à grande apropriação do FUSE a entidades e OPCs, dado que se torna uma solução demasiado desenvolvida para projetos caseiros e pequenos.

Para a classificação dos Stakeholders, utilizou-se como base a "Mendelow's Matrix" [45]. A atribuição dos níveis ('Alto', 'Médio', 'Baixo') obedeceu aos seguintes critérios:

- **Poder:** Capacidade da entidade em influenciar decisões, alocar recursos ou bloquear o andamento do projeto.
- **Interesse:** Grau de impacto que os resultados do projeto terão nas operações ou estratégia da entidade.

Tabela 3.1: Stakeholders identificados

Nome	Poder	Interesse	Justificação
StabilityBubble / NovaForensic	Alto	Alto	Entidade promotora e futura fornecedora/exploradora comercial da solução FUSE.
OPCs	Alto	Alto	Utilizadores finais críticos; o seu feedback valida a utilidade operacional e requisitos forenses.
Paulo Baltarejo Sousa (Orientador)	Alto	Médio	Orientação académica e validação científica da metodologia e resultados.
Francisco Loureiro (Supervisor)	Alto	Alto	Supervisão empresarial e alinhamento do produto com a estratégia de mercado.
Gestores de Segurança	Médio	Médio	Potenciais clientes empresariais que beneficiam da centralização de sistemas CCTV.
Fornecedores de Câmaras	Baixo	Baixo	O FUSE visa a eliminação da dependência de um só fornecedor, que tanto pode ser um novo fator decisivo para a escolha do fabricante.

3.3.2 Risk Management

Relativamente à gestão de riscos, trata-se de um processo contínuo que se iniciou com o levantamento preliminar no Project Charter. Embora a análise inicial focasse riscos mais genéricos (e.g., dependência de hardware), o planeamento aprofundado permitiu identificar ameaças mais específicas e definir estratégias de mitigação concretas. A Tabela 3.2 consolida os riscos, atribuindo-lhes uma probabilidade e um impacto, combinando alguns identificados na fase inicial com novos riscos técnicos decorrentes da complexidade da análise de vídeo e integração de redes. A quantificação do risco segue uma matriz de probabilidade e impacto (P×I), onde ambas as variáveis são classificadas numa escala de Likert [46] de 1 a 5. Esta escala foi definida da seguinte forma:

- **Probabilidade (P):** 1 representando um acontecimento raro ou extremamente improvável, e 5 algo que seja extremamente provável acontecer, possivelmente previsto.
- **Impacto (I):** 1 compreende uma insignificância ou ligeiro atraso, enquanto que 5 impacta criticamente, possivelmente impossibilitando o projeto ou condicionando o resultado do mesmo.

A multiplicação destes fatores resulta no Risco Quantificado, permitindo priorizar as estratégias de mitigação para as ameaças com pontuação mais elevada, conforme demonstrado na Tabela 3.2.

Tabela 3.2: Identificação e gestão de riscos associados ao projeto

ID	Descrição	Causa	P	I	P*I	Estratégia
1	Indisponibilidade de Hardware (Graphics Processing Unit (GPU))	A análise de vídeo requer hardware gráfico potente, que é escasso ou não disponível	3	4	12	Mitigar
2	Incompatibilidade de Protocolos	Determinada câmara não suporta o protocolo RTSP, impossibilitando a integração prevista.	2	2	4	Aceitar
3	Falsos Positivos na Deteção	Pipeline de AI gera demasiados alertas falsos em condições adversas (chuva, noite).	3	3	9	Mitigar
4	Atraso no Cronograma	A complexidade da integração de múltiplos sistemas excede o tempo previsto para o semestre letivo.	3	5	15	Mitigar

A Tabela 3.2 apresenta quatro riscos identificados, dos quais três requerem estratégias de mitigação e um é aceite como parte do âmbito do projeto. Pela análise à tabela, destaca-se os 1º e 4º riscos, Indisponibilidade de Hardware (GPU) e Atraso no Cronograma, com os índices de risco mais elevados sendo eles 12 e 15, respetivamente. Por consequente, conclui-se que grande parte do sucesso do projeto e dos resultados obtidos dependerão intrinsecamente da gestão rigorosa dos recursos computacionais e do cumprimento dos prazos estipulados, bem como o seguimento do planeamento efetuado.

As estratégias de resposta detalhadas para cada risco são as seguintes:

Risco 1 - Indisponibilidade de Hardware (GPU): A estratégia de mitigação consiste em garantir que a integração com a pipeline de análise automática seja feita de forma modular e desacoplada, permitindo a flexibilidade da escolha do modelo de AI utilizado conforme o hardware disponível no momento. Esta abordagem assegura que o sistema possa adaptar-se a diferentes configurações de hardware sem comprometer a funcionalidade core.

Risco 2 - Incompatibilidade de Protocolos: A opção pela estratégia de "Aceitação" serve para delimitar claramente o âmbito do projeto. O MVP a ser desenvolvido não pretende ser universalmente compatível com todo o conjunto de câmaras existentes, mas sim provar o conceito através de um protocolo standard habitualmente presente (RTSP), excluindo câmaras que não suportem este protocolo. Esta decisão permite focar o esforço de engenharia na inteligência do sistema e não na compatibilidade de drivers.

Risco 3 - Falsos Positivos na Deteção: A mitigação será realizada através da implementação de um sistema de ajuste de sensibilidade configurável pelo utilizador, permitindo que este defina parâmetros como os segundos necessários de deteção do objeto antes do alerta ser gerado. Esta funcionalidade permite reduzir falsos positivos em condições adversas, como chuva ou condições de pouca luz.

Risco 4 - Atraso no Cronograma: A estratégia de mitigação assenta na adoção de uma abordagem de desenvolvimento incremental. Será assegurada a estabilidade do núcleo de visualização e deteção básica (pipeline bi-fásica) como um MVP robusto, antes de iterar para as funcionalidades avançadas de extração de atributos (pipeline tri-fásica). Caso o desenvolvimento da pipeline tri-fásica se revele incompatível com o tempo disponível, esta será tratada como trabalho futuro, garantindo sempre a entrega de um produto funcional.

A estratégia de mitigação para os riscos prioritários (Riscos 1 e 4) assenta fundamentalmente na modularidade e no desenvolvimento incremental. Ao garantir que a arquitetura do sistema é flexível quanto aos modelos de AI e que as funcionalidades são entregues por fases, assegura-se que, mesmo na eventualidade destes riscos se materializarem, o projeto resultará sempre num produto funcional (MVP), salvaguardando a dissertação. A monitorização destes riscos será realizada periodicamente em cada reunião de ponto de situação com o orientador e supervisor, permitindo o ajuste dinâmico das estratégias de resposta caso a probabilidade ou impacto de algum fator sofra alterações ao longo do ciclo de vida do projeto.

Bibliografia

[1] Honghai Liu, Shengyong Chen e Naoyuki Kubota. «Intelligent Video Systems and Analytics: A Survey». Em: *IEEE Transactions on Industrial Informatics* 9.3 (2013), pp. 1222–1233. doi: 10.1109/TII.2013.2255616.

[2] Vlado Damjanovski. *CCTV: From light to pixels*. 3rd. Oxford: Butterworth-Heinemann, 2014. isbn: 978-0124046078.

[3] W. Daniel Kissling et al. «Development of a cost-efficient automated wildlife camera network in a European Natura 2000 site». Em: *Basic and Applied Ecology* 79 (2024), pp. 141–152. issn: 1439-1791. doi: https://doi.org/10.1016/j.baae.2024.06.006. url: https://www.sciencedirect.com/science/article/pii/S1439179124000458.

[4] Nozomi Networks. *New Reolink P2P Vulnerabilities Show IoT Security Camera Risks*. Acedido em: 12/2025. Jul. de 2021. url: https://www.nozominetworks.com/blog/new-reolink-p2p-vulnerabilities-show-iot-security-camera-risks.

[5] Kaushik Ragothaman et al. «Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions». Em: *Sensors (MDPI)* 23.4 (2023), p. 1805. doi: 10.3390/s23041805. url: https://www.mdpi.com/1424-8220/23/4/1805.

[6] Diário de Notícias. *Falta de polícias e de viaturas e instalações e equipamentos em mau estado. Relatório aponta as falhas da PSP e GNR*. Baseado em relatório da IGAI. Jun. de 2024. url: https://www.dn.pt/sociedade/falta-de-policias-e-de-viaturas-e-instalacoes-e-equipamentos-em-mau-estado-relatorio-aponta-as-falhas-da-psp-e-gnr.

[7] Briony J. Oates. *Researching Information Systems and Computing*. SAGE Publications, 2006. isbn: 9781412902236. url: https://us.sagepub.com/en-us/nam/researching-information-systems-and-computing/book226687.

[8] Politécnico do Porto. *Despacho P.PORTO/P-040/2020 - Código de Boas Práticas e de Conduta do P.PORTO*. 2020. url: https://www.ipp.pt/comunidade/missao-equidade-diversidade-inclusao/DespachoP.PORTOP0402020CodigodeBoasPraticasedeConduipdf.

[9] Association for Computing Machinery. *ACM Code of Ethics and Professional Conduct*. 2018. url: https://www.acm.org/code-of-ethics/software-engineering-code.

[10] European Union. *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. 2024. url: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[11] Alberto Sampaio. «Improving Systematic Mapping Reviews». Em: *SIGSOFT Softw. Eng. Notes* 40.6 (nov. de 2015), pp. 1–8. issn: 0163-5948. doi: 10.1145/2830719.2830732. url: https://doi.org/10.1145/2830719.2830732.

[12] David Moher et al. «Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement». Em: *International Journal of Surgery* 8.5 (2010). PII: S1743-9191(10)00040-3, pp. 336–341. url: https://www.sciencedirect.com/science/article/pii/S1743919110000403.

[13] Mateus Rocha Resende. «Sistema de Videomonitoramento Seguro com Acesso Remoto Utilizando VPN, DNS Dinâmico e Software Livre». por. Em: (mai. de 2025). Accepted: 2025-07-23T13:28:52Z Publisher: Universidade Federal de Uberlândia. url: https://repositorio.ufu.br/handle/123456789/46462 (acedido em 28/12/2025).

[14] Yasser Mesmoudi et al. «Design and implementation of a smart gateway for IoT applications using heterogeneous smart objects». Em: *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*. Nov. de 2018, pp. 1–7. doi: 10.1109/CloudTech.2018.8713348.

[15] Vinícius A. Barros et al. «An IoT multi-protocol strategy for the interoperability of distinct communication protocols applied to web of things». Em: *Proceedings of the 25th Brazillian Symposium on Multimedia and the Web*. WebMedia '19. event-place: Rio de Janeiro, Brazil. New York, NY, USA: Association for Computing Machinery, 2019, pp. 81–88. isbn: 978-1-4503-6763-9. doi: 10.1145/3323503.3349546. url: https://doi.org/10.1145/3323503.3349546.

[16] Jürgen Dobaj et al. «A Microservice Architecture for the Industrial Internet-Of-Things». Em: *Proceedings of the 23rd European Conference on Pattern Languages of Programs*. EuroPLoP '18. event-place: Irsee, Germany. New York, NY, USA: Association for Computing Machinery, 2018. isbn: 978-1-4503-6387-7. doi: 10.1145/3282308.3282320. url: https://doi.org/10.1145/3282308.3282320.

[17] Rachid Mafamane et al. «Study of the heterogeneity problem in the Internet of Things and Cloud Computing integration». Em: *2020 10th International Symposium on Signal, Image, Video and Communications (ISIVC)*. Abr. de 2021, pp. 1–6. doi: 10.1109/ISIVC49222.2021.9487539.

[18] Christopher Schwarzer, Andrei Günter e Matthias König. «IAL: Information Abstraction Layer to Include Multimedia in Building Automation Systems». Em: *2021 17th International Conference on Intelligent Environments (IE)*. ISSN: 2472-7571. Jun. de 2021, pp. 1–8. doi: 10.1109/IE51775.2021.9486461.

[19] Silvio Barra, Ferdinando D'Alessandro e Oleksandr Sosovskyy. «Exploring Architectural Choices and Emerging Challenges in Data Management for IoT: A Focus on Digital Innovation and Smart Cities». Em: *Adjunct Proceedings of the 32nd ACM Conference on User Modeling, Adaptation and Personalization*. UMAP Adjunct '24. event-place: Cagliari, Italy. New York, NY, USA: Association for Computing Machinery, 2024, pp. 429–436. isbn: 979-8-4007-0466-6. doi: 10.1145/3631700.3665238. url: https://doi.org/10.1145/3631700.3665238.

[20] Anjus George e Arun Ravindran. «Distributed Middleware for Edge Vision Systems». Em: *2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT)*. ISSN: 1949-4106. Out. de 2019, pp. 193–194. doi: 10.1109/HONET.2019.8908023.

[21] David L. Gomez et al. «Strategies for Assuring Low Latency, Scalability and Interoperability in Edge Computing and TSN Networks for Critical IIoT Services». Em: *IEEE Access* 11 (2023), pp. 42546–42577. issn: 2169-3536. doi: 10.1109/ACCESS.2023.3268223.

[22] Roger Immich et al. «Multi-tier Edge-to-Cloud Architecture for Adaptive Video Delivery». Em: *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*. Ago. de 2019, pp. 23–30. doi: 10.1109/FiCloud.2019.00012.

[23] Matheus HS Muniz et al. «Pragmatic interoperability in IoT: a systematic mapping study». Em: *Proceedings of the 25th Brazillian Symposium on Multimedia and the*

Web. WebMedia '19. event-place: Rio de Janeiro, Brazil. New York, NY, USA: Association for Computing Machinery, 2019, pp. 73–80. isbn: 978-1-4503-6763-9. doi: 10.1145/3323503.3349561. url: https://doi.org/10.1145/3323503.3349561.

[24] Joseph Bugeja, Désirée Jönsson e Andreas Jacobsson. «An Investigation of Vulnerabilities in Smart Connected Cameras». Em: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Mar. de 2018, pp. 537–542. doi: 10.1109/PERCOMW.2018.8480184.

[25] Suppakorn Boonprasert, Kittiphan Techakittiroj e Naebboon Hoonchareon. «Low-Cost Sky Camera with Centralized Storage Systems». Em: *2024 21st International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. ISSN: 2837-6471. Mai. de 2024, pp. 1–4. doi: 10.1109/ECTI-CON60892.2024.10594931.

[26] Daniel-Florin Hriţcan e Doru Balan. «Exposing IoT Platforms Securely and Anonymously Behind CGNAT». Em: *2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)*. ISSN: 2247-5443. Set. de 2024, pp. 1–4. doi: 10.1109/RoEduNet64292.2024.10722287.

[27] Jinpo Fan, Zhiqiang Wang e Changchun Li. «Design and Implementation of IoT Gateway Security System». Em: *2019 International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM)*. Out. de 2019, pp. 156–162. doi: 10.1109/AIAM48774.2019.00039.

[28] Stefania Guarino et al. «Data Acquisition System for Thermal Monitoring in High-Voltage Step Down Substation using Raspberry Pi and IoT Sensors». Em: *2025 IEEE International Conference on Environment and Electrical Engineering and 2025 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*. ISSN: 2994-9467. Jul. de 2025, pp. 1–6. doi: 10.1109/EEEIC/ICPSEurope64998.2025.11169145.

[29] Muhammad Asim et al. «SecT: A Zero-Trust Framework for Secure Remote Access in Next-Generation Industrial Networks». Em: *IEEE Journal on Selected Areas in Communications* 43.6 (jun. de 2025), pp. 2293–2311. issn: 1558-0008. doi: 10.1109/JSAC.2025.3560015.

[30] Diwen Xue et al. «OpenVPN is Open to VPN Fingerprinting». Em: *Commun. ACM* 68.1 (dez. de 2024). Place: New York, NY, USA Publisher: Association for Computing Machinery, pp. 79–87. issn: 0001-0782. doi: 10.1145/3618117. url: https://doi.org/10.1145/3618117.

[31] Syed Rafiul Hussain, Shahriar Nirjon e Elisa Bertino. «Securing the Insecure Link of Internet-of-Things Using Next-Generation Smart Gateways». Em: *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. ISSN: 2325-2944. Mai. de 2019, pp. 66–73. doi: 10.1109/DCOSS.2019.00032.

[32] Stephan Hohmann, Tobias Mueller e Marius Stübs. «Bridge Me If You Can! Evaluating the Latency of Securing Profinet». Em: *2021 International Conference on Information Networking (ICOIN)*. ISSN: 1976-7684. Jan. de 2021, pp. 621–626. doi: 10.1109/ICOIN50884.2021.9333897.

[33] Yongchao Dang et al. «EWDC: Integrating DECT-2020 With Wi-Fi for Enhanced Wireless Direct Connectivity». Em: *IEEE Internet of Things Journal* 12.15 (ago. de 2025), pp. 31783–31796. issn: 2327-4662. doi: 10.1109/JIOT.2025.3574407.

[34] Mehmet Bezenk e Hayriye Korkmaz. «Remote Access Solution for Industrial Devices with VPN». Em: *2024 Innovations in Intelligent Systems and Applications Conference (ASYU)*. ISSN: 2770-7946. Out. de 2024, pp. 1–8. doi: 10.1109/ASYU62119.2024.10757061.

[35] Kit-Lun Tong et al. «DAIoTtalk: A Data-Decentralized Pub-Sub AIoT Platform». Em: *2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*. ISSN: 2577-2465. Jun. de 2025, pp. 1–6. doi: 10.1109/VTC2025-Spring65109.2025.11174754.

[36] Ander Garcia et al. «Containerized Edge Architecture for Centralized Industry 4.0 Fleet Management». Em: *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*. ISSN: 2768-1734. Out. de 2023, pp. 1–5. doi: 10.1109/WF-IoT58464.2023.10539473.

[37] Sabarishraj K et al. «Efficient Implementation of Firmware Over-the-Air Update using Raspberry Pi 4 and STM32F103C8T6». Em: *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. ISSN: 2766-2101. Jul. de 2024, pp. 1–6. doi: 10.1109/CONECCT62155.2024.10677143.

[38] Roberta Avanzato, Francesco Beritelli e Corrado Rametta. «Enhancing Perceptual Experience of Video Quality in Drone Communications by Using VPN Bonding». Em: *IEEE Embedded Systems Letters* 15.1 (mar. de 2023), pp. 1–4. issn: 1943-0671. doi: 10.1109/LES.2022.3182466.

[39] Rahma Trabelsi, Ghofrane Fersi e Mohamed Jmaiel. «A fog and blockchain-based distributed Virtual Private Networks (VPN)». Em: *2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. ISSN: 2325-2944. Abr. de 2024, pp. 130–137. doi: 10.1109/DCOSS-IoT61029.2024.00028.

[40] Marwa Qaraqe et al. «PublicVision: A Secure Smart Surveillance System for Crowd Behavior Recognition». Em: *IEEE Access* 12 (2024), pp. 26474–26491. issn: 2169-3536. doi: 10.1109/ACCESS.2024.3366693.

[41] Deiescart D'Mitrio C. Maceda e Glenn V. Magwili. «Scada Web-Based Instrumentation and Control Laboratory with Real-Time Remote Monitoring and Control System for Columban College». Em: *2022 IEEE 14th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. ISSN: 2770-0682. Dez. de 2022, pp. 1–6. doi: 10.1109/HNICEM57413.2022.10109507.

[42] Maria J. Grant e Andrew Booth. «A typology of reviews: an analysis of 14 review types and associated methodologies». Em: *Health Information and Libraries Journal* 26.2 (2009), pp. 91–108. doi: 10.1111/j.1471-1842.2009.00848.x. url: https://onlinelibrary.wiley.com/doi/full/10.1111/j.1471-1842.2009.00848.x.

[43] Glenn Jocher, Ayush Chaurasia e Jing Qiu. *Ultralytics YOLO*. 2023. url: https://github.com/ultralytics/ultralytics.

[44] Puneet Goswami et al. «Real-time evaluation of object detection models across open world scenarios». Em: *Applied Soft Computing* 163 (2024), p. 111921. issn: 1568-4946. doi: https://doi.org/10.1016/j.asoc.2024.111921. url: https://www.sciencedirect.com/science/article/pii/S1568494624006951.

[45] Aubrey L. Mendelow. «Environmental Scanning: The Impact of the Stakeholder Concept». Em: *ICIS 1981 Proceedings* (1981), p. 20. url: https://aisel.aisnet.org/icis1981/20/.

[46] Rensis Likert. «A technique for the measurement of attitudes». Em: *Archives of Psychology* 22.140 (1932), pp. 1–55. url: https://psycnet.apa.org/record/1933-01885-001.

Apêndice A

Questionário e Entrevistas

O conteúdo deste anexo refere-se ao questionário e entrevistas realizados em conjunto com agentes da investigação criminal da GNR e da PSP para validação do problema identificado.