UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE AUTOMAÇÃO E SISTEMAS
CURSO DE GRADUAÇÃO EM ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Cliff Alves Ribeiro

Decodificando a Comunicação em Redes Automotivas: Engenharia Reversa na Comunicação de Centrais Veiculares

Florianópolis
2024

Cliff Alves Ribeiro

Decodificando a Comunicação em Redes Automotivas: Engenharia Reversa na Comunicação de Centrais Veiculares

Relatório final da disciplina DAS5511 (Projeto de Fim de Curso) como Trabalho de Conclusão do Curso de Graduação em Engenharia de Controle e Automação da Universidade Federal de Santa Catarina em Florianópolis.
Orientador: Prof. Carlos Barros Montez, Dr.
Supervisor: Rene Engels, Eng.

Florianópolis
2024

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

Ribeiro, Cliff Alves
Decodificando a comunicação em redes automotivas : Engenharia reversa na comunicação de centrais veiculares / Cliff Alves Ribeiro ; orientador, Carlos Barros Montez, coorientador, Rene Engels, 2024.
72 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Tecnológico, Graduação em Engenharia de Controle e Automação, Florianópolis, 2024.

Inclui referências.

1. Engenharia de Controle e Automação. 2. Engenharia reversa. 3. Rede CAN. 4. Protocolos de comunicação. 5. Diagnóstico automotivo. I. Montez, Carlos Barros. II. Engels, Rene. III. Universidade Federal de Santa Catarina. Graduação em Engenharia de Controle e Automação. IV. Título.

Cliff Alves Ribeiro

Decodificando a Comunicação em Redes Automotivas: Engenharia Reversa na Comunicação de Centrais Veiculares

Esta monografia foi julgada no contexto da disciplina DAS5511 (Projeto de Fim de Curso) e aprovada em sua forma final pelo Curso de Graduação em Engenharia de Controle e Automação

Florianópolis, 11 de julho de 2024.

Prof. Marcelo De Lellis Costa de Oliveira, Dr.
Coordenador do Curso

Banca Examinadora:

Documento assinado digitalmente
Carlos Barros Montez
Data: 30/07/2024 18:27:22-0300
CPF: ***.035.027-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Carlos Barros Montez, Dr.
Orientador
UFSC/CTC/DAS

Documento assinado digitalmente
RENE ENGELS
Data: 30/07/2024 17:30:46-0300
Verifique em https://validar.iti.gov.br

Rene Engels, Eng.
Supervisor
Empresa Doutor-IE

João Paulo Zomer, Eng.
Avaliador
Instituição UFSC

Prof. Hector Bessa Silveira, Dr.
Presidente da Banca
UFSC/CTC/DAS

Este trabalho é dedicado aos meus queridos pais e irmão, aos colegas de trabalho, e ao meu venerado primo Gabriel Ribeiro.

AGRADECIMENTOS

Agradeço imensamente aos meus pais e irmão por terem me apoiado durante toda a graduação, aos meus caros colegas de trabalho que sempre me motivaram a expandir conhecimentos, e a todos que de alguma forma contribuíram para que eu chegasse onde estou.

“No que diz respeito ao empenho, ao compromisso,
ao esforço, à dedicação, não existe meio termo.
Ou você faz uma coisa bem feita ou não faz.”
(Senna, 1989)

DECLARAÇÃO DE PUBLICIDADE

Florianópolis, 01 de julho de 2024.

Na condição de representante da Doutor-IE na qual o presente trabalho foi realizado, declaro não haver ressalvas quanto ao aspecto de sigilo ou propriedade intelectual sobre as informações contidas neste documento, que impeçam a sua publicação por parte da Universidade Federal de Santa Catarina (UFSC) para acesso pelo público em geral, incluindo a sua disponibilização *online* no Repositório Institucional da Biblioteca Universitária da UFSC. Além disso, declaro ciência de que o autor, na condição de estudante da UFSC, é obrigado a depositar este documento, por se tratar de um Trabalho de Conclusão de Curso, no referido Repositório Institucional, em atendimento à Resolução Normativa n° 126/2019/CUn.

Por estar de acordo com esses termos, subscrevo-me abaixo.

gov.br
Documento assinado digitalmente
RENE ENGELS
Data: 30/07/2024 09:11:17-0300
Verifique em https://validar.iti.gov.br

Rene Engels
Doutor-IE

RESUMO

O presente projeto de final de curso tem como objetivo documentar a comunicação veicular via rede CAN para o futuro desenvolvimento de uma ferramenta de diagnóstico automotivo eficiente e adaptada às especificidades do mercado brasileiro, utilizando engenharia reversa para decodificar os protocolos de comunicação proprietários (do fabricante) da unidade de controle eletrônico do motor. O estudo selecionou o veículo Peugeot 208 I [2015] - 1.5 8V Flex 89/93cv (TU4-YFY) com central do motor VALEO V34.5 como objeto de análise, aplicando as ferramentas de *software* CANoe e de *hardware* VN1630 log para coletar e simular dados de comunicação veicular. A metodologia incluiu a coleta de dados, análise, desenvolvimento de simulações e validação com aparelhos de diagnóstico automotivo. A pesquisa destacou a importância de soluções de diagnóstico precisas e padronizadas para reduzir falhas, aumentar a eficiência das oficinas e diminuir os custos operacionais. Os resultados obtidos demonstraram a eficácia da abordagem proposta, com a documentação detalhada dos dados coletados e a validação das simulações, proporcionando um alicerce robusto para o desenvolvimento de *scanners* automotivos mais assertivos e confiáveis. A aplicação prática deste trabalho visa contribuir significativamente para o setor de engenharia e reparação automotiva, melhorando a qualidade e a segurança dos serviços oferecidos.

Palavras-chave: Engenharia reversa. Protocolos de comunicação. Rede CAN. Diagnóstico automotivo. CANoe. VN1630 log.

ABSTRACT

This final project aims to document vehicle communication via the CAN network for the future development of an efficient automotive diagnostic tool tailored to the specificities of the Brazilian market. It involves reverse engineering to decode proprietary communication protocols from the engine control unit manufacturer. The study selected the Peugeot 208 I [2015] - 1.5 8V Flex 89/93hp (TU4-YFY) with VALEO V34.5 engine control unit for analysis, utilizing CANoe software and VN1630 hardware log tools to collect and simulate vehicle communication data. The methodology included data collection, analysis, simulation development, and validation with automotive diagnostic equipment. The research highlighted the importance of accurate and standardized diagnostic solutions to reduce failures, increase workshop efficiency, and lower operational costs. The results demonstrated the effectiveness of the proposed approach, providing detailed documentation of collected data and validation of simulations, laying a robust foundation for the development of more precise and reliable automotive scanners. The practical application of this work aims to significantly contribute to the automotive engineering and repair sector, enhancing the quality and safety of offered services.

Keywords: Reverse engineering. Communication protocols. CAN network. Automotive diagnosis. CANoe. VN1630 log.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CAN	Controller Area Network
CRC	Cyclic Redundancy Check
ECU	Electronic Control Unit
ID	Identifier
KWP	Keyword Protocol 2000
OBD	On-Board Diagnostics
ODX	Open Diagnostic Data Exchange
OSI	Open Systems Interconnection
PID	Parameter Identifier
SGW	Security Gateway
SID	Service Identifier
UCE	Unidade de Controle Eletrônico
UDS	Unified Diagnostic Services
VIN	Vehicle Identification Number

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO DO TEMA

O avanço tecnológico na indústria automotiva tem sido notável nas últimas décadas, com os veículos modernos incorporando uma variedade de sistemas eletrônicos que gerenciam desde funções básicas até complexas operações de controle, segurança e conforto dos ocupantes. Entre esses sistemas, a unidade de controle eletrônico do motor desempenha um papel crucial, monitorando e ajustando inúmeros parâmetros para otimizar o desempenho e a eficiência do veículo. A comunicação eficiente e precisa entre os diversos sistemas eletrônicos presentes em um veículo e os aparelhos de diagnóstico, ou comumente chamados como *scanners*, é fundamental para a manutenção e a reparação dos veículos, sendo facilitada por padrões e protocolos específicos de comunicação em rede.

Com a crescente complexidade dos sistemas automotivos, hoje os veículos modernos são equipados com múltiplas centrais veiculares que se comunicam entre si para garantir o funcionamento eficiente e seguro do veículo. Essa comunicação é realizada por meio de redes veiculares, como a *Controller Area Network* (CAN), a *Local Interconnect Network* (LIN), ou a *K-Line* (Linha K) utilizando protocolos de diagnóstico como *Keyword Protocol 2000* (KWP) e *Unified Diagnostic Services* (UDS). Essas redes e protocolos são essenciais para a troca de informações entre os componentes eletrônicos do veículo, possibilitando o monitoramento e o controle em tempo real.

No Brasil, a introdução de normas específicas para o diagnóstico veicular, como o diagnóstico de bordo (OBD) do Brasil de segunda geração, ou simplesmente OBD BR-2, tem sido crucial para padronizar e regulamentar a comunicação entre as ECUs e os *scanners* automotivos. A OBD BR-2, por exemplo, estabelece os requisitos para o diagnóstico a bordo dos veículos fabricados no país a partir de 2010, alinhando-se às normas internacionais OBD-II. Essas regulamentações visam não apenas melhorar a eficiência do diagnóstico, mas também garantir a conformidade com as exigências ambientais e de segurança.

A engenharia reversa, neste contexto, emerge como uma ferramenta poderosa para entender os protocolos de comunicação veicular e decodificar os dados transmitidos na rede. Aplicando técnicas de engenharia reversa, é possível interceptar e analisar as mensagens trocadas entre as ECUs e os *scanners* automotivos, permitindo a criação de soluções de diagnóstico mais eficientes e customizadas para o mercado brasileiro. Esta prática é particularmente relevante para o desenvolvimento de aparelhos de diagnóstico automotivo que precisam ser compatíveis com uma ampla gama de veículos, incluindo aqueles que utilizam protocolos proprietários e não padronizados.

A pesquisa será conduzida através de uma série de etapas, incluindo a coleta de dados de comunicação, análise dos protocolos utilizados, documentação dos dados e a

simulação da central veicular para responder com os dados coletados as mensagens a qual o *scanner* automotivo solicita. Utilizando um veículo Peugeot 208 I [2015] - 1.5 8V Flex 89/93cv (TU4-YFY) como caso de estudo, a engenharia reversa será aplicada para decodificar as mensagens da rede CAN da central eletrônica do motor e desenvolver um modelo de diagnóstico que possa ser replicado para outras centrais e veículos que seguem normas similares.

1.2 MOTIVAÇÃO DO TRABALHO

A evolução tecnológica no setor automotivo tem transformado profundamente a forma como os veículos são projetados, fabricados e mantidos. Os modernos sistemas de controle eletrônico, particularmente as unidades de controle do motor, desempenham um papel vital na operação eficiente e segura dos automóveis. No entanto, a complexidade crescente desses sistemas também traz novos desafios para diagnósticos e reparos automotivos, destacando a necessidade de ferramentas de diagnóstico avançadas e precisas.

No contexto das oficinas mecânicas brasileiras, há uma demanda significativa por ferramentas de diagnóstico que sejam não apenas precisas, mas também acessíveis e adaptadas às peculiaridades do mercado local. Embora as normas OBD-II e OBD BR-2 tenham sido implementadas para padronizar o diagnóstico veicular, muitas oficinas enfrentam desafios ao lidar com veículos de diferentes fabricantes que utilizam protocolos de comunicação proprietários. Essa falta de padronização dificulta o processo de diagnóstico e reparo, aumentando o tempo de inatividade dos veículos e os custos de manutenção. Este trabalho visa abordar essa necessidade, fornecendo uma solução que decodifique eficientemente as comunicações veiculares, permitindo o desenvolvimento de *scanners* automotivos mais eficientes, precisos, acessíveis e adaptados ao mercado nacional.

Reparadores automotivos, frequentemente dependentes de aparelhos de diagnóstico, enfrentam dificuldades ao lidar com códigos de falha do veículo ou configurar centrais virgens devido a problemas no desenvolvimento dos próprios *scanners*. Estes problemas podem gerar falhas graves e até mesmo condenar centrais veiculares de alto valor. Além dos aspectos técnicos e de mercado, há também uma motivação econômica e ambiental. Um diagnóstico mais eficiente pode reduzir significativamente o tempo necessário para identificar e corrigir falhas, diminuindo o tempo de inatividade dos veículos nas oficinas e, consequentemente, os custos operacionais. Isso resulta em uma economia direta para proprietários de veículos e oficinas mecânicas. Além disso, diagnósticos precisos podem ajudar a identificar problemas que afetam a eficiência do combustível e as emissões de poluentes, contribuindo para a redução do impacto ambiental dos veículos.

O *scanner* automotivo em desenvolvimento pela empresa Doutor-IE visa ofere-

cer funcionalidades equivalentes aos *scanners* originais das montadoras, mas com adaptações específicas para o mercado brasileiro. Para alcançar esse objetivo, é essencial decodificar e interpretar as mensagens de diagnóstico trocadas entre os diferentes sistemas do veículo. Portanto, este trabalho visa não apenas auxiliar no desenvolvimento de uma ferramenta de diagnóstico eficaz, mas também contribuir para a segurança e a confiabilidade dos veículos em nossas estradas.

Este projeto também possui uma motivação acadêmica, profissional e pessoal. Do ponto de vista acadêmico, ele representa uma oportunidade de aplicar os conhecimentos adquiridos ao longo do curso de Engenharia de Controle e Automação em um projeto prático e relevante. Profissionalmente, o desenvolvimento deste projeto permitirá contribuir de forma significativa para a empresa Doutor-IE, fortalecendo suas capacidades de inovação e sua posição no mercado de reparação automotiva. Do ponto de vista pessoal, a paixão pelo mundo automobilístico instiga a compreender e buscar novas estratégias que beneficiem o mercado automotivo.

1.3 A EMPRESA

A Doutor-IE é uma empresa brasileira que se destaca como referência em documentação técnica online para diagnóstico e reparação automotiva profissional, através do seu aplicativo Plataforma Doutor-IE. Com mais de 25 anos de experiência, a Doutor-IE desenvolve informações técnicas detalhadas para manutenção, diagnóstico e reparo de sistemas automotivos, atendendo todo o mercado de reposição automotiva, incluindo oficinas independentes, centros automotivos e redes de oficinas. Sua especialização em criar documentação técnica para a reparação automotiva a posiciona como uma líder confiável e inovadora no setor.

Além da Plataforma Doutor-IE, a empresa está comprometida com a formação e o treinamento de profissionais da área automotiva. Para isso, oferece cursos e treinamentos especializados, visando capacitar mecânicos e técnicos. Esses cursos são disponibilizados de forma gratuita através das redes sociais e de forma paga, com um conteúdo mais abrangente, por meio do evento anual Circuito Doutor-IE. Este evento, realizado em São Paulo, reúne mais de 60 palestrantes, incluindo especialistas nacionais e internacionais, e oferece mais de 60 palestras em três dias. O Circuito Doutor-IE é o maior evento de conteúdo técnico para reparadores automotivos profissionais da América Latina. Esses programas educacionais são essenciais para garantir que os profissionais do setor estejam atualizados com as últimas tecnologias e metodologias de diagnóstico, contribuindo para a melhoria contínua da qualidade dos serviços automotivos no Brasil.

O compromisso da empresa com a inovação é refletido em sua abordagem de pesquisa e desenvolvimento. Mantendo uma equipe de engenheiros e técnicos altamente qualificados, a empresa investe continuamente na exploração de novas tec-

nologias e métodos para aprimorar seus produtos. Este foco em inovação permite à Doutor-IE liderar o setor de informação técnica automotiva no Brasil, oferecendo soluções que atendem às crescentes demandas de um mercado em constante evolução. A eficácia dessa abordagem é demonstrada pelo aumento significativo no número de clientes assinantes da Plataforma Doutor-IE, que cresceu de aproximadamente 1.200 clientes ativos em outubro de 2019, quando ingressei na empresa, para 6.700 clientes ativos em junho de 2024.

A empresa Doutor-IE, localizada em Florianópolis, capital de Santa Catarina, aproveita um ambiente altamente inovador característico da cidade conhecida como a Ilha do Silício brasileira, devido à concentração de empresas de tecnologia. Estrategicamente posicionada no bairro universitário Trindade, próximo à Universidade Federal de Santa Catarina (UFSC), a empresa se beneficia de um ambiente dinâmico e propício ao constante progresso. A certificação pela consultoria global GPTW (*Great Place To Work*) evidencia seu comprometimento com o desenvolvimento e bem-estar dos colaboradores, promovendo um ambiente de trabalho estimulante e de crescimento mútuo.

1.3.1 Plataforma Doutor-IE

A Plataforma Doutor-IE é o principal produto da empresa, sendo uma ferramenta essencial para oficinas automotivas, funcionando como um "funcionário adicional" que facilita o trabalho dos reparadores e aumenta a lucratividade das oficinas. Esta plataforma online, atualizada diariamente, oferece suporte técnico profissional ao vivo, exclusivo no Brasil, através de um chat integrado.

A Plataforma pode ser acessada simultaneamente em até três dispositivos por oficina, compatível com Windows, Android e iOS. Com um vasto acervo de conteúdos técnicos, é a principal ferramenta de informação técnica no Brasil, cobrindo desde reparos básicos até diagnósticos avançados. A Plataforma Doutor-IE é vital para o dia a dia das oficinas, proporcionando confiança e eficiência no trabalho.

Ela elimina a necessidade de buscas demoradas e arriscadas na internet, centralizando todas as informações técnicas necessárias em um único lugar. Com mais de 200 mil buscas mensais, a Plataforma atende milhares de oficinas em todo o Brasil. O acervo inclui manuais técnicos em português de todas as montadoras, nacionais e importadas, organizados em grupos específicos para facilitar a busca e agilizar o serviço.

Os principais grupos de informações oferecidos pela Plataforma incluem:

Elétrica: Diagramas elétricos, fusíveis e relés, injeção eletrônica, oscilogramas e testes, imobilizador de partida, central de carroceria, alarmes e travas, conector DLC, sistemas de controle de emissões, entre outros.

Mecânica: Fluidos, aditivos e filtros, torques de aperto, ajustes e especificações do motor, correias dentada e auxiliar, vistas explodidas de injetores e bombas, sincronismos e correias auxiliares.

Revisões e Advertências: Revisões periódicas, reset das indicações de serviço no painel, luzes e sinalizações do painel, monitoramento de pressão, rodas e pneus, diagnóstico via painel de instrumentos.

A plataforma atende uma ampla gama de veículos, incluindo automóveis e caminhonetes na linha CAR, utilitários e SUVs na linha SUV, caminhões e ônibus na linha TRUCK, e veículos híbridos e elétricos na linha EV. Tornando-se assim uma solução abrangente que é indispensável para o setor de reparação automotiva, cobrindo todas as linhas de automóveis que uma oficina pode atender.

A missão da Doutor-IE é fornecer soluções eficazes, inovadoras e confiáveis que otimizem o diagnóstico e a manutenção de veículos, facilitando o trabalho dos profissionais da área e contribuindo para a eficiência e segurança dos automóveis. A visão da empresa é seguir sendo reconhecida como líder no mercado de informação técnica automotiva, oferecendo produtos e serviços que atendam às necessidades específicas do mercado brasileiro e que estejam alinhados com os mais altos padrões internacionais de qualidade e inovação.

1.3.2 Futuro

A Doutor-IE está firmemente comprometida com a inovação e a excelência, direcionando seus esforços para o futuro. Os planos da empresa incluem a expansão de sua linha de produtos, como o atual desenvolvimento de um novo aparelho de diagnóstico, a integração de tecnologias emergentes como inteligência artificial e Internet das Coisas (IoT) nas soluções de diagnóstico existentes, e a exploração de novos mercados. O objetivo central dessas iniciativas é oferecer as melhores ferramentas e serviços possíveis para o setor automotivo. Para a Plataforma Doutor-IE, a meta é alcançar uma presença em mais de 50% das oficinas mecânicas brasileiras até 2028, consolidando-se como uma referência indispensável no mercado.

1.4 ORGANIZAÇÃO DO DOCUMENTO

Este Projeto de Fim de Curso (PFC), intitulado "Decodificando a Comunicação em Redes Automotivas: Engenharia Reversa na Comunicação de Centrais Veiculares", está estruturado para fornecer uma visão abrangente e detalhada dos aspectos teóricos e práticos envolvidos na realização deste trabalho. A seguir, apresenta-se a organização dos capítulos que compõem este documento:

Capítulo 1 - Introdução: Este capítulo oferece uma visão geral do projeto, incluindo a contextualização do tema, a motivação para a realização do trabalho, os objetivos gerais e específicos, e a justificativa da relevância do estudo no contexto do diagnóstico automotivo e da engenharia reversa. Adicionalmente, descreve brevemente a empresa Doutor-IE, destacando sua atuação no mercado automotivo, seus produtos e serviços, e seu papel no desenvolvimento deste projeto.

Capítulo 2 - Fundamentação Teórica: Neste capítulo, são abordados os conceitos fundamentais, protocolos e normas de comunicação veicular, discorrendo sobre OBD-II, OBD BR-2, CAN, KWP, e UDS. Há também uma discussão sobre a importância do diagnóstico automotivo eficiente e a segurança das redes automotivas.

Capítulo 3 - Metodologia: Este capítulo apresenta as técnicas e metodologias de engenharia reversa aplicadas às comunicações veiculares. Discute a decodificação de mensagens CAN, a análise de protocolos de comunicação e a interpretação dos dados capturados. Além disso, aborda o processo de escolha do veículo utilizado como estudo de caso, a descrição das atividades de pesquisa realizadas em campo para coleta de dados, bem como os métodos e ferramentas utilizados. Inclui as etapas iniciais de análise dos dados coletados para compreensão dos protocolos e mensagens, a aplicação de técnicas de engenharia reversa para decodificação das mensagens de comunicação, e explora o desenvolvimento de arquivos ODX, que padronizam a representação dos dados de diagnóstico.

Capítulo 4 - Desenvolvimento: Este capítulo detalha o processo de engenharia reversa aplicado aos dados coletados, assim como o registro e organização dos dados obtidos durante a coleta e análise. Inclui também a validação dos dados documentados e as conclusões derivadas dessa análise.

Capítulo 5 - Conclusão: Neste capítulo, é apresentado um resumo dos principais resultados e contribuições do projeto para o campo do diagnóstico automotivo. Reflete sobre os desafios enfrentados durante o projeto e oferece sugestões para trabalhos futuros.

Capítulo 6 - Referências Bibliográficas: Este segmento lista todas as fontes bibliográficas consultadas e citadas ao longo do documento, conforme as normas de referência acadêmica.

Esta estrutura visa proporcionar uma leitura clara e organizada do trabalho realizado, facilitando a compreensão dos métodos, resultados e implicações do projeto no contexto do diagnóstico automotivo e da engenharia reversa.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo da Fundamentação Teórica aborda a evolução dos sistemas de diagnóstico automotivo, destacando três fases principais: a introdução dos sistemas eletrônicos nos anos 1970, a adoção dos sistemas OBD-I pela General Motors nos anos 1980 e a padronização global com o OBD-II nos anos 1990. Essa evolução reflete a transição de métodos de diagnóstico manual para diagnósticos computadorizados mais precisos e abrangentes, permitindo a monitoração contínua e otimização dos veículos modernos.

Além disso, explora-se a rede CAN, desenvolvida pela Bosch nos anos 1980, que revolucionou a comunicação eletrônica veicular devido à sua robustez e capacidade de operar em ambientes adversos. A CAN é fundamental para a integração dos sistemas eletrônicos do veículo, sendo amplamente adotada não apenas no setor automotivo, mas também em outras áreas como automação industrial e sistemas médicos.

Também são discutidas as normas e protocolos de comunicação veicular, como UDS e KWP, essenciais para garantir a interoperabilidade e desempenho dos sistemas de diagnóstico. Esses padrões são cruciais para o desenvolvimento de ferramentas de diagnóstico universalmente aplicáveis e para avanços na tecnologia automotiva.

2.1 EVOLUÇÃO DOS SISTEMAS DE DIAGNÓSTICO AUTOMOTIVO

Os sistemas de diagnóstico automotivo evoluíram significativamente ao longo dos anos, impulsionados pelo aumento da complexidade dos veículos e pela necessidade crescente de monitorar e manter o desempenho de diversos sistemas automotivos. Essa evolução pode ser dividida em três grandes fases: os primeiros sistemas de diagnóstico, os avanços nos sistemas eletrônicos e a introdução das Unidades de Controle Eletrônico.

2.1.1 Primeiros sistemas de diagnóstico

Na década de 1970, com a crescente integração de eletrônica nos veículos, surgiram os primeiros sistemas de diagnóstico automotivo. Antes desse período, o diagnóstico dependia principalmente de inspeções visuais e testes manuais, exigindo habilidades avançadas dos reparadores. Problemas mecânicos eram identificados pela observação de desgastes em componentes, ajustes de carburadores e análise de ruídos e vibrações.

A introdução de computadores nos veículos marcou uma nova era no diagnóstico. O primeiro computador automotivo foi desenvolvido para controlar a injeção eletrônica de combustível, permitindo um controle mais preciso do motor, melhor desempe-

nho e redução de emissões. Este avanço foi fundamental para os futuros diagnósticos computadorizados.

Em 1980, a General Motors foi pioneira ao lançar o OBD-I, o primeiro sistema de diagnóstico a bordo. Este sistema permitia aos técnicos acessar informações básicas sobre o desempenho do motor e outros componentes eletrônicos através de um conector específico e não padronizado. Embora o OBD-I oferecesse a capacidade de ler códigos de falha para identificar problemas específicos, ele apresentava limitações significativas, como falta de padronização entre fabricantes e restrições a sistemas específicos, o que dificultava diagnósticos abrangentes.

2.1.2 Avanços nos sistemas eletrônicos

Com o avanço da tecnologia e a crescente complexidade dos veículos, os sistemas eletrônicos automotivos se tornaram mais sofisticados e integrados, levando ao desenvolvimento de sistemas de diagnóstico mais avançados.

Em meados da década de 1990, o sistema OBD-II foi introduzido como um padrão obrigatório nos Estados Unidos, revolucionando o diagnóstico automotivo. O OBD-II trouxe padronização para os conectores de diagnóstico e códigos de falha, permitindo uma leitura mais detalhada e precisa dos sistemas do veículo. Este sistema não só monitorava o desempenho do motor, mas também outros componentes críticos, como o sistema de emissões e a transmissão.

A introdução das ECUs (*Electronic Control Units*) transformou ainda mais o diagnóstico automotivo. As ECUs são microcomputadores dedicados que controlam e monitoram funções específicas do veículo, como a gestão do motor, a transmissão, o sistema de freios e o controle de tração. Cada ECU coleta dados de vários sensores e ajusta os parâmetros de operação em tempo real para otimizar o desempenho e a eficiência do veículo.

A rede de comunicação CAN (*Controller Area Network*) é amplamente utilizada na indústria automotiva, permitindo a comunicação entre diversas ECUs de forma eficiente e rápida. Isso facilitou o diagnóstico integrado de múltiplos sistemas, permitindo que problemas em uma parte do veículo fossem rapidamente identificados e corrigidos.

Atualmente, os veículos modernos possuem sistemas de diagnóstico sofisticados que utilizam tecnologias como telemetria, diagnósticos remotos e atualizações de *software over-the-air* (OTA). Isso permite que os problemas sejam identificados e resolvidos de forma remota, muitas vezes sem a necessidade de levar o veículo a uma oficina.

Em resumo, a evolução dos sistemas de diagnóstico automotivo acompanhou o progresso tecnológico dos veículos, proporcionando maior precisão, eficiência e capacidade de monitorar e manter a complexa rede de sistemas eletrônicos dos automóveis modernos.

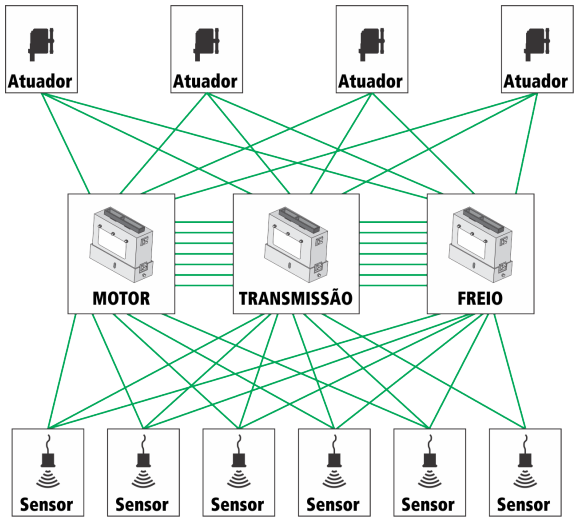
2.2 REDES DE COMUNICAÇÃO VEICULAR

As redes de comunicação veicular são fundamentais para o funcionamento dos sistemas automotivos modernos, possibilitando a troca de informações entre diversos módulos eletrônicos que compõem um veículo. Elas garantem a coordenação eficiente e a integração funcional de componentes como motor, transmissão, sistemas de segurança e entretenimento, e são essenciais para a operação coesa dos complexos sistemas presentes nos veículos atuais.

Nos veículos contemporâneos, a quantidade de componentes eletrônicos e a complexidade dos sistemas aumentaram significativamente. Para que todos esses sistemas funcionem de maneira integrada, é necessário um meio eficiente e confiável de comunicação entre eles. As redes de comunicação veicular foram desenvolvidas com essa finalidade, oferecendo um meio robusto para a troca de dados e garantindo a eficiência e a integridade na operação dos sistemas automotivos.

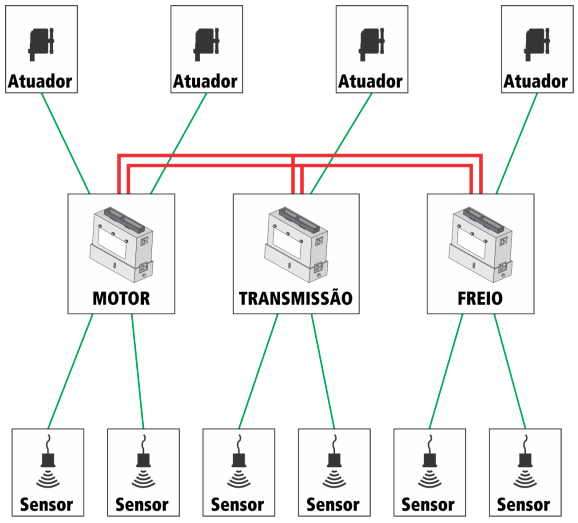
Um marco significativo na história das redes automotivas foi a introdução do protocolo de comunicação CAN (*Controller Area Network*) pela Bosch na década de 1980. A rede CAN revolucionou a comunicação automotiva ao permitir que múltiplos sistemas eletrônicos trocassem informações de maneira eficiente e em tempo real, eliminando a necessidade de complexos sistemas de fiação. A Figura 1 e Figura 2 ilustram o sistema de fiação sem e com uma rede de comunicação integrando as unidades de controle.

Figura 1 – Arquitetura sem rede de comunicação.



Fonte: Ilustração interna da Doutor-IE.

Figura 2 – Arquitetura com rede de comunicação.



Fonte: Ilustração interna da Doutor-IE.

A rede CAN foi projetada para ser uma rede robusta e flexível, capaz de operar em ambientes ruidosos, proporcionando alta imunidade a interferências eletromagné-

ticas e garantindo a integridade dos dados transmitidos. Essa capacidade de operar de maneira confiável em ambientes adversos fez com que a CAN predominasse na indústria automotiva até os dias de hoje.

Atualmente, existem diversos tipos de redes e protocolos de comunicação utilizados nos veículos, cada um com características e aplicações específicas.

2.3 INTRODUÇÃO À REDE CAN

A rede CAN é um sistema de comunicação serial que permite a troca de dados entre ECUs sem a necessidade de um computador central. Ela é baseada em uma topologia de barramento, onde todos os nós (dispositivos conectados) podem se comunicar diretamente uns com os outros através de um par de fios trançados. A rede CAN é especialmente projetada para aplicações que requerem alta confiabilidade e capacidade de detectar e corrigir erros automaticamente. Esta rede foi desenvolvida pela Bosch na década de 1980 e desde então se tornou uma escolha popular devido à sua capacidade de comunicação rápida e confiável em ambientes adversos. Além do setor automotivo, a CAN é usada em automação industrial, equipamentos médicos e sistemas de controle predial.

2.3.1 Arquitetura da rede CAN

A CAN é uma rede serial baseada no modelo OSI, que segue as camadas de enlace de dados e física. A especificação ISO 11898 define as características destas camadas para a comunicação CAN. A arquitetura da rede CAN pode ser dividida nas primeiras duas camadas do modelo OSI, como ilustrado na Figura 3.

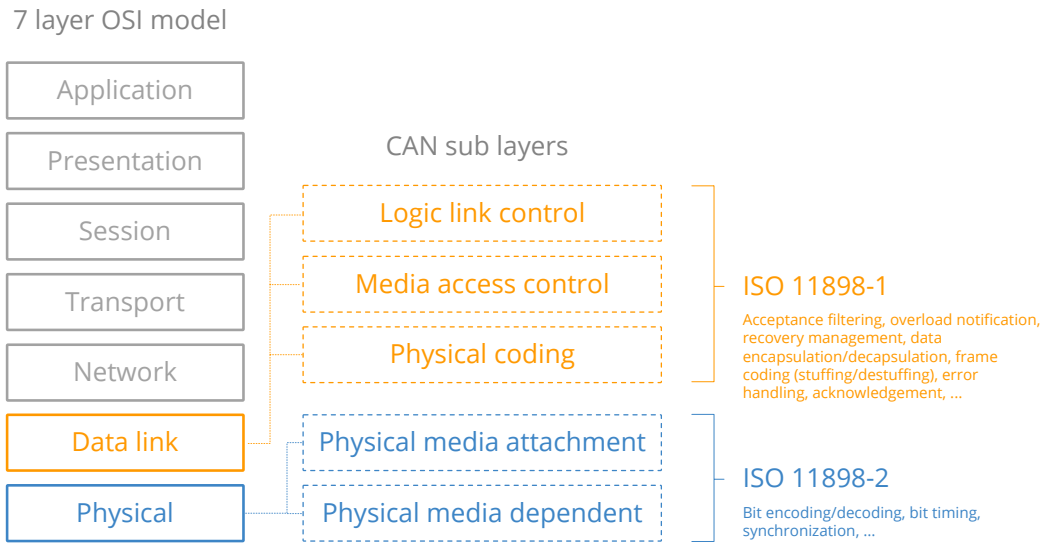
2.3.1.1 Camada física

A camada física da rede CAN define os aspectos elétricos e mecânicos da comunicação. Ela especifica como os dados são transmitidos fisicamente através do meio de transmissão, que normalmente é um cabo de par trançado.

A rede CAN utiliza a sinalização diferencial para transmitir dados. Isso significa que dois fios (CAN High e CAN Low) são usados para criar uma diferença de tensão, que representa os bits de dados. Quando o sinal é dominante (diferença de tensão alta, representa um bit 0), há uma diferença significativa de tensão entre CAN High e CAN Low (tipicamente 2V). Quando o sinal é recessivo (diferença de tensão baixa, representa um bit 1), os fios têm quase a mesma tensão.

A implementação física de uma rede CAN requer o uso de transceptores CAN que são dispositivos que realizam a conversão dos sinais digitais do controlador para os níveis de tensão apropriados na rede CAN. Eles devem suportar curtos-circuitos e ter proteção contra descargas eletrostáticas (ESD) e sobrecarga térmica.

Figura 3 – Camadas que a CAN segue do modelo OSI.



Fonte: CSS Electronics.

A sinalização diferencial ajuda a aumentar a imunidade a ruídos, pois qualquer interferência elétrica tende a afetar os dois fios de forma semelhante, cancelando-se mutuamente.

Para evitar reflexões de sinal e garantir a integridade dos dados, a rede CAN utiliza resistores de terminação (tipicamente 120 ohms) em cada extremidade do barramento.

2.3.1.2 Camada de enlace de dados

A camada de enlace de dados é responsável pelo controle de acesso ao barramento, pela detecção e correção de erros e pelo formato das mensagens trocadas entre os nós da rede.

As mensagens na rede CAN são compostas por vários campos, incluindo um identificador, dados e um código de verificação de erro Cyclic Redundancy Check (CRC). Existem dois tipos de quadros de dados na rede CAN: o *frame* padrão, que utiliza um identificador de 11 bits, e o *frame* estendido, com um identificador de 29 bits. A CAN é configurada geralmente como uma topologia em barramento, onde todos os dispositivos (nós) são conectados ao mesmo par de fios. A rede pode operar em diferentes velocidades de transmissão, comumente até 1 Mbps, mas pode ser ajustada para velocidades menores dependendo da distância e da necessidade de imunidade a ruídos.

A CAN utiliza um método de arbitragem não destrutivo baseado em prioridade

para acessar o barramento. Cada mensagem tem um identificador que determina sua prioridade. Quando dois ou mais nós tentam transmitir simultaneamente, o nó com a mensagem de maior prioridade continua a transmissão, enquanto os outros esperam.

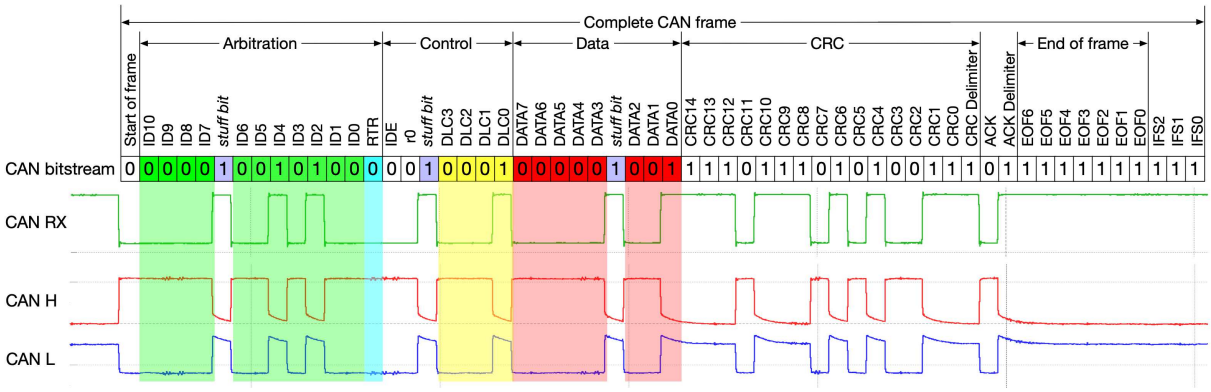
2.3.2 Formato da mensagem CAN

Na rede CAN há dois formatos de mensagens principais: o formato padrão (*Standard* CAN) com um identificador de 11 bits e o formato estendido (*Extended*CAN) com um identificador de 29 bits. A descrição detalhada de cada um destes formatos está indicada abaixo:

2.3.2.1 Formato de mensagem CAN padrão (11 Bits)

A figura 4 ilustra a rede CAN com seus respectivos quadros, os quais podem ser visualizados a nível de bit com o sinal da CAN H e CAN L.

Figura 4 – Formato da mensagem CAN.



Fonte: Wikipedia.

Tabela 1 – Formato de mensagem CAN de 11 bits.

SOF	ID	RTR	IDE	r0	DLC	Data	CRC	ACK	EOF

Fonte: O autor.

SOF (*Start of Frame*): Um único bit dominante que marca o início de uma mensagem e é usado para sincronizar os nós no barramento após estar inativo.

ID de 11 bits (*Identifier*): Um identificador de 11 bits que estabelece a prioridade da mensagem, onde o valor binário mais baixo indica maior prioridade.

RTR (*Remote Transmission Request*): Um único bit dominante que é usado quando informações são requeridas de outro nó.

IDE (*Identifier Extension*): Um único bit dominante que indica que nenhum bit de extensão de identificador está sendo transmitido.

r0: Bit reservado para uso futuro.

DLC (*Data Length Code*): Um código de 4 bits que contém o número de bytes de dados sendo transmitidos.

***Data*:** Até 64 bits (8 bytes) de dados de aplicação podem ser transmitidos, incluindo o tamanho da mensagem no campo *Data*, o SID, o PID e os dados da mensagem. Esse *frame* será abordado com mais detalhes no capítulo de Desenvolvimento.

CRC (Cyclic Redundancy Check): Um código de 16 bits (15 bits mais delimitador) que contém a soma de verificação dos dados de aplicação precedentes para detecção de erro.

ACK (*Acknowledgment*): Cada nó que recebe uma mensagem sem erros sobrescreve este bit recessivo na mensagem original com um bit dominante, indicando que uma mensagem livre de erros foi enviada.

EOF (*End of Frame*): Um campo de 7 bits que marca o final de uma mensagem CAN e desativa o *bit-stuffing*, indicando um erro de *stuffing* quando dominante.

2.3.2.2 Formato de mensagem CAN estendido (29 Bits)

A CAN estendida engloba todas as funcionalidades da CAN padrão, adicionando capacidades ampliadas por meio de um identificador estendido de 29 bits, proporcionando maior flexibilidade e complexidade na gestão de prioridades e organização de mensagens na rede.

Tabela 2 – Formato de mensagem CAN de 29 bits.

SOF	ID	SRR	IDE	ID 18-bit	RTR	r1	r0	DLC	Data	CRC	ACK	EOF	IFS

Fonte: O autor.

SRR (*Substitute Remote Request*): Substitui o bit RTR na localização da mensagem padrão como um espaço reservado no formato estendido.

IDE: Um bit recessivo no campo de extensão do identificador que indica que mais bits de identificador seguem. Uma extensão de 18 bits segue o IDE.

ID de 18 bits (*Identifier*): Um identificador de 18 bits que estabelece a prioridade da mensagem, onde o valor binário mais baixo indica maior prioridade. Complementa o *Identifier* de 11 bits, que somando-os apresentam 29 bits de identificador.

r1: Após os bits RTR e r0, um bit reservado adicional foi incluído antes do bit DLC.

2.3.3 Funcionamento da rede CAN

O funcionamento da rede CAN é caracterizado pela sua capacidade de transmitir dados de forma eficiente e confiável, mesmo em ambientes adversos. Quando um nó deseja enviar uma mensagem, ele coloca os dados no barramento. Todos os nós da rede recebem essa mensagem, mas apenas o nó destinatário ou os nós interessados processam a informação.

A CAN utiliza um mecanismo de arbitragem não destrutivo baseado na prioridade da mensagem para gerenciar o acesso ao barramento. Mensagens com identificadores mais baixos têm prioridade mais alta. Se dois nós tentam transmitir simultaneamente, o nó com a mensagem de maior prioridade continua a transmissão enquanto o outro desiste, garantindo que as mensagens mais importantes sejam sempre transmitidas primeiro. Isso é crucial em sistemas automotivos, onde mensagens de alta prioridade, como comandos de freio, devem ser enviadas imediatamente.

Se um nó detecta que uma mensagem foi corrompida, ele envia um quadro de erro e a mensagem é retransmitida. Esse mecanismo assegura que a comunicação se mantenha confiável, mesmo na presença de interferências ou falhas temporárias.

A rede CAN é projetada para ser altamente interoperável, permitindo que dispositivos de diferentes fabricantes se comuniquem de maneira eficiente. Isso facilita a integração de novos módulos e a expansão da rede sem a necessidade de grandes alterações no sistema.

2.4 NORMAS E PROTOCOLOS DE COMUNICAÇÃO VEICULAR

Os sistemas de diagnóstico veicular são essenciais para a manutenção e eficiência dos veículos modernos. Eles utilizam normas e protocolos específicos que permitem a comunicação entre os sistemas internos do veículo e os *scanners*. Normas e protocolos têm funções distintas: normas estabelecem requisitos técnicos e critérios de qualidade, enquanto protocolos definem como a comunicação deve ocorrer entre diferentes sistemas.

Uma norma é um documento que define critérios e diretrizes para garantir a uniformidade e a qualidade em um determinado campo, segurança ou desempenho. Por exemplo, normas ISO definem padrões globais para sistemas de gestão de qualidade.

Por outro lado, um protocolo é um conjunto de regras que governa como os dados são formatados, transmitidos, recebidos e interpretados em uma comunicação entre dispositivos. É fundamental para assegurar a compatibilidade e eficiência na interação entre sistemas diferentes, como o protocolo CAN amplamente usado nas redes de comunicacão veiculares.

As normas predominantemente utilizadas pelos fabricantes de veículos são a UDS e a KWP. Uma breve descrição de suas origens e dos serviços específicos por

elas suportados será apresentada nas seções subsequentes.

2.4.1 OBD I (*On-Board Diagnostics I*)

O OBD I foi introduzido na Califórnia na década de 1980 em resposta à crescente preocupação com as emissões de poluentes e a necessidade de uma manutenção mais eficiente dos veículos. Nos Estados Unidos, a Agência de Proteção Ambiental (EPA) e o Conselho de Recursos do Ar da Califórnia (CARB) estabeleceram diretrizes para reduzir as emissões de veículos, levando à criação do OBD I. Foi a primeira norma de diagnóstico embarcado, estabelecendo requisitos mínimos para a detecção e controle de falhas nos sistemas de emissões.

O OBD I permitia a leitura de códigos de falha genéricos através de um conector específico, possibilitando o diagnóstico de problemas no sistema de emissão e outros componentes eletrônicos do veículo. Cada fabricante tinha seu próprio padrão, o que dificultava a padronização do diagnóstico entre diferentes marcas de veículos.

2.4.1.1 Identificadores de serviço (SID)

No OBD I, os identificadores de serviço eram proprietários, variando entre os fabricantes de veículos, o que limitava a interoperabilidade e dificultava a criação de ferramentas de diagnóstico universais. Não fornecia informações detalhadas sobre o desempenho do motor ou outros sistemas críticos do veículo.

2.4.2 OBD II (*On-Board Diagnostics II*)

Introduzido em 1996 nos EUA (Estados Unidos da América), o OBD II foi uma evolução do OBD I, visando a melhoria na eficiência do monitoramento de emissões e a padronização entre veículos e dispositivos de diagnóstico. Ele foi criado para lidar com a crescente complexidade dos sistemas veiculares e garantir uma gestão mais eficaz das emissões.

O OBD II padronizou o conector de 16 pinos e os códigos de falha, facilitando o uso de ferramentas de diagnóstico universais. Esta padronização foi estendida para muitos países ao redor do mundo. A norma atende sistemas críticos do veículo como motor e transmissão.

Os protocolos OBD II incluem:

ISO 9141-2 (K-Line): Este protocolo é comumente usado em veículos europeus e asiáticos. É um protocolo de comunicação serial que define como os dados de diagnóstico são transferidos entre a ECU do veículo e o *scanner* de diagnóstico.

SAE J1850: Este protocolo foi amplamente utilizado em veículos americanos. Existem duas variações sendo o PWM (*Pulse Width Modulation*) e o VPW (*Variable Pulse*

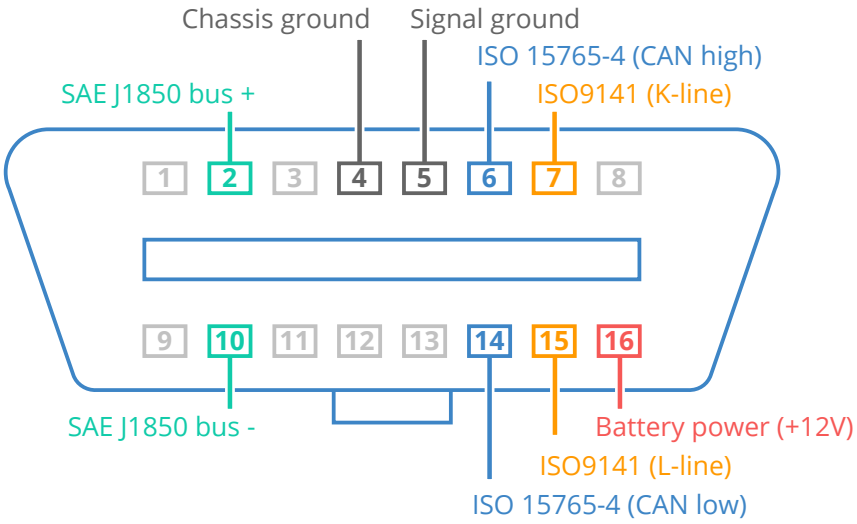
Width).

ISO 15765 (CAN): Utilizado amplamente devido à sua velocidade e robustez.

ISO 14230 (KWP 2000): Amplamente utilizado por fabricantes europeus e asiáticos.

A Figura 5 ilustra o conector de diagnóstico padronizado de 16 pinos, presente nos veículos atuais, junto com os protocolos utilizados.

Figura 5 – Conector OBD II.



Fonte: CSS Electronics.

2.4.2.1 Identificadores de serviço (SID)

Os serviços padronizados do OBD II são bytes específicos utilizados em protocolos de diagnóstico veicular que definem as funções ou ações a serem realizadas pela ECU em resposta a uma solicitação de diagnóstico. Cada identificador de serviço corresponde a uma operação específica, como ler dados de sensores ou apagar códigos de falha. Eles permitem a execução de uma ampla gama de tarefas de diagnóstico e manutenção em veículos.

Serviço 0x01: Permite a leitura de parâmetros operacionais em tempo real, como temperatura do motor, rotação por minuto (RPM), velocidade do veículo, etc.

Serviço 0x02: Fornece acesso aos dados operacionais capturados no momento em que um código de falha foi detectado.

Serviço 0x03: Permite a leitura dos códigos de falha atuais armazenados na memória da ECU.

Serviço 0x04: Apaga os códigos de falha e dados congelados da memória da ECU.

Serviço 0x05: Permite a leitura dos resultados dos testes realizados na sonda lambda, que monitora o nível de oxigênio no escapamento.

Serviço 0x06: Fornece acesso aos resultados dos testes de monitoramento dos sistemas de controle de emissões.

Serviço 0x07: Permite a leitura de códigos de falha que foram detectados, mas que ainda não causaram a ativação da luz de advertência no painel.

Serviço 0x08: Utilizado para acionar e monitorar componentes específicos do sistema de emissões.

Serviço 0x09: Fornece acesso a informações gerais do veículo, como o número de identificação do veículo (Vehicle Identification Number (VIN)) e outras informações de identificação.

Serviço 0x0A: Permite a leitura de códigos de falha que foram registrados como permanentes pela ECU.

2.4.3 OBD BR1 e OBD BR2

As normas OBD BR1 e OBD BR2 são baseadas no OBD II e foram desenvolvidas para atender às necessidades específicas do mercado brasileiro e alinhar-se com as regulamentações ambientais locais. Elas foram criadas para monitorar e controlar as emissões de poluentes, bem como para garantir a eficiência e segurança dos veículos.

Essas normas monitoram o sistema de emissões, garantindo que os veículos atendam às normas ambientais brasileiras. Facilitam a identificação e correção de falhas nos sistemas de controle do motor e emissões. Similar ao OBD II, esses padrões permitem a leitura de códigos de falha específicos para ajudar na manutenção do veículo.

A OBD BR1 é focada em garantir a conformidade básica com as normas de emissões e foi introduzida no início dos anos 2000 como parte de uma série de medidas para reduzir as emissões de veículos no Brasil. Já a OBD BR2 foi introduzida em meados de 2010 com requisitos mais rigorosos e abrangentes para o monitoramento e diagnóstico dos sistemas de emissão, oferecendo maior capacidade de diagnóstico e monitoramento, incluindo a detecção precoce de falhas e a manutenção preventiva.

2.4.4 KWP 2000 (*Keyword Protocol 2000*)

O KWP 2000 foi introduzido na década de 1990 e está definido nas normas ISO 14230 e ISO 15765. Ele foi projetado para melhorar a comunicação entre os sistemas

eletrônicos do veículo e os dispositivos de diagnóstico, suportando uma ampla gama de funções e tipos de dados.

O KWP 2000 foi desenvolvido para fornecer um protocolo de comunicação eficiente para o diagnóstico e programação de ECUs. Ele atende à necessidade de um diagnóstico detalhado e flexível, particularmente em veículos europeus. Ele permite uma transferência eficiente de dados, facilitando a integração com diferentes tipos de sistemas eletrônicos no veículo.

2.4.4.1 Identificadores de serviço (SID)

Serviço 0x10 (*Start Diagnostic Session*): Muda o sistema para um modo específico de diagnóstico. Há a sessão padrão e a sessão extendida, sendo que a última possibilita funções avançadas como reprogramação de ECU.

Serviço 0x11 (ECU *Reset*): Pode ser usado para simular um reinício do sistema, limpando falhas temporárias ou resetando parâmetros.

Serviço 0x12 (*Read Freeze Frame Data*): Lê os dados congelados. Estes são dados capturados no momento em que uma falha é detectada, fornecendo um *snapshot* do estado do veículo com seus parâmetros no momento em que ocorreu a falha.

Serviço 0x13 (*Read Diagnostic Trouble Codes*): Lê os códigos de falha de diagnóstico (DTCs) armazenados na memória da ECU.

Serviço 0x14 (*Clear Diagnostic Information*): Limpa os códigos de falha e outras informações de diagnóstico da memória da ECU.

Serviço 0x17 (*Read Status Of Diagnostic Trouble Codes*): Lê o estado dos códigos de falha de diagnóstico, indicando se um DTC está ativo, pendente ou se é do passado.

Serviço 0x18 (*Read Diagnostic Trouble Codes By Status*): Lê códigos de falha específicos com base no estado do DTC, permitindo uma filtragem mais detalhada.

Serviço 0x1A (*Read ECU Identification*): Lê as informações de identificação da ECU, como o número de peça ou versão do *software*.

Serviço 0x20 (*Stop Diagnostic Session*): Encerra a sessão de diagnóstico atualmente ativa, retornando a ECU ao seu estado normal de operação (sessão padrão).

Serviço 0x21 (Read Data By Local Identifier): Lê dados específicos da ECU usando um identificador local. É uma forma rápida de acessar dados predefinidos.

Serviço 0x22 (*Read Data By Common Identifier*): Lê dados específicos usando um identificador comum que pode ser compartilhado entre diferentes ECUs.

Serviço 0x23 (*Read Memory By Address*): Lê uma área específica da memória da ECU baseada em um endereço fornecido.

Serviço 0x26 (*Set Data Rates*): Define as taxas de transmissão de dados para comunicação entre a ECU e o aparelho de diagnóstico.

Serviço 0x27 (*Security Access*): Garante o acesso a funções protegidas da ECU, exigindo a troca de uma chave de segurança.

Serviço 0x2C (*Dynamically Define Local Identifier*): Permite ao aparelho de diagnóstico definir dinamicamente identificadores locais para acessar novos dados ou realizar testes específicos.

Serviço 0x2E (*Write Data By Common Identifier*): Escreve dados em um identificador comum, permitindo atualizações ou ajustes de parâmetros padronizados.

Serviço 0x2F (*Input Output Control By Common Identifier*): Controla diretamente entradas e saídas da ECU usando um identificador comum. Realiza os conhecidos testes de atuadores.

Serviço 0x30 (*Input Output Control By Local Identifier*): Controla entradas e saídas da ECU usando um identificador local. Realiza os conhecidos testes de atuadores.

Serviço 0x31 (*Start Routine By Local Identifier*): Inicia uma rotina de teste ou manutenção específica usando um identificador local.

Serviço 0x32 (*stop Routine By Local Identifier*): Para uma rotina em execução na ECU que foi iniciada por um identificador local.

Serviço 0x33 (*Request Routine Results By Local Identifier*): Solicita os resultados de uma rotina de teste ou manutenção específica.

Serviço 0x34 (*Request Download*): Inicia uma transferência de dados para a ECU, frequentemente usada para *download* de *software*.

Serviço 0x35 (*Request Upload*): Solicita a transferência de dados da ECU para o aparelho de diagnóstico.

Serviço 0x36 (*Transfer Data*): Transferência contínua de dados entre a ECU e o aparelho de diagnóstico após a solicitação de *download* ou *upload*.

Serviço 0x37 (*Request Transfer Exit*): Finaliza a transferência de dados iniciada anteriormente.

Serviço 0x38 (*Start Routine By Address*): Inicia uma rotina de teste ou manutenção específica usando um endereço de memória.

Serviço 0x39 (*Stop Routine By Address*): Para uma rotina em execução na ECU que foi iniciada por um endereço de memória.

Serviço 0x3A (*Request Routine Results By Address*): Solicita os resultados de uma rotina de teste ou manutenção específica por endereço de memória.

Serviço 0x3B (*Write Data By Local Identifier*): Escreve dados em um identificador local, permitindo a atualização de parâmetros específicos.

Serviço 0x3D (*Write Memory By Address*): Escreve dados diretamente em uma área específica da memória da ECU.

Serviço 0x3E (*Tester Present*): Envia uma mensagem de manutenção para manter a comunicação ativa.

Serviço 0x80 (*ESC Code*): Código de escape para serviços executados durante a sessão estendida.

2.4.5 UDS (*Unified Diagnostic Services*)

O UDS, definido pela norma ISO 14229 publicada inicialmente em 2006, foi desenvolvido para unificar os serviços de diagnóstico em uma única estrutura aplicável a uma ampla gama de sistemas veiculares. A criação do UDS foi motivada pela necessidade de um padrão mais versátil e abrangente para facilitar o diagnóstico e a manutenção de sistemas eletrônicos complexos.

O UDS oferece um conjunto completo de serviços que permitem o diagnóstico, manutenção e reprogramação de sistemas veiculares. Suporta operações avançadas, como o *download* de *software* e testes específicos de componentes, facilitando a gestão de sistemas eletrônicos sofisticados nos veículos.

Ele consolidou diferentes serviços de diagnóstico sob um único padrão, simplificando o desenvolvimento de ferramentas e permitindo uma integração mais fácil e eficiente com sistemas veiculares de diferentes fabricantes.

2.4.5.1 Identificadores de serviço (SID)

Serviço 0x10 (*Diagnostic Session Control*): Muda o sistema para um modo específico de diagnóstico. Há a sessão padrão e a sessão extendida, sendo que a última possibilita funções avançadas como reprogramação de ECU.

Serviço 0x11 (ECU*Reset*): Reinicia a unidade de controle eletrônico, podendo limpar falhas temporárias ou reiniciar parâmetros.

Serviço 0x14 (*Clear Diagnostic Information*): Apaga códigos de falha e outros dados armazenados na memória de diagnóstico.

Serviço 0x19 (*Read DTC Information*): Fornece informações sobre os códigos de falha armazenados, incluindo seu status e dados associados.

Serviço 0x22 (*Read Data by Identifier*): Permite a leitura de valores de parâmetros específicos usando um identificador único (PID).

Serviço 0x23 (*Read Memory by Address*): Lê dados de uma área específica da memória da ECU.

Serviço 0x24 (*Read Scaling Data by Identifier*): Lê os dados de escala para os parâmetros de diagnóstico.

Serviço 0x27 (*Security Access*): Fornece acesso a níveis de segurança específicos para operações críticas como reprogramação de ECU.

Serviço 0x28 (*Communication Control*): Habilita ou desabilita comunicações específicas no barramento do veículo.

Serviço 0x2A (Request Transfer Exit): Finaliza uma transferência de dados iniciada anteriormente.

Serviço 0x2C (*Routine Control*): Executa, para ou controla rotinas de teste ou manutenção específicas.

Serviço 0x2E (*Write Data by Identifier*): Permite a gravação de dados em um PID (*Parameter Identifier*) específico.

Serviço 0x2F (*Input Output Control by Identifier*): Controla diretamente entradas e saídas do veículo. Realiza os conhecidos testes de atuadores.

Serviço 0x31 (*Routine Control*): Inicia, para ou controla rotinas de teste específicas, geralmente usadas para diagnóstico avançado.

Serviço 0x34 (*Request Download*): Inicia uma transferência de dados para a ECU, frequentemente usada para atualização de software.

Serviço 0x35 (*Request Upload*): Este serviço inicia o processo de *upload* de dados da ECU para o aparelho de diagnóstico. Ele permite que o cliente especifique quais dados deseja extrair da ECU e define os parâmetros para a transferência de dados.

Serviço 0x36 (*Transfer Data*): Transfere os dados para a ECU após o início da transferência.

Serviço 0x37 (*Request Transfer Exit*): Finaliza a transferência de dados iniciada anteriormente.

Serviço 0x3D (*Write Memory by Address*): Este serviço permite que o *scanner* escreva dados diretamente em um endereço específico da memória da ECU.

Serviço 0x3E (*Tester Present*): Envia uma mensagem de manutenção para manter a comunicação ativa.

Serviço 0x83 (*Access Timing Parameter*): Este serviço permite que o aparelho de diagnóstico ajuste os parâmetros de tempo para a comunicação de diagnóstico com a ECU. Isso pode incluir o ajuste dos intervalos de tempo de resposta e *timeout*, garantindo que a comunicação seja mantida eficiente e dentro dos requisitos específicos da aplicação.

Serviço 0x84 (*Secured Data Transmission*): Este serviço permite a transferência de dados entre o aparelho de diagnóstico e a ECU de maneira segura, garantindo que os dados não sejam interceptados ou modificados por terceiros. Inclui mecanismos de criptografia e autenticação para proteger a integridade e a confidencialidade dos dados transmitidos.

Serviço 0x85 (*Programming Session*): Inicia uma sessão de programação para atualizar ou modificar o *software* da ECU.

Serviço 0x86 (*Response on Event*): Este serviço permite que a ECU envie automaticamente uma resposta para o aparelho de diagnóstico quando um evento específico ocorrer. Isso pode incluir a mudança de estado de um sensor ou a detecção de uma falha, facilitando a monitoração contínua sem a necessidade de solicitações repetidas do *scanner*.

Serviço 0x87 (*Link Control*): Este serviço permite que o aparelho de diagnóstico ajuste os parâmetros de comunicação do *link*, como a velocidade de transmissão de dados quando está muito rápida ou muito lenta. Isso ajuda a manter a eficiência e a estabilidade da comunicação, adaptando-a a diferentes condições de operação e requisitos de dados.

2.4.6 Segurança das redes automotivas

A segurança das redes automotivas é uma preocupação crescente à medida que os veículos modernos incorporam tecnologias avançadas, como conectividade à

internet e funções de direção autônoma. Essas tecnologias oferecem benefícios significativos em termos de eficiência, segurança e experiência do usuário, mas também expõem os veículos a uma ampla gama de ameaças cibernéticas.

Em veículos modernos, sensores como LiDAR, câmeras e radares, essenciais para a percepção ambiental, são particularmente vulneráveis a ataques cibernéticos, que podem distorcer a interpretação do ambiente pelo sistema de controle. A comunicação entre os diversos sistemas do veículo também está sujeita a riscos consideráveis. A interceptação ou a modificação de dados críticos pode levar a comportamentos imprevisíveis e potencialmente perigosos. Outro desafio significativo é a segurança das redes internas do veículo, como a CAN. A inserção de mensagens maliciosas nessas redes pode comprometer o funcionamento de sistemas de controle críticos. Além disso, veículos autônomos que se comunicam com infraestruturas externas, como semáforos inteligentes e serviços de nuvem, podem ser alvos de ataques que exploram essas interfaces.

Para esses e outros desafios de segurança nas redes automotivas, foi implementado em alguns veículos uma UCE denominada SGW.

2.4.6.1 *Security Gateway* (SGW)

O *Security Gateway* desempenha um papel crucial na segurança das redes automotivas, protegendo as centrais veiculares contra ameaças de ataques externos. Sua principal função é servir como um guardião que filtra e gerencia o tráfego de dados, garantindo que apenas comunicações autorizadas e seguras sejam permitidas. As principais funções dessa central está listada abaixo.

Isolamento de redes: Ele isola as redes internas umas das outras e das redes externas (como do conector de diagnóstico do veículo), minimizando o risco de que uma vulnerabilidade em um segmento possa comprometer o sistema inteiro. Esse isolamento é fundamental para evitar que um ataque em uma parte do sistema se espalhe para outras partes.

Filtragem e monitoramento de tráfego: O dispositivo monitora continuamente o tráfego de dados, filtrando mensagens para bloquear comunicações suspeitas ou maliciosas. Ele verifica cada mensagem que passa através dele, assegurando que apenas dados autorizados e seguros possam ser transmitidos.

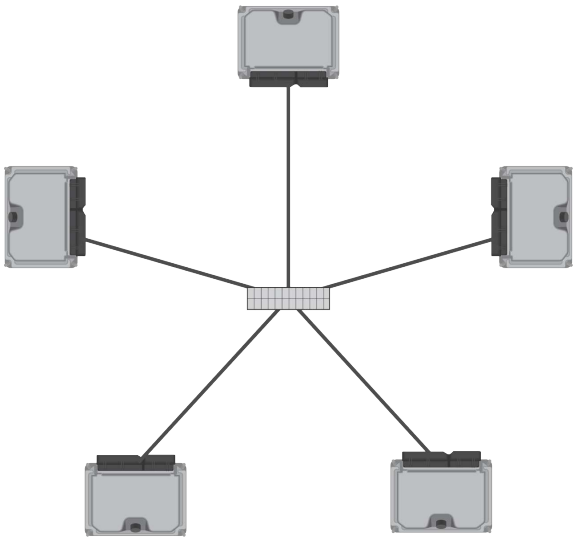
Autenticação e autorização: O *Security Gateway* autentica dispositivos e mensagens, garantindo que apenas entidades confiáveis possam se comunicar com os sistemas críticos do veículo. Isso impede que dispositivos não autorizados ou *hackers* acessem ou manipulem a rede interna do veículo.

Gerenciamento de políticas de segurança: Ele implementa e gerencia políticas de segurança que definem quais dispositivos e mensagens têm permissão para acessar diferentes partes da rede. Essas políticas são ajustadas dinamicamente para responder a novas ameaças e garantir a conformidade com as normas de segurança.

Criptografia e Proteção de Dados: O *Security Gateway* utiliza técnicas de criptografia para proteger os dados em trânsito e em repouso, garantindo que informações sensíveis não sejam interceptadas ou adulteradas.

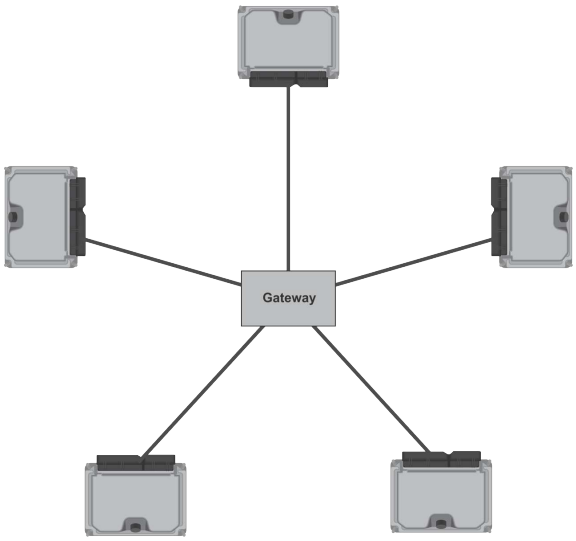
A Figura 6 ilustra uma arquitetura de rede sem o SGW, permitindo que um conector intermediário tenha acesso ao barramento de dados transmitidos entre as centrais, enquanto que a Figura 7 ilustra uma arquitetura de rede com o SGW, isolando as centrais do veículo de uma possível comunicação externa antes de passar pelo *Security Gateway*.

Figura 6 – Arquitetura sem SGW.



Fonte: Ilustração interna da Doutor-IE.

Figura 7 – Arquitetura com SGW.



Fonte: Ilustração interna da Doutor-IE.

A implementação de diversas normas de segurança é fundamental para assegurar a integridade e a proteção das redes automotivas. Entre as normas destacam-se a ISO/SAE 21434, SAE J3061 e ISO 26262, entre outras.

A ISO/SAE 21434 é uma norma dedicada à engenharia de cibersegurança para veículos rodoviários. Ela define requisitos para proteger sistemas automotivos contra ameaças cibernéticas, abrangendo análise de riscos e estratégias de mitigação.

Complementarmente, a SAE J3061 fornece um guia de cibersegurança específico para sistemas ciberfísicos veiculares. Este documento apresenta metodologias

para identificar e avaliar riscos potenciais em sistemas veiculares, orientando a implementação de medidas de segurança adequadas.

A ISO 26262, por sua vez, foca na segurança funcional dos sistemas elétricos e eletrônicos em veículos. Ela estabelece requisitos para garantir a operação segura de sistemas críticos mesmo em condições de falha, orientando o desenvolvimento seguro de software e hardware para minimizar os riscos associados a falhas funcionais.

Essas normas e protocolos são essenciais para o desenvolvimento de sistemas automotivos que não apenas atendam aos requisitos funcionais, mas também sejam robustos frente a uma ampla gama de ameaças e vulnerabilidades, assegurando a confiabilidade dos veículos modernos.

2.5 DIAGNÓSTICO AUTOMOTIVO

Com o avanço da tecnologia automotiva, os veículos modernos têm se tornado sistemas altamente complexos, incorporando uma vasta rede de unidades de controle eletrônico interligadas que gerenciam tudo, desde a injeção de combustível até a climatização interna do veículo. Quando um problema ocorre, ele pode se manifestar de maneiras que afetam múltiplos sistemas simultaneamente, tornando a localização e a correção da falha uma tarefa complexa e demorada sem as ferramentas adequadas. Neste contexto, os *scanners* automotivos emergem como instrumentos indispensáveis para a detecção e resolução de problemas, permitindo a interação eficaz com as diversas redes de comunicação do veículo.

Os aparelhos de diagnóstico automotivo, ou de diagnóstico veicular, são ferramentas que permitem a comunicação direta com as ECUs dos veículos. Eles são projetados para ler e interpretar parâmetros do veículo em tempo real, identificar códigos de falha, executar testes de atuadores como pulsar injetores de combustível ou acionar eletroválvulas e atualizar *softwares* ou reprogramar ECUs.

A utilização de *scanners* tem um impacto direto na eficiência e precisão do diagnóstico, oferecendo diversos benefícios técnicos e operacionais. A capacidade de acessar e interpretar rapidamente os dados das ECUs e identificar códigos de falha reduz significativamente o tempo necessário para diagnosticar problemas complexos, melhorando a eficiência operacional das oficinas e minimizando o tempo de inatividade dos veículos, o que aumenta a satisfação do cliente. Além disso, o acesso detalhado a dados e a capacidade de realizar testes específicos proporcionam um diagnóstico mais preciso, reduzindo a probabilidade de erros e a necessidade de reparos repetidos. Essa precisão no diagnóstico resulta em reparos mais eficazes e maior confiabilidade do veículo, diminuindo custos e melhorando a segurança.

A capacidade de monitorar e testar sistemas interconectados permite a detecção de problemas que afetam múltiplos sistemas, algo difícil de identificar sem o uso de uma ferramenta de diagnóstico. Isso é especialmente relevante para veículos moder-

nos, onde uma falha em um sistema pode causar efeitos em cadeia em outros. Além disso, aparelhos de diagnóstico automotivos auxiliam na conformidade com normas e regulamentos de emissões e segurança, que exigem monitoramento contínuo e relatórios precisos. A conformidade com essas normas é crucial para evitar penalidades e garantir que os veículos operem de maneira segura e eficiente.

3 METODOLOGIA

Este capítulo detalha a metodologia empregada no estudo dos protocolos de comunicação de redes automotivas, diagnósticos e *Freeze Frame*. Com enfoque na rede CAN devido à sua robustez e domínio no mercado, explorou-se a estrutura de comunicação entre as ECUs e a aplicação de protocolos diagnósticos específicos para identificar e resolver falhas. A análise abrangente visa estabelecer um diagnóstico eficiente e uma manutenção preventiva, fundamentais para a otimização e segurança dos veículos. Além disso, a engenharia reversa da rede CAN será explorada, destacando técnicas para captura e análise de mensagens para documentar comunicações entre ECUs, essenciais para o desenvolvimento de ferramentas de diagnóstico avançadas.

3.1 DEFINIÇÃO DE UM VEÍCULO DE BASE

A definição de um veículo de base é um passo crucial no desenvolvimento deste projeto, pois garante que os dados coletados e analisados sejam representativos e aplicáveis ao objetivo do estudo. A escolha do veículo de base envolve uma série de critérios técnicos e logísticos que permitem a execução eficiente das etapas subsequentes do projeto.

3.1.1 Critérios para a escolha do veículo

A escolha do veículo deve assegurar a conformidade com a norma OBD BR-II, que é específica para o mercado brasileiro nos veículos fabricados a partir de 2010. Esta norma é fundamental para garantir que o veículo selecionado esteja equipado com o sistema de diagnóstico de bordo apropriado e uma interface de diagnóstico OBD-II padronizada.

Também é necessário que o veículo possua uma central de motor que se comunique via rede CAN, uma vez que este protocolo é amplamente utilizado em sistemas de comunicação automotiva e será o foco das análises de engenharia reversa.

O veículo deve ser um modelo amplamente disponível e representativo do mercado brasileiro. Isso assegura que os resultados obtidos possam ser aplicados de forma mais ampla e contribuam para a indústria automotiva nacional.

3.1.2 Veículo selecionado

Com base nos critérios acima, o veículo escolhido para servir como base no presente estudo é o Peugeot 208 I [2015] - 1.5 8V Flex 89/93cv (TU4-YFY) com central do motor VALEO V34.5. Este modelo foi selecionado devido à sua conformidade com a norma OBD BR-II, a presença de uma central de motor que utiliza a rede CAN para comunicação e sua ampla disponibilidade no mercado brasileiro.

A Figura 8 ilustra o veículo que será utilizado como objeto de estudo.

Figura 8 – Ilustração do Peugeot 208 I [2015] - 1.5 8V Flex 89/93cv (TU4-YFY).

Fonte: Plataforma Doutor-IE.

A definição de um veículo de base é uma etapa fundamental que garante a relevância e a aplicabilidade do projeto de engenharia reversa na comunicação de centrais veiculares. A escolha criteriosa do Peugeot 208 I [2015] atende aos requisitos técnicos e logísticos necessários para o sucesso do projeto, permitindo a coleta de dados precisa e a análise detalhada das comunicações automotivas, contribuindo para o avanço do diagnóstico automotivo no contexto brasileiro. O veículo em questão foi gentilmente cedido como objeto de estudo por um amigo, Pedro Ribeiro.

3.2 FUNÇÕES E UTILIZAÇÕES DE UM *SCANNER*

Dentro do contexto de oficinas mecânicas e diagnóstico automotivo, um *scanner* é uma ferramenta essencial que serve para se comunicar com as ECUs de um veículo. *Scanners* são dispositivos utilizados para acessar, ler e interpretar os dados e códigos de falha gerados pelas centrais veiculares, que são sistemas computadorizados responsáveis por monitorar e controlar uma série de funções críticas do veículo, como o motor, a transmissão, os sistemas de freio, e outros sistemas de segurança e conforto.

3.2.1 Leitura de códigos de falha (DTCs)

A função mais básica de um *scanner* automotivo é ler os códigos de falha armazenados na memória das ECUs. Esses códigos, conhecidos como *Diagnostic Trouble Codes* (DTCs), são gerados quando o sistema do veículo detecta um erro

ou mal funcionamento. Os códigos ajudam os mecânicos a identificar rapidamente a origem do problema, facilitando um diagnóstico mais preciso e uma reparação eficaz.

3.2.2 Monitoramento em tempo real

Scanners permitem o monitoramento em tempo real de vários parâmetros operacionais do veículo. Eles podem exibir dados ao vivo, como a temperatura do motor, a pressão do combustível, a velocidade do veículo, as rotações do motor (RPM), entre outros. Essa funcionalidade é crucial para a análise de desempenho e para diagnósticos que exigem uma compreensão dinâmica do estado do veículo.

3.2.3 Execução de testes de atuadores e rotinas

Além de ler informações, aparelhos de diagnóstico avançados podem enviar comandos às ECUs para ativar ou testar diferentes componentes e sistemas do veículo. Isso inclui testes de atuadores (como injetores de combustível, válvulas ou motores elétricos), bem como a execução de rotinas de teste para verificar a funcionalidade dos sistemas (como ponteiros do painel de instrumentos ou sistema de som).

3.2.4 Reprogramação e configurações

Em alguns casos, os *scanners* também são usados para reprogramar as ECUs com novos parâmetros ou atualizações de software, ajustar configurações ou realizar codificações que alteram o comportamento de certos sistemas do veículo. Isso é particularmente comum em veículos mais modernos, onde muitas funções são controladas por software.

3.2.5 Importância da engenharia reversa

Na engenharia reversa, o *scanner* é utilizado como um meio de entender como as ferramentas de diagnóstico interagem com as ECUs. Ao monitorar as trocas de mensagens entre um aparelho de diagnóstico de confiança e as centrais, os engenheiros podem decifrar o protocolo de comunicação, entender as especificações dos comandos e as respostas das ECUs. Essas informações são cruciais para desenvolver novos produtos de diagnóstico que sejam compatíveis e eficazes, assegurando que eles possam interagir corretamente com os sistemas do veículo.

3.3 ENGENHARIA REVERSA DA REDE CAN

A engenharia reversa da rede CAN no projeto da Doutor-IE emprega uma metodologia detalhada para capturar, analisar e documentar as comunicações entre as

UCEs, especialmente focando nas interações entre um *scanner* de diagnóstico confiável e a central do motor do veículo, que é a UCE de estudo. Este processo é essencial para entender e replicar as funcionalidades dos diagnósticos automotivos avançados, permitindo que a Doutor-IE desenvolva um *scanner* que não só lê, mas também interpreta e executa comandos de maneira precisa e eficiente.

3.3.1 Identificação e acesso

O acesso à rede CAN é tipicamente realizado através do conector de diagnóstico do veículo. Instrumentos como osciloscópios são utilizados para monitorar a atividade na rede e calcular a sua velocidade.

3.3.2 Captura de dados

Utilizando equipamentos especializados, como o *hardware* VN1630 log e o *software* CANoe, a equipe da Doutor-IE captura as mensagens trocadas entre o *scanner* confiável e a central do motor. Essa captura não só registra as interações mas também prepara o terreno para simulações que ajudarão na interpretação e análise das comunicações.

A captura de dados deve ser executada sob condições controladas, assegurando que o veículo esteja conectado a um carregador de bateria para manter a tensão operacional adequada. Adicionalmente, é essencial que o veículo apresente um funcionamento saudável, a fim de garantir a coerência dos dados.

3.3.3 Análise das comunicações

A análise detalhada dessas comunicações é feita para desvendar os comandos e respostas trocados. Isso envolve decompor cada mensagem para entender os dados transmitidos, como comandos de atuadores, leituras de sensores e outras funções de diagnóstico. Essa etapa é fundamental para entender o que cada byte transmitido representa e como o *scanner* deve interpretar e responder a esses comandos.

3.3.4 Documentação e padronização

Os dados analisados são documentados utilizando o formato ODX, que permite padronizar as informações de diagnóstico de maneira que sejam acessíveis e interoperáveis com diversas ferramentas e sistemas. A documentação detalhada inclui a funcionalidade de cada comando e resposta, garantindo que o *scanner* da Doutor-IE possa replicar essas funcionalidades com precisão.

3.4 PESQUISA DA REDE DE COMUNICAÇÃO

A metodologia de pesquisa da rede de comunicação do veículo é uma componente crítica no processo de engenharia reversa, fornecendo a fundação necessária para uma coleta de dados acurada e para uma análise meticulosa dos sistemas de comunicação automotiva. No âmbito deste estudo, a pesquisa compreendeu várias etapas fundamentais: a localização precisa do conector de diagnóstico, a análise do diagrama elétrico da rede, a verificação da presença de um *security gateway*, e a identificação do protocolo de comunicação empregado no veículo. Esta estratégia metódica é essencial para assegurar a eficácia e a precisão da engenharia reversa.

3.4.0.1 Localização do conector de diagnóstico

A fase inicial da pesquisa de campo envolveu a determinação precisa da localização do conector de diagnóstico do veículo. Por meio da utilização da Plataforma Doutor-IE, que é uma base de dados especializada em informações técnicas automotivas, conseguimos identificar exatamente a posição do conector OBD-II no veículo em análise. A correta localização deste conector é crucial, visto que ele constitui o principal ponto de acesso para a comunicação com as Unidades de Controle Eletrônico (UCEs) e para a subsequente coleta de dados da rede de comunicação.

3.4.1 Análise do diagrama elétrico da rede

Após a localização do conector de diagnóstico, procedeu-se à análise do diagrama elétrico da rede CAN do veículo. Este diagrama proporciona uma visão abrangente das conexões entre as ECUs e os pinos do conector de diagnóstico. Através desta análise, foi possível identificar os pinos associados às linhas CAN High (CAN-H) e CAN Low (CAN-L), informação vital para a seleção adequada dos equipamentos de captura de dados, como o *hardware* VN1630 log da Vector. Esta etapa assegura que todas as comunicações relevantes sejam precisamente registradas.

Adicionalmente, o diagrama elétrico revela componentes críticos de segurança, tais como o *security gateway*. Este dispositivo desempenha um papel fundamental na proteção da rede interna do veículo contra acessos não autorizados e ataques cibernéticos, regulando o fluxo de dados entre as redes internas e o conector de diagnóstico. A identificação do *security gateway* é crucial, pois influencia diretamente a metodologia empregada na coleta de dados e nas estratégias de engenharia reversa. Em determinadas situações, torna-se necessário incluir o identificador (Identifier (ID)) do *gateway* no pacote de dados enviado pelo aparelho de diagnóstico para a UCE, garantindo assim a resposta correta da central usando o mesmo ID empacotado na mensagem.

3.4.2 Identificação do protocolo de comunicação

A pesquisa preliminar abrange também a identificação do protocolo de comunicação empregado no veículo, uma informação acessível por meio do diagrama elétrico disponível na Plataforma Doutor-IE. A compreensão exata do protocolo de comunicação, seja CAN, CAN FD, K-Line, FlexRay ou Ethernet Automotiva, é crucial para elaborar um plano eficaz de coleta de dados. Essa identificação é fundamental para a seleção apropriada do hardware de interface de rede compatível, que é utilizado na Doutor-IE. A escolha precisa deste hardware assegura compatibilidade com o protocolo de rede e que os dados sejam capturados de maneira eficiente e precisa, evitando a perda de informações vitais.

3.4.3 Importância da pesquisa na engenharia reversa

A preparação adequada é fundamental na engenharia reversa, pois compreender a arquitetura da rede, a localização dos pontos de acesso e o protocolo de comunicação permite a configuração correta dos equipamentos de captura de dados. Esse entendimento evita erros que poderiam comprometer a integridade dos dados coletados, assegurando a precisão necessária para uma análise eficaz.

A eficiência na coleta de dados é garantida por meio de uma pesquisa básica bem conduzida. Esta abordagem economiza tempo e recursos ao direcionar os esforços para os pontos de interesse mais relevantes. Assim, a coleta de dados torna-se mais direcionada e produtiva, maximizando a qualidade e a quantidade de informações obtidas.

A segurança é outro aspecto crucial abordado pela pesquisa. Verificar a presença de um *security gateway* ajuda a planejar estratégias para lidar com possíveis barreiras de segurança. Isso garante que a coleta de dados não comprometa a segurança do veículo nem viole protocolos de segurança, mantendo a integridade do automóvel.

A metodologia de pesquisa da rede de comunicação desempenha um papel fundamental no sucesso da engenharia reversa de veículos. Ao localizar o conector de diagnóstico, analisar o diagrama elétrico da rede, verificar a presença de um *security gateway* e identificar o protocolo de comunicação utilizado, é possível garantir que a coleta de dados seja realizada de maneira precisa e eficiente. A pesquisa fornece a base necessária para a execução de um processo de engenharia reversa detalhado e rigoroso, contribuindo para a segurança e a eficiência dos dados a serem coletados.

3.5 COLETA DE DADOS

A coleta de dados é uma etapa essencial no processo de engenharia reversa de veículos, permitindo a análise detalhada das comunicações entre a UCE e o aparelho

de diagnóstico. Esta fase envolve a determinação da velocidade da rede, a configuração do hardware de captura e a documentação sistemática dos dados obtidos. A metodologia adotada assegura que todas as informações relevantes sejam registradas com precisão, estabelecendo uma fundação robusta para simulações futuras e análises detalhadas em bancada..

3.5.1 Ferramentas e equipamentos Utilizados

OBD Box: Permite a conexão simultânea do *scanner* automotivo e do *hardware* de coleta de dados.

Dispositivo de coleta de dados VN1630 log da Vector: Captura precisa das comunicações veiculares.

Software CANoe da Vector: Utilizado para a configuração do dispositivo de coleta, análise dos dados capturados e simulação da UCE.

***Scanner* de referência no mercado global:** Esta pesquisa emprega uma ferramenta avançada de diagnóstico veicular, capaz de ler e interpretar códigos de falha, monitorar parâmetros operacionais em tempo real, e executar testes ativos para uma verificação e manutenção eficientes dos sistemas do veículo.

Cabos diversos: Utilizados para conectar e interligar todos os dispositivos, incluindo a OBD Box, o aparelho de diagnóstico automotivo, o dispositivo VN1630 log e o notebook. Estes cabos garantem a transmissão eficiente e confiável de dados entre os componentes, assegurando a integridade e a precisão das informações.

Collection APP: Desenvolvido para documentar e organizar os dados da UCE durante a coleta, facilitando a análise e futura simulação em bancada.

As Figuras 9, 10 e 11 ilustram algumas das ferramentas utilizados.

3.5.2 Conexões

A conexão adequada dos equipamentos ao veículo é o ponto inicial da coleta de dados. Utiliza-se uma OBD Box, permitindo uma conexão em paralelo e simultânea do *scanner* automotivo e do dispositivo de captura de dados VN1630 log. Com isso, o dispositivo consegue interceptar as mensagens trocadas entre o aparelho de diagnóstico e a UCE do motor do veículo de estudo.

A OBD Box é acoplada ao conector de diagnóstico do veículo, estabelecendo a interface inicial para a comunicação. O *scanner* automotivo é então conectado à tomada OBD II da OBD Box, permitindo a interação com a central do motor. Os pinos tipo banana são inseridos nos conectores fêmeas da OBD Box, possibilitando a ligação

Figura 9 – *Hardware* de coleta VN1630 log.

Fonte: Site oficial da Vector.

Figura 10 – *Scanner* de referência.

Fonte: Site oficial da Autel.

Figura 11 – OBD Box.

Fonte: Imagens da internet.

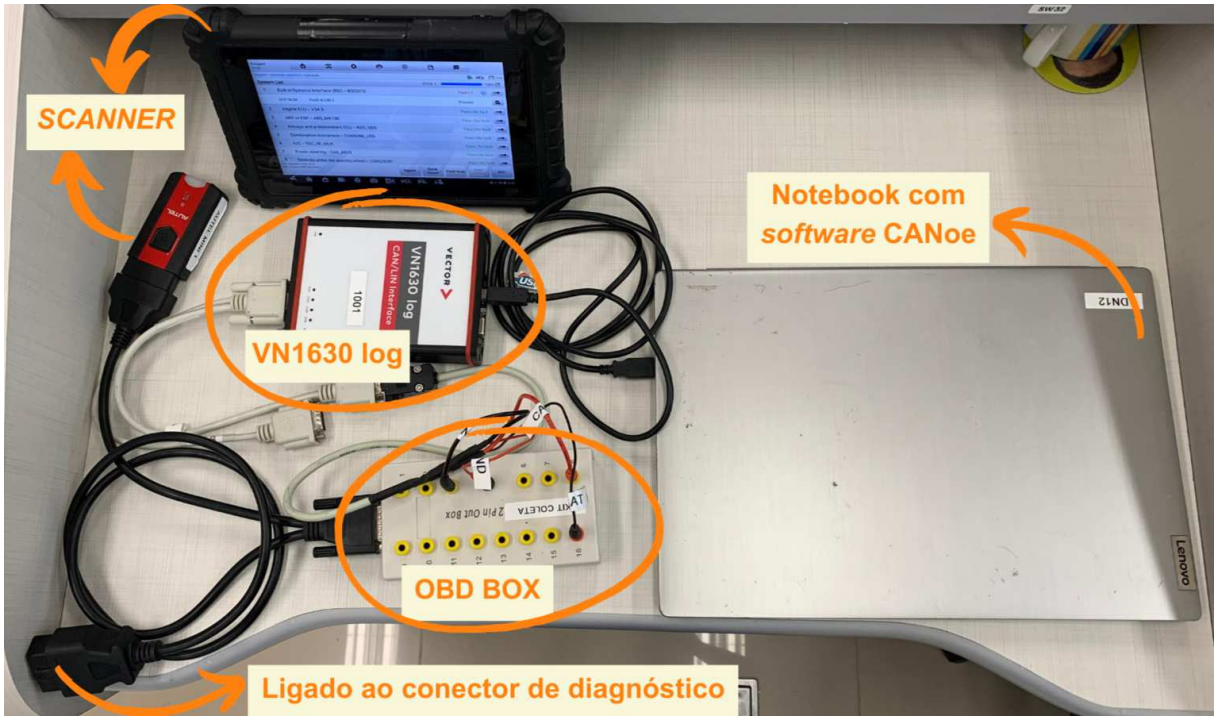
ao *hardware* VN1630 log. Para completar a configuração, um cabo de conexão USB é utilizado para conectar o dispositivo de captura a um notebook, que opera com uma licença do *software* CANoe. Este software é previamente configurado para reconhecer e gerenciar a interação com o *hardware* de coleta, preparando o sistema para a efetiva captura de dados.

A Figura 12 esquematiza em bancada a conexão que será realizada no veículo durante a coleta de dados.

3.5.3 Configuração do VN1630 Log

Com os equipamentos devidamente conectados, a próxima etapa envolve a configuração do *hardware* VN1630 log da Vector, um dispositivo de interface de rede

Figura 12 – Conexões em bancada.



Fonte: O autor.

especializado em capturar e registrar comunicações veiculares. A configuração inicia-se com a ligação dos cabos a OBD Box que por sua vez já está conectado ao conector de diagnóstico do veículo, assegurando a conexão correta aos pinos CAN High (CAN-H) e CAN Low (CAN-L).

No software CANoe, o hardware VN1630 log é configurado para a captura dos dados da rede CAN. Isso inclui a escolha do canal correto do VN1630 log e a especificação dos parâmetros de captura, como filtros de mensagem para focar em IDs específicos e minimizar a quantidade de dados irrelevantes. A configuração detalhada do software é crucial para garantir que todos os dados relevantes sejam capturados com precisão.

3.5.4 Determinação da velocidade da rede

Com a configuração do dispositivo de captura de dados realizada, a próxima etapa envolve determinar a velocidade da rede CAN, uma variável crucial para a configuração apropriada do hardware de captura. Esta determinação pode ser realizada por meio de um osciloscópio, que permite a medição direta dos sinais elétricos na rede e a identificação da taxa de transmissão através da análise dos tempos de subida e descida dos pulsos. Alternativamente, o software de análise de dados CANoe pode ser configurado para detectar automaticamente as velocidades padrão amplamente

utilizadas na indústria automotiva, tais como 125 kbps, 250 kbps, 500 kbps e 1 Mbps.

3.5.5 Documentação da coleta

A documentação meticulosa dos dados coletados é efetuada utilizando um programa em Python que desenvolvi especificamente para esta finalidade. Este *software* desempenha um papel crucial no registro das informações vitais das UCEs, compilando-as em um único arquivo de texto. Este arquivo contém todos os dados essenciais das centrais coletadas e serve como uma ferramenta valiosa para a documentação precisa dos dados de cada central durante a documentação dos dados analisados no ODX. O arquivo de texto resultante é essencial para os processos subsequentes de análise e revisão. A documentação produzida inclui:

Nome da UCE: Identificação da unidade de controle eletrônico para referência futura.

Pinos utilizados no conector de diagnóstico: Registro dos pinos específicos utilizados para a comunicação com o veículo.

IDs de *request* e *response*: Identificação dos IDs de *request* (aparelho de diagnóstico) e de *response* (UCE do veículo), que são cruciais para decodificar as mensagens CAN.

Velocidade da rede: Registro da velocidade de comunicação da rede, essencial para a configuração de futuros testes e simulações.

ID do Gateway: Identificação do ID do security gateway, se presente, para entender sua influência na comunicação.

Quantidade de bytes de header: No caso de comunicações via protocolo K-Line, a documentação inclui a quantidade de bytes de header. Para esse projeto não será utilizado.

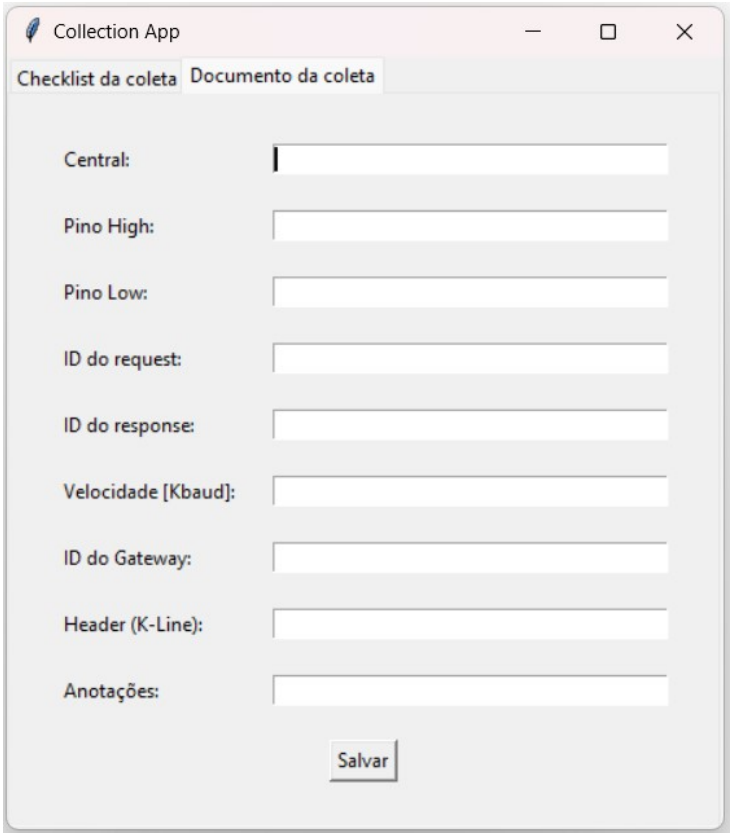
Campo de anotações gerais: Espaço para registrar possíveis peculiaridades ou falhas observadas durante a coleta de dados, fornecendo contexto adicional para a análise.

A Figura 13 ilustra a interface do documento da coleta desenvolvido e utilizado.

3.6 ANÁLISE

Para a análise e simulação dos dados coletados, as mesmas conexões estabelecidas durante a fase de coleta de dados no veículo serão utilizadas. Contudo, em vez de conectar a OBD Box diretamente ao conector de diagnóstico do veículo, esta configuração será emulada em bancada, utilizando uma fonte de 12V para simular a

Figura 13 – ColectionApp: programa para documentar as ECUs na coleta de dados.



Fonte: O autor.

alimentação do conector de diagnóstico. A fase de pré-análise constitui um momento crítico no desenvolvimento do projeto, oferecendo uma avaliação inicial dos dados coletados. Este estágio preliminar é essencial para identificar desafios e peculiaridades que possam surgir, preparando o terreno para uma análise mais profunda e uma documentação detalhada subsequente.

3.6.1 Pré-análise

A pré-análise dos dados coletados constitui uma fase crucial na engenharia reversa veicular, assegurando a integridade e a relevância das informações obtidas. O processo começa com a visualização dos logs de dados, que foram coletados durante a pesquisa de campo, utilizando ferramentas de análise especializadas como o CANalyzer ou o CANoe, ambos da empresa Vector.

Inicialmente, realiza-se uma inspeção visual dos logs para identificar quaisquer problemas evidentes, tais como a presença de dados ausentes ou corrompidos, e para verificar se os dados estão em conformidade com as expectativas estabelecidas. Esta etapa é fundamental para garantir que os dados registrados sejam adequados para análises mais detalhadas.

Durante a identificação dos identificadores de mensagem, os IDs presentes nos logs são catalogados e analisados para determinar quais dispositivos estão se comunicando na rede. A identificação correta dos IDs, tanto do aparelho de diagnóstico automotivo quanto das UCEs envolvidas, é essencial para decifrar a estrutura da comunicação veicular.

Posteriormente, procede-se à pré-análise dos serviços de diagnóstico empregados durante as comunicações, que incluem a leitura de parâmetros, realização de testes em atuadores, e execução de rotinas diagnosticas. Esta análise preliminar verifica a conformidade dos serviços com os padrões, assegurando que as comunicações estejam aderindo às normas definidas (KWP ou UDS).

3.6.2 Conversão dos logs para CAPL

O processo de análise inicia com a conversão dos logs de dados coletados, empregando o programa ScannerWorkspace, desenvolvido por João Rafael Caye, colega de trabalho e graduação, como parte de seu projeto de conclusão no semestre de 2023.2. Este programa transforma os logs no formato BLF (extensão proprietária da Vector) em *scripts* na linguagem CAPL (*CAN Access Programming Language*). O ScannerWorkspace facilita a geração automática de *scripts* que permitem uma análise detalhada ao nível de bit das UCEs documentadas, e também possibilita a emulação das centrais coletadas replicando todas as respostas originais do veículo. Esta funcionalidade é crucial para eliminar erros humanos na transcrição manual dos dados para simulação e análise.

Para detalhes adicionais sobre o desenvolvimento e as aplicações deste projeto, é recomendável consultar a monografia intitulada "Geração automática de arquivos para simulação em bancada de mensagens de diagnósticos veiculares adquiridas da rede CAN", que foi orientada pelo professor Carlos Barros Montez. Este trabalho descreve como o programa ScannerWorkspace não apenas aumenta a eficácia e precisão na simulação das UCEs, mas também melhora significativamente a produtividade do desenvolvedor ao facilitar uma análise detalhada.

3.6.3 Configuração do CANoe

Com os arquivos CAPL gerados, o *software* CANoe é configurado para simular as centrais eletrônicas. Esta simulação reproduz o comportamento do veículo, facilitando a interação do *scanner* com o CANoe como se estivesse diretamente conectado ao veículo real.

A simulação é iniciada entrando com o aparelho de diagnóstico na aplicação específica do veículo coletado, preferencialmente utilizando o VIN do carro para evitar erros de seleção. O *scanner* então interage com a simulação do veículo através do CANoe, replicando as mesmas respostas obtidas do veículo durante a coleta de dados.

Durante a simulação, todas as funções disponíveis no módulo são testadas como se estivessem sendo operadas de fato no veículo real. Nesta fase, cada bit das mensagens de resposta da simulação é meticulosamente variado em tempo real, permitindo a decodificação e documentação do conteúdo de cada PID, testes de atuadores, rotinas, e funções especiais do veículo, tais como escrita de dados, telecodificação, e ajustes nos sistemas ADAS, entre outros.

Essa variação minuciosa dos bits nas respostas da simulação é crucial para identificar como cada bit influencia a visualização no aparelho de diagnóstico, determinando se um byte representa texto ou uma variação linear de algum parâmetro, exemplificado de 0% (0x00) a 100% (0x255). Entender o papel de cada bit nas respostas permite documentar adequadamente como o aparelho de diagnóstico em desenvolvimento deve processar esses dados, garantindo a replicação exata das consultas realizadas pelo *scanner* durante a fase de coleta de dados.

3.6.4 Documentação

A documentação dos dados coletados, realizada simultaneamente à análise, segue um formato padronizado conhecido como ODX (*Open Diagnostic Data Exchange*). Este padrão é amplamente adotado por fabricantes de veículos e desenvolvedores de dispositivos de diagnóstico automotivo devido à sua eficácia na garantia de uniformidade e interoperabilidade. Para este projeto específico, os dados serão meticulosamente documentados utilizando a versão do ODX desenvolvida por Rene Engels, que adapta este padrão internacional às necessidades específicas de nossa aplicação, assegurando uma integração e análise de dados precisas e eficientes.

O ODX é uma metodologia padrão de documentação para a indústria automotiva, essencial para a padronização das comunicações de diagnóstico entre veículos e ferramentas de diagnóstico. A adoção do ODX por fabricantes de veículos e empresas de desenvolvimento de dispositivos de diagnóstico automotivo reflete sua eficácia em criar uma base comum para o intercâmbio de informações diagnósticas.

A documentação abrangente inclui a descrição minuciosa de todos os parâmetros e mensagens capturadas, detalhando elementos como o nome da UCE, os pinos de conexão no conector de diagnóstico, os identificadores de mensagens (IDs) para requisição e resposta, a velocidade da rede e a identificação quando há um *gateway* presente. Adicionalmente, são documentadas as especificidades de comunicação, como o número de bytes no cabeçalho de mensagens em protocolos específicos, como o K-Line.

Essa metodologia sistemática de documentação garante que todas as informações essenciais sejam organizadas e registradas detalhadamente, facilitando simulações em bancada e análises futuras. A abordagem padronizada assegura que os dados coletados sejam compreensíveis e diretamente aplicáveis ao desenvolvimento

contínuo e à manutenção de sistemas veiculares, promovendo uma integração eficiente e uma operação segura e confiável dos sistemas automotivos.

4 DESENVOLVIMENTO

4.1 ENGENHARIA REVERSA

A engenharia reversa é um processo crítico no contexto deste projeto, pois envolve a análise detalhada e a compreensão dos sistemas de comunicação entre a central eletrônica do motor do veículo e os dispositivos de diagnóstico. O objetivo é decodificar as mensagens trocadas e entender os protocolos de comunicação empregados. Este subcapítulo descreve as etapas, métodos e ferramentas utilizadas na execução da engenharia reversa, abordando desde a pesquisa preliminar até a análise das informações obtidas.

4.1.1 Pesquisa

O desenvolvimento do projeto inicia-se com a pesquisa preliminar, essencial para garantir uma abordagem meticulosa e eficiente na engenharia reversa. A primeira etapa consiste em localizar o conector de diagnóstico do veículo. Utilizando a Plataforma Doutor-IE, identificamos a posição exata do conector, como mostra a Figura 14, que é crucial para a conexão dos equipamentos de coleta de dados.

Posteriormente, analisa-se o diagrama elétrico do veículo para ter uma noção do protocolo de comunicação utilizado, que no caso do Peugeot 208 I [2015] 1.5 8V Flex 89-93cv (TU4-YFY) VALEO V34.5 é a rede CAN. Esta análise do diagrama elétrico também envolve a identificação dos pinos do conector de diagnóstico aos quais as centrais estão conectadas, garantindo que todos os pontos de comunicação sejam conhecidos. Além disso, verificamos a arquitetura da rede para identificar a presença de um *secutity gateway*, que pode influenciar na metodologia de coleta de dados.

A Figura 15 ilustra o diagrama elétrico do veículo, o qual podemos observar a rede CAN conectada aos pinos 6 (CAN High) e 14 (CAN Low), e 3 (CAN High) e 8 (CAN Low) do conector de diagnóstico. Também podemos notar que a UCE da BSI atua como um segregador da rede, semelhante ao *secutity gateway*, isolando as redes internas da rede de diagnóstico, além de possivelmente monitorar o tráfego de mensagens. A UCE da BSI não possui um ID de *Gateway*.

4.1.2 Coleta de dados

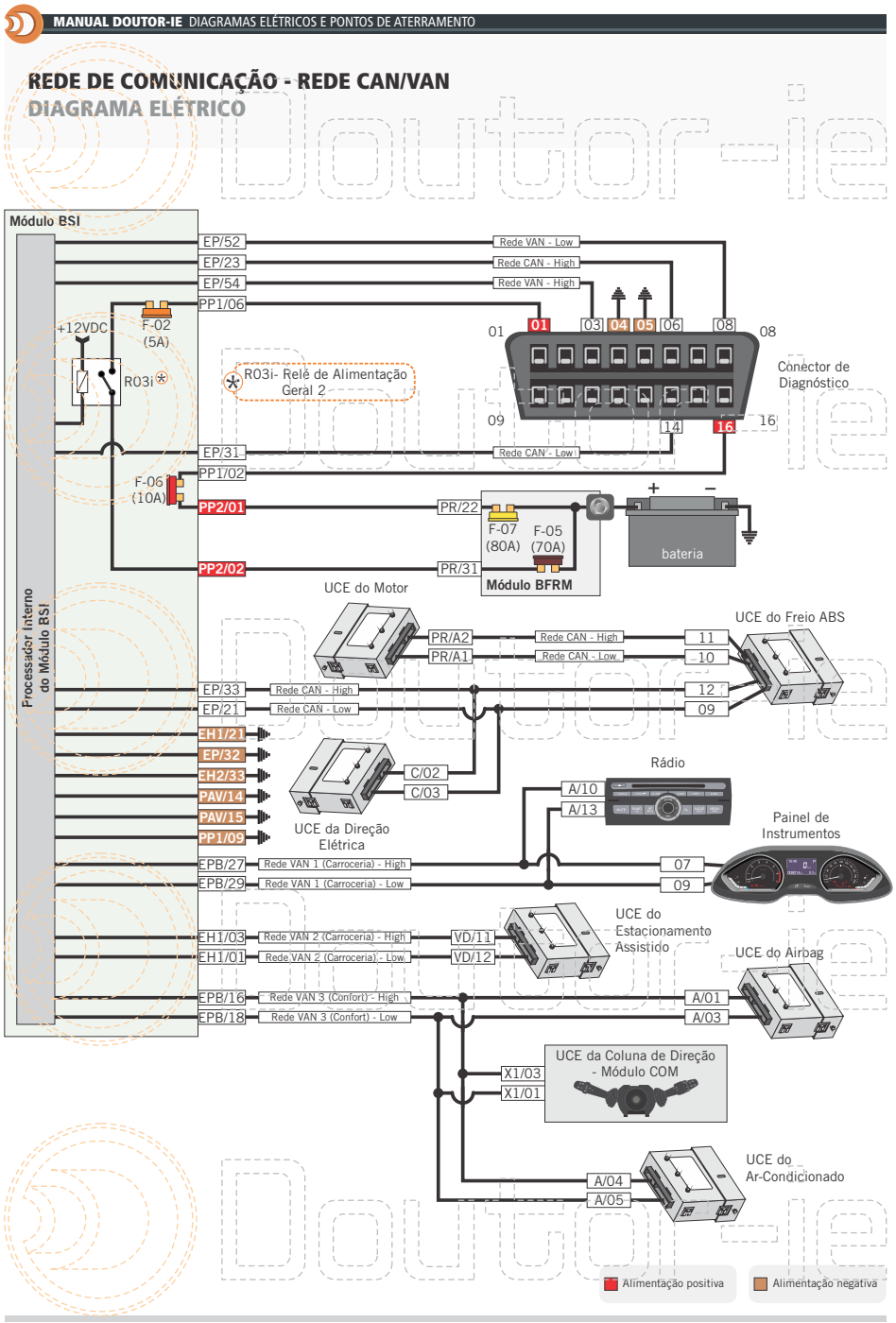
A coleta de dados consiste na interceptação das mensagens trocadas entre a UCE do motor do veículo e o *scanner* automotivo. Para isso, utilizou-se o *software* CANoe e o *hardware* VN1630 log da empresa Vector, que são ferramentas robustas e amplamente reconhecidas no setor automotivo para a análise de redes de comunicação veiculares.

Figura 14 – Localização do conector de diagnóstico.

Fonte: Plataforma Doutor-IE.

A conexão de cabos no processo de coleta de dados começa com a ligação da OBD Box ao conector de diagnóstico do veículo. Em seguida, o aparelho de diagnóstico

Figura 15 – Diagrama elétrico da rede de comunicação.



Fonte: Plataforma Doutor-IE.

automotivo é plugado na ponta da OBD Box, permitindo a comunicação direta com a central do motor. Os pinos banana são inseridos nos terminais fêmeas da OBD Box,

conectando-se ao dispositivo VN1630 log. Finalmente, um cabo de interface liga o dispositivo de captura a um notebook, onde o CANoe está configurado para capturar os dados de comunicação veicular em tempo real. Esta configuração garante uma captura precisa e completa das mensagens trocadas na rede CAN do veículo. A Figura 16 ilustra como é feita a ligação dos equipamentos no veículo, enquanto que através da Figura 12, disposta no capítulo anterior, possui a descrição da ligação realizada. E então, chave do veículo é colocada na posição de linha 15, estágio de acessórios do comutador de ignição, para alimentar a tomada de diagnóstico.

Figura 16 – *Setup* de coleta plugado no veículo.

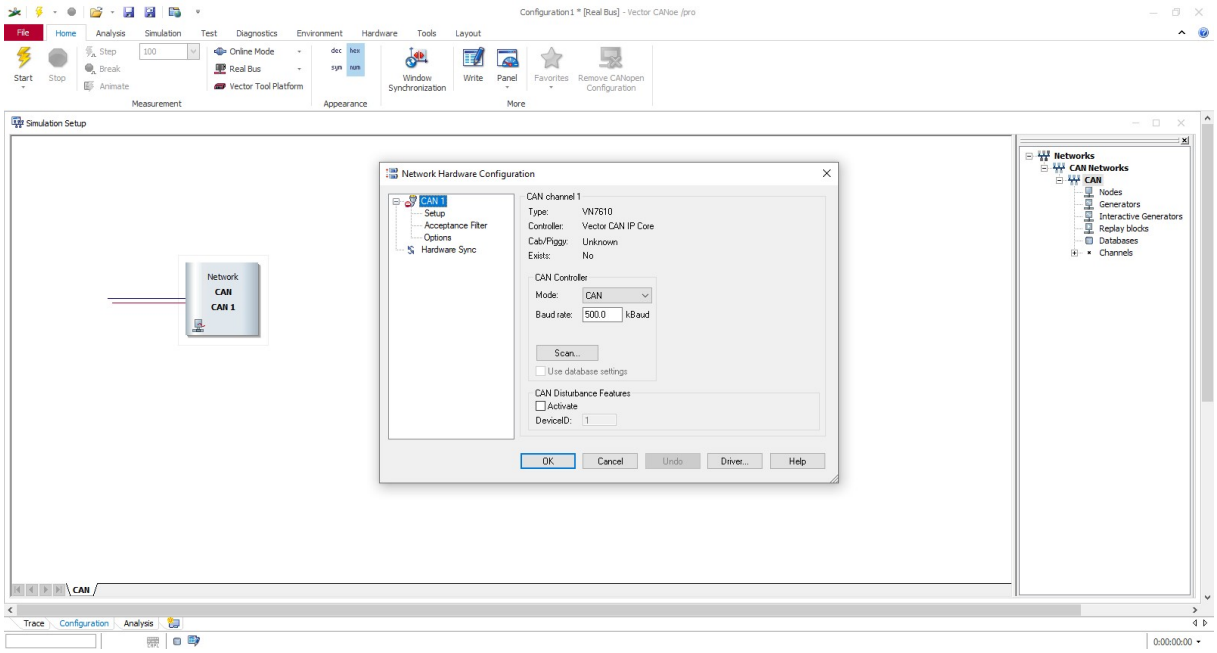
Fonte: O autor.

Para assegurar a integridade do veículo, é gravado a tela do aparelho de diagnóstico sincronizada com a gravação do log da rede. Este procedimento permite identificar eventuais problemas de configuração ou exclusão de informações importantes durante a coleta de dados com o *scanner*. Foi escolhido um *scanner* de referência no mercado global, ilustrado pela Figura 10, que possui um disparo de mensagens similar ao do *scanner* padrão original da fabricante do veículo. Este aparelho de diagnóstico foi escolhido por sua capacidade de interpretação precisa dos dados e por

possuir uma interface amigável.

Durante a fase de coleta de dados, é estabelecida uma pasta dedicada no notebook para armazenar os arquivos de log gerados durante o a coleta do veículo. Simultaneamente, o CANoe é configurado especificamente para a coleta, ajustando-se para corresponder à velocidade da rede e ao canal utilizado pelo dispositivo de captura de dados VN1630 log. Para este projeto, utilizando o Peugeot 208 como referência, o CANoe é capaz de identificar automaticamente a velocidade da rede, que é tipicamente 500 kBaud, eliminando a necessidade de medição manual com osciloscópio.

Figura 17 – Detecção automática da rede de 500 kBaud.



Fonte: CANoe.

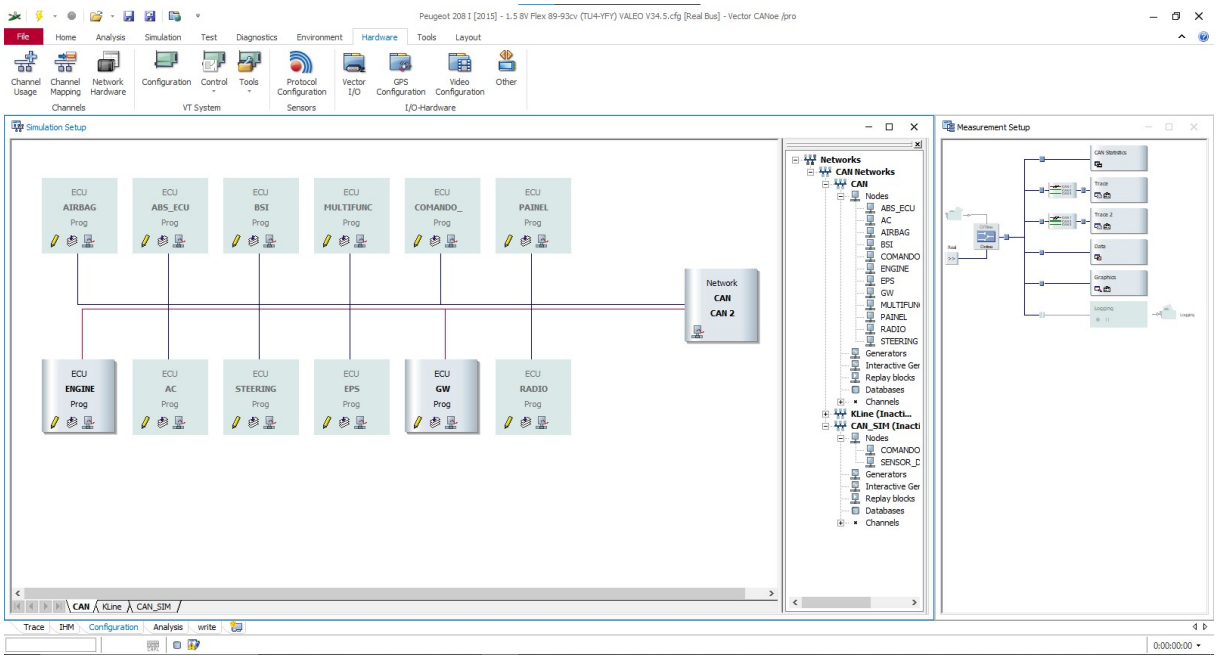
O dispositivo VN1630 log intercepta as mensagens trocadas entre o *scanner* e a UCE do motor. Simultaneamente, utilizamos o CollectionAPP, desenvolvido em Python, para gerar um documento de texto estruturado contendo informações cruciais como IDs de *request* e *response*, pinos utilizados no conector de diagnóstico, velocidade da rede, e observações relevantes. Esta documentação inicial é vital para a precisão da análise subsequente.

4.1.3 Análise da UCE do motor

Com os dados capturados, a próxima etapa é a análise dos protocolos de comunicação empregados pela UCE do motor do Peugeot 208 I 2015 através de uma simulação das redes de comunicação do veículo. Esta análise é fundamental para identificar os padrões de mensagens e os serviços de diagnóstico utilizados.

Nessa etapa o CANoe é configurado com os arquivos CAPL gerados e com o canal utilizado pelo VN1630 log para comunicação com o aparelho de diagnóstico. A arquitetura da rede é montada na simulação, com cada bloco representando uma UCE do veículo. A Figura 18 ilustra as UCEs que o veículo possui e que futuramente serão desenvolvidas utilizando o mesmo princípio da UCE do motor.

Figura 18 – UCEs presentes no veículo em desenvolvimento.



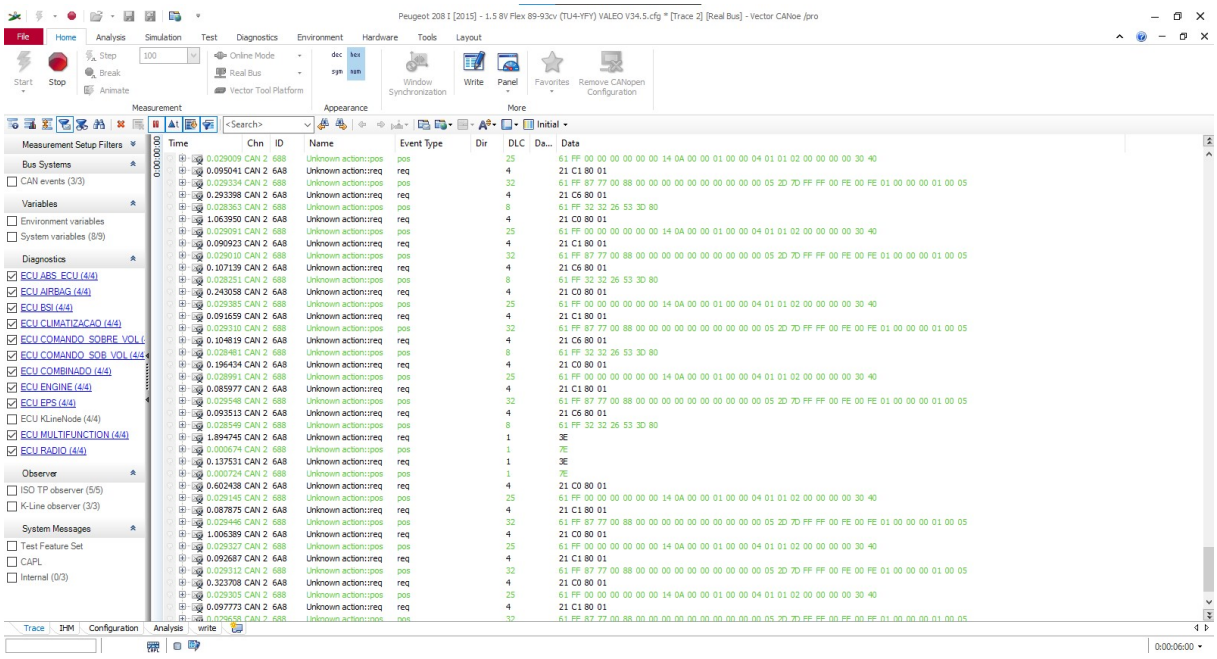
Fonte: CANoe.

Iniciamos então a comunicação do *scanner* com a simulação, e todas as mensagens trocadas são exibidas na janela *Trace* do CANoe, conforme ilustrado na Figura 19. Essa análise detalhada é acompanhada por uma documentação meticulosa.

A análise das mensagens CAN capturadas envolveu a decodificação dos identificadores (IDs) das centrais presentes na rede e dos dados contidos nas mensagens. Essa análise permitiu a identificação de serviços de diagnóstico específicos, incluindo leitura de dados, limpeza de códigos de falha e escrita de valores de parâmetros que são específicos do protocolo de comunicação KWP (*Keyword Protocol 2000*). Durante a fase de análise, o *scanner* interage com a simulação que responde como se fosse o próprio veículo, permitindo testar todas as funções presentes no módulo do motor em tempo real. Para entender detalhadamente o significado de cada bit das mensagens, variamos sistematicamente cada bit, documentando os resultados.

Essa abordagem detalhada permite identificar claramente as funções e os comportamentos esperados dos parâmetros veiculares. Esse processo é fundamental para a futura implementação no *scanner* da Doutor-IE, garantindo que a ferramenta seja

Figura 19 – Troca de mensagens do *scanner* com a emulação da UCE do motor.



Fonte: CANoe.

capaz de interpretar corretamente as mensagens de diagnóstico e oferecer funcionalidades avançadas aos reparadores automotivos.

4.2 DOCUMENTAÇÃO DOS DADOS COLETADOS

A documentação dos dados coletados é uma etapa crucial no processo de engenharia reversa da comunicação em redes automotivas. Esta seção detalha os procedimentos adotados para registrar, organizar e interpretar os dados obtidos durante a fase de coleta. A precisão e a organização meticulosa desses dados são fundamentais para assegurar que os resultados sejam reproduzíveis e que o conhecimento gerado possa ser utilizado de maneira eficaz no *scanner* da Doutor-IE.

4.2.1 Cadastro dos dados utilizando o ODX

ODX (*Open Diagnostic Data Exchange*) é um formato de arquivo padronizado, definido pela norma ISO 22901, utilizado para descrever dados de diagnóstico de veículos. Ele permite a troca estruturada de informações de diagnóstico entre diferentes sistemas e ferramentas automotivas, facilitando a interoperabilidade e a consistência na comunicação.

O principal objetivo do ODX é fornecer uma linguagem comum para descrever serviços de diagnóstico, parâmetros, e mensagens de comunicação entre as unidades de controle eletrônico e as ferramentas de diagnóstico. O ODX possibilita que enge-

nheiros e técnicos definam, compartilhem e utilizem dados de diagnóstico de forma eficiente e precisa, independentemente do fabricante do veículo.

Devido à complexidade intrínseca à estrutura da documentação das centrais no ODX, uma descrição textual completa e compreensível se torna impraticável. A documentação no ODX incorpora uma gama abrangente de elementos técnicos e estruturais, cuja compreensão detalhada exige uma análise profunda. Para uma exploração completa, recomenda-se a consulta aos documentos detalhados disponibilizados no apêndice sigiloso.

O ODX utilizado neste projeto foi inicialmente desenvolvido pelo supervisor, Rene Engels. Originalmente concebido em *Visual Basic for Applications* (VBA), o ODX da Doutor-IE está atualmente em processo de migração para uma nova implementação desenvolvida em Flutter. Este avanço reflete a busca contínua por soluções mais robustas e adaptáveis dentro do contexto de engenharia da Doutor-IE.

4.2.2 Estrutura da mensagem na rede CAN

Para entender a estrutura do campo *Data* das mensagens CAN conforme ilustrado pela Figura 4, vamos detalhar a sequência utilizada:

ID das centrais (*Identifier*): Cada mensagem CAN inclui um identificador que representa quem está enviando. Existem dois tamanhos de identificadores, sendo que para a central de estudo temos um ID de 11 bits.

Tamanho da mensagem: O campo *Data* contém o código de comprimento dos dados (DLC), que informa o tamanho dos dados sendo transferidos. O campo de dados contém até 8 bytes, ou seja, cada pacote de mensagem transmite até 8 bytes de dados.

SID (*Service Identifier*): Este byte é o primeiro no campo de dados e identifica o serviço que está sendo solicitado. Por exemplo, no serviço "StartCommunication"do KWP, o SID é 0x81.

PID (*Parameter Identifier*): O identificador do parâmetro específico que está sendo solicitado ou ajustado. Este valor define qual parâmetro está sendo solicitada dentro do serviço definido pelo SID.

Dados: Dependendo do serviço e do PID, podem ser incluídos dados adicionais que especificam valores, condições ou resultados associados à solicitação.

No protocolo de comunicação, a indicação de que uma mensagem constitui uma resposta a uma solicitação é feita através de uma convenção no campo SID. Especificamente, ao valor original do SID na solicitação é adicionado o deslocamento hexadecimal de 0x40 para formar o SID da resposta correspondente. Por exemplo, se

um SID na solicitação é 0x21, então o SID na resposta correspondente será ajustado para 0x61.

4.2.3 Categorias e classes dos serviços de diagnóstico

As categorias e classes foram estabelecidas para organizar e facilitar a interpretação dos diversos serviços de diagnóstico e controle. A seguir, cada categoria utilizada na documentação e suas classes associadas são detalhadas:

Categoria localParameter: Classes *read* e ECU ID são utilizadas para leitura de parâmetros locais específicos e identificação da UCE, respectivamente.

Categoria testerPresent: A classe *start* representa o vínculo da comunicação entre o dispositivo de diagnóstico e a UCE, mantendo-se ativa ao longo de toda a sessão de diagnóstico.

Categoria inputOutput: Classe *control* inicia o processo, *reset* para o processo e *return* monitora as etapas do processo. Envolve o controle de entradas e saídas da UCE, incluindo testes de atuadores.

Categoria ecuReset: Classe *reset* permite o reinício da UCE, limpando falhas temporárias e reiniciando parâmetros.

Categoria routineControl: Classe *start* inicia o processo, *requestResults* monitora as etapas do processo e *stop* para o processo. Controle de rotinas específicas de diagnóstico e manutenção.

Categoria requestDownloaded: Classe *requestDownloaded*, utilizada para iniciar transferências de dados para a UCE, como downloads de software.

Categoria init: Classe *start*, inicia a comunicação de diagnóstico.

Categoria end Classe *start*, encerra a comunicação de diagnóstico.

Categoria dtcs Classes *read* e *clear*. Leitura e limpeza de códigos de falha (DTCs), respectivamente.

Categoria securityAccess Classes *seed* e *key*. Garantia de acesso seguro a funções protegidas da UCE, exigindo autenticação através de uma espécie de chave e fechadura.

4.2.4 Exemplo da documentação de um PID de leitura de parâmetros

Com base na Figura 19, podemos exemplificar a documentação referente ao PID de leitura de parâmetros 0xC0. Por se tratar de uma leitura, utiliza o SID (*Service*

ID) 0x21. Na figura também está evidente os IDs de 11 bits de *request* (*scanner*) e *response* (UCE do motor), 0x6A8 e 0x688 respectivamente. Também, pela figura, é possível notar o campo DLC da estrutura de mensagem CAN, indicando o tamanho total da mensagem, sendo o *request* de 4 bytes e o *response* de 25 bytes.

O PID a ser documentado possui categoria *localParameter* e classe *read*, para leitura de parâmetros locais. Importante salientar que toda a troca de mensagens ocorre em formato hexadecimal.

Segue a subestrutura do campo *Data* na mensagem CAN:

Tabela 3 – Categoria localParameters e classe read.

	SID	**PID**	**Data**
Request (0x6A8)	0x21	0xC0	0x8001
Response (0x688)	0x61	0xFF	zz

Fonte: O autor.

Na documentação, o campo zz significa um *proxy data*, que é relacionado aos dados coletados e servindo para emular os parâmetros entre UCE do veículo e *scanner* para propósitos de teste e análise dos bits. O valor 0x8001 no *request* é constante, mantendo-se inalterado em diferentes operações. O nome dos parâmetros é determinado pelo aparelho de diagnóstico.

A estrutura detalhada de *proxy data* é analisada e documentada como segue:

***Byte position* 0: Regime motor -** Tamanho de 2 bytes, fator 0,125 e *ofsset* 0; valores lineares de 0x0000 (0 RPM) até 0xFFF7 (8190,875 RPM).

***Byte position* 2: Velocidade do veículo -** Tamanho de 1 byte, fator 1 e *ofsset* 0; valores lineares de 0x00 (0 km/h) até 0xFF (255 km/h).

***Byte position* 3: Estado do interruptor primário do freio -** Tamanho de 1 byte. *Text table*: 0x00 - Liberado; 0x01 - Pressionado;

***Byte position* 4: Estado do interruptor secundário do freio -** Tamanho de 1 byte. *Text table*: 0x00 - Liberado; 0x01 - Pressionado;

***Byte position* 5: Posição do pedal da embreagem -** Tamanho de 1 byte. *Text table*: 0x00 - Liberado; 0x01 - Pressionado;

***Byte position* 6: Pista 1ª do sensor de posição do pedal do acelerador -** Tamanho de 1 byte, fator 19,529411764705882 e *ofsset* 0; valores lineares de 0x00 (0 mV) até 0xFF (4980 mV).

***Byte position* 7: Pista 2ª do sensor de posição do pedal do acelerador -** Tamanho de 1 byte, fator 19,529411764705882 e *ofsset* 0; valores lineares de 0x00 (0 mV) até 0xFF (4980 mV).

***Byte position* 8: Posição do pedal do acelerador -** Tamanho de 1 byte, fator 0,39 e *ofsset* 0; valores lineares de 0x00 (0 %) até 0xFF (100 %).

***Byte position* 9: Informações do sensor de ponto duro do pedal do acelerador -** Tamanho de 1 byte. *Text table*: 0x00 - Liberado; 0x01 - Pressionado;

***Byte position* 10: Posição de marcha -** Tamanho de 1 byte. *Text table*: 0x00 - R; 0x01 - N; 0x02 - 1; 0x03 - 2; 0x04 - 3; 0x05 - 4; 0x06 - 5; 0x07 - 6;

***Byte position* 11: Configuração da transmissão na memória da ECU -** Tamanho de 1 byte. *Text table*: 0x00 - Transmissão manual longa ou curta; 0x01 - Transmissão manual; 0x02 - Transmissão automática;

***Byte position* 12: *Status* do imobilizador do motor codificado -** Tamanho de 1 byte. *Text table*: 0x00 - Imobilizador desativado; 0x01 - Imobilizador eletrônico bloqueado;

***Byte position* 13: Estado de despertar da ECU -** Tamanho de 1 byte. *Text table*: 0x01 - Acionamento parcial; 0x02 - Despertar parcialmente interno; 0x03 - Estado transitório; 0x04 - Acionamento principal; 0x05 - Despertar principal rebaixado; 0x06 - Inicializar/mudar para o modo dormente;

***Byte position* 14: Estado do motor -** Tamanho de 1 byte. *Text table*: 0x00 - Em preparação; 0x01 - corte/parado; 0x02 - Partida acionada; 0x03 - Partida autônoma; 0x04 - Motor funcionando; 0x05 - Desligado; 0x06 - Reinicialização acionada; 0x07 - Reinicialização autônoma;

***Byte position* 15: Reservado -** Tamanho de 1 byte.

***Byte position* 16: Operação do motor -** Tamanho de 1 byte. *Text table*: 0x00 - Em marcha lenta; 0x01 - Falha de injeção; 0x02 - Pedal pressionado; 0x03 - Velocidade excessiva do motor;

***Byte position* 17: Estado do controle de cruzeiro -** Tamanho de 1 byte. *Text table*: 0x00 - Inativo; 0x01 - Ativo;

***Byte position* 18: Velocidade de referência do controle de cruzeiro -** Tamanho de 1 byte, fator 1 e *ofsset* 0; valores lineares de 0x00 (0 km/h) até 0xFF (255 km/h).

***Byte position* 19: Estado do limitador de velocidade -** Tamanho de 1 byte. *Text table*: 0x00 - Inativo; 0x01 - Ativo;

***Byte position* 20: Velocidade de referência do limitador de velocidade -** Tamanho de 1 byte, fator 1 e *ofsset* 0; valores lineares de 0x00 (0 km/h) até 0xFF (255 km/h).

***Byte position* 21: Velocidade de referência do motor em marcha lenta -** Tamanho de 1 byte, fator 16 e *ofsset* 0; valores lineares de 0x00 (0 RPM) até 0xFF (4080 RPM).

***Byte position* 22: Pocentagem de álcool -** Tamanho de 1 byte, fator 0,39 e *ofsset* 0; valores lineares de 0x00 (0 %) até 0xFF (100 %).

Esta documentação metódica no ODX permite uma representação estruturada e detalhada do PID 0xC0, crucial para aplicações de diagnóstico. A natureza livre de documentação sem padrões estabelecidos pode introduzir incertezas, especialmente quando variáveis não padronizadas são envolvidas. Portanto, a utilização do ODX é fundamental para garantir consistência e precisão na documentação dos parâmetros de diagnóstico.

4.3 VALIDAÇÃO E RESULTADOS

A validação da metodologia de engenharia reversa empregada neste projeto foi conduzida através de uma abordagem meticulosa que incluiu a simulação da central do motor e a revisão por pares realizada por outro especialista da Doutor-IE. A simulação da central do motor foi crucial para confirmar a precisão dos dados documentados, permitindo uma avaliação detalhada da integridade e da aplicabilidade das informações coletadas durante a fase de engenharia reversa.

4.3.1 Simulação da central do motor

A central do motor foi emulada utilizando o *software* CANoe, que permitiu a reprodução das condições reais de operação do veículo. Esta simulação possibilitou a verificação dos parâmetros e das funcionalidades descritas nos documentos de engenharia reversa, garantindo que as informações documentadas refletissem de maneira precisa e fiel as operações da UCE.

4.3.2 Revisão por outro especialista

A revisão dos dados e da metodologia foi realizada por um especialista em engenharia automotiva que também é membro da equipe da Doutor-IE. Esta revisão por pares teve como objetivo identificar potenciais inconsistências ou erros nos dados documentados, aumentando a confiabilidade dos resultados da engenharia reversa. A expertise complementar do revisor assegurou uma análise crítica e aprofundada, essencial para a validação final do projeto. Durante essa revisão, foi constatado que não houve erros na documentação, o que reforça a precisão e a qualidade do trabalho realizado. Além disso, a estrutura robusta de pesquisa, coleta e análise, aliada à

simulação, acelerou significativamente o processo de desenvolvimento das centrais veiculares.

4.3.3 Injeção de mensagens na rede

Complementarmente, a eficácia do método utilizado foi testada através da injeção de mensagens selecionadas na rede CAN do veículo. Essa etapa permitiu avaliar a resposta da central do motor às mensagens sintetizadas, verificando se os comportamentos observados durante a simulação correspondiam às expectativas baseadas nos dados coletados. A capacidade de injetar mensagens e observar as respostas reais proporcionou uma validação prática e convincente da funcionalidade e da precisão dos procedimentos de engenharia reversa.

A injeção de mensagens foi realizada utilizando a linguagem de programação Python, através de um hardware ELM327 com comandos AT. Com base na documentação realizada, foi possível utilizar esse padrão para enviar as mensagens a uma nova central de motor de outro veículo que respondeu na mesma estrutura, porém com dados diferentes, o que era de se imaginar.

Essas etapas de validação confirmaram não apenas a acurácia dos dados coletados e documentados, mas também a robustez da metodologia de engenharia reversa adotada. O processo detalhado de simulação, revisão por um especialista e teste direto na rede CAN assegurou que a abordagem utilizada fosse tanto verificável quanto eficaz, fundamentando a confiança na aplicabilidade dos resultados para o desenvolvimento contínuo de ferramentas de diagnóstico avançadas na Doutor-IE.

4.4 DISCUSSÃO SOBRE OS RESULTADOS

Os resultados obtidos no projeto de engenharia reversa na comunicação de centrais veiculares, com foco na central do motor do veículo estudado, demonstram um sucesso notável na decodificação e compreensão dos protocolos de comunicação interna. A análise realizada possibilitou uma compreensão detalhada do funcionamento e da estrutura das mensagens trocadas entre as unidades de controle eletrônico (UCEs) e os dispositivos de diagnóstico. O método aplicado permitiu identificar precisamente os padrões de comunicação, as sequências de comandos e as respostas das ECUs, facilitando significativamente o desenvolvimento de ferramentas de diagnóstico avançadas com enfoque no mercado brasileiro.

Um dos principais resultados foi a capacidade de replicar e simular o comportamento da central do motor em bancada, permitindo a realização de testes e diagnósticos detalhados sem a necessidade de intervenção direta no veículo. Isso não apenas reduz o risco de danos potenciais ao sistema durante os testes, mas também proporciona uma plataforma segura e controlada para a análise de falhas e o desenvolvimento

de soluções corretivas.

Além disso, o sucesso do projeto contribui para a consolidação da reputação da empresa como líder em inovação e qualidade em serviços de diagnóstico automotivo. Atrai novos clientes e parceiros interessados em tecnologias de diagnóstico avançadas, ampliando significativamente as oportunidades de mercado e de colaboração técnica. Esses fatores, combinados, não apenas aumentam a rentabilidade da empresa, mas também fortalecem sua posição estratégica no setor automotivo.

Em resumo, os resultados do projeto não apenas confirmam a eficácia das técnicas de engenharia reversa aplicadas, mas também reforçam a importância estratégica de continuar investindo em pesquisa e desenvolvimento. Este foco em inovação garante que a empresa permaneça na liderança, na busca por oferecer produtos e serviços que respondem às rápidas mudanças tecnológicas e às crescentes demandas de um mercado globalizado.

5 CONCLUSÃO

A conclusão desta fase do projeto proporciona uma oportunidade valiosa para refletir sobre as etapas completadas e avaliar a eficácia dos métodos empregados. Até o momento, temos avançado significativamente no desenvolvimento do *scanner* automotivo da Doutor-IE, com a documentação das centrais veiculares progredindo de forma consistente. Nosso objetivo é oferecer uma solução mais integrada e eficiente para mecânicos e especialistas em reparos automotivos, ainda que a ferramenta não esteja totalmente finalizada.

Do ponto de vista organizacional, espera-se que a futura implementação desta ferramenta no mercado resulte em melhorias significativas nos processos internos das oficinas, proporcionando um serviço mais ágil e satisfatório para os clientes. Financeiramente, apesar do investimento inicial ser considerável, antecipamos uma compensação a longo prazo por meio do lançamento do produto, aumento da clientela e maior eficiência operacional.

É crucial reconhecer as limitações do projeto até o momento e identificar áreas que necessitam de melhorias. Para trabalhos futuros, sugere-se a expansão das funcionalidades de inteligência artificial para permitir uma análise ainda mais profunda e automatizada dos dados coletados. Explorar parcerias com fabricantes de automóveis também poderia ser benéfico para garantir compatibilidade com uma gama mais ampla de modelos e marcas.

Em resumo, esta etapa do projeto alcançou seus objetivos principais e ofereceu uma visão promissora de uma solução robusta e inovadora para o diagnóstico automotivo. Os benefícios observados prometem impactar positivamente tanto a operação das oficinas quanto a satisfação dos clientes das oficinas (donos dos carros). Com base nos resultados até agora e nas sugestões para futuras investigações, estou confiante no potencial de continuidade e expansão deste projeto.

Para futuros projetos, também sugere-se a implementação de algoritmos matemáticos avançados para a decodificação do *seed and key*, permitindo a manipulação de mais de 4 bytes de *seed* e *key*. Isso aumentaria significativamente a segurança e a flexibilidade do sistema. Além disso, a implementação de um *stack* do *scanner* é essencial. Esse *stack* refere-se ao conjunto de camadas de *software* que gerenciam a interface do *scanner* com o usuário, incluindo a coleta, processamento e apresentação de dados de diagnóstico. Essas implementações serão necessárias para o completo desenvolvimento de um *scanner* automotivo *aftermarket* utilizando os padrões originais das fabricantes de veículos.

REFERÊNCIAS

CONTRIBUTORS, Wikipedia. **CAN bus**: Wikipedia, The Free Encyclopedia. [*S.l.*], 2024. Disponível em: https://en.wikipedia.org/wiki/CAN_bus. Acesso em: 29 jun. 2024.

ELECTRONICS, CSS. **CAN Bus Explained - A Simple Intro (2020)**: A Simple Intro to CAN Bus: Basics, Pin Out, Signal Levels, Topology, Cable Lengths & Termination. [*S.l.*], 2020. Disponível em: https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial. Acesso em: 29 jun. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 11898-1**: Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling. Geneva, Switzerland, dez. 2015.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 11898-2**: Road vehicles — Controller area network (CAN) — Part 2: High-speed medium access unit. Geneva, Switzerland, dez. 2016.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14229-1**: Road vehicles — Unified Diagnostic Services (UDS) — Part 1: Specification and requirements. Geneva, Switzerland, out. 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14230-3**: Diagnostic systems — Keyword Protocol 2000 — Part 3: Application layer. Geneva, Switzerland, mar. 1999.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 15764-4**: Road vehicles — Diagnostics on Controller Area Networks (CAN) — Part 4: Requirements for emissions-related systems. Geneva, Switzerland, nov. 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 21434**: Road vehicles — Cybersecurity engineering. Geneva, ago. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 26262**: Road vehicles — Functional safety. Geneva, dez. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 9141-3**: Road vehicles — Diagnostics systems — Part 3: Verification of the communication between vehicle and OBD II scan tool. Geneva, Switzerland, jul. 2000.

SOCIETY OF AUTOMOTIVE ENGINEERS. **SAE J3061**: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Warrendale, PA, jan. 2016.

TEXAS INSTRUMENTS. **Introduction to the Controller Area Network (CAN)**: A Detailed Guide. Dallas, TX, ago. 2002.

VECTOR INFORMATIK GMBH. **CAPL Programming Handbook**. Stuttgart, Germany, 2010. CAN Access Programming Language.