UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

DANIEL HENRIQUE POHREN

ESTUDO DO IMPACTO DE TRANSIENTES ELÉTRICOS EM PROTOCOLOS DE COMUNICAÇÃO EM SISTEMAS EMBARCADOS

Porto Alegre
2020

DANIEL HENRIQUE POHREN

ESTUDO DO IMPACTO DE TRANSIENTES ELÉTRICOS EM PROTOCOLOS DE COMUNICAÇÃO EM SISTEMAS EMBARCADOS

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Rio Grande do Sul como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.
Área de concentração: Controle e Automação

ORIENTADOR: Prof. Dr. Carlos E. Pereira

Porto Alegre
2020

DANIEL HENRIQUE POHREN

ESTUDO DO IMPACTO DE TRANSIENTES ELÉTRICOS EM PROTOCOLOS DE COMUNICAÇÃO EM SISTEMAS EMBARCADOS

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: ______________________________
Prof. Dr. Carlos E. Pereira, UFRGS
Doutor pela Technische Universitat Stuttgart, Alemanha

Banca Examinadora:

Prof. Dr. Ivan Müller, UFRGS
Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Prof. Dr. João César Netto, UFRGS
Doutor pela Université Catholique de Louvain, Bélgica

Prof. Dr. Rafael Kunst, UNISINOS
Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Coordenador do PPGEE: ______________________
Prof. Dr. João Manoel Gomes da Silva Jr.

Porto Alegre, Março de 2020.

DEDICATÓRIA

Para alcançar este objetivo, muitos obstáculos foram transpostos, fazendo com que diversas vezes eu não pudesse dar a devida atenção a pessoas muito importantes em minha vida. Estes momentos só são amenizados quando posso ver que os sacrificios foram recompensados, e que o sofrimento não foi em vão. Dedico esta vitória à minha companheira, parceira, amiga e esposa Luiza, que desde o início foi a maior incentivadora para que eu vencesse as barreiras. Dedico sobretudo aos meus pais, que sempre acreditaram em mim e me incentivaram a buscar e lutar pelos meus sonhos.

AGRADECIMENTOS

Agradeço à Deus e a minha família pelo apoio incondicional, aos meus colegas de trabalho, por darem suporte nos momentos de minha ausência, ao meu colega de aula e de pesquisa Alexandre, por compartilhar sua experiência e parceria durante toda a elaboração do trabalho, ao pessoal do DELET pelo suporte durante este período, ao professor Dr. Edison, pelo incentivo na elaboração de publicações e ao professor Dr. Carlos Eduardo, meu orientador, por me dar total apoio e liberdade no desenvolvimento deste trabalho. A empresa PRODEPRED Automação, cujo apoio incondicional foi decisivo durante todo o período deste mestrado.

RESUMO

O aumento da complexidade e responsabilidade dos dispositivos embarcados nos veículos hoje, tem orientado os esforços no desenvolvimento de sistemas de controle para que estes sejam mais rápidos, precisos, robustos e principamente seguros. Com isso, estes dispositivos estão levando os protocolos de comunicação a um patamar inédito de exigência, tanto no quesito de capacidade como confiabilidade. Protocolos como CAN, CAN-FD e FlexRay entre outros, tem sido utilizados devido às suas características de segurança e a capacidade de atender aos requisitos temporais dos diversos circuitos embarcados. O desenvolvimento e utilização cada vez mais frequente de dispositivos focados em segurança, fazem com que a comunicação entre os diversos componentes destes dispositivos seja exigida ao máximo, levando à necessidade de respostas confiáveis ao extremo. Sistemas como freios ABS, suspensão ativa, frenagem autonoma de emergência, controle de velocidade e distância adaptativo, entre outros, que envolvem várias ECUs distribuídas ao longo do veículo, dispões de frações de segundo para a reação do sistema, entre o sinal de entrada e a atuação correspondente, demandando uma comunicação segura e tolerante à falhas. Os veículos hoje estão passando por grandes mudanças conceituais, trazendo cada vez mais elementos onde o funcionamento demanda mais energia das fontes de alimentação. Diversos sistemas existentes nos veículos geram ruídos como os Transientes Elétricos Rápidos, ou "Electric Fast Transient" (EFT), que estão presentes nas mais simples operações cotidianas do veículo, como ligar e desligar o farol, o ar condicionado, o limpador de para brisas, ou mesmo o acionamento de iluminação diurna (DRL), etc. Neste trabalho foram realizados diversos ensaios, utilizando ECUs com diferentes funções e protocolos, para identificar a susceptibilidade dos referidos sistemas e os protocolos à pesença destes ruídos. Visando atender às normas IEC 62228 e a ISO26262, este trabalho demandou o projeto e construção de dois circuitos eletrônicos diferentes, um circuito observando os dados de tempos de subida e de descida (*rise and fall time*) dos pulsos de EFT, e outro observando a arquitetura do layout da placa de circuito impresso (PCB), as suas entradas, saídas, componentes, etc. Estes ensaios visaram identificar o quanto estes protocolos são suscetíveis à estes tipos de ruídos, utilizando métricas de análise baseadas nos tempos de latência e variação de jitter dos pacotes de comunicação.

Palavras-chave: Comunicação, Protocolo, CAN, CAN-FD, FlexRay, ISO 26262, IEC 62228, IEC 61000, ISO 7637, EFT.

ABSTRACT

The increasing complexity and accountability of embedded devices in vehicles today has driven efforts to develop control systems to make them faster, accuratest, safest, robustest. Thus, these devices are taking communication protocols to an unprecedented level of demand, both in terms of capacity and reliability. Protocols such as CAN, CAN-FD and FlexRay among others have been used due to their safety characteristics and the ability to meet the time requirements of various embedded circuits. The increasing development and use of safety-focused devices, means that communication between the various components of these devices is required to the utmost, leading to the need for extremely reliable responses. Systems such as ABS brakes, active suspension, autonomous emergency braking, adaptative cruise control, among others, which involve various ECUs distributed throughout the vehicle, have milliseconds for system reaction, between input signal and concrete actuation, requiring safe and failure tolerant communication. Vehicles today are undergoing major conceptual changes, bringing more and more elements whose operation require more energy from power supplies. These systems generate noise such as "Electric Fast Transient" (EFT), which are present in the simplest daily operations of the vehicle, such as turning the headlight on, the air conditioner, the windscreen wiper, or even the daytime running light (DRL), etc. In this work several tests were carried out, using different ECUs with different functions and different protocols to identify the susceptibility of these systems and the protocols to these noises. In order to comply with IEC 62228 and ISO 26262 standards, this work required the design and construction of two different electronic circuits, one circuit observing the rise and fall time data of the EFT pulses, and the other observing the architecture of the printed circuit board (PCB) layout, its inputs and outputs, components, etc. These tests aimed to identify how susceptible these protocols are to these types of noise, using analysis metrics based on latency time and jitter variation of communication packets.

Keywords: Protocol, CAN, CAN-FD, FlexRay, EFT.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ACC	Adaptative Cruise Control
A/D	Conversor Analógico - Digital
ARM	Advanced Risc Machine
AUTOSAR	AUtomotive Open System ARchitecture
BACNet	Building Automation Control Network
BBW	Break By Wire
bps	Bites per second
Bps	Bytes per second
BRS	Bit Rate Switch
CAN	Control Area Network
CAN-FD	Control Area Network with Flexible Data-Rate
CLP	Controlador Lógico Programável
CRC	Cyclic Redundancy Check
CSMA/BA	Carrier Sense Multiple Access with Bit wise Arbitration
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
D/A	Conversor Digital - Analógico
DRL	Daytime Running Light
DSP	Digital Signal Processing
ECU	Electronic Control Unit
EDL	Extended Data Length
E/E	Electric/Electronic
ESD	Electrostatic Discharge
EFT	Electrical Fast Transient
EMC	Electromagnetic Compatibility
ESI	Error State Indicator
FTT-CAN	Flexible Time-Triggered communication on CAN

GND	Ground
GPIO	Generic Port Input Output
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OEM	Original Equipment Manufacturer
OSI	Open System Interconnection
LIN	Local Interconnect Network
LED	Light Emiter Diode
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
MOST	Media Oriented System Transport
NCS	Network Control System
PCB	Printed Circuit Board
PC	Personal Computer
PROFIBUS	Proccess Field Bus
RF	Radio Frequency
RISC	Reduced Instruction Set Computer
RL	Load Resistence
RTE	Runtime Enviroment
RTOS	Real Time Operational System
Sa	Samples
SAE	Society of Automotive Engineering
SDCD	Sistema Digital de Controle Distribuído
SPI	Serial Peripheral Interface
TDMA	Time Division Multiple Access
TT-CAN	Time-Triggered communication on CAN
USB	Universal Serial Bus
VFB	Virtual Functional Bus

LISTA DE SÍMBOLOS

$\approx$	Aproximado
°C	Graus celsius
μC	Micro Controlador
μs	Micro segundos
ns	Nano segundos
G	Giga
m	Metro
mm	Milimetro
M	Mega
K	Kilo
Kg	Kilograma
Vp	Volts de pico
Vpp	Volts de pico a pico
Hz	Hertz
Vcc	Volts corrente contínua
Vds	Volts *drain - source*
Pa	Pascal

SUMÁRIO

1 INTRODUÇÃO

Protocolos de comunicação são responsáveis por conectar e integrar diferentes sistemas de controle em rede, e em diferentes domínios de aplicação (Avionica, Sistemas Automotivos, Automação Industrial, etc.). Protocolos veiculares de comunicação como CAN, CAN-FD, LIN e FlexRay, são comumente aplicados para interconectar unidades de controle eletrônico (ECU), onde alguns deles são responsáveis pelo controle de processos críticos. Devido à crescente complexidade dos sistemas de controle veiculares distribuídos, o protocolo CAN, que foi um dos protocolos pioneiros aplicados em redes automotivas, sofreu atualizações e evoluções, criando variações da versão original com o objetivo de melhorar a confiabilidade e a flexibilidade.

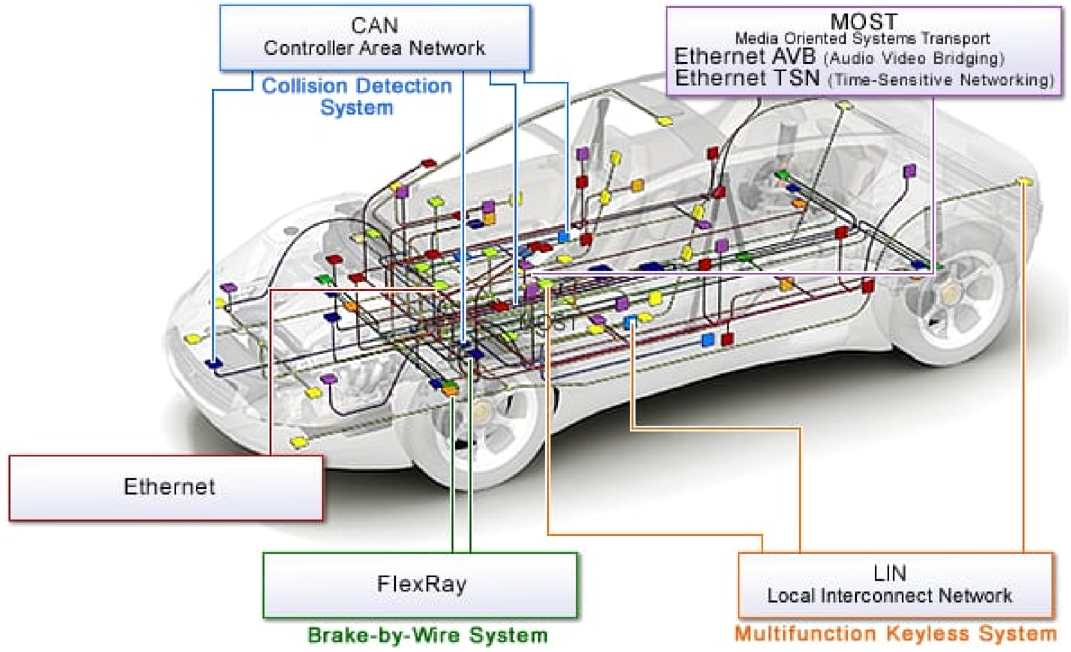
Devido à crescente demanda por maior largura de banda de comunicação em redes intra-veiculares, e para atender à requisitos temporais e a maior quantidade de dados dos modernos sistemas de controle embarcados, um novo protocolo foi desenvolvido pela Robert Bosch GmbH, o CAN com taxa de dados flexível (CAN-FD). As principais inovações do CAN-FD incluem o aumento de velocidade, maior que 1 Mbps, e maior quantidade de dados transmitidos, de 8 a 64 bytes. Assim, além de aumentar a taxa de transmissão, também é possível aumentar a quantidade de dados transmitidos.

Além do CAN-FD, outras versões do protocolo CAN foram criadas, como o TT-CAN, FTT-CAN, junto com outros protocolos diferentes. Um protocolo com uma grande ascenção no mercado, tendo em vista sua capacidade de comunicação em canal duplo, que fornece redundancia física, bem como sua maior velocidade que pode superar os 10Mbps, é o FlexRay. No entanto, todos esses aspectos evolutivos apresentados por estes protocolos, podem não ser suficiente no caso de interferências que prejudiquem a comunicação, degradando assim o desempenho da ECU, devido ao carregamento da rede, perdas de pacote ou mesmo um apagão na comunicação.

Neste contexto, o presente trabalho enfoca os problemas relacionados à degradação do desempenho dos protocolos CAN, CAN-FD, e FlexRay devido a falhas geradas por interferências eletromagnéticas, aplicando como estudo de caso, os transientes elétricos rápidos (EFT). A escolha por estes protocolos, deve-se ao fato destes representarem a maioria das redes de comunicação embarcadas, responsáveis por tarefas criticas, diretamente relacionadas à segurança do veículo e dos ocupantes.

Entretanto, com a complexidade dos atuais sistemas eletrônicos de controle embarcado, a comunicação precisa de mecanismos tolerantes a falhas que permitam o diagnóstico e a detecção de interferências ocasionais ou repetitivas. Na Figura 1 pode-se observar que as plataformas de veículos automotivos de hoje, utilizam não apenas um protocolo, mas em alguns casos, vários protocolos com funcionalidades diferentes, integrados através de um gateway central (KUMAR; RAMESH, 2014).

Figura 1 – Exemplo de arquitetura de rede intra-veicular embarcada.


CAN
Controller Area Network
Collision Detection System
MOST
Media Oriented Systems Transport
Ethernet AVB (Audio Video Bridging)
Ethernet TSN (Time-Sensitive Networking)
Ethernet
FlexRay
Brake-by-Wire System
LIN
Local Interconnect Network
Multifunction Keyless System

Fonte: (RENESAS - IN-VEHICLE NETWORKING SOLUTIONS, 2019).

Portanto, a análise do impacto de ruídos EFT nestes protocolos, permite verificar como os sistemas de controle podem ser afetados por estes transientes. Com o objetivo de explorar esta questão, este trabalho utiliza uma metodologia de ensaios baseado em (PANNILA; EDIRISINGHE, 2014) (FONTANA; HUBING, 2015), juntamente com o desenvolvimento do hardware de teste, baseado em padrões industriais e atendendo as normas IEC 62228 (IEC-62228, 2016) e ISO 26262 (ISO-26262, 2018). Os dados de comunicação são monitorados pelos módulos CAN BUS Analyser (MICROCHIP), CAN-FD Analyser (GRID CONNECT) e o módulo VN8970 (Vector Informatik GmbH).

A análise subsequente dos dados de comunicação é realizada com a plataforma de hardware e software Vector CANoe/Analyzer (Vector Informatik GmbH). Esta plataforma permite, além da avaliação completa do comportamento da comunicação, o desenvolvimento de novos dispositivos (através de simulações) para redes intra-veiculares. Os dados coletados servem para uma análise de performance e confiabilidade dos barramentos, permitindo uma avaliação precisa sobre a influência destas interferencias na comunicação e possibilitando um estudo direcionado para soluções de hardware e software, que permitam minimizar ou mesmo mitigar as interferências na comunicação.

1.1 Objetivos

O objetivo deste trabalho é desenvolver uma proposta que permita avaliar o desempenho dos protocolos de comunicação embarcada na presença de falhas, e efetuar ensaios com a injeção de ruídos do tipo *EFT* na rede de comunicação entre ECUs que utilizam os protocolos *CAN, CAN-FD e FlexRay*, obdecendo as normas ISO 26262 e IEC 62228, verificando a suceptibilidade destas ECUs e os protocolos a este tipo de ruído. Para realizar estes testes, foram desenvolvidos procedimentos e hardwares específicos que atendem as normas acima citadas.

1.2 Organização

Este trabalho está organizado em nove partes distintas, primeira parte a introdução, segunda parte a base teórica sobre protocolos de comunicação e normas, a terceira parte aborda a proposta em si, a quarta parte descreve os trabalhos relacionados, a quinta parte descreve os projetos elaborados para as placas de geração e injeção de EFT, a sexta parte trata dos ensaios práticos no protocolo CAN, a setima parte descreve os ensaios realizados com o protocolo CAN-FD, a oitava parte descreve os ensaios como protocolo FlexRay e a última parte trata das conclusões e trabalhos futuros.

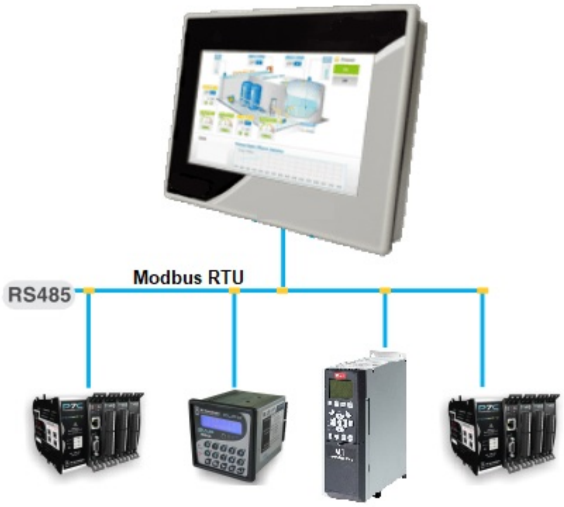
2 FUNDAMENTAÇÃO TEÓRICA

2.1 Redes de comunicação

Nas últimas décadas, com o crescente e rápido desenvolvimento de novos circuito eletrônicos e microprocessadores, a necessidade dos sistemas interagirem entre si aumentou exponencialmente. Este crescimento fez com que diversos dispositivos fossem interligados em uma rede de comunicação, o que gerou a necessidade de serem criados meios padronizados, para que os dispositivos pudessem trocar informações de maneira rápida e confiável. Devido a isso, foram desenvolvidos os protocolos de comunicação, que são padronizações de como os dispositivos irão se comportar em uma rede e como enviarão ou receberão dados.

Diversos protocolos foram desenvolvidos ao longo das últimas decadas, focados em diversas aplicações diferentes, alguns dedicados a automação industrial e utilizados na comunicação em chão de fábrica como ModBus (MODICON, 1979), que é considerado hoje o protocolo do tipo *FIELDBUS* mais utilizado no mundo, o PROFIBUS (CENA; DURANTE; VALENZANO, 1995), o DeviceNet (SCHIFFER; VANGOMPEL; VOSS, 2006), etc. Um exemplo de rede Modbus pode ser visto na Figura 2. Também foram desenvolvidos protocolos dedicados a automação predial como o BACNet (ASHRAE, 2016), o LonWorks (ISO-14908/1, 2012), entre outros. No ambiente embarcado automotivo, vários protocolos foram desenvolvidos, entre eles o *CAN*, o *LIN*, o *MOST*, o *FlexRay*, etc.

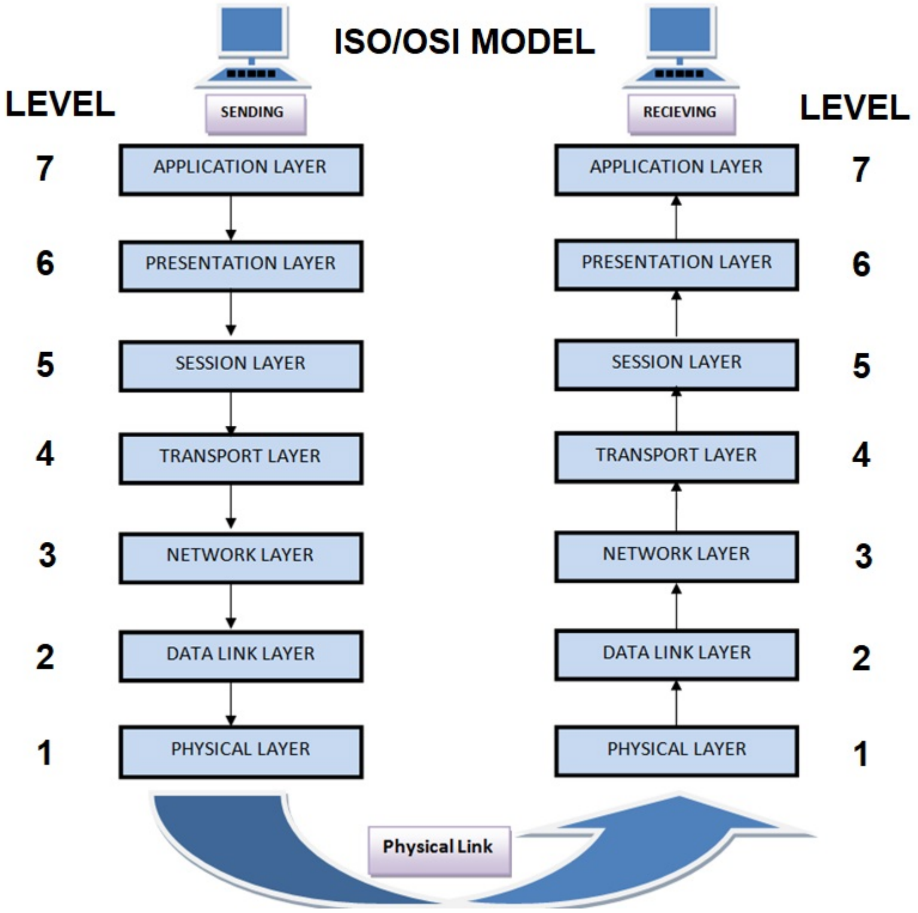
Figura 2 – Exemplo de rede Modbus.



Fonte: Autor.

As redes de comunicação baseiam-se em conjuntos de protocolos, divididos em camadas, como o modelo ISO/OSI (TANENBAUM; WETHERALL, 1999), sendo este conjunto responsável por garantir o suporte necessário às aplicações construídas sobre o mesmo. Na Figura 3 é visto este modelo.

Figura 3 – Modelo ISO/OSI de comunicação.



Fonte: (TANENBAUM; WETHERALL, 1999).

No ambito de redes embarcadas em veículos, vários protocolos vem sendo desenvolvidos ao longo das décadas, sempre buscando velocidade, capacidade de transmissão, confiabilidade dos dados e principalmente segurança.

As redes estão cada vez maiores, mais complexas e acumulando funções de extrema importância no funcionamento dos diversos dispositivos do veículo. Assim os protocolos também são projetados, baseando suas funcionalidades nas características que os dispositivos demandam.

Várias características servem como base para o desenvolvimento dos protocolos embarcados, seja o numero de dispositivos na rede, a quantidade de dados transmitidos, restrições temporais, a flexibilidade no tratamento de dados, a capacidade de permitir interrupções não esperadas para transmissões emergenciais, etc. Diversas são as maneiras de tratar estas condições nos protocolos, alguns reservam janelas temporais para as transmissões e outros utilizam um processo tipo interrupção. Os protocolos que lançam mão de eventos agendados por tempo são chamados periódicos (*Time-Triggered*), já os outros que utilizam os próprios eventos em si (*Event-Triggered*) são os considerados esporádicos (XIA; SUN, 2008).

2.1.1 Protocolos *Time-Triggered*

Em uma rede de comunicação composta por dispositivos multimestre, a concorrência entre os elementos desta rede pelo uso do meio de transmissão existe, porém esta concorrência é gerenciada por artifícios de escalonamento, que dependendo do protocolo, são definidos em hardware ou em software.

Nos protocolos com comunicação periódica ou *Time-Triggered*, a metodologia de escalonamento é baseada no método TDMA (*Time Division Multiple Access*). As vantagens no uso deste método são a baixa latência, baixo jitter e comportamento previsível. Uma característica importante para o funcionamento deste método é o sincronismo de base de tempo dos elementos da rede. Este método tem como ônus, a baixa capacidade de mudança dos pacotes de dados, uma vez que a estrutura de rede deve ser projetada levando em conta todas as características dos dados que trafegarão nesta rede.

2.1.2 Protocolos *Event-Triggered*

Nos protocolos de comunicação do tipo *Event-Triggered*, a solicitação de acesso ao meio de comunicação é feita sob demanda, ou seja, na ocorrência do evento. Esta solicitação se inicia pelo acesso ao meio físico, que é definido como a primeira camada do modelo ISO/OSI. Esta abordagem garante maior flexibilidade ao sistema, uma vez que a entrada ou saída de elementos da rede, não irá interferir na maneira com que os demais irão acessar o meio físico. Uma consequência inevitável neste tipo de gerenciamento de acesso ao meio é a colisão, uma vez que as solicitações são feitas de maneira assíncrona, 2 ou mais elementos podem solicitar o acesso simultaneamente. Estas colisões geralmente aumentam o tempo de latência na comunicação, e normalemente interferem também no jitter. Normalmente cada protocolo tem seu algoritmo para a resolução das colisões, passando por fatores de multiplicação pelo endereço na rede ou por geração de tempo randômico, sempre visando distanciar no tempo os acessos coincidentes.

Exemplos de protocolos que utilizam a metodologia *Event-Triggered* são o CAN e o Ethernet. O CAN utiliza como metodologia de acesso ao meio a estratégia CSMA/BA (*Carrier Sense Multiple Access with Bitwise Arbitration*), já o Ethernet utiliza o método CSMA/CD (*Carrier Sense Multiple Access with Colision Detection*).

2.2 Protocolo CAN

2.2.1 Histórico

O primeiro e mais antigo protocolo amplamente utilizado em redes embarcadas automotivas é o CAN (*Controller Area Network*), que teve o início de seu desenvolvimento em meados dos anos 1980, através dos pesquisadores Wolfhard Lawren, da Universidade de Ciências Aplicadas Braunschweig-Wolfenbüttel, e Horst Wettstein, da Universidade de Karlsruhe, que aplicaram o conceito das arquiteturas eletrônicas, especificamente a de rede distribuída na rede CAN (MIESTERFELD, 1999).

Os pesquisadores foram assistidos pelas empresas da área automobilística Mercedez Benz e Robert Bosch. O objetivo das empresas era desenvolver um novo protocolo que atendesse aos requisitos de engenharia para as plataformas de sistemas distribuídos embarcados, já que os protocolos até então existentes não os atendiam.

Em fevereiro de 1986, em Detroit - USA, onde aconteceu o congresso da SAE (*Society of Automotive Engineering*), foi apresentado o estudo de uma rede *Multi-Mestre* serial e síncrona (BOSCH et al., 1991). A rede CAN surgiu pela primeira vez em veículos automotores de passeio em 1992, utilizado pela Mercedez Benz. Neste mesmo ano foi criado um grupo de usuários deste protocolo, denominado *CAN in Automation*(CiA). Este grupo é formado por engenheiros do mundo todo, que vem debatendo até os dias de hoje qualquer mudança técnica necessária para a rede. Atualmente é o segundo protocolo mais utilizado no mundo, sendo utilizado tanto na area embarcada como na area industrial.

2.2.2 Características

A rede de comunicação composta por ECUs (*Eletronic Control Unit*) que utilizam o protocolo CAN, consiste em um par de fios trançados, onde todas as ECUs estão interligadas de forma paralela, ou seja, o sinal trafega por todos os módulos simultaneamente. A adoção deste tipo de meio físico foi em função da demanda por um sistema de interligação simples e barata, porém este meio físico trouxe o desafio de equacionar os acessos simultâneos. Por se tratar de um meio físico conflitante, onde todos os elementos que estão conectados à rede, podem, sem nenhum tipo de aviso ou predição, acessar o barramento simultaneamente, gerando as chamadas *colisões* na comuniação, o desenvolvimento deste protocolo teve que se preocupar em tratar estes múltiplos acessos, e consequentemente, estas colisões.

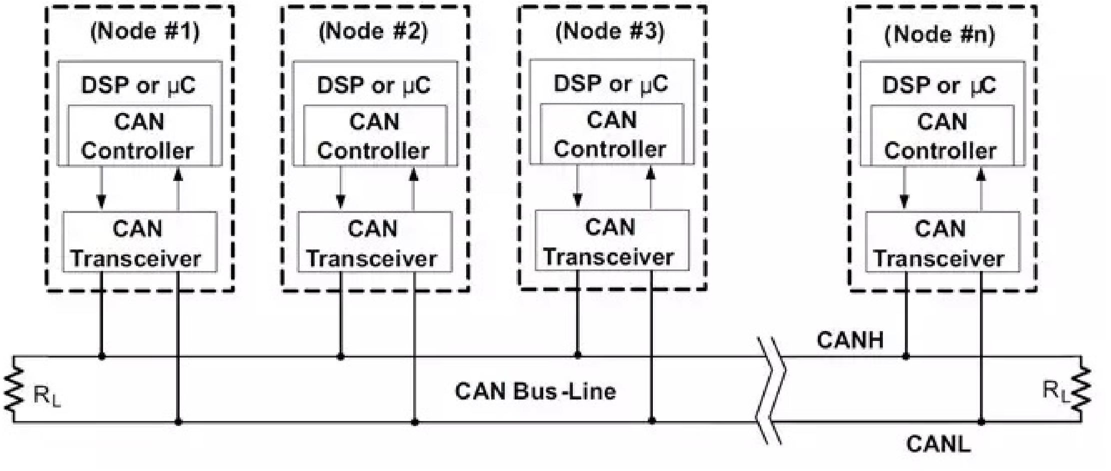
O protocolo CAN (*Controller Area Network*) é baseado na transmissão de mensagens onde cada uma possui um identificador, identificador este que também é responsável por indicar a prioridade da mensagem. Através deste procedimento, os conflitos existentes durante o acesso ao meio são resolvidos. A mensagem com menor prioridade é a com o maior identificador, sendo a mensagem prioritária a com o menor identificador. Quando o acesso acontece simultaneamente, aquele que possui a prioridade menor identifica a colisão e cessa sua transmissão imediatamente, e aguarda a disponibilidade do barramento para tentar a retransmissão. A camada física do protocolo é definida conforme a Tabela 1 (ISO-11898/93, 1993).

Tabela 1 – Tabela da norma ISO 11898.

Norma	Descrição
ISO 11898 - 1	Especifica a camada de dados
ISO 11898 - 2	Especifica alta velocidade taxa de até 1Mbps
ISO 11898 - 3	Especifica baixa velocidade taxa de 40 até 125Kbps
ISO 11898 - 4	Especifica *time-triggered*
ISO 11898 - 5	Especifica a camada fisica para taxa até 1Mbps
ISO 11898 - 6	Especifica camada fisica para taxa de até 1Mbps com *Wake-up*

A taxa de transmissão de dados pode chegar a 1 *Mbit/s*, e a maior distância atendida pelo protocolo pode chegar a até 5km, porém a velocidade atingida nesta distância é muito baixa. Na Figura 4 pode-se observar uma rede CAN básica.

Figura 4 – Exemplo de rede CAN.



Fonte: Autor.

2.3 Protocolo CAN-FD

2.3.1 Histórico

O protocolo CAN-FD (*Controller Area Network with Flexible Data-Rate*) é uma evolução do protocolo CAN e foi introduzido na 13ª Conferência Internacional do CAN, que aconteceu em 2012, na cidade de Nuemberg - Alemanha, pelas empresas Robert Bosch e Vector (HARTWICH, 2012).

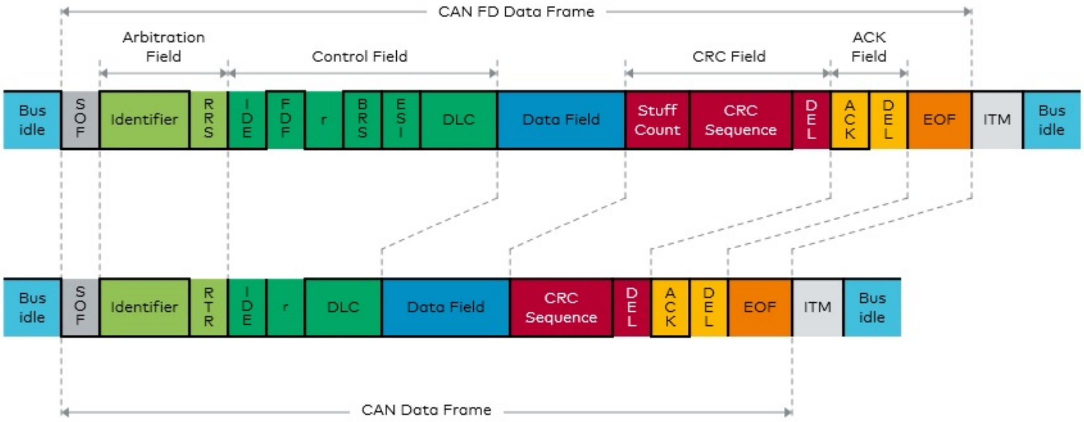
O CAN-FD tem toda sua estrutura baseada no CAN, sendo a principal diferença a quantidade de dados (limitado a *64 bytes*) que o novo protocolo suporta. No desenvolvimento de uma alternativa ao já limitado protocolo CAN, várias linhas haviam sido exploradas, mas a principal diretiva era manter a estrutura simples e a compatibilidade com o CAN, visando uma migração amigável de uma plataforma para outra. Outro objetivo era o aumento da velocidade de barramento, uma vez que a velocidade do CAN estava limitada a 1Mbps. O desenvolvimento do protocolo levou em consideração manter no máximo possível, intocados o hardware e o software do protocolo, facilitando a sua aplicação. Desta forma, a alternativa encontrada foi alterar o controlador do protocolo CAN, implementando este com as diretivas do CAN-FD. Estas alterações foram implementadas, para que uma ECU com protocolo CAN-FD pudesse ser incluída em uma rede CAN. Como o frame dos protocolos são diferentes, o CAN-FD utilizou os bits reservados do protocolo CAN, para definir que tipo de frame está sendo transmitido. Desta forma, um receptor pode identificar que se trata de um frame CAN ou CAN-FD.

2.3.2 Características

Sendo uma evolução do CAN, e tendo como diretivas principais o aumento da taxa de transmissão e o tamanho do frame, o protocolo CAN-FD tem a capacidade de ser inserido em uma rede CAN, sendo este nó reconhecido apenas no ambito do controlador.

A mensagem CAN FD possui os mesmos elementos de uma mensagem CAN, a principal diferença é que no padrão CAN FD o campo de dados e o campo de CRC podem ser maiores que no clássico padrão CAN. A validação de uma mensagem CAN FD requer, assim como no CAN, a inserção de um bit de reconhecimento (*Acknowledge Bit*) por pelo menos uma das ECUs da rede. Como os dois padrões possuem basicamente a mesma estrutura, pode-se afirmar que a diferenciação entre uma mensagem CAN e uma CAN FD está no bit reservado “r”, localizado no campo dos bits de controle (Figura 5). No CAN FD este campo é substituído pelos bits EDL (*Extended Data Length*), BRS (*Bit Rate Switch*) e ESI (*Error State Indicator*).

Figura 5 – Comparativo entre os frames CAN e CAN-FD.



Fonte: Vector Informatik GMBH.

2.4 Protocolo FlexRay

2.4.1 Histórico

O protocolo FlexRay é tido como um protocolo focado na confiabilidade e segurança, foi desenvolvido pelo consórcio (*FlexRay Consortium*) criado pelas empresas BMW, Daimler-Chrysler, Philips e Freescale (MAKOWITZ; TEMPLE, 2006). Os objetivos iniciais para o desenvolvimento do protocolo foram (MAKOWITZ; TEMPLE, 2006):

- **Alta Velocidade:** Uma ordem de grandeza maior que o CAN
- **Determinismo:** Para oferecer suporte a aplicações críticas com restrições temporais
- **Tolerância a falhas:** Para que fosse possível substituir sistemas críticos discretos

Em 2009, com a publicação da versão 3.0 das especificações do *FlexRay*, o consórcio foi desfeito. A partir deste momento, as especificações foram transformadas em normas ISO, sob a denominação 17458 (ISO-17458, 2013). Esta norma é dividida em cinco partes, conforme listado na Tabela 2.

Tabela 2 – Tabela da norma ISO 17458.

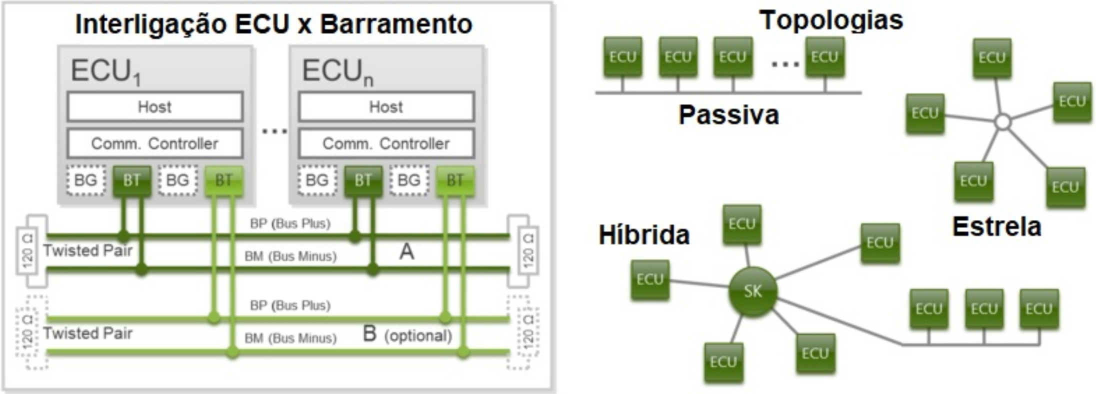
Norma	Descrição
ISO 17458 - 1:2013	General information and use case definition
ISO 17458 - 2:2013	Data link layer specification
ISO 17458 - 3:2013	Data link layer conformance test specification
ISO 17458 - 4:2013	Electrical physical layer specification
ISO 17458 - 5:2013	Electrical physical layer conformance test specification

2.4.2 Características

Como o *FlexRay* trata-se de um sistema de comunicação (hardware e software) diferente em relação ao CAN, toda a arquitetura que o envolve também é diferente. A começar pelo hardware, onde existem dois canais redundantes, permitindo que a comunicação seja feita simultaneamente por dois meios físicos distintos (*canal A e B*). Estes meios físicos, além de duplicados, tem uma taxa de transmissão dez vezes maior que o CAN, ou seja, chega a 10Mbps. Somado a isso, o hardware dos transceivers foram exaustivamente testados, para que alcançassem os requisitos exigidos pela norma (ISO-17458, 2013).

Considerando todos os cuidados que foram tomados na definição do hardware e do software do protocolo, uma rede *FlexRay*, ao contrário de outras redes de mercado, pode ser constituída de diferentes topologias de interligação, ou seja, pode ser interligada em série (*barramento passivo*), estrela ativa ou híbrida (ISO-17458, 2013). As conexões das ECUs *FlexRay* e as topologias de interligação são mostradas na Figura 6.

Figura 6 – Barramentos A e B FlexRay e topologias.



Fonte: Autor.

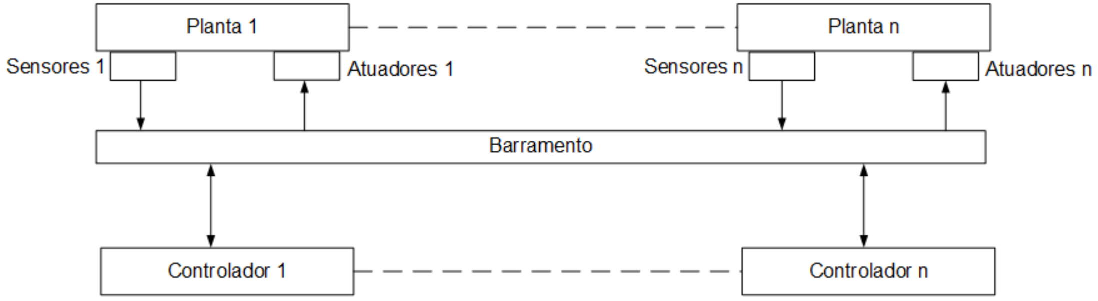
2.5 Rede de Controle

A rede de controle ou sistema de controle em rede (*NCS - Network Control Systems*), consiste em sistemas onde os elementos estão distribuídos geograficamente ao longo da planta. O conceito inicial de NCS era de certa forma distorcido, pois os sensores e atuadores remotos se comunicavam com o controlador central através dos seus sinais elétricos padronizados na instrumentação, como sinais de corrente e tensão, e não via comunicação de dados. Com este conceito, vários sistemas foram implementados utilizando um controlador centralizado com dispositivos de campo espalhados ao longo da planta, utilizando controladores do tipo *CLP* e alguns *SDCD's*.

Os sistemas de controle em rede atuais se beneficiaram do avanço dos processadores, o que permitiu a miniaturização de unidades processadoras, que possibilitaram a elementos simples se conectar a uma rede, e através desta, enviar as informações já tratadas de forma digital através de um protocolo, ao elemento controlador

As redes de controle se popularizaram cada vez mais, levando em conta o rápido crescimento na oferta de novas tecnologias de redes e protocolos. Tendo em vista que, sistemas críticos que antes eram discretos, ou seja, utilizavam o conceito de sinais elétricos e não comunicação de dados, para que pudessem se adequar as novas tendências, as *NCS's* obrigatoriamente deveriam oferecer condições de respostas temporais e garantia de entrega dos dados de forma confiável, e para isso, os protocolos e os elementos formadores da rede deveriam também avançar, desta forma os dados podem ser transmitidos de maneira confiável através de uma rede com comunicação compartilhada. Na Figura 7, é visto um exemplo básico de *NCS*.

Figura 7 – Conceito de um *NCS*



Fonte: (HESPANHA; NAGHSHTABRIZI; XU, 2007).

Quando comparado aos sistemas convencionais de controle, que utilizam sinais elétricos de corrente e tensão, para levar e trazer os valores dos sensores e atuadores ao controlador, a introdução de sistemas que utilizam a comunicação de dados como meio de levar e trazer estas informações, traz também uma série de fatores que devem ser levados em consideração, fatores estes que podem degradar o desempenho da malha de controle, ou até mesmo inviabilizar esta malha (LIXIAN; HUIJUN; KAYNAK, 2013). Em virtude destes fatos, muitos métodos de modelagem, teste e análise são desenvolvidos e utilizados, visando minimizar ou até mesmo mitigar os efeitos destas interferências na comunicação dos *NCS*.

Os sistemas de controle em rede tem como *background*, a teoria de controle propriamente dita e a teoria de comunicação, sendo que estas duas devem trabalhar em harmonia, para que os sistemas funcionem. Porém, as teorias nos mostram caminhos ambíguos, já que a teoria de controle está centrada na análise de sistemas dinâmicos que são interligados através de canais ideais, enquanto a teoria de comunicação baseia-se na transmissão de dados através de meios imperfeitos (HESPANHA; NAGHSHTABRIZI; XU, 2007).

Existem duas classificações distintas ao citar-se *NCS*, *Controle da Rede* e *Controle Sobre a Rede* (GUPTA; CHOW, 2009).

- ***Controle da Rede*: ** Este campo de estudo envolve pesquisas nas áreas de comunicação e redes de forma a torna-los propícios para o uso em sistemas de controle de tempo real.Como exemplos temos: Controle de rotemamento, redução de congestionamento, protocolos de rede, etc.

- ***Controle Sobre a Rede*: ** Neste caso, o foco está diretamente relacionado às estratégias de controle e projetos de sistemas de controle, operando sobre uma rede de comunicação compartilhada, de forma a minimizar os impactos dos efeitos introduzidos em função da utilização da rede e dos protocolos de comunicação.

O foco deste trabalho é, baseado no conceito *Controle Sobre a Rede*, realizar ensaios com três diferentes tipos de rede e protocolos, buscando identificar a susceptibilidade destas redes à ruídos do tipo *EFT*.

2.6 Normas e Padrões

Como este trabalho baseia-se principalmente sobre duas normas específicas, a IEC 62228 (IEC-62228, 2016) e a ISO 26262 (ISO-26262, 2018), um breve descritivo sobre estas normas se faz necessário.

2.6.1 IEC 62228

A norma IEC 62228 (IEC-62228, 2016) trata da compatibilidade eletromagnética dos transceivers de comunicação *CAN e CAN-FD* e também aos procedimentos de teste e avaliação destes tranceivers e dos respectivos protocolos.

A norma foi redigida pela Comissão Eletrotecnica Internacional (International Eletrotechnical Comission - IEC) e está na sua versão de 2016.

Esta norma trata do seguinte escopo:

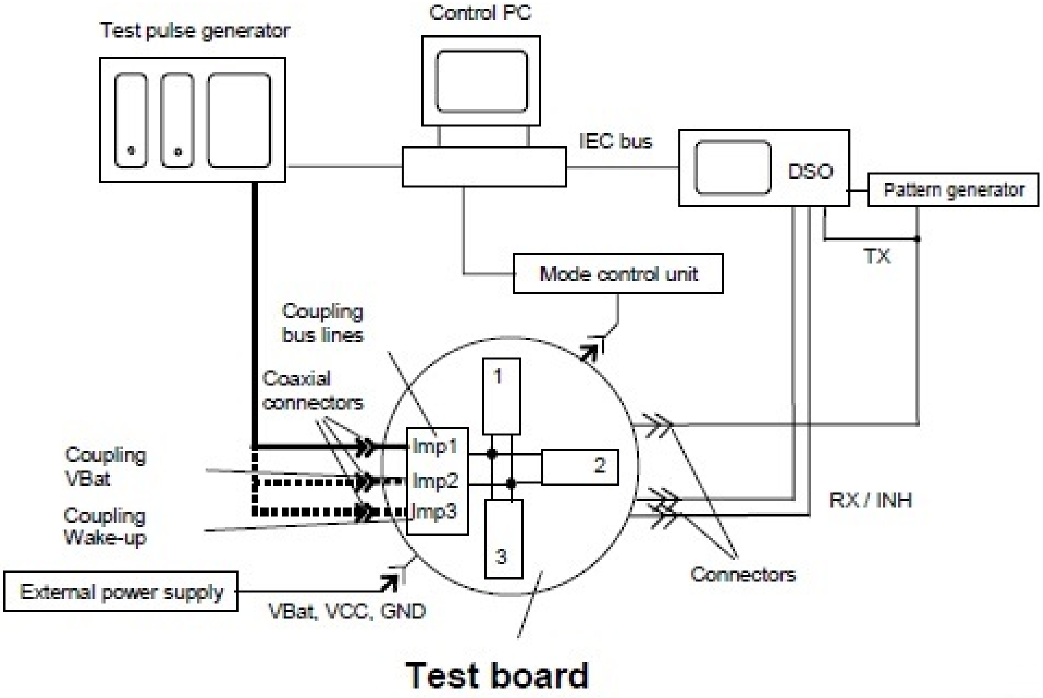
- Imunidade à ruídos RF em modo comum sobre as linhas de sinal
- Emissões causadas por sinais não simétricos relacionados ao domínio Tempo e Frequência
- Imunidade referente a transientes
- Imunidade referente a discargas eletroestáticas - ESD

Como servem de base para a IEC 62228, algumas outras normas também foram referenciadas, onde se destacam:

- IEC 62132 - Circuitos Integrados - Medições de imunidade eletromagnética
- IEC 61000-4 Compatibilidade Eletromagnética - Técnicas de testes e medições
- ISO 7637 - Veículos Automotivos - Distúrbios Elétricos Conduzidos e Acoplados

Neste projeto, a referência principal desta norma é a definição do hardware a ser utilizado para os testes, suas características específicas e a instrumentação necessária. Na figura 8 pode ser visualizado um "Set-up" básico para o atendimento à norma no quesito de hardware de teste.

Figura 8 – Exemplo de "Set-up"para testes de imunidade à impulso acoplado



Fonte: (IEC-62228, 2016).

2.6.2 ISO 26262

A ISO 26262 (ISO-26262, 2018) é uma norma cujo foco é a segurança automotiva, e que substitui a norma IEC 61508, com o objetivo de adaptar a referida norma aos requisitos de veículos híbridos e elétricos. Esta norma especifica as funcionalidades de segurança à veiculos automotores de passageiros com peso de até 3500Kg.

Esta norma teve seu início de estudo em meados de 2002 de forma individual, e em 2004 foi formado um grupo de estudos de diversas empresas da área automotiva, fabricantes de peças e montadoras como SIEMENS, TRW, BOSCH, VW, BMW, AUDI, FORD, entre outras. Em 2005 foi publicado sua primeira versão oficial, já sob a denominação atual de ISO 26262.

O foco principal desta norma são os possíveis danos causados por malfuncionamento do comportamento de elementos de segurança no veículo, como direção assistida, freios ABS, suspensão ativa, frenagem de emergência, entre outras.

A estrutura dos processos de segurança incluem:

- Planos de segurança e Objetivos de segurança
- Documentação relacionada à segurança
- Rastreabilidade dos itens relacionados à segurança
- Ciclo de vida dos itens referentes à segurança
- Validação, verificação e avaliação independente

Esta norma definie uma série de diretivas, procedimentos, avaliações e análises referente à segurança, aplicado desde o fabricante do mais singelo componente até a montadora, sempre observado os parâmetros de segurança do condutor e dos passageiros.

Elementos ativos ou passivos, que atuam direta ou indiretamente com os sistemas considerados como críticos para a segurança, devem atender a esta norma, sob risco de não ser habilitado para a instalação em veículos fabricados pelos signatários da referida norma.

Como esta norma está diretamente associada ao projeto aqui abordado, onde o estudo de caso trata-se de uma suspensão ativa, o atendimento desta norma se faz imprescindível para que os resultados possam ser considerados pela indústria do setor.

2.6.3 AUTOSAR

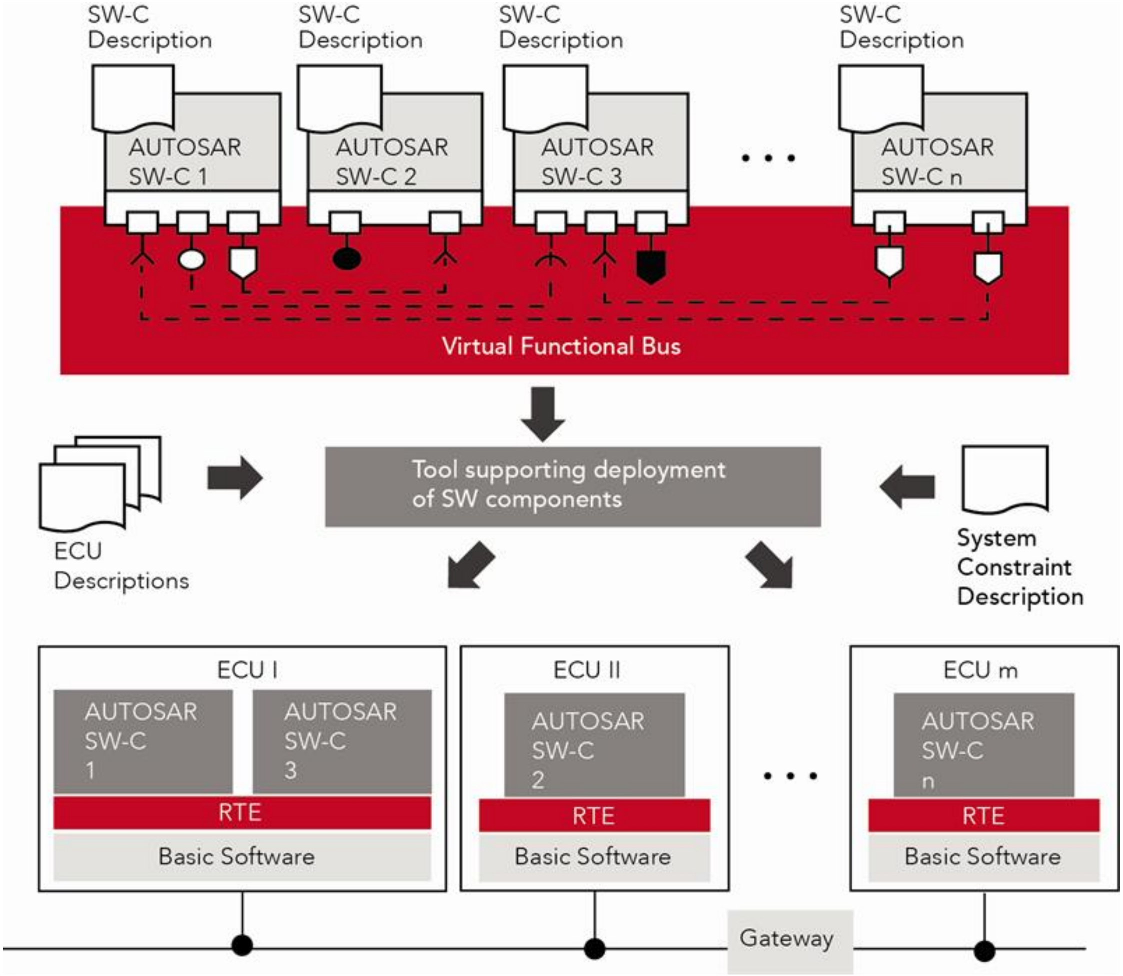
O AUTOSAR (AUTomotive Open System ARchitecture) é uma parceria entre fabricantes de peças e montadoras de veículos automotores com o objetivo de desenvolver e estabelecer uma arquitetura E/E (Eletrica/Eletrônica) realmente "aberta" e padronizada. De forma técnica e simplificada, pode-se resumir os esforços de padronização como segue:

- Gerenciar o aumento da complexidade dos sistemas E/E decorrente do crescimento das funcionalidades
- Implementar a flexibilidade para a modificação, a renovação e substituição de produtos
- Implementar a escalabilidade das soluções entre diferentes linhas de produtos
- Implementar a confiabilidade e a qualidade dos sistemas E/E
- Permitir a identificação de erros nas fases iniciais de projeto

A estrutura básica da arquitetura do AUTOSAR descreve o uso de uma estrutura de hardware e de software, ambos certificados, onde o software deve rodar sobre a estrutura de hardware certificada. Não é possível afirmar que um software é certificado AUTOSAR, se o mesmo não roda em uma estrutura de hardware certificada, ou se está rodando em uma estrutura de hardware não certificada. Da mesma maneira, não é possível considerar um hardware certificado, se o mesmo não é compatível com um software certificado.

Estas características físicas e lógicas visam a capacidade de intercambiabilidade entre os elementos de diferentes fabricantes e de diferentes plataformas, tanto de hardware como de software. A principal característica do sistema AUTOSAR é o chamado "Ambiente de Execução" (RunTime Enviroment - RTE), onde os sistemas devem ter completa compatibilidade. Para que esta compatibilidade seja praticamente perfeita, a plataforma de software do AUTOSAR cria um barramento virtual funcional (Virtual Functional bus - VFB) entre os componentes do sistema embarcado, o que facilita a comunicação entre diferentes componentes de software e diferentes equipamentos no veículo. Na figura 9 pode ser visto o barramento virtual do AUTOSAR.

Figura 9 – Barramento Funcional Virtual do AUTOSAR



Fonte: (AUTOSAR - TECHNICAL OVERVIEW, 2006).

2.7 Fatores que afetam a imunidade de circuitos integrados

As tecnologias empregadas na produção de circuitos integrados e microcontroladores de baixo custo e consumo hoje em dia, utilizam transistores com gates na casa de $7x10^{-9}$m, ou seja, são transistores com capacidade de gerar ou responder a sinais com tempos de subida e descida (*rise and fall time*) na casa de nano e até pico segundos. Como resultado, os microcontroladores são capazes de responder aos transientes elétricos rápidos (EFT) injetados nos seus pinos, ou em outros componentes periféricos do circuito, interpretando estes ruídos como sinais válidos, interferindo assim no seu funcionamento. Somado a esta característica, o layout da placa de circuito impresso (PCB) também interfere diretamente na susceptibilidade dos circuitos integrados aos ruídos. No passado, quando os aspectos referentes à compatibilidade eletromagnética (EMC) eram desconhecidos, era comum os projetistas lançarem mão de projetos existentes como base para novos projetos, imaginando que o referido projeto havia sido desenvolvido com todos os cuidados necessários, ou seja, com filtros, blindagens, etc (ARORA, 2011). Esta abordagem é uma das piores possível, pois pode acarretar em alto custo de retrabalho e também baixo resultado, traduzindo, um projeto ineficiente.

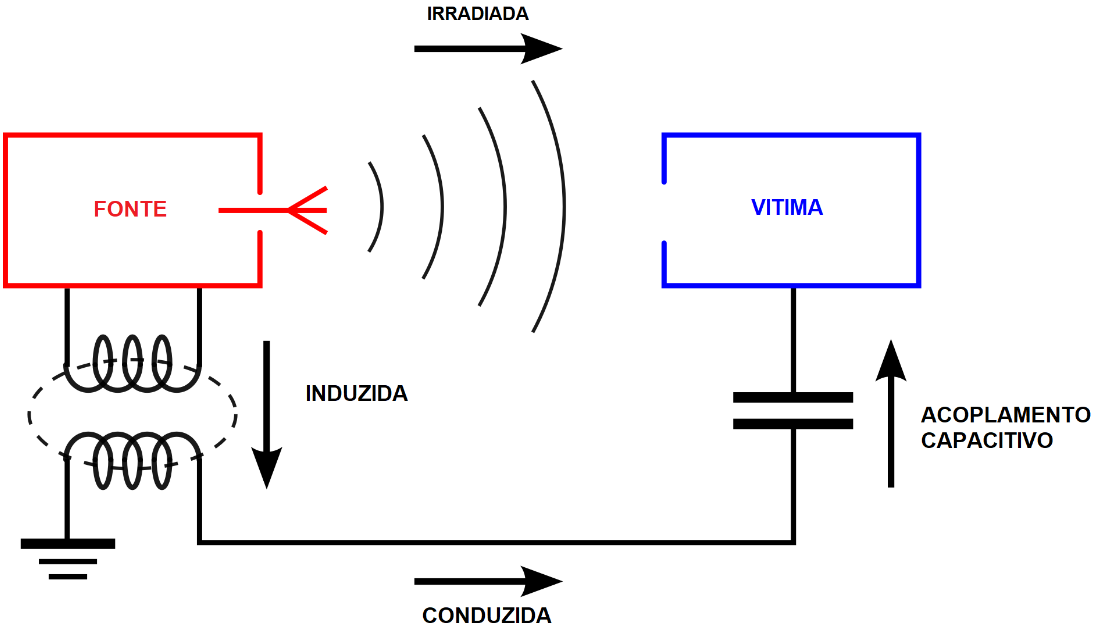
O desenvolvimento de um projeto deve levar em conta vários fatores, mas principalmente o sucesso final, e para isso, as diretivas de compatibilidade eletromagnetica acabam sendo mais importantes que apenas custo baixo. Um grande erro cometido no desenvolvimento de projetos de circuitos eletrônicos, é acreditar que os problemas referentes a EMC podem ser resolvidos depois do produto finalizado. Levando em conta estas definições, é extremamente aconselhável, no processo de desenvolvimento de um circuito eletrônico, antes de dar o mesmo como finalizado, a construção de protótipos. Nestes protótipos, vários testes podem ser realizados, no proprio cenário de uso do referido produto, trazendo para os desenvolvedores a visão real do comportamento, suas possíveis falhas e a possibilidade das correções ainda no ambiente da engenharia.

2.8 A susceptibilidade eletromagnética.

Todo o projeto deve garantir que o produto final seja imune aos ruídos eletromagnéticos existentes no meio ambiente, assim sendo, é importante que atenda as premissas de EMC, sejam elas voltadas às funcionalidades, sejam relacionadas à construção, relacionadas aos ambientes onde irão ser instalados ou mesmo a um conjunto de todas estas demandas. Ser capaz de prever se um evento transitório pode interferir na funcionalidade normal do sistema eletrônico e pode causar um mau funcionamento ou até destruição, pode ajudar a definir a proteção durante a fase de concepção e desenvolvimento do sistema.

A segurança e a confiabilidade dos sistemas eletrônicos embarcados são tão importantes como sua capacidade de funcionar corretamente sem sofrer interferências indevidas geradas por distúrbios eletromagnéticos. Entre a variedade de distúrbios que podem interferir com o funcionamento normal de um sistema eletrônico, estão os ruídos do tipo EFT / BURST, definido na norma IEC 61000-4-4 (IEC-61000/4-4, 2015), sendo estes os mais ameaçadores (BAUER; DEUTSCHMANN; WINKLER, 2015). Como mostrado na Figura 10, existem vários tipos de acoplamentos que geram diferentes tipos de interferências nos circuitos eletrônicos.

Figura 10 – Exemplo de 4 tipos de acoplamento de ruídos.



Fonte: (ARORA, 2011).

Um projeto de hardware que envolve circuitos integrados processadores e drivers de comunicação, deve levar em conta as diretivas focadas em EMC, uma vez que estes circuitos são suscetiveis a tipos de ruídos como o EFT (ARORA, 2011) entre outros.

Para aumentar a criticidade deste projeto, o mesmo foi utilizado para a injeção de ruídos EFT na comunicação CAN, CAN-FD e FlexRay, ou seja, o projeto recebeu uma carga extra de preocupação no que tange aos cuidados com EMC.

Em projetos de circuitos eletrônicos e, principalmente em projetos de circuitos impressos, sempre devem ser observados os itens tidos como principais nas emissões de ruídos. Um destes itens chaves é a corrente, pois com o aumento de velocidade dos processadores, o aumento de consumo de corrente é proporcional, e esta corrente circulando por trilhas que podem formar um loop, geram campo magnético proporcional ao tamanho desta área e a corrente circulante. Como o sinal de comunicação e de acionamento dos pinos do processador se alternam, a corrente se alterna também, criando a oscilação necessária para a criação do referido campo magnético e, consequentemente gerando ruídos internos na própria PCB. Na equação 1 é mostrada a relação entre o ruído EMI, a corrente e a área do loop.

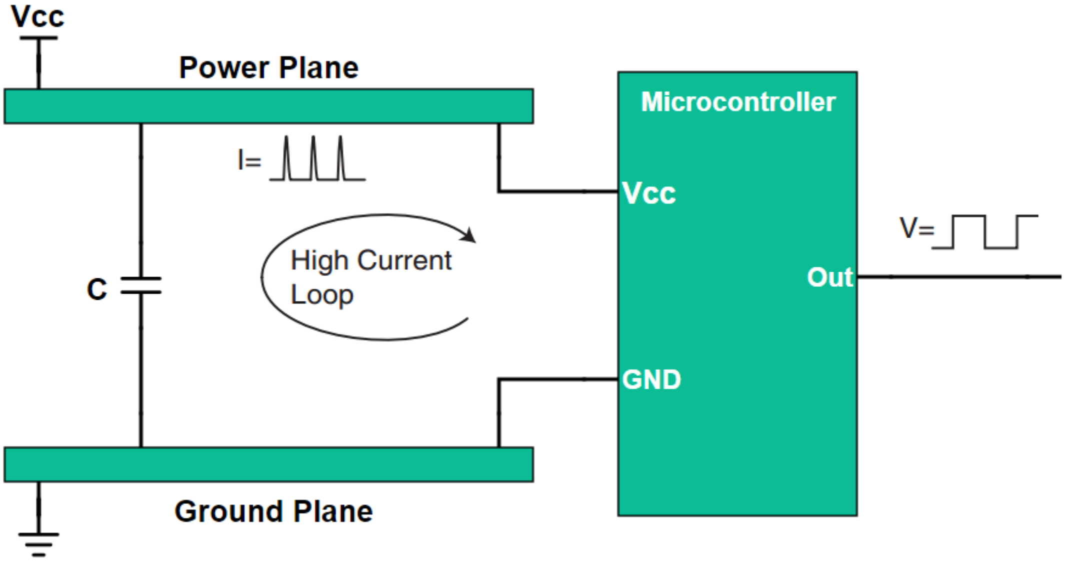
$$EMI(V/m) = kIAf^2 \tag{1}$$

Onde:

k = Constante de proporcionalidade
I = Corrente (A)
A = Area do loop (m^2)
f = Frequência (MHz)

Na Figura 11 pode-se observar a formação do loop de corrente, cuja variação gera o ruído.

Figura 11 – Exemplo do loop gerador de ruído.



Fonte: (ARORA, 2011).

2.9 Normas, certificações e regulamentações sobre EMC

Existem muitas normas que abordam projetos, construção e ensaios de circuitos eletrônicos visando a imunidade à ruídos e a EMC. O caso em questão é diretamente afetado por ruídos referente a compatibilidade eletromagnética, desta forma, o projeto foi baseado nas normas listadas na Tabela 3.

Tabela 3 – Tabela da norma IEC 61000 e suas áreas relacionadas.

Norma	Descrição
IEC 61000-3-2	Limites de emissões de harmônicos na corrente
IEC 61000-4-3	Teste de imunidade a radiação de rádio frequência
IEC 61000-4-4	Teste de imunidade a EFT/Burst
IEC 61000-4-5	Teste de imunidade a Surge
IEC 61000-4-6	Teste de imunidade a distúrbios conduzidos de rádio frequência

As normas acima são baseadas nas normas ISO 7637:2002 (ISO-7637, 2002), que abordam as condições para os testes e os equipamentos a serem utilizados nas simulações. As normas em si focam no produto final como um todo, e não nos subcircuitos que o compõe, entretanto, como os testes propostos nos ensaios de susceptibilidade dos protocolos levam em consideração diversas etapas, o projeto dos hardwares necessários para a realização dos ensaios observou estas normas de forma individual, ou seja, por circuito. Sendo assim, tanto o hardware responsável pela geração dos pulsos EFT como o harware que contém os drivers de comunicação foram projetados, construídos e testados obedecendo as normas listadas acima, porém com especial atenção a norma IEC 61000-4-4 (IEC-61000/4-4, 2015). Esta norma merece destaque neste trabalho, pois o objetivo dos ensaios é focado em ruídos do tipo EFT, justamente o que é tratado nesta norma. Como se trata de ensaios com injeção de EFT/Burst, a norma exige que alguns parâmetros sejam obedecidos, tanto no que se refere aos pulsos propriamente ditos, instrumentos e as condições climáticas, como os parâmetros mostrados na Tabela 2.9.

Tabela 4 – Condições climáticas para ensaios da IEC 61000-4-4.

PARÂMETRO	VALOR
Temperatura ambiente	15°C até 35°C
Humidade Relativa	25% até 75%
Pressão atmosférica	80 kPa até 106kPa

Vários outros parâmetros são exigidos pelas normas, no que se refere ao hardware de teste, bem como aos instrumentos utilizados para coletar os dados, porém estes itens serão abordados mais a frente neste trabalho.

3 TRABALHOS RELACIONADOS

3.1 Trabalhos relacionados aos protocolos ensaiados

É possível encontrar na literatura publicada recentemente, trabalhos focados em mecanismos que tem como objetivo principal reduzir ou eliminar o impacto de ruídos do tipo *EFT* em sistemas embarcados. o desenvolvimento de redes intra veiculares serão destacados neste trabalho, uma vez que o foco aqui é identificar os problemas causados por ruídos na comunicação nas redes intraveiculares.

Em (PIPER et al., 2015) o trabalho relatado discute uma abordagem de monitoramento de tarefas visando proteger tarefas críticas da interferência com garantias de desempenho temporal. A abordagem é baseada na Norma ISO 26262 (ISO-26262, 2018). A proposta visa destacar as diferenças em relação às ferramentas existentes, como o uso da arquitetura de sistemas abertos automotivos, o que também permite esse monitoramento. No entanto, não considera monitorar tarefas críticas que podem propagar erros.

Em (MARQUES et al., 2012), é apresentado um trabalho que utiliza comunicação com uma janela de tempo flexível no protocolo *CAN* (FTT-CAN). Este trabalho propõe uma abordagem de programação de tráfego on-line na qual retransmissões são agendadas com base na janela de tempo restante devido o tráfego. São adicionadoas ferramentas de monitoramento de falhas ao protocolo *FTT-CAN* para monitorar a atividade do barramento e retransmitir mensagens omitidas, com o único foco em redundância temporal, visando tratar erros de comunicação em sistemas acionados por tempo. Este trabalho não foca em identificar as falhas e nem tampouco suas origens.

Outro trabalho relevante na área é relatado em (MARQUES et al., 2014), também baseado no *FTT-CAN*, apresentando uma abordagem na qual a rede transmite suas mensagens em instantes de tempo especificados combinando uma abordagem TT com programação de tráfego online. Esse recurso permite o uso da redundância temporal com retransmissões de mensagens desencadeadas pela ocorrência de erros.

Seguindo os mesmos princípios dos trabalhos acima mencionados, o trabalho proposto em (PATTANAIK; CHANDRASEKARAN, 2012) apresenta um modelo de recuperação e previsão de confiabilidade em sistemas embarcados automotivos baseados no protocolo *CAN*. O modelo foca na interação de diferentes módulos de software responsáveis por tarefas críticas. São utilizados cálculos para definir a probabilidade de falha de acordo com o registro de eventos específicos. O modelo considera várias fontes de falha que são indexados e analisados com um algoritmo de previsão. O mecanismo é avaliado verificando a ativação periódica de módulos de redundância diferentes.

Em (FONTANA; HUBING, 2015), o trabalho foi baseado no estudo do impacto de ruídos do tipo *EFT* na comunicação *CAN*, porém com ênfase na susceptibilidade dos drivers de comunicação (hardware), e não nos impactos referentes ao protocolo em si.

Este trabalho levou em conta os dados coletados por (PANNILA; EDIRISINGHE, 2014), onde foram elaborados ensaios com o objetivo de identificar os ruídos gerados de forma espontânea através de tarefas comuns no interior do veículo (Ignição, Ar Cond., Farol). Os dados dos transitórios medidos nas três principais operações são apresentadas com um tempo de duração do pulso e pico de amplitude em volts. Apesar do valor inerente a estes dados, eles não estão relacionados ao desempenho do protocolo (jitter, pacotes perdidos) e seu impacto nas restrições temporais de execução das tarefas.

O trabalho em (HUANG et al., 2016) apresenta o estudo de falhas transistórias em uma aplicação específica. Apresenta uma proposta de esquema tolerante a falhas com inteligência incorporada e resiliente a coordenação para um sistema "break-by-wire"(BBW). É baseado na análise das características de propagação de falhas transitórias. O experimento conduzido tem como objetivo avaliar o desempenho do sistema BBW em um barramento de comunicação baseado no protocolo TTCAN lançando mão de falhas simuladas usando um analisador/simulador *CAN*. Neste experimento, as falhas transitórias são simuladas, não se tratando de injeções reais sistema.

Em (KER; YEN, 2010) é enfatizada a proteção do sistema contra ruídos do tipo *EFT* com o objetivo de detectar sinais positivos e negativos dos transientes. Como resultado deste artigo, a imunidade à ruídos tipo *EFT* é melhorada, concentrando-se nos componentes semicondutores do tipo CMOS. O problema gerado pelo ruído *EFT* é abordado, porém não à nível de protocolo, mas sim dos efeitos causados sobre os circuitos integrados. A análise das falhas criadas no protocolo precisam ser abordadas como item principal da pesquisa.

De maneira semelhante, em (KELKAR; KAMAL, 2014), os autores desenvolveram um diagnóstico de falhas técnicas para mitigar seu impacto em um sistema distribuído baseado em CAN. Um algoritmo adaptativo de diagnóstico de falhas foi criado, para detectar nós defeituosos na rede e ao mesmo tempo, permita um novo ponto de entrada do nó durante um ciclo de diagnóstico. Os resultados deste artigo fornecem evidências da possibilidade de se fazer um diagnóstico em tempo real. No entanto, se o diagnóstico for correlacionado com falhas e eventos transitórios como EFT, é possível fazer melhorias por meio de novos mecanismos de diagnósticos.

O trabalho de (YIN; HUANG, 2015) apresenta uma análise de desempenho para um sistema de suspensão de veículo, com base em um método para detecção de falhas através de isolamento do defeito. O método usa dados coletados de quatro acelerômetros instalados nos cantos do veículo. O cálculo é feito com base em uma técnica que distingue os dados bons dos dados com falha, para tal, é utilizado um algoritmo de lógica "fuzzy"para os cálculos. O desempenho e eficácia do método são demonstrados por simulação em um sistema de referência. Apesar de suas contribuições, o referido trabalho não considera dados reais de redes veiculares. Por outro lado, a análise prática aqui apresentada mostra a importância da confiabilidade e segurança desses sistemas.

O estudo realizado em (LANGE et al., 2016) foi baseado na crescente necessidade para o uso de vários elementos diferentes embutidos nos veículos, que pode exigir interconexão entre diferentes barramentos, como *CAN, CAN-FD e FlexRay*, com o uso de conversores de protocolo (gateways). O uso desse tipo de mix bus, combinado com o uso de gateways, pode aumentar a suscetibilidade da comunicação ao ruído e à coexistência de atrasos no ambiente onde esses sistemas estão instalados (bem como aqueles incluídos pelos novos componentes). No entanto, os parâmetros de comunicação (Jitter, latência, perda de pacotes etc.) e ruído do tipo *EFT* não foram levados em consideração em seu estudo, e além disso, os dados coletados foram obtidos por meio de simulações.

Outro estudo significativo na área é descrito em (WOO et al., 2016), onde uma arquitetura de segurança foi projetada para o veículo com base no protocolo *CAN-FD*, que inclui os requisitos da ISO 26262. Este documento fornece um design de gerenciamento, criptografia de dados e protocolos de autenticação para o *CAN-FD* e conduziu uma análise de desempenho da arquitetura de segurança com base em um modelo avançado. No entanto, este trabalho avaliou o protocolo *CAN-FD* de uma perspectiva de segurança, mas não conseguiu abordar a questão do ruído, da interferência e seus efeitos no desempenho do protocolo, que estão relacionados aos fatores de segurança abordados pela norma supra citada.

O trabalho em (LIU; BAI; ZHEN, 2017) apresenta um mecanismo de retransmissão imediato para a recuperação de erros transitórios em mensagens críticas de sistemas de segurança acionadas por tempo em uma rede FlexRay. O trabalho utiliza um método estatístico de análise de probabilidade de falhas, e a retransmissão é determinada com uma análise de tempo. Os autores enfatizam que, com falhas transitórias, erros de bits são inevitáveis nos atuais cabos trançados, gerando erros de comunicação. Apesar das contribuições, o trabalho não considera falhas transitórias especificamente em mensagens críticas e ele não aborda falhas geradas por ruídos do tipo *EFT*.

Outro trabalho relevante neste sentido é (LEE et al., 2018), que apresenta um algoritmo de agendamento focado na confiabilidade, para melhorar a comunicação FlexRay. O método reduz a probabilidade de falhas transitórias em um ciclo de clock usando um mecanismo de retransmissão para melhorar a complexidade do tratamento dos dados, usando o método da tabela de pesquisa, para garantir que o sistema tenha uma confiabilidade dentro dos patamares aceitáveis para este protocolo. No entanto, os testes não consideram transientes reais e falta uma análise de redes embarcadas reais de veículos.

Tabela 5 – Resumo dos trabalhos relacionados

Referência.	Foco do trabalho	Oportunidades de melhoria
(PANNILA; EDIRISINGHE, 2014)	Estudo de transientes elétricas geradas no sistema elétrico do veículo.	O trabalho não considerou o impacto das transientes na comunicação.
(FONTANA; HUBING, 2015)	Análise do impacto de ruídos EFT nos transceivers CAN.	Os testes levaram em consideração apenas os impactos nos drivers de comunicação.
(PIPER et al., 2015)	O trabalho avalia o monitoramento de tarefas criticas sob interferências elétricas.	Os testes focam na diferença das ferramentas de testes utilizadas para avaliar a comunicação.
(MARQUES et al., 2012)	Este trabalho utiliza uma ferramenta de retransmissão em função de uma janela de tempo flexível.	Os testes focam apenas em um método de retransmissão de dados perdidos.
(MARQUES et al., 2014)	Este trabalho utiliza uma função de retransmissão baseada em TT e ET.	O trabalho está baseado na retransmissão de dados perdidos ou em função de eventos.
(PATTANAIK; CHANDRASEKARAN, 2012)	Este trabalho foca interação entre diferentes módulos na rede e um cálculo de probabilidade de falha.	Os testes foram conduzidos considerando apenas a capacidade de redundância, não observando os impactos na comunicação.
(HUANG et al., 2016)	O trabalho apresenta um estudo de método tolerante à falhas sobre o protocolo TTCAN	Todo o trabalho foi baseado em simulações e não levou em conta as normas.
(KER; YEN, 2010)	O trabalho enfatiza a necessidade de proteção do barramento contra ruídos do tipo EFT.	O foco do trabalho é sobre os componentes CMOS do hardware de comunicação, não foi observada a performance da comunicação frente aos ruídos EFT.
(YIN; HUANG, 2015)	O trabalho apresenta um estudo para minimizar os impactos de transitórios na comunicação baseado no isolamento do problema.	Os testes não levaram em conta a rede de comunicação ou os protocolos em si.
(LANGE et al., 2016)	Este trabalho foi baseado nas redes híbridas existentes e a sua susceptibilidade a ruídos	A performance da rede frente à ruídos do tipo EFT ou mesmo as métricas de Latência e Jitter não foram analisadas.
(WOO et al., 2016)	Este trabalho focou na arquitetura de uma rede CAN-FD aplicada à segurança intraveicular	A performance da rede frente à ruídos não foi avaliada.
(LIU; BAI; ZHEN, 2017)	Este trabalho apresenta um mecanismo de retransmissão baseado na janela de tempo.	Este trabalho não considera os ruídos tipo EFT e seus impactos.
(LEE et al., 2018)	Este trabalho apresenta um algoritmo de retransmissão de dados tolerante à falhas no protocolo FlexRay.	Este trabalho não considera transientes reais e análise em redes físicas também reais.
[Este trabalho]	Desenvolvimento de hardware para testes de acordo com a ISO 62228 para análise do impacto na comunicação dos protocolos CAN, CAN-FD e FlexRay.	(Implementações) Testes realizados em cenários físicos com bases reais, com hardware dedicado e de acordo com as normas ISO 62228 e IEC 26262 e suas bases.

3.2 Contribuições deste trabalho

Como pode ser observado nos artigos acima listados, existem vários trabalhos que focam na questão da confiabilidade da comunicação, quando se aborda assuntos como itens de segurança e itens com restrições temporais críticas. Porém estes trabalhos estão direcionados para a questão física da comunicação, ou seja, focam nos componentes de hardware, sejam eles transceivers ou controladores, mas não abordam as questões principais da comunicação, que é a troca dos dados de forma segura e confiável.

Seguindo esta linha de raciocínio, este trabalho propõe a construção de dois hardwares com funções distintas e que atendam os princípios apontados nas normas IEC 62228 e ISO 26262, com o objetivo de ensaiar em canários controlados, para capturar dados decorrentes das interferências geradas pelos ruídos inseridos no barramento de comunicação.

Estes dados coletados, poderão ser utilizados, no futuro, para a elaboração de mecanismos de redução ou mitigação das falhas acarretadas pela existência de ruídos *EFT* nos barramentos de comunicação.

4 PROPOSTA DE TRABALHO

4.1 Visão Geral

Como já citado anteriormente, o objetivo deste trabalho é permitir que sejam efetuados ensaios com o entuito de avaliar a susceptibilidade dos protocolos embarcados à falhas, que no caso específico, serão falhas do tipo ruídos *EFT*.

As malhas de controle estão cada vez mais atreladas a capacidade de comunicação dos barramentos, e desta forma, são susceptíveis aos problemas inerentes destes barramentos. Como os veículos estão utilizando de forma crescente ECUs com restrições temporais cada vez mais justas no tempo de uso e resposta, toda e qualquer interferência que atrase a comunicação ou mesmo faça com que informações sejam perdidas, precisa ser diminuída e se possível, erradicada.

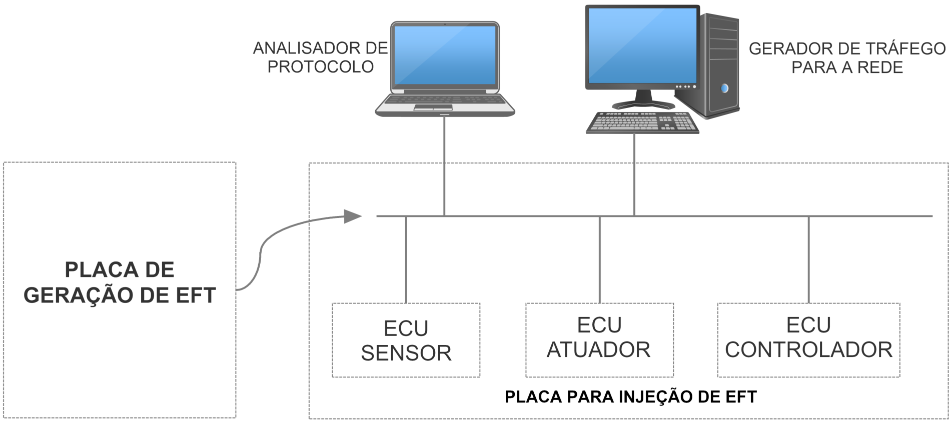
Levando em consideração estas premissas da comunicação, e tendo em vista que os testes, para que possam ter um significado real e fidedigno, todo e qualquer procedimento a ser realizado com os barramentos de comunicação, precisam ser baseados em normas e procedimentos certificados pela comunidade científica internacional. Com base nestes dados, este projeto buscou subsídios nos requisitos existentes nas normas que regem procedimentos de teste com drivers de comunicação e com os seus respectivos barramentos, para a elaboração de hardware e de procedimentos que atendessem estas normas, e também fossem suportados por normas específicas para testes com ruídos injetados, irradiados e conduzidos.

Desta forma o projeto foi totalmente baseado em construir um "set up" de hardware que atenda aos requisitos das normas IEC 62228 (IEC-62228, 2016) e ISO 26262 (ISO-26262, 2018) e suas respectivas normas de suporte, como a IEC 61000-4 (IEC-61000/4-4, 2015) e a ISO 7637-1 (ISO-7637, 2002), e executar os ensaios com base nestas normas, para que, de posse dos dados coletados, fosse possível avaliar a real susceptibilidade dos protocolos *CAN, CAN-FD e FlexRay* aos ruídos do tipo *EFT*.

Neste sentido foram projetados dois hardwares, um com foco na injeção de ruídos do tipo *BURST de EFT* e outro com foco em gerar os pulsos a serem injetados. Desta maneira, foi possível ensaiar vários cenários de injeção de *BURST de EFT*, utilizando uma rede de comunicação real composta de três *ECUs*, rodando software aplicativo real, como o estudo de caso adotado, que foi uma suspensão ativa, no modelo "Quarter Car Model". Nenhum dos ensaios foram realizados através de simulações, tendo em vista o foco do trabalho ser de levar um barramento de comunicação embarcado ao seu extremo e registrá-lo, tanto na questão de carga como na questão de injeção de ruídos.

Conforme cita a IEC 62228-3 (IEC-62228, 2016) e visto na Figura 12, para a realização de um teste relacionado à comunicação em concordância com esta norma, é necessário que exista uma placa única onde, no mínimo 3 drivers de comunicação devem estar montados, em formato estrela, com alimentação externa e que o sinal de interferência eletromagnética seja injetado com acoplamento capacitivo no centro desta estrela na linha de comunicação. Também para a realização destes testes, devem ser utilizados instrumentos com características mínimas definida na norma, como o uso de osciloscópio, com largura de banda mínima de 500MHz.

Figura 12 – Metodologia Geral de Ensaios, segundo a IEC 62228.



Fonte: (IEC-62228, 2016).

Este projeto tem como objetivo principal, criar uma plataforma em concordância com as normas IEC 62228 e ISO 26262, que permita ensaiar barramentos de comunicação padrões da indústria automotiva (*CAN, CAN-FD e FlexRay*, com a injeção de ruídos do tipo *EFT*, gerados de forma controlada e baseados em dados publicados em estudos científicos. Estes ensaios visam coletar dados em diversos cenários diferentes, para cada protocolo e observar o impacto das interferências geradas na comunicação e suas consequências.

Além dos requisitos citados pelas normas acima, outros parâmetros foram considerados para o projeto, como a certificação *AUTOSAR*, muito difundida na industria automobilística, a utilização do sistema operacional de tempo real de plataforma livre (*FreeRTOS*) levando em consideração a observação das restrições temporais das ECUs envolvidas.

O conjunto de dados gerados pelos ensaios, tem como um dos principais objetivos, alimentar um algoritmo desenvolvido para tratar estes dados, e identificar de forma dinâmica e peventivamente as falhas e suas causas. Este algoritmo não é objetivo deste trabalho, pois faz parte da tese de doutorado do mestre Alexandre Roque, deste PPGEE.

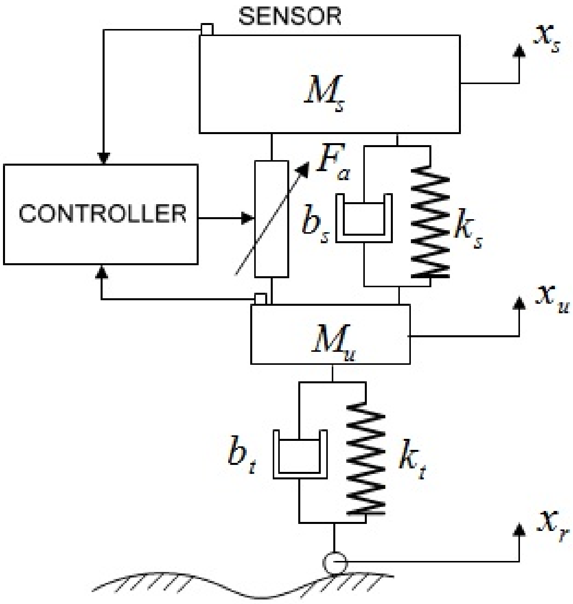
4.2 Detalhamento dos Modelos de Aplicação

4.2.1 Malha de Controle

O hardware projetado deve desempenhar funções idênticas às funções desempenhadas pelas ECUs nos sistemas embarcados nos veículos automotivos. Desta forma, o projeto precisa compreender uma estrutura que possa ser configurada com pelo menos as funções das ECUs que serão abordadas no estudo de caso específico, ou seja, uma suspensão ativa. Focado nesta prerrogativa, se buscou na literatura várias estruturas de controle, que utilizassem os protocolos a serem estudados, como meio de comunicação, e consequentemente, quantas ECUs seriam necessárias para esta finalidade.

Uma das estruturas mais comuns e largamente utilizada em trabalhos é o *Quarter Car Model*(AGHARKAKLI; SABET; BAROUZ, 2012), um modelo composto por um conjunto *massa-mola-amortecedor*, que é utilizado para representar a quarta parte da suspensão ativa de um veículo. Com este modelo, é possível modelar vários ensaios, em diversos cenários, com vários protocolos, sempre considerando o uso de três ECUs (*Sensor, Atuador e Controlador*). Na Figura 13 é visto o modelo "quarter car".

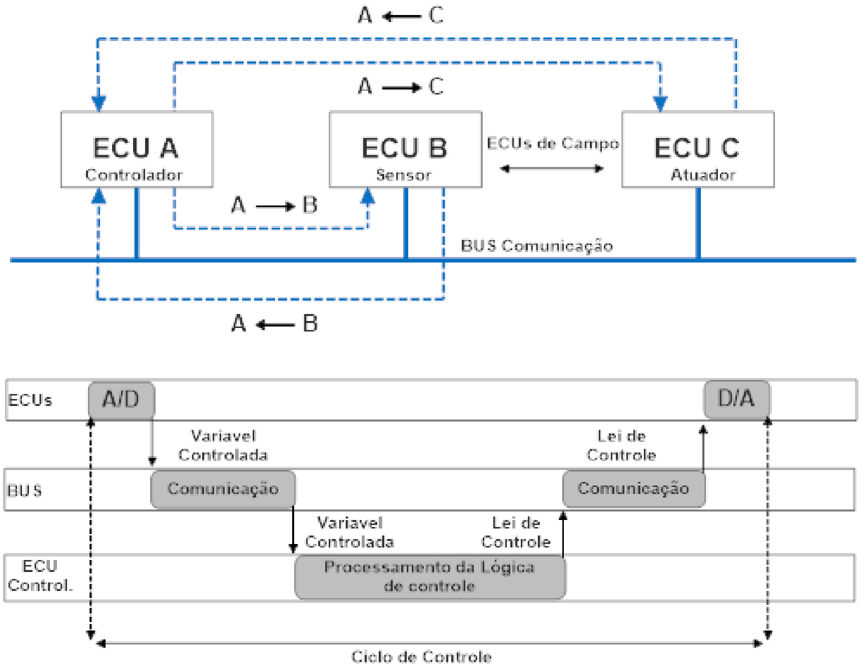
Figura 13 – Modelo *Quarter Car*.



Fonte: (AGHARKAKLI; SABET; BAROUZ, 2012).

O modelo adotado como malha de controle a ser analisado, demanda o uso de três *ECUs*, sensor, atuador e controlador. A *ECU* sensor (A/D) tem a finalidade de ler o valor da posição da suspensão e informar à *ECU* controlador. A *ECU* atuador (D/A) por sua vez, tem a finalidade de receber a informação de posição proveniente do controlador, e informar em caráter de *feedback* ao controlador a posição atual. a *ECU* controlador por sua vez, recebe as informações do sensor e do atuador, calcula a nova posição do atuador de acordo com a lógica, e posteriormente realimenta o atuador com esta nova posição. Este ciclo de comunicação, cálculo e atuação é chamado de *Ciclo de Controle*. Na Figura 14, é visto o esquema deste ciclo.

Figura 14 – Esquema do Ciclo de Controle.



Fonte: Autor

4.2.2 Bus de Comunicação

Como é necessário que a placa para a injeção de EFT contenha os drivers de comunicação, e ao utilizarmos três ECUs devido o conceito adotado, isso significa que o projeto deverá conter três drivers de comunicação para cada protocolo, sendo que o *FlexRay* deverá ter seis drivers (três para o canal A e três para o canal B). Isso define que as três CPU's que serão utilizadas, devem cada uma delas ter, pelo menos, um canal *CAN*, um canal *CAN-FD* e um canal duplo (A e B) *FlexRay*. Estas diretivas delimitaram bastante as opções de processadores compatíveis, sendo que a opção realmente completa (com os três protocolos), não foi localizada.

Seguindo estas prerrogativas, a pesquisa foi direcionada para o atendimento do protocolo *FlexRay*, uma vez que não foi encontrado na forma de circuitos integrados independentes, um controlador para este protocolo. Assim sendo, foram selecionados alguns processadores que continham o controlador para o protocolo *FlexRay*, porém estes não continham as duas versões do protocolo *CAN* desejados. As pesquisas direcionaram para dois processadores, o TMS570LS da Texas e o SPC56 da ST, ambos certificados para o uso do sistema operacional de tempo real "open source"(*FreeRTOS*), ambos com ferramentas de programação e "debug" gratuitas, ambos com as certificações da IEC 61508 e ISO 62228, ambos com os controladores *CAN, LIN, FlexRay e Ethernet*, porém sem o controlador *CAN-FD*. Desta forma, seja qual for a escolha, está definido que um controlador externo de *CAN-FD* deveria ser adicionado ao projeto.

4.2.3 Seleção do processador para o projeto

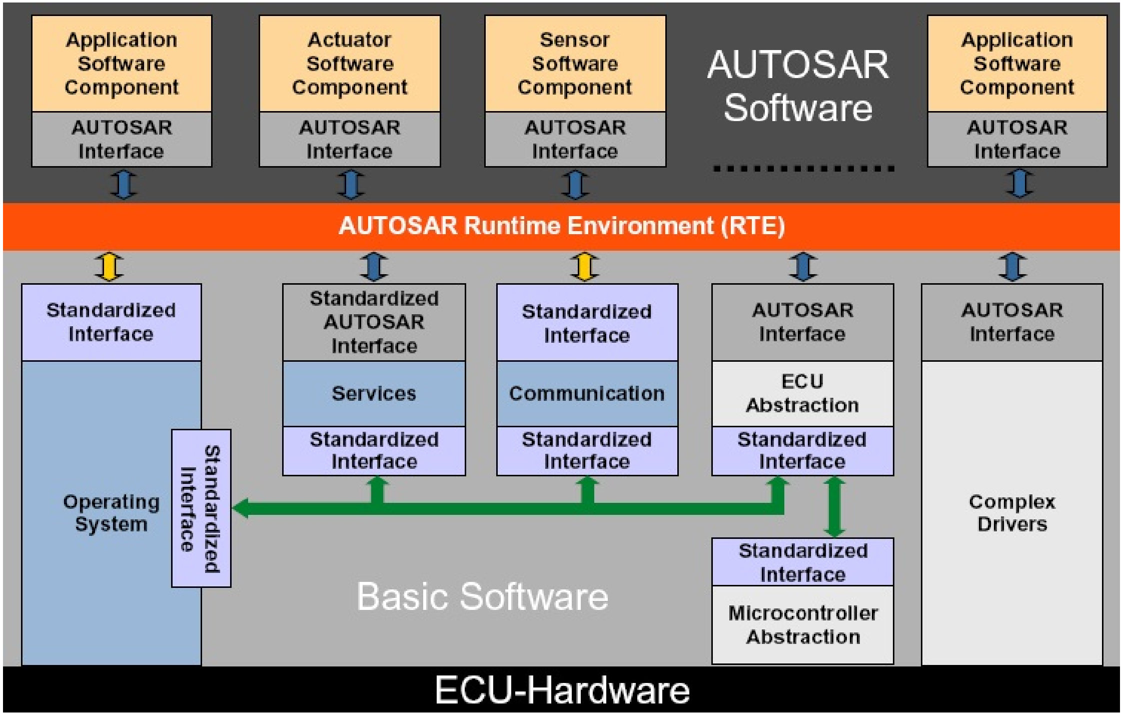
Como dito anteriormente, o projeto de circuitos eletrônicos devem levar em consideração vários fatores demasiadamente importantes, seja a compatibilidade eletromagnética (EMC), seja a certificação em orgãos verificadores ou mesmo o atendimento as normas dedicadas as areas de atuação do referido produto.

No caso da seleção de circuitos integrados como os processadores, além das características citadas, o atendimento a requisitos funcionais de orgãos reguladores ou mesmo a capacidade de executar funções específicas, são determinantes na escolha. No caso do uso de processadores em circuitos embarcados em veículos automotores, estes devem atender a várias normas diferentes, sejam elas referente a confiabilidade, a segurança, a restrições temporais, entre outras. Os dois processadores previamente escolhidos atendem às normas IEC 61508 e ISO 62228, ou seja, ambos seriam uma boa escolha. Porém a escolha estava realmente focada no maior índice de conformidade com as normas e diretivas do mercado automotivo.

Para facilitar esta escolha, foi criado em 2005 o AUTOSAR (AUTOSAR - TECHNICAL OVERVIEW, 2006), um padrão entre montadoras de veículos, fabricantes de circuitos integrados, desenvolvedores de softwares e fornecedores da industria automobilistica.

O AUTOSAR visa facilitar a utilização de componentes de software e hardware entre diferentes plataformas de veículos, OEMs e fornecedores. Para conseguir isso, o AUTOSAR define uma metodologia que suporta um processo de desenvolvimento distribuído e controlado por funções e padroniza a arquitetura de software para cada ECU. O AUTOSAR também especifica interfaces de software compatíveis no nível do aplicativo (FENNEL et al., 2006). A Figura 15 apresenta a arquitetura básica do AUTOSAR.

Figura 15 – Arquitetura básica do AUTOSAR.



Fonte: (AUTOSAR - TECHNICAL OVERVIEW, 2006).

4.2.4 Definição do uso da familia HERCULES® da Texas

Como mencionado anteriormente, a seleção do processador é de extrema importância para o projeto, levando em conta os requisitos de EMC e as especificações da industria automobilistica. Desta forma ficou claro que a escolha do processador deveria passar por um componente já habilitado nestes quesitos, bem como com um mínimo de certificações, e de preferência que fosse certificado AUTOSAR, o que facilitaria o caminho para a implementação dos protocolos a serem auditados.

A escolha por um processador que atendesse as especificações do AUTOSAR praticamente era obrigatório, uma vez que o uso de outros componentes gerariam mais demandas e testes para a homologação do dispositivo. De posse desta definição, a busca se direcionou para processadores que atendiam aos requisitos do AUTOSAR, e também tivessem em seu core as funcionalidades dos protocolos a serem estudados.

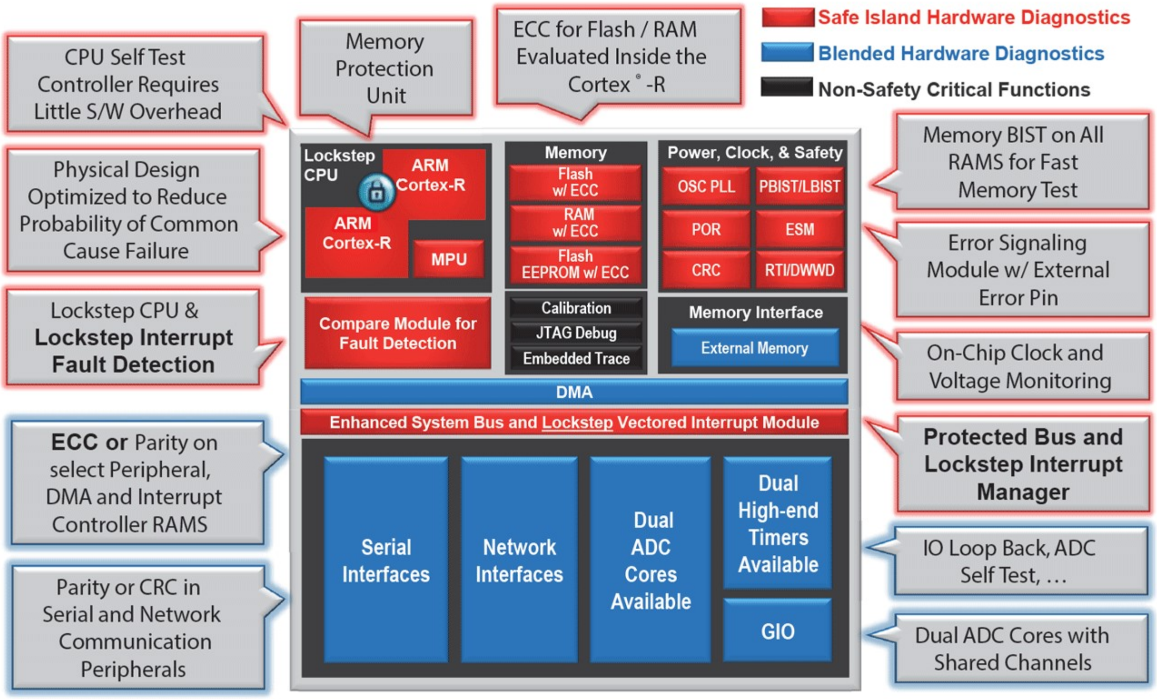
Outra questão importante na definição do processador, eram as compatibilidades e certificações das normas de segurança embarcadas para veículos automotores representadas pela IEC 61508 (IEC-61508, 2010), que aponta os quesitos de segurança tanto em nível de hardware como de software. A pesquisa levando em consideração estes diversos itens eliminatórios direcionou a escolha para a familia HERCULES® da Texas Instruments, e mais especificamente, o processador TMS570LS3137, uma vez que a familia SPC56 da ST, não tem a homologação do AUTOSAR.

Este processador reúne os pré requisitos tanto do AUTOSAR como da IEC 61508, tendo também em seu core 2 canais de comunicação FlexRay, 3 canais de comunicação CAN, 3 canais de comunicação SPI, comunicação Ethernet MAC 10/100 e 1 canal de comunicação LIN.

Trata-se de um processador ARM cortex R4F de 32 bits arquitetura RISC de 180 MHz, com 3 MB de memória FLASH e 256 KB de memória RAM. Este processador tem como aplicações sugeridas pelo fabricante sistemas de freios ABS, sistema de controle de estabilidade eletrônica, controle de direção elétrica, controle de inversores para veículos elétricos e veículos híbridos elétricos, entre outras.

A arquitetura do processador TMS570LS3137 é vista na Figura 16, onde pode-se verificar que as questões referente à segurança foram resolvidas por hardware, aumentando assim a confiabilidade do processador.

Figura 16 – Arquitetura básica do processador TMS570LS3137.


Safe Island Hardware Diagnostics
Blended Hardware Diagnostics
Non-Safety Critical Functions
CPU Self Test Controller Requires Little S/W Overhead
Memory Protection Unit
ECC for Flash / RAM Evaluated Inside the Cortex®-R
Physical Design Optimized to Reduce Probability of Common Cause Failure
Lockstep CPU & Lockstep Interrupt Fault Detection
ECC or Parity on select Peripheral, DMA and Interrupt Controller RAMS
Parity or CRC in Serial and Network Communication Peripherals
Lockstep CPU
ARM Cortex-R
ARM Cortex-R
MPU
Memory
Flash w/ ECC
RAM w/ ECC
Flash EEPROM w/ ECC
Power, Clock, & Safety
OSC PLL
PBIST/LBIST
POR
ESM
CRC
RTI/DWWD
Compare Module for Fault Detection
Calibration
JTAG Debug
Embedded Trace
Memory Interface
External Memory
DMA
Enhanced System Bus and Lockstep Vectored Interrupt Module
Serial Interfaces
Network Interfaces
Dual ADC Cores Available
Dual High-end Timers Available
GIO
Memory BIST on All RAMS for Fast Memory Test
Error Signaling Module w/ External Error Pin
On-Chip Clock and Voltage Monitoring
Protected Bus and Lockstep Interrupt Manager
IO Loop Back, ADC Self Test, ...
Dual ADC Cores with Shared Channels

Fonte: (IEC 60730 AND UL 1998 SAFETY STANDARD COMPLIANCE MADE EASIER WITH TI HERCULES MCUS, 2013).

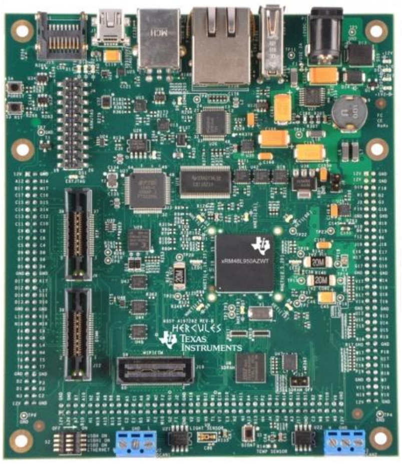
A familia de processadores HERCULES® obtiveram em 2019 a renovação do certificado concedido pela certificadora TÜV SÜD Product Service GmbH, com validade até 2022, referente as normas listadas abaixo:

IEC 61508-1:2010
IEC 61508-2:2010
ISO 26262-2:2018
ISO 26262-5:2018
ISO 26262-7:2018
ISO 26262-8:2018
ISO 26262-9:2018

Após a definição do processador a ser utilizado, outro questionamento que veio à tona é se seria necessário que o projeto da placa de injeção de EFT, que contém os drivers de comunicação, tivesse o processador inserido no projeto da PCB. Este questionamento permeiou as discussões por várias semanas, uma vez que a inclusão do processador na placa, implicaria na necessidade de muito mais depuração no hardware, e somado a isso, este item não fazia parte do objetivo do projeto.

A solução encontrada foi utilizar uma placa de desenvolvimento para o processador, desenvolvida pela própria fabricante Texas, que já teria o hardware do processador, memórias, barramentos e comunicação USB com o computador resolvidos, dimunindo assim os desafios do projeto. Depois da decisão formalizada, a escolha da placa foi rápida, sendo escolhida a TMS570LS31HDK que é mostrada na Figura 17.

Figura 17 – Placa de desenvolvimento TMS570LS31HDK



Fonte: Autor.

Esta placa como já dito, é composta de processador, memória, drivers de comunicação para porta Ethernet, porta USB Host e Device, cartão de memória Micro-SD, LEDs de sinalização da fonte e de GPIOs, drivers CAN (portas CAN-1 e CAN-2), sensores de temperatura e luminosidade. Outro fator de destaque, são os barramentos de comunicação direcionados aos conectores header na parte inferior da placa, o que facilitou a conexão com a placa de injeção que foi projetada.

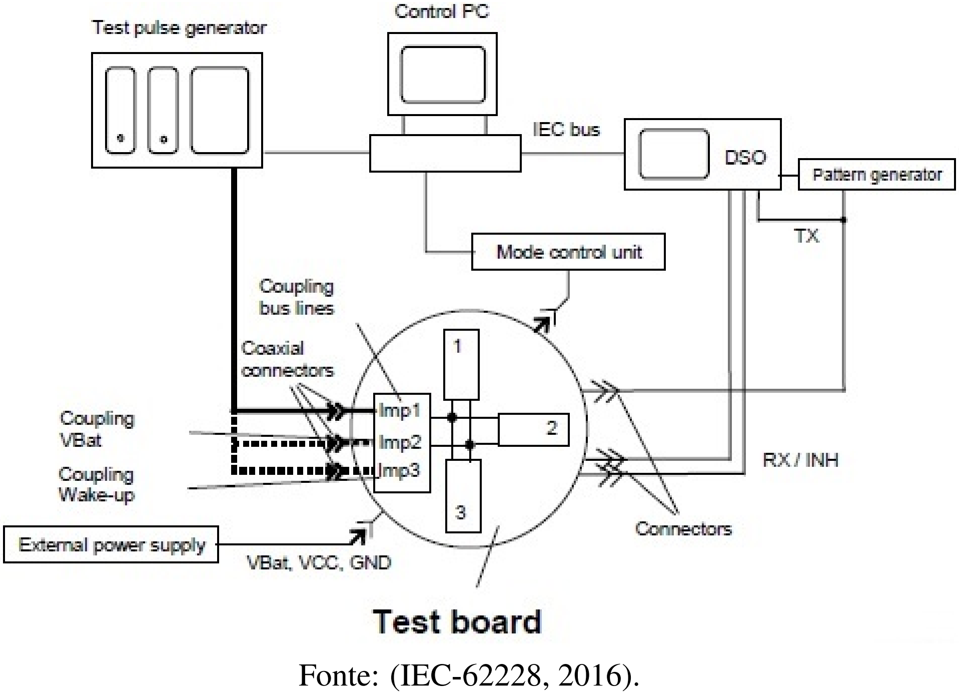
4.3 Projeto da placa principal para injeção de *EFT*

Os processos que envolveram os projetos elaborados para este trabalho iniciaram com os primeiros testes realizados com o protocolo CAN, utilizando os processadores Arduino Mega, com as placas shield de comunicação CAN-BUS da SEED, que utiliza o controlador CAN MCP2515 e o driver CAN MCP2551, ambos da Microchip e uma placa de injeção de ruídos EFT construída com transistores bipolares TIP35C e TIP36C. Com este circuito foram realizados os testes que geraram o artigo publicado na conferência IEEE ICCA/ACA - 2016, em Curicó - Chile (ROQUE et al., 2016) e o artigo publicado no periódico IEEE - Transactions on Electromagnetic Compatibility (ROQUE et al., 2017). Os problemas com este "set-up" de equipamentos era que o mesmo não atendia as normas ISO 26262 e IEC 62228, o qual era o objetivo do trabalho. Devido a isso, nestes artigos, foi citado que os ensaios eram "baseados" nas normas, e não que as atendiam. Nestes artigos, podem ser vistos o circuito eletrônico do injetor de EFT e a foto da placa montada, utilizando uma PCB padrão.

Como já citado anteriormente, existem vários requisitos que devem ser atendidos, para que seja possível homologar um produto, um ensaio, etc., em normas vigentes como um todo, principalmente em normas específicas referente à segurança. Para que fosse possível citar que o hardware e os ensaios estavam em conformidade com as normas ISO 26262 e IEC 62228, o processo deveria ser totalmente reiniciado, com os projetos voltando ao estado inicial de definições e seleção de hardware.

Como o intuito era realizar todos os testes já efetuados novamente, para poder certificar o atendimento às normas, bem como realizar os testes com *CAN-FD e FlexRay*, também em conformidade com as referidas normas, foi definido que o projeto da placa para injeção de EFT acomodaria os três protocolos (*CAN, CAN-FD e FlexRay*). Para tal, o primeiro passo era obter as especificações das referidas normas para a construção do hardware. Na Figura 18 é visto o "set-up"para os testes de susceptibilidade à ruídos injetados no barramento de comunicação, na alimentação ou na linha de "wake-up".

Figura 18 – "Set-up" para testes de imunidade à EFT de acordo com a IEC 62228.



Fonte: (IEC-62228, 2016).

O atendimento à uma norma específica, em alguns casos, traz a necessidade do entendimento das normas que serviram como base, pois muitos itens importantes não estão descritos nas normas "principais" do projeto, mas estão detalhadas nas normas que a basearam. Desta forma, para se afirmar o total atendimento às normas ISO 26262 e IEC 62228, várias outras normas foram pesquisadas, como a norma IEC 61000 e a ISO 7637. Estas duas últimas definem mais especificamente o "set-up" para os ensaios e a característica do hardware a ser testado propriamente dito.

Os primeiros ensaios feitos com o "set-up" já citado, não estavam em conformidade com as normas ISO 26262 e IEC 62228, pois as normas base não eram atendidas e, vários quesitos, entre eles, o osciloscópio utilizado, que foi um osciloscópio digital de 70 MHz. A norma exige para os testes, um osciloscópio com largura de banda mínima de 500 MHz. Com todas estas informações, além das considerações sobre a necessidade do projeto atender a compatibilidade eletromagnética (*EMC*), as sugestões feitas pelas normas sobre o arranjo para os drivers de comunicação, etc., o projeto para o hardware onde as injeções de EFT seriam feitas teve o direcionamento definido.

4.3.1 Definição da placa para injeção de EFT e interligação às CPU's

Apesar de se tratar de um projeto de circuito eletrônico, a parte mecânica é de extrema importância, pois esta parte definie como, onde e de que maneira o projeto será fisicamente acomodado. Neste caso, a opção foi trabalhar com as placas das CPU's e a placa para injeção de EFT (definida como placa principal), sem um envólucro de proteção, apenas utilizando espaçadores para nivelamento das placas.

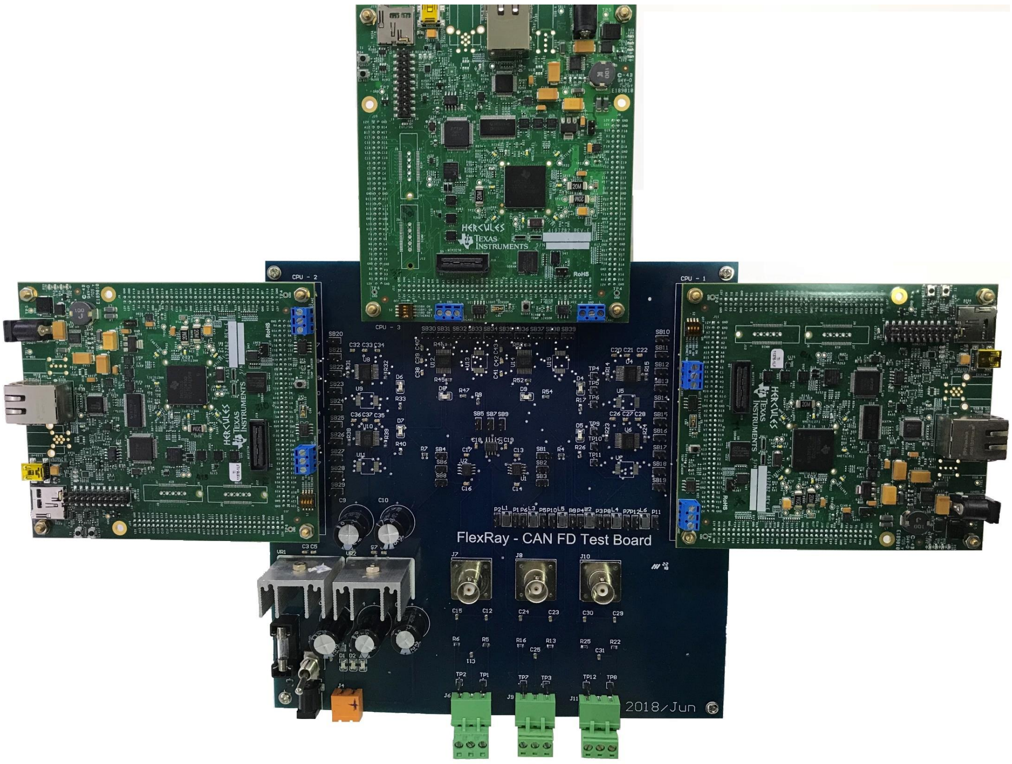
Como as placas das CPU's deveriam ser encaixadas na placa principal através de um conector do tipo "header", que fica na parte inferior da CPU, a placa principal deveria acomodar esta conexão, e ao mesmo tempo permitir uma fixação das placas da CPU. A solução adotada foi utilizar diretamente na placa pricipal os conectores "header"macho e a furação para a fixação das placas da CPU.

Como as placas da CPU tem um tamanho expressivo (110 x 125mm), acomodá-las lado a lado não era uma opção satisfatória, desta forma a opção que melhor atendeu às necessidades operacionais do projeto, e ao mesmo tempo facilitava o atendeimento às normas, era a instalação destas placas na forma de um "T" invertido. Desta forma a conexão dos cabos de injeção seria feita pela parte inferior e as CPU's ficariam acomodadas na parte superior da placa principal, como pode ser visto na Figura 19.

O foco deste projeto foi o desenvolvimento de uma placa para injeção de EFT para o uso com os protocolos *CAN-FD e FlexRay*, uma vez que os ensaios com o protocolo *CAN* já haviam sido concluídos. Como previsto na norma, a placa principal contempla fonte de alimentação externa, neste caso de 12 Vcc, com reguladores internos para as fontes de 5 Vcc e 3,3 Vcc. Como as injeções seriam feitas diretamente na placa, através dos conectores BNC, um conector para a comunicação *CAN-FD* e dois para a comunicação *Flex-Ray* (canais A e B). Nesta versão do projeto, não foram incluídos conectores DB9, para que fosse possível a interligação da placa principal a outros elementos da rede de forma padronizada.

Como já citado anteriormente, as normas fornecem "sugestões"de arranjo, para o projeto de layout das placas de testes, visando auxiliar os projetistas nesta tarefa. Desta forma, conforme a norma IEC 62228, a sugestão de montagem dos drivers de comunicação *CAN-FD* utiliza o formato em "estrela", na Figura 20, é mostrado o layout adotado na placa principal e a sugestão da norma. Por se tratar de uma placa com duas faces, a linha de comunicação *CAN-FD High* é mostrada na face superior, já a linha de comunicação

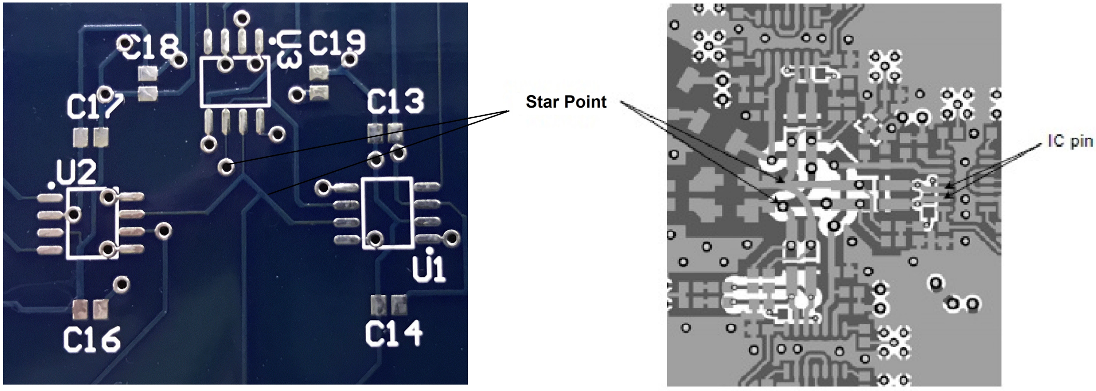
Figura 19 – Placa principal na sua versão inicial.



Fonte: Autor

CAN-FD Low está disposta na face inferior, atendendo o modelo sugerido.

Figura 20 – Ponto estrela na placa principal e na sugestão da IEC 62228.



Placa principal para injeção de EFT

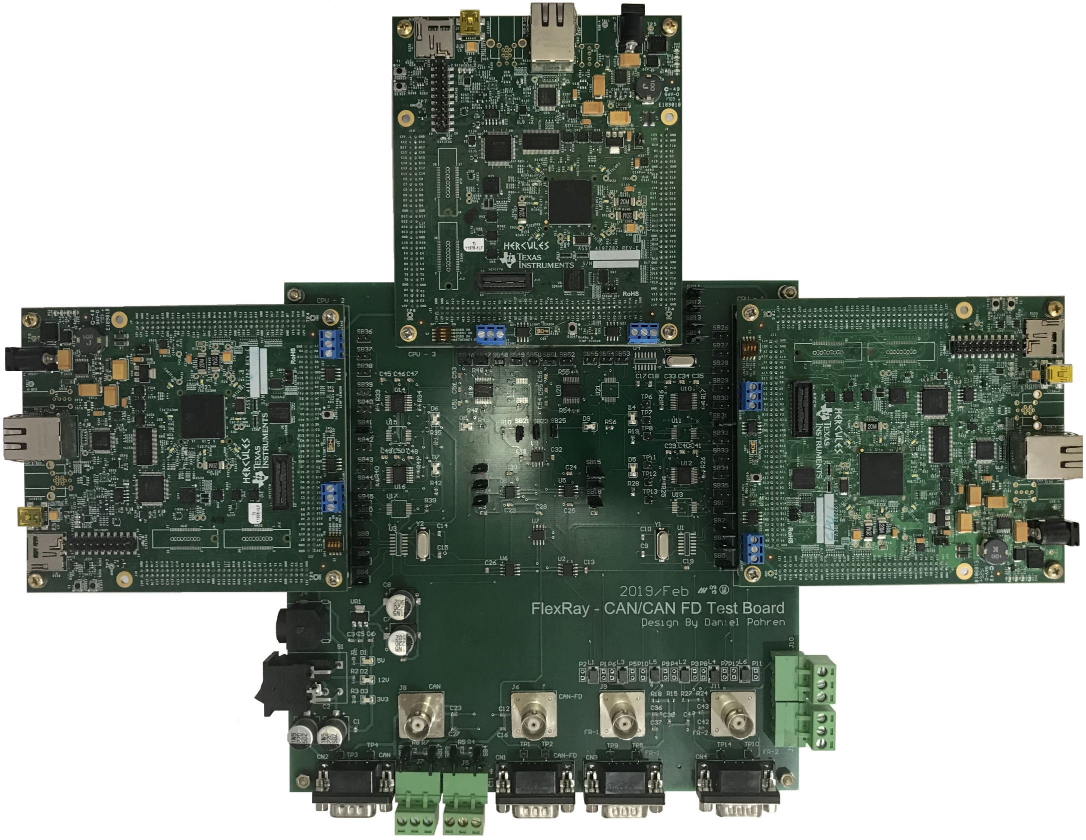
Sugestão de layout IEC 62228

Fonte: Autor

4.3.2 Revisão da placa para injeção de EFT

A versão inicial da placa principal foi utilizada nos ensaios com o protocolo *CAN-FD*, os quais embasaram o artigo publicado na revista *IEEE - Trasactions on Industrial Electronics* (POHREN et al., 2019), porém várias dificuldades foram verificadas: os reguladores de tensão sobreaqueciam, não havia como conectar diretamente os cabos com conectores *DB9*, que são utilizados para interligar os módulos de análise de comunicação *GRID Connect CAN-FD e Vector VN8970*, bem como não tinha sido programado para comportar testes com o protocolo *CAN*. Desta forma, optou-se por projetar e construir a segunda versão da placa principal, resolvendo os itens acima descritos. Nesta nova versão, foi utilizada uma fonte externa chaveada com tensões de 12 Vcc e 5 Vcc, ficando internamente à placa apenas o regulador de 3,3 Vcc. Assim como na versão incial, foram utilizados os controladores MCP 2517 da Microchip, como controladores *CAN-FD*, através da interface SPI (*Serial Peripheral Interface*). Os mesmos principios foram mantidos, o ponto de conexão tipo estrela entre os drivers de comunicação, nesta versão com 2 estrelas (*CAN e CAN-FD*). O layout da placa manteve o mesmo conceito de "T" invertido, com as CPU's sendo conectadas através dos conectores headers na parte inferior das mesmas, conforme pode ser visto na Figura 21.

Figura 21 – Placa principal versão II.



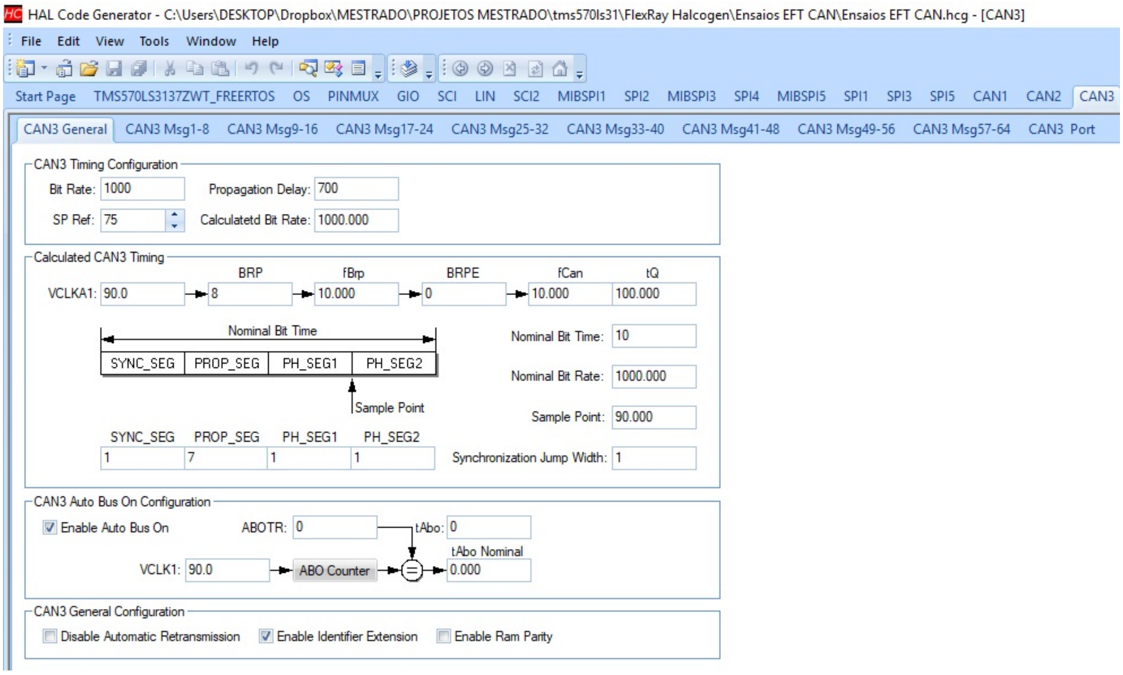
Fonte: Autor.

4.3.3 Programação das funções das ECUs

Após os projetos definidos e a placa para a injeção de EFT montada, era necessária a configuração das ECUs com suas devidas funcionalidades, ou seja, *sensor*, *controlador* e *atuador*. Para tal tarefa, a familia HERCULES® disponibiliza a ferramenta de software

CCS (*Code Composer Studio*), que é a mistura de um compilador para códigos C^{++} e um montador para aplicações pré programadas. Também é disponibilizada uma ferramenta chamada *HALCoGen* (Hardware Abstraction Layer Code Generator), sendo esta última uma ferramenta dedicada às configurações de harware necessárias para a inicialização e as funcionalidades básicas do processador. A ferramenta *HALCoGen* facilita a configuração de todo o hardware do processador, uma vez que a seleção das funcionalidade são feitas de forma gráfica, e após estas seleções, a ferramenta gera automaticamente as pré configurações iniciais do processador. Na Figura 22, pode-se visualizar a tela de configuração inicial do controlador *CAN3* utilizando o sistema operacional *FreeRTOS*. As portas *CAN1 e CAN2* já são utilizadas na própria placa TMS570LS31HDK, com os drivers SN65HVDA5410. Os programas utilizados nos ensaios estão listados nos apendices deste trabalho.

Figura 22 – Tela de configuração de hardware do HALCoGen.



HAL Code Generator - C:\Users\DESKTOP\Dropbox\MESTRADO\PROJETOS MESTRADO\tms570ls31\FlexRay Halcogen\Ensaios EFT CAN\Ensaios EFT CAN.hcg - [CAN3]

CAN3 Timing Configuration

Bit Rate: 1000 Propagation Delay: 700

SP Ref: 75 Calculatetd Bit Rate: 1000.000

Calculated CAN3 Timing

	BRP	fBrp	BRPE	fCan	tQ
VCLKA1: 90.0	8	10.000	0	10.000	100.000

Nominal Bit Time: 10

Nominal Bit Rate: 1000.000

Sample Point: 90.000

SYNC_SEG	PROP_SEG	PH_SEG1	PH_SEG2
1	7	1	1

Synchronization Jump Width: 1

CAN3 Auto Bus On Configuration

☑ Enable Auto Bus On

ABOTR: 0 tAbo: 0

VCLK1: 90.0 tAbo Nominal 0.000

CAN3 General Configuration

☐ Disable Automatic Retransmission ☑ Enable Identifier Extension ☐ Enable Ram Parity

Fonte: Autor.

4.4 Projeto da placa injetora de EFT

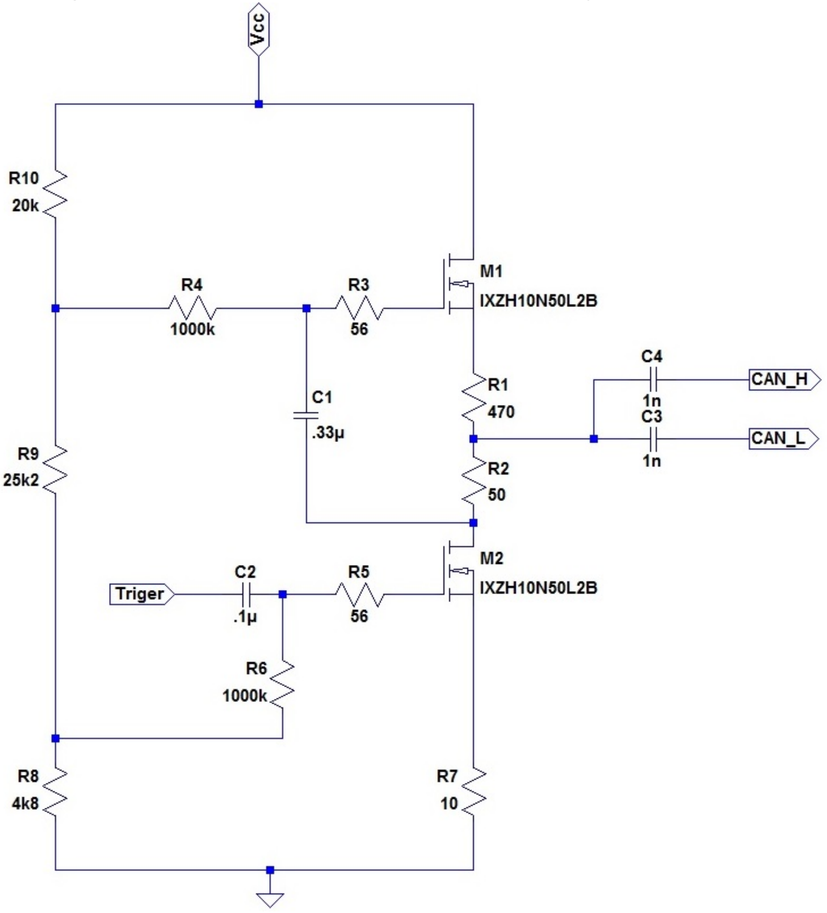
O atendimento às normas exige que o injetor de EFT também obedeça a parâmetros restritos, fazendo com que o uso de componentes comuns não seja viável. Conforme dito anteriormente, o primeiro "set-up" foi projetado apenas levando em consideração as características dos sinais que seriam gerados. As normas demandam características específicas dos componentes, bem como dos sinais gerados, como tempo de subida (*rise time*) e tempo de descida (*fall time*). Os sinais gerados devem ter um tempo de subida inferior a 5ns (cinco nano segundos) com tolerância de +30% (trinta) por cento. Para se alcançar estes valores, os transistores também devem ter estes tempos baixos e ter a capacidade de suportar os níveis de tensão dos pulsos que serão gerados.

4.4.1 Primeira versão do injetor de EFT

Considerando que o protótipo inicial do injetor de *EFT*, que utilizava transistores bipolares como drivers de potência, não atendia as normas que norteiam este trabalho, optou-se por considerar tal hardware como a versão "beta", desta forma, esta é a primeira versão que levou em consideração os tempos de subida (*rise time*) e descida (*fall time*), bem como os valores limites de operação, necessários para o atendimento às normas bases deste projeto. Cabe aqui salientar que a publicação realizada com base naquele set-up de hardware "beta", devido ao não atendimento às normas já citadas, esta publicação não pode referenciar tais normas, o que encorajou o projeto do novo sistema de injeção de **??**.

Focado nestas condições, foi selecionado o transistor do tipo MOSFET para aplicações de RF da *IXYS* modelo *IXZH10N50L2B*, com capacidade de corrente de 10A (amperes) e tensão máxima de V_{DS} de 500 Vcc. Este circuito pode ser visto na Figura 23.

Figura 23 – Versão inicial do circuito de injeção de EFT.



Fonte: Autor.

Neste circuito a tensão a ser aplicada como EFT deve ser o valor da tensão de alimentação do circuito (Vcc), porém o valor correto aplicado deve ser aferido diretamente no circuito, tendo em vista as quedas de tensão do circuito. Este circuito foi aplicado nos ensaios do protocolo *CAN-FD*, onde os resultados foram satisfatórios. Nos ensaios iniciais para o protocolo *FlexRay*, uma instabilidade dos tempos foi observada, fazendo com que o circuito tivesse oscilações de tempos de subida. Levando em consideração esta oscilação, e que os transistores não eram componentes comuns de mercado, optou-se por projetar um circuito novo, partindo do zero.

4.4.2 Segunda versão do injetor de EFT

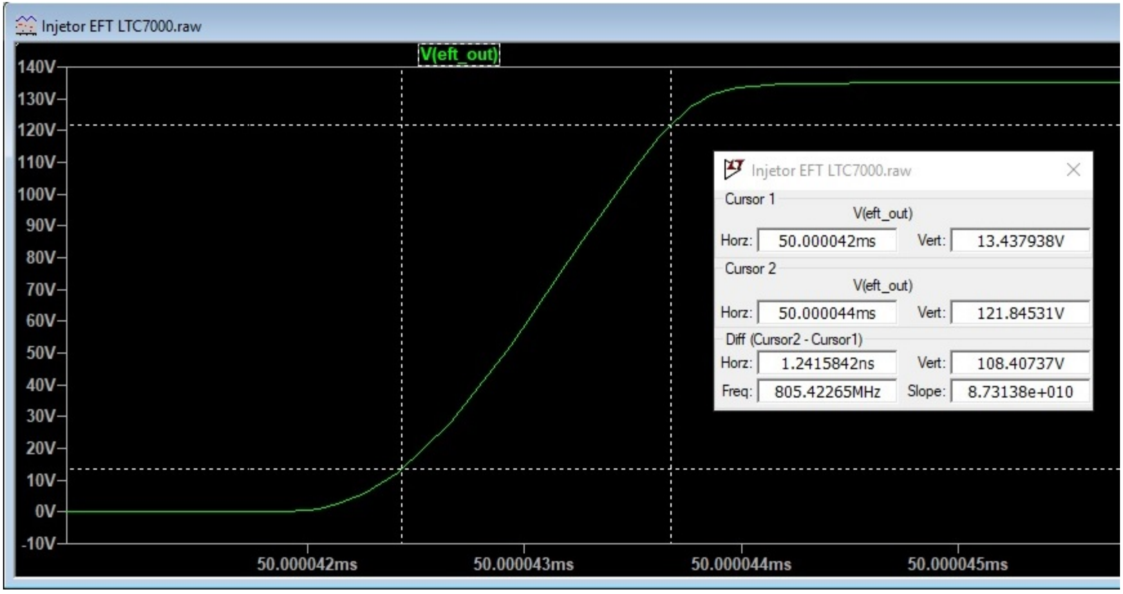
No projeto anterior, a escolha de transistores e do circuito foi baseada em conceitos encontrados na literatura e em *Datasheets* dos fabricantes, porém não foram feitas simulações do circuito. Como o projeto do novo circuito iniciaria do zero, a decisão de iniciar pelas simulações, e só depois partir para a montagem física foi o caminho mais acertado.

Para iniciar o novo projeto, foi escolhido como simulador *SPICE* o LT Spice XVII da Analog Devices$^{\text{TM}}$. Os requisitos para o novo projeto continuavam sendo:

- Tempo de subida (*rise time*) menor que 5ns
- Tensão de operação > 100 Vcc
- Capacidade de corrente > 1 Amp.

De posse destes requisitos, o primeiro parâmetro utilizado como balizador na escolha foi a tensão máxima de operação, no caso do integrado driver para MOSFET utilizado, LTC7000 é de 135 Vcc, sem necessidade do uso de fonte auxiliar. O próximo passo foi a escolha de um transistor compatível com este driver e com os parâmetros acima listados, cuja escolha foi o *BSZ900N20S3* da familia OptiMOS$^{\text{TM}}$ da Infineon. Este conjunto demonstrou nas simulações que os tempos de subida (*rise time*) atendiam perfeitamente os parâmetros exigidos pela norma, como mostrado na Figura 24.

Figura 24 – Simulação dos pulsos EFT/Burst utilizando LTspice.



Injetor EFT LTC7000.raw

Cursor 1
V(eft_out)
Horz: 50.000042ms Vert: 13.437938V

Cursor 2
V(eft_out)
Horz: 50.000044ms Vert: 121.84531V

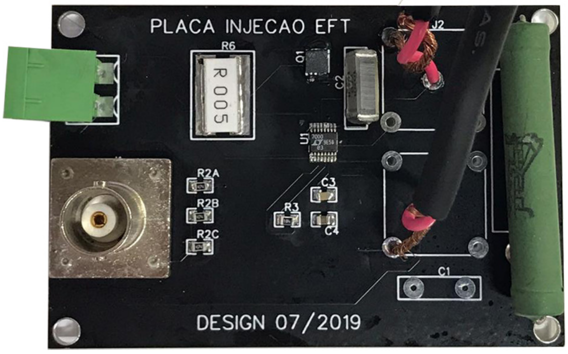
Diff (Cursor2 - Cursor1)
Horz: 1.2415842ns Vert: 108.40737V
Freq: 805.42265MHz Slope: 8.73138e+010

Fonte: Autor.

Como pode ser observado na imagem, esta simulação foi realizada com o valor máximo para este driver, sem o uso de fonte externa, que é de 135 Vcc. Neste caso, o tempo de subida (*rise time*), foi de $\approx$ 1,24ns, bem inferior ao tempo limite que é de 5ns + 30%. O valor do tempo de subida é calculado levando em conta o tempo transcorrido para a forma de onda subir de 10% até 90%, que no caso da simulação, os valores exatos seriam de 13,5 Vcc (10%) e 121,5 Vcc (90%), com uma diferença de tensão equivalente à 108 Vcc.

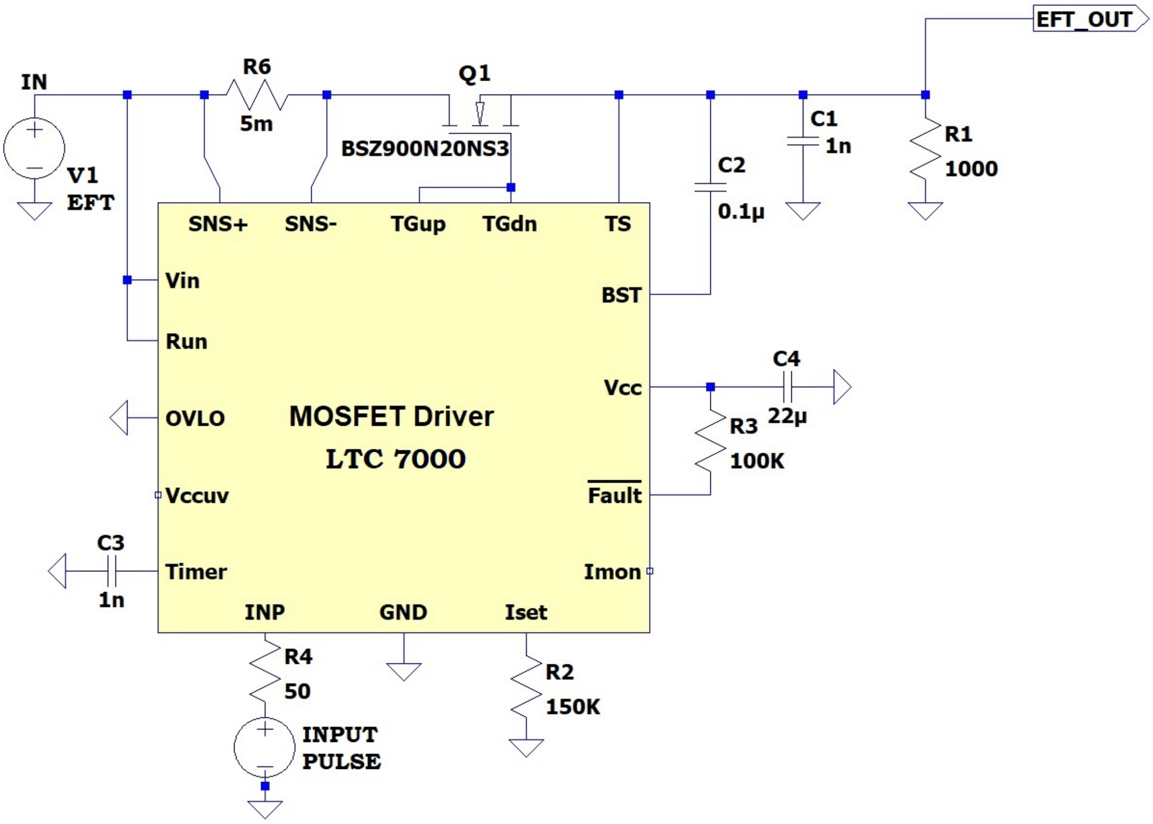
Porém como o movimento dos cursores dá-se de forma manual, os mesmos estão ajustados nos valores de $\approx$ 13,43 Vcc e $\approx$ 121,84 Vcc, com uma excursão entre os pontos de ≈ 108,4 Vcc. Como pode-se observar, esta condição é mais severa do que os valores padrões para os cálculos dos tempos de subida. A placa construída e o circuito utilizado para o injetor de EFT são mostrados nas Figuras 26 e 25.

Figura 25 – Placa montada do injetor de EFT.



Fonte: Autor.

Figura 26 – Circuito do injetor de EFT.



Fonte: Autor.

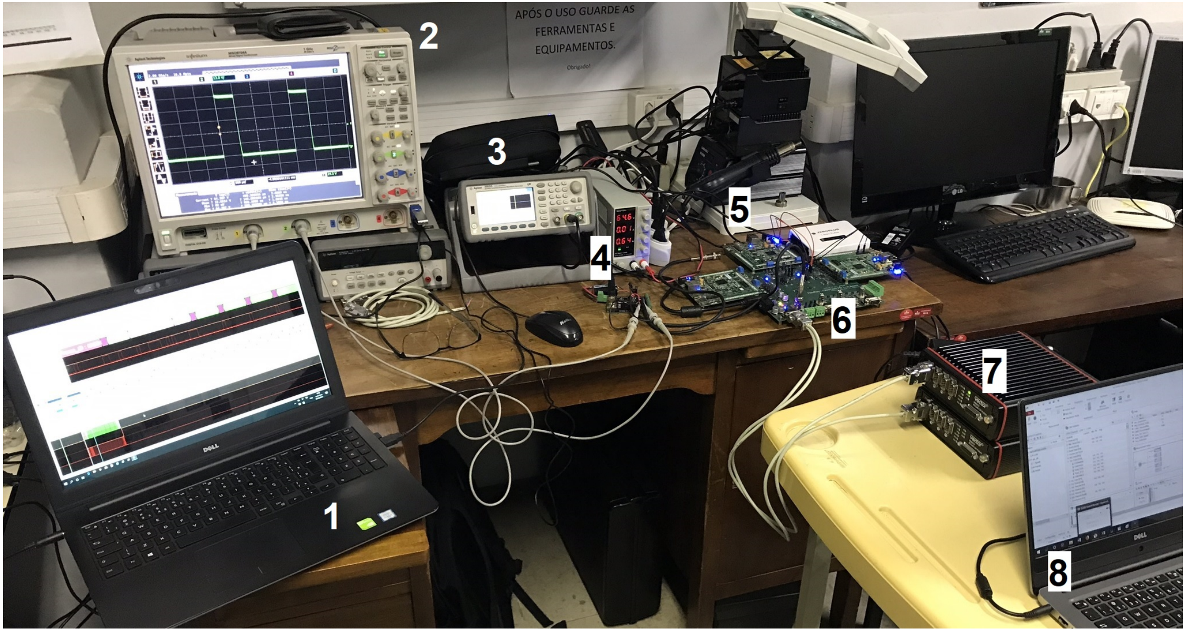
4.5 Set-up montado para os ensaios

Os ensaios realizados com os protocolos *CAN, CAN-FD e FlexRay* foram baseados nos distúrbios gerados pelos ruídos EFT injetados nas linhas de comunicação nas redes acima citadas. Porém o projeto do injetor de EFT construído especialmente para estes ensaios, precisa de alguns equipamentos externos para completar a sua funcionalidade.

O injetor de EFT foi projetado considerando um gerador de pulsos (*BURST*) externo e uma fonte de tensão de EFT externa. Para os ensaios foram utilizados um gerador de funções arbitrário Agilent modelo *33522A* e uma fonte de alimentação chaveada de 0 a 120Vcc x 3 Amp. Para certificar os valores das variáveis ajustadas, foi utilizado o osciloscópio Agilent, modelo *MSO9104A* com varredura de 1GHz a 20 GSa/s. Na Figura 27 pode ser visto o "set-up"completo na sua última versão, onde foram efetuados os testes com os três protocolos. A identificação de cada item é vista na lista abaixo:

1. Programa analisador de protocolos *LAP-C Standard*
2. Osciloscópio Agilente *MSO9104A*
3. Gerador de funções arbitrário Agilent *33522A*
4. Fonte de alimentação chaveada 0 a 120 Vcc x 3 Amp.
5. Placa processador HERCULES$^{\text{TM}}$ *TMS570LS31HDK*
6. Placa principal para injeção de EFT
7. Módulos *VN8900* Vector
8. Programa analisador de comunicação *CANoe* Vector

Figura 27 – Set-up completo para os ensaios.



Fonte: Autor.

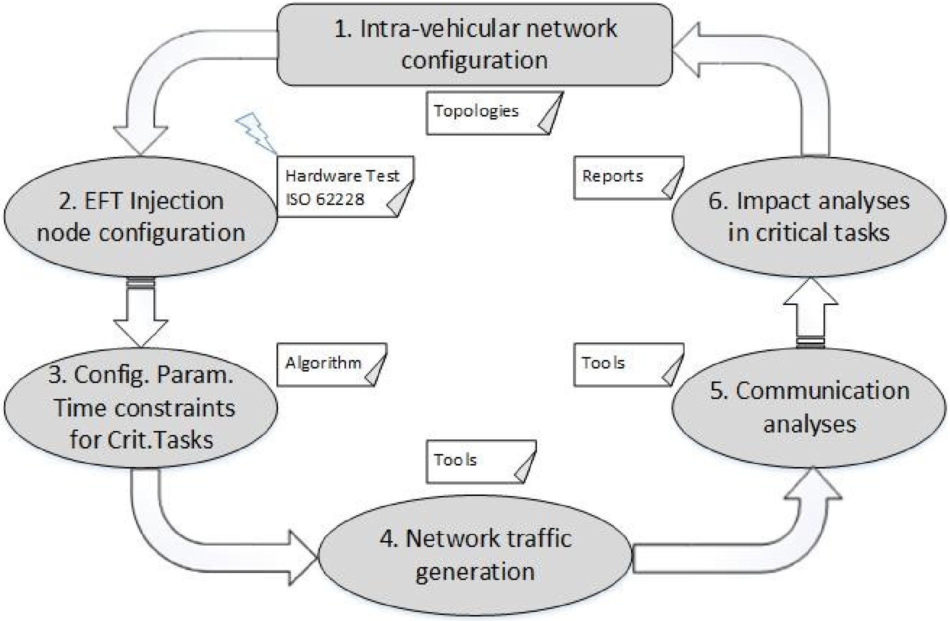
5 ENSAIOS COM PROTOCOLOS EMBARCADOS

5.1 Metodologia aplicada nos ensaios

Com o objetivo de investigar a imunidade do protocolo de comunicação *CAN* relacionado à ruídos EFT, distúrbios foram injetados na rede de comunicação com o objetivo de analisar o comportamento desta rede. Os transientes injetados na rede estão de acordo com a norma IEC 62228.

Este método é dividido em seis etapas, sendo a primeira etapa composta da configuração da rede *CAN* e das funcionalidades dos nós, na segunda etapa é definida a arquitetura para a injeção do *EFT*, onde os valores de duração do *BURST* e número de pulsos aplicados são configurados em um gerador de funções, utilizando a função *BURST*, já a amplitude do *EFT* é ajustada através da fonte que alimenta a etapa de potência do circuito. Na etapa três, os parâmetros de tempo e restrições temporais são ajustados em cada nó de forma individual, uma vez que cada nó tem uma função pré definida, visando simular um malha composta de *SENSOR, ATUADOR e CONTROLADOR*. Os ensaios seguem o método visto na Figura 28.

Figura 28 – Fluxograma do método de análise adotado.


1. Intra-vehicular network configuration
Topologies
Hardware Test ISO 62228
Reports
2. EFT Injection node configuration
6. Impact analyses in critical tasks
Algorithm
Tools
3. Config. Param. Time constraints for Crit.Tasks
5. Communication analyses
Tools
4. Network traffic generation

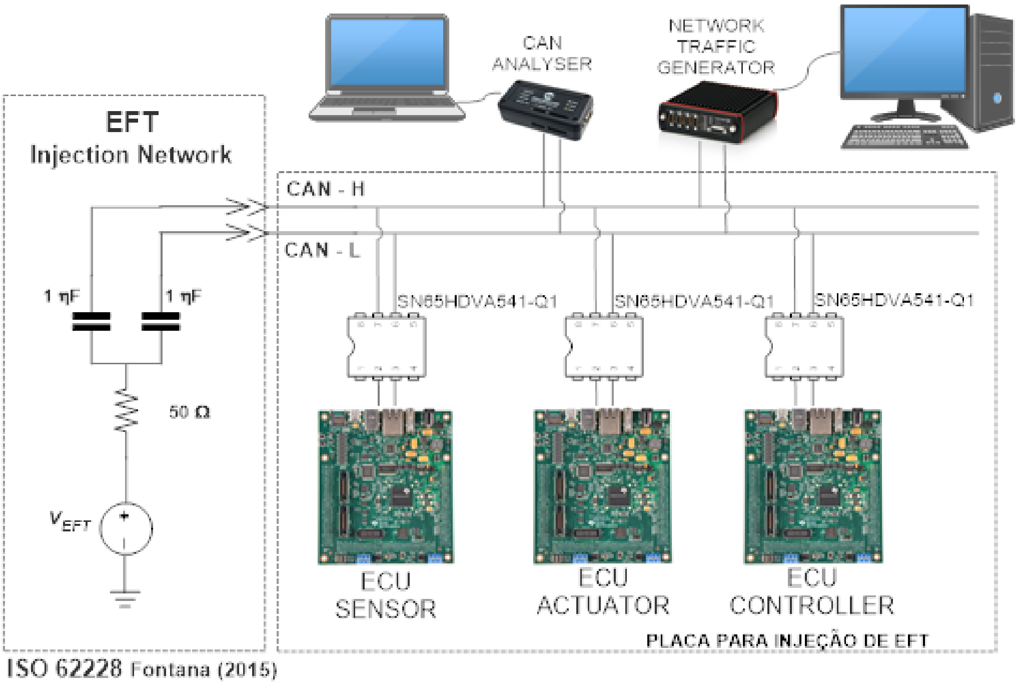
Fonte: Autor.

De acordo com (FONTANA; HUBING, 2015), o uso desta norma serve como uma padronização para os testes de EMC em transceivers de comunicação *CAN, CAN-FD e FlexRay*, em que se encaixam os transientes do tipo EFT, que tem um acoplamento capacitivo nas linhas de comunicação, alimentação e "wake-up". A metodologia dos ensaios executados segue uma sequência, visando garantir a robustes e confiabilidade dos dados aquisicionados. Os ruídos EFT são injetados na rede de comunicação, especificamente no centro da "estrela"definida na norma ISO 62228. Esta metodologia foi aplicada em todos os ensaios do três protocolos aqui abordados, *CAN, CAN-FD e FlexRay*.

5.2 Ensaios com o protocolo *CAN*.

De acordo com a metodologia de ensaios já abordada, o procedimento para os ensaios com cada protocolo é a montagem do set-up necessário, bem como a configuração da aplicação inserida nas ECUs. No diagrama da Figura 29 é mostrado o metodo utilizado para a injeção de EFT, bem como a arquitetura da rede e seus componentes.

Figura 29 – Fluxograma do método de injeção de EFT adotado no protocolo CAN.



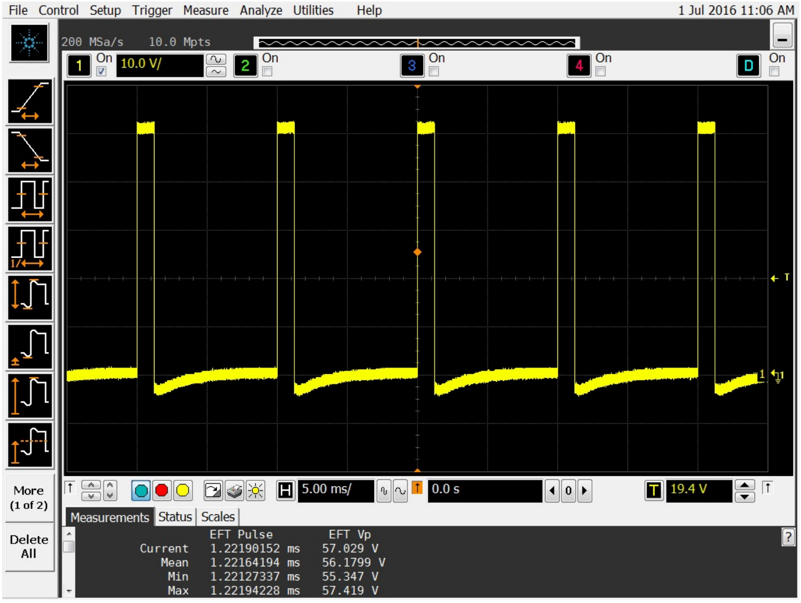
Fonte: Autor.

Na Figura 30 é visto na tela do osciloscópio um exemplo dos pulsos *BURST EFT* injetados na comunicação CAN.

5.2.1 Descrição dos procedimentos de testes

Para investigar a imunidade da rede CAN sob injeção de EFT, um cenário com três nós CAN é configurado seguindo as funções ilustradas na Figura 31. O nó 1 funciona como o sensor, enviando as informações de valores que simulam a leitura de um sensor de variação da suspensão, utilizando o *"Time Triggered"* de 25ms como lei de controle. O nó 2 funciona como atuador, recebendo a informação de posição a ser adotada do controlador (nó 3) e informando a atual posição para este nó, para o calculo da nova posição a ser adotada. O nó 3 tem a função de controlador, recebendo a informação de posição do sensor (nó 1), a posição atual da suspenção (nó 2), calculando a posição

Figura 30 – BURST EFT 57Vp e 1,2ms visto no osciloscópio.



```
200 MSa/s    10.0 Mpts
1 On 10.0 V/
H 5.00 ms/    0.0 s
T 19.4 V

              EFT Pulse          EFT Vp
    Current   1.22190152 ms    57.029 V
       Mean   1.22164194 ms    56.1799 V
        Min   1.22127337 ms    55.347 V
        Max   1.22194228 ms    57.419 V
```

Fonte: Autor.

Figura 31 – Algoritmo de controle adotado nos testes.

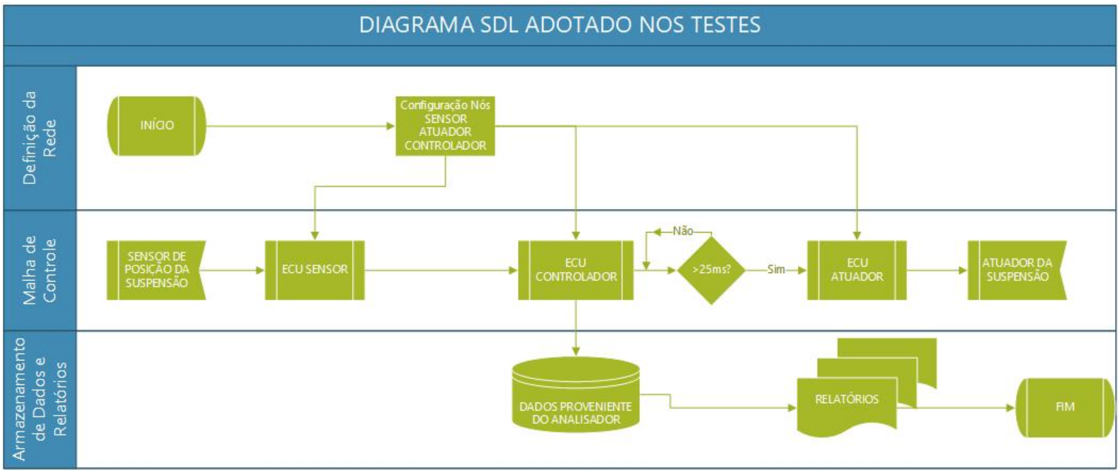


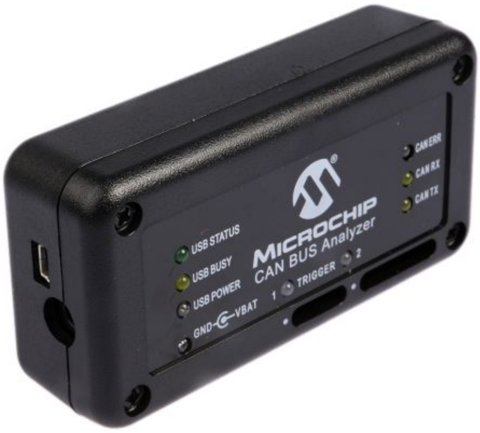
DIAGRAMA SDL ADOTADO NOS TESTES
Definição da Rede
Malha de Controle
Armazenamento de Dados e Relatórios
INÍCIO
Configuração Nós SENSOR ATUADOR CONTROLADOR
SENSOR DE POSIÇÃO DA SUSPENSÃO
ECU SENSOR
ECU CONTROLADOR
Não
>25ms?
Sim
ECU ATUADOR
ATUADOR DA SUSPENSÃO
DADOS PROVENIENTE DO ANALISADOR
RELATÓRIOS
FIM

Fonte: Autor.

desejada e informando ao atuador (nó 2) a nova posição a ser adotada. Toda esta malha de controle tem como regra temporal de controle o tempo de 25ms.

Estes testes tem o objetivo de verificar o impacto dos ruídos *EFT* na comunicação, em especial nas métricas de *Latência e Jitter*. Estes testes são importantes, pois sinalizam a susceptibilidade do protocolo *CAN* a estes tipos de ruídos. O método de teste aplicado, requer que os dados sejam armazenados, para uma análise mais criteriosa posteriormente, e como os ensaios eram focados principalmente no atendimento às normas de injeção de EFT e não nas ferramentas utilizadas, a ferramenta escolhida foi o CAN BUS Analyser, da Microchip, um analisador de baixo custo, com capacidade de armazenar as informações do tráfego na rede, bem como gerar simultaneamente um tráfego pré determinado, para carregar o barramento. Na Figura 32 é mostrado o *CAN BUS Analyser*, da Microchip.

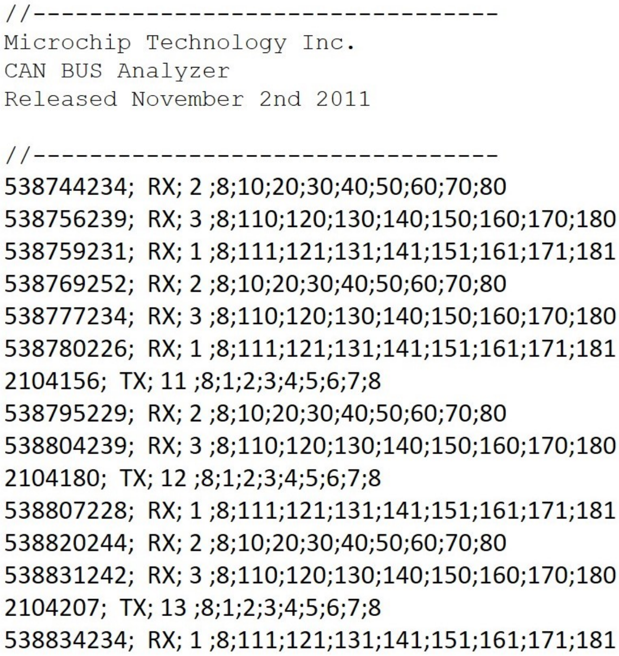
Figura 32 – Ferramenta da Microchip para registro e análise em redes CAN.



Fonte: Autor.

Este analisador suporta a rede *CAN* 2.0b de alta velocidade, com taxas de até 1Mbits (ISO 11898-2), se conecta à rede através de terminais com parafusos tipo KF ou conector DB9. Utiliza uma conexão USB tipo 2 para interligação com o software instalado no PC. Para determinar a imunidade da comunicação contra os ruídos EFT, foram injetados distúrbios na rede com amplitudes com valores de 19V, 37V e 57V e registrando logs de comunicação para análise posterior. Na Figura 33 pode-se ver uma planilha com os dados gerados pelo software CANAnalyser, da Microchip.

Figura 33 – Dados coletados no bus CAN pelo software CANAnalyser da Microchip.



```
//--------------------------------
Microchip Technology Inc.
CAN BUS Analyzer
Released November 2nd 2011

//--------------------------------
538744234;  RX; 2 ;8;10;20;30;40;50;60;70;80
538756239;  RX; 3 ;8;110;120;130;140;150;160;170;180
538759231;  RX; 1 ;8;111;121;131;141;151;161;171;181
538769252;  RX; 2 ;8;10;20;30;40;50;60;70;80
538777234;  RX; 3 ;8;110;120;130;140;150;160;170;180
538780226;  RX; 1 ;8;111;121;131;141;151;161;171;181
2104156;  TX; 11 ;8;1;2;3;4;5;6;7;8
538795229;  RX; 2 ;8;10;20;30;40;50;60;70;80
538804239;  RX; 3 ;8;110;120;130;140;150;160;170;180
2104180;  TX; 12 ;8;1;2;3;4;5;6;7;8
538807228;  RX; 1 ;8;111;121;131;141;151;161;171;181
538820244;  RX; 2 ;8;10;20;30;40;50;60;70;80
538831242;  RX; 3 ;8;110;120;130;140;150;160;170;180
2104207;  TX; 13 ;8;1;2;3;4;5;6;7;8
538834234;  RX; 1 ;8;111;121;131;141;151;161;171;181
```

Fonte: Autor.

Nesta tabela pode ser observado na segunda coluna o termo "*RX*", que significa que o analisador está recebendo estas informações provenientes do barramento *CAN*, a função "*TX*" significa que este analisador está enviando dados para a rede em forma de "trafego". A terceira coluna indica o endereço de cada nó na rede, sendo que os nós 1, 2 e 3 são referentes às *ECUs* sensor, atuador e controlador e o nó 11 é referente ao analisador (como gerador de tráfego).

5.2.2 Resultados dos ensaios com protocolo CAN

De acordo com o citado anteriormente, uma sequência de ruídos tipo *EFT* foi injetada na linha de comunicação, com pulsos de 198 e 675μs e 1,2ms. Estes ruídos tinham, respectivamente as amplitudes de 19, 37 e 57 Vcc, que foram geradas utilizando um gerador de forma de onda arbitrário, com a função *BURST*, o uso de uma fonte de alimentação externa como fonte para o circuito de injeção de *EFT* e o uso do osciloscópio como método de ajuste dos valores dos pulsos injetados.

Tabela 6 – Tabela de Transientes *EFT* segundo (PANNILA; EDIRISINGHE, 2014)

FUNÇÃO	AMPLITUDE	TEMPO
Ignição	57 Vp	1,2ms
Ar Condicionado	37 Vp	675μs
Faróis	19 Vp	198μs

Foi definido uma sequência de 5ms para o ciclo de *BURST* dos pulsos de EFT e 1000 ciclos de comunicação de malha (*Sensor - Controlador - Atuador*). Para que fosse possível a análise do impacto de ruídos *EFT* na comunicação, foram realizados testes de comunicação, utilizando a configuração de rede com os três nós, sem a aplicação de nenhuma interferência externa, para que fosse possível uma coleta de dados "limpa", que foram utilizados como base de comparação para os demais ensaios. Na Figura 34 pode-se obeservar o gráfico de performance e o comportamento de resposta da comunicação com uma lei de controle de 25ms e sem injeção de *EFT*.

Com a lei de controle fixada em 25ms, e os tempos de comunicação oscilando na casa de 1ms, pode-se observar que o *Jitter* mantém-se inferior a 1ms, podendo-se observar também apenas três picos em um universo de 1000 leituras.

Na Figura 35, pode-se observar que o impacto na comunicação com um *BURST* de 19 volts e 198μs como *EFT* não é significante mas existe, é possível observar um aumento nos picos de tempo de comunicação, que sem a injeção se limitavam à $\approx$ 28ms, e agora chegam à casa de $\approx$ 53ms.

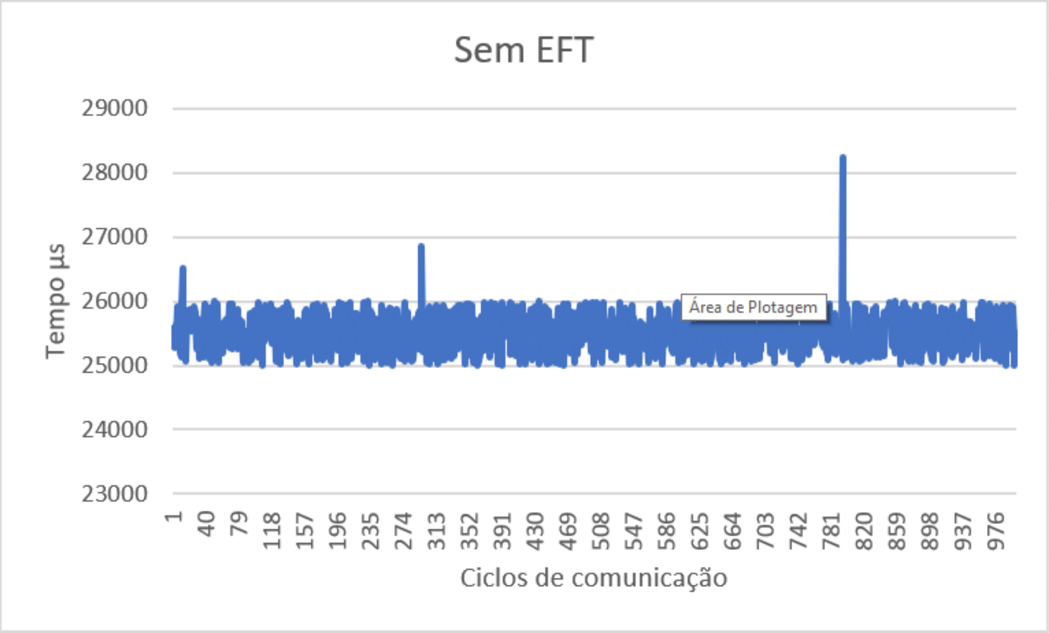
Dando sequência aos estudos, o próximo ensaio realizado foi com a injeção de *EFT* de 37 volts e 675μs de duração do *BURST*, como pode-se ver na Figura 36, já neste cenário, como facilmente identificado no gráfico, vários ciclos de comunicação são afetados e existe um significativo aumento do atraso na comunicação.

Outro experimento realizado foi com *EFT* de 57 volts e 1200μs de duração do *BURST*. Na comunicação com esta injeção pode-se observar um grande aumento no atraso da comunicação dos ciclos de controle. Na Figura 37 pode-se verificar o comportamento da comunicação CAN em face aos ruídos *EFT* injetados, onde houve um significativo aumento nas interferência bem como no atraso, que neste caso é de $\approx$ 60ms.

Na Tabela 5.2.2 pode-se verificar as diferenças entre os tempos de *Jitter* dos ensaios com e sem a injeção de *EFT* e na Figura 38 os valores em forma gráfica.

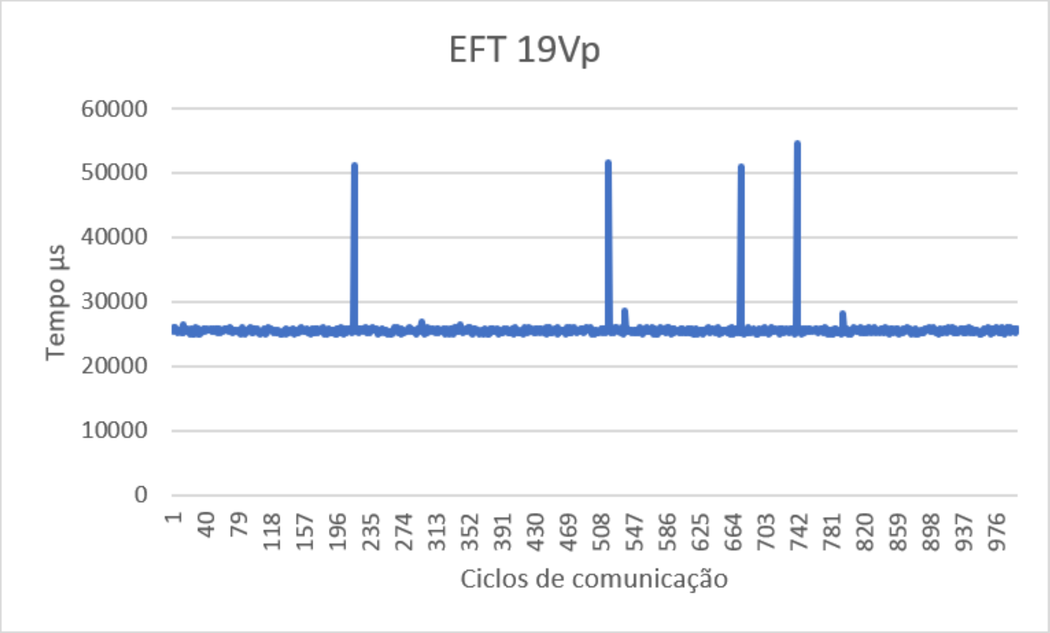
Com os dados apresentados, é possível observar que o *Jitter* médio sofreu um acrescimo de *21,76%* quando aplicamos um *EFT* de 19 Vp, quando é aplicado um *EFT* de 37 Vp, o acréscimo referente ao *Jitter* médio aumenta em *120,47%* e por fim, ao aplicarmos o *EFT* de 57 Vp, o aumento é de *220,44%*. Os valores utilizados são referente ao

Figura 34 – Gráfico da performance da comunicação CAN sem EFT.



Fonte: Autor.

Figura 35 – Gráfico da performance da comunicação CAN com EFT de 19 volts.



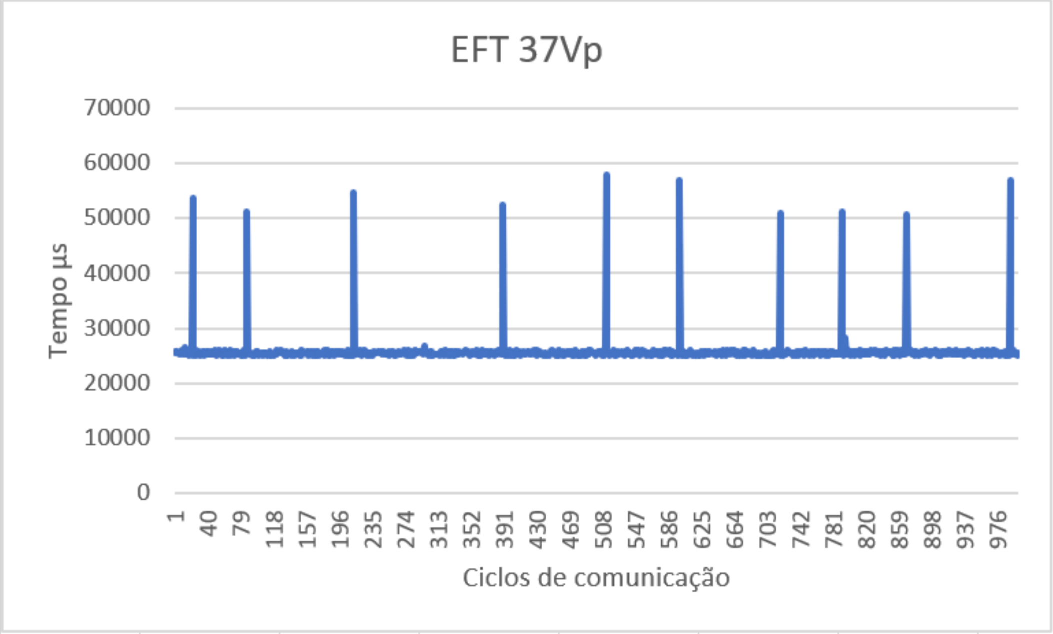
Fonte: Autor.

Jitter médio, pois ao utilizarmos os valores de pico, a diferença, no pior caso, sobe para $\approx$ *1034,02%*.

A grande variação dos resultados é decorrente de não existir propositalmente um sincronismo entre o ciclo de controle na comunicação e a geração e injeção dos pulsos de *BURST EFT* na rede.

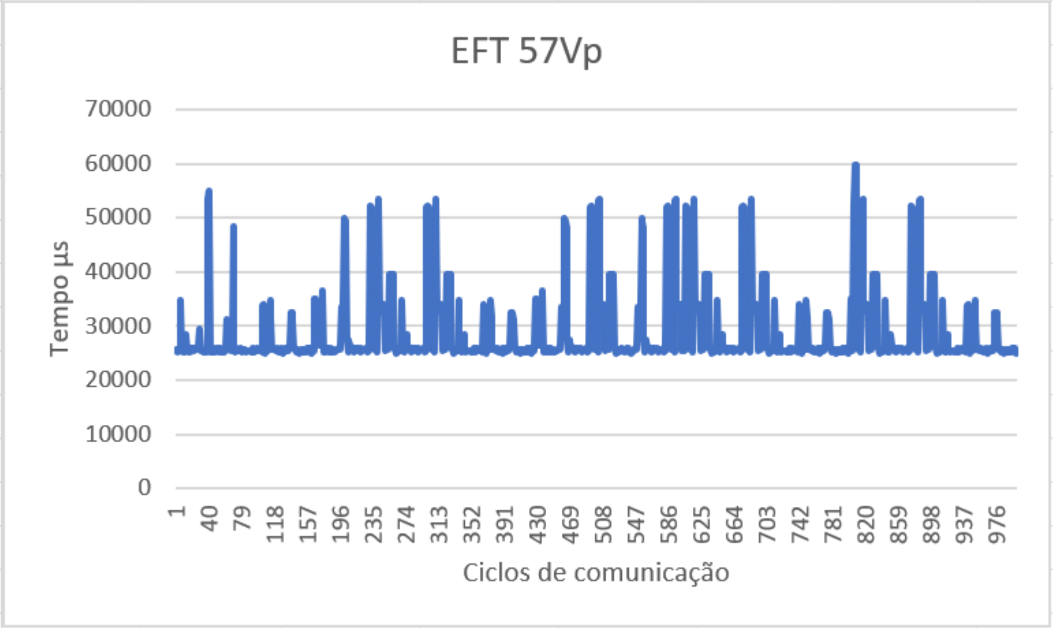
Esta falta de sincronismo é proposital, pois os ruídos gerados internamente em um veículo também são espúrios, ou seja, não temos uma predição do seu acontecimento. Com a existência da variação na injeção, em algumas vezes a injeção coincide com a

Figura 36 – Gráfico da performance da comunicação CAN com EFT de 37 volts.



Fonte: Autor.

Figura 37 – Gráfico da performance da comunicação CAN com EFT de 57 volts.



Fonte: Autor.

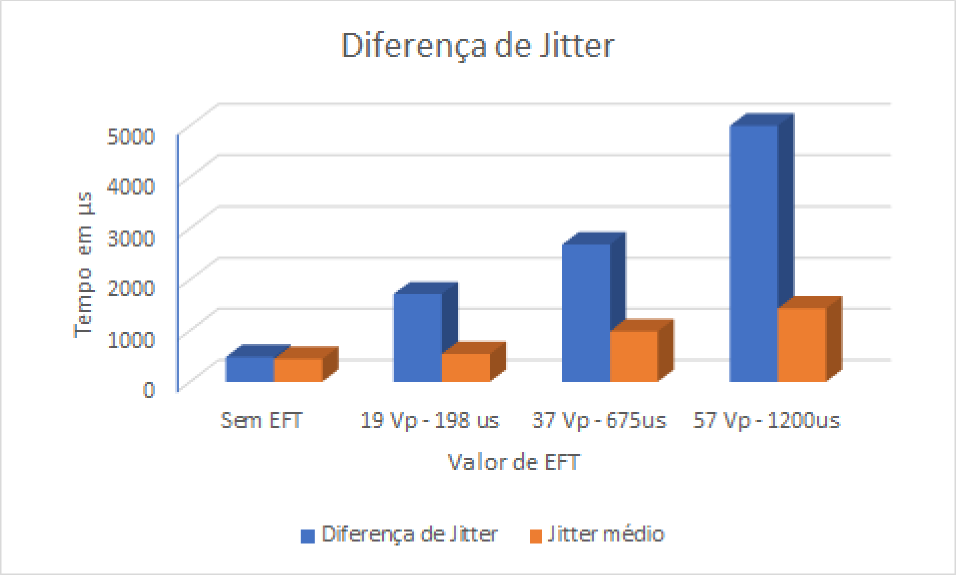
comunicação, e neste caso, os efeitos são mais visíveis. Também os pulsos com maior duração do *BURST* são mais sentidos, pois existe uma maior probabilidade destes pulsos coincidirem com a comunicação do ciclo de controle.

De qualquer forma, fica claro que o protocolo CAN é susceptível à ruídos do tipo *EFT*, e que estes ruídos geram uma instabilidade na comunicação, o que afeta diretamente a confiabilidade do protocolo nas tarefas onde as restrições temporais são rígidas e críticas.

Tabela 7 – Tabela de resultados dos testes na comunicação CAN.

Valor EFT	Diferença de Jitter	Jitter médio
Sem EFT	484,57μs	446,14μs
19Vp - 198μs	1714,34μs	543,24μs
37 Vp - 675μs	2685,61μs	983,61μs
57 Vp - 1200μs	5010,56μs	1429,62μs

Figura 38 – Gráfico das diferenças de Jitter na comunicação CAN.



Fonte: Autor.

5.3 Ensaios com protocolo CAN-FD

A injeção dos pulsos *EFT* na placa para injeção, especificamente na estrela formada pelos drivers de comunicação do protocolo *CAN-FD* obedecem as mesmas especificações da norma ISO 62228 e já citadas anteriormente. Na Figura 39 é mostrado o método adotado para a injeção de *EFT*, e a estrutura da rede e seus componentes.

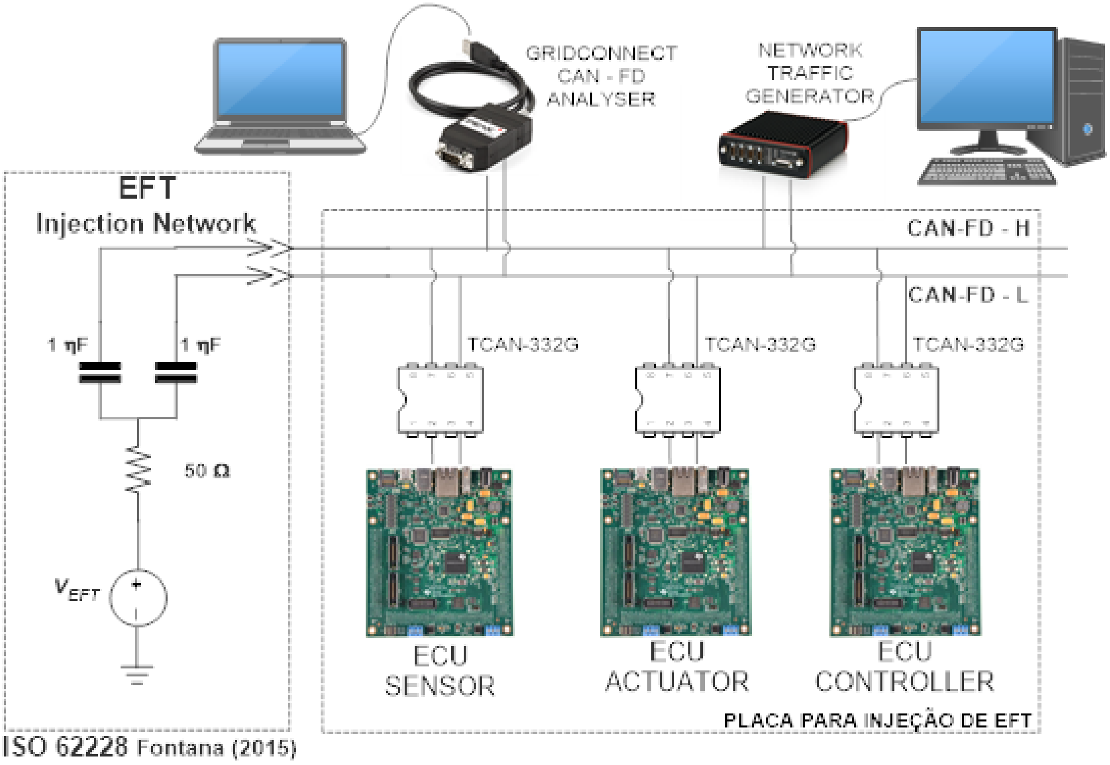
5.3.1 Descrição dos procedimentos para os testes com CAN-FD

Para possibilitar a realização dos ensaios da susceptibilidade do protocolo *CAN-FD* aos ruídos do tipo *EFT*, foram configurados três nós simulando uma malha de controle de suspensão ativa (*Sensor–Controlador–Atuador*), utilizando as placas *HERCULES*^{TM}, cada uma exercendo a função de uma *ECU*. Na Tabela 8, podem ser visualizados os dados trocados entre os três elementos que compõe esta malha.

As mensagens listadas acima são transmitidas ciclicamente, e representam a condição normal de funcionamento desta malha de controle. De acordo com estes parametros, a rede *CAN-FD* foi configurada para trabalhar com velocidades de 1 e 4 Mbps durante os ensaios, com cinco pacotes de 8 Bytes cada. Estes pacotes são ligados a lei de controle e os demais dados caracterizados pela malha configurada. Varios pacotes esporádicos foram inseridos, para caracterizar uma carga no barramento, durante os ensaios.

Desta forma, a carga do barramento oscilou entre 30% e 60%, devido ao fato que o tráfego era gerado de forma exporádica. Os testes foram elaborados para diagnosticar a

Figura 39 – Diagrama do método de injeção de EFT adotado para CAN-FD.



Fonte: Autor.

Tabela 8 – Configuração dos nós da rede.

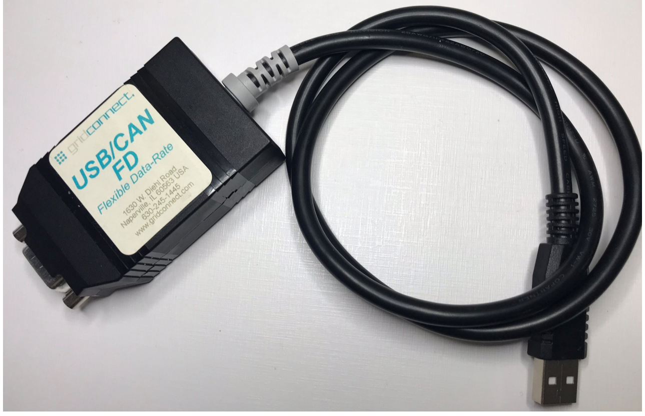
Nó	Função	Mensagens / TX–RX
Sensor	Conjunto *Massa-Mola-Amortecedor*. Parametros da suspensão ativa.	MSG–Velocidade vertical do corpo MSG–Deflexão da suspensão MSG–Deflexão dos pneus
Atuador	Ajuste da posição vertical da suspensão.	MSG–Ajust–Vert–Susp.
Control.	Calculo da posição apropriada da suspensão e ajuste. Lei de controle	MSG–Alg.–Controle

influência dos ruídos *EFT* na comunicação *CAN-FD*, e registrar os dados da comunicação para uma posterior avaliação.

Esta malha de controle se comporta de maneira semelhante à malha testada com o protocolo *CAN*, porém utilizando um período de ciclo de controle menor, com a lei de controle setada para 5ms como *"Time Triggered"*. O nó sensor(1), é responsável por receber a informação da posição da suspensão e informar ao nó controlador (3). O nó atuador (2) recebe do nó controlador a informação da posição que a suspensão deve assumir e o nó controlador (3) por sua vez, é responsável por tratar estas informações de acordo com a lei de controle e informar ao nó atuador a nova posição a ser assumida.

Os testes tem a finalidade de capturar os dados da comunicação, em especial os parâmetros de *Latência e Jitter*, para que estes possam ser analisados futuramente. Os procedimentos de testes passam pela etapa de aquisição de dados, que é feita através da ferramenta de análise do protocolo *CAN-FD* da GridConnect, o *CAN-FD Analyser*, que consiste em duas partes, software e hardware, este último mostrado na Figura 40.

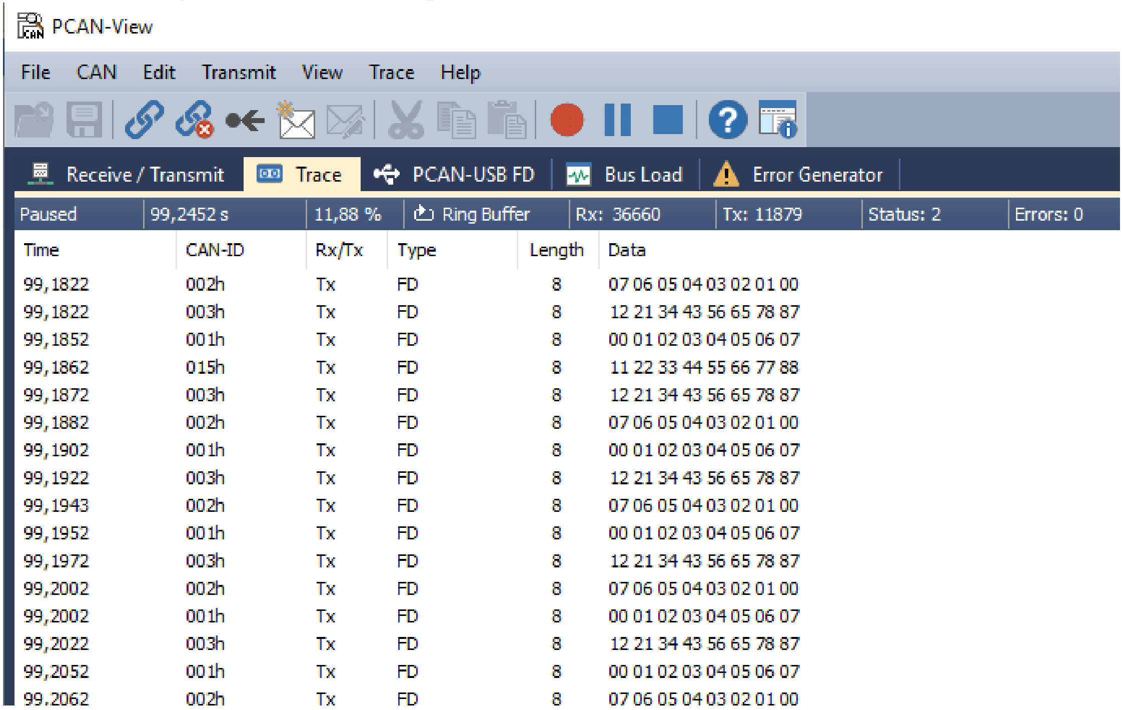
Figura 40 – Hardware Grid Connect para análise da comunicação em CAN-FD.



Fonte: Autor.

Este analisador suporta as redes *CAN* (ISO-11898/93, 1993) e *CAN-FD* (BOSCH, 2012) com velocidades de até 4Mbps, bastando apenas uma configuração simples. A ferramenta de hardware vem acompanhada das ferramentas de software para coleta, geração de tráfego e armazenamento das informações provenientes do barramento. A conexão à rede é feita através do conector padrão DB9. A interligação com o computador que abriga os softwares é feita através de uma conexão USB tipo 2. Na Figura 41, pode-se observar a tela do software *CAN-FD Analyser* da GridConnect.

Figura 41 – Software para análise da comunicação em CAN-FD.



Paused | 99,2452 s | 11,88 % | Ring Buffer | Rx: 36660 | Tx: 11879 | Status: 2 | Errors: 0

Time	CAN-ID	Rx/Tx	Type	Length	Data
99,1822	002h	Tx	FD	8	07 06 05 04 03 02 01 00
99,1822	003h	Tx	FD	8	12 21 34 43 56 65 78 87
99,1852	001h	Tx	FD	8	00 01 02 03 04 05 06 07
99,1862	015h	Tx	FD	8	11 22 33 44 55 66 77 88
99,1872	003h	Tx	FD	8	12 21 34 43 56 65 78 87
99,1882	002h	Tx	FD	8	07 06 05 04 03 02 01 00
99,1902	001h	Tx	FD	8	00 01 02 03 04 05 06 07
99,1922	003h	Tx	FD	8	12 21 34 43 56 65 78 87
99,1943	002h	Tx	FD	8	07 06 05 04 03 02 01 00
99,1952	001h	Tx	FD	8	00 01 02 03 04 05 06 07
99,1972	003h	Tx	FD	8	12 21 34 43 56 65 78 87
99,2002	002h	Tx	FD	8	07 06 05 04 03 02 01 00
99,2002	001h	Tx	FD	8	00 01 02 03 04 05 06 07
99,2022	003h	Tx	FD	8	12 21 34 43 56 65 78 87
99,2052	001h	Tx	FD	8	00 01 02 03 04 05 06 07
99.2062	002h	Tx	FD	8	07 06 05 04 03 02 01 00

Fonte: Autor.

5.3.2 Valores de *EFT* utilizados nos testes

A injeção dos *"BURST"de EFT* foram efetuadas de acordo com a Tabela 9, e com o barramento sofrendo o carregamento já citado. Estes testes foram realizados obedecendo os parâmetros exigidos nas normas *IEC 62228 e ISO 26262*.

Tabela 9 – Tabela de sequência de transientes *EFT* para os testes

Tensão de pico - Vp	TEMPO de BURST
47 volts	675μs
57 volts	1,2ms
63 volts	500μs
67 volts	500μs

O hardware de injeção de *EFT* foi setado de acordo com a tabela, utilizando como fonte de sinal de pulso para o *BURST* o gerador de funções, como fonte de alimentação para suprir a tensão aplicada de *BURST* uma fonte de alimentação DC chaveada ajustável, e um osciloscópio como instrumento de acompanhamento e certificação dos valores injetados. Este procedimento de ajustes para injeção é repetido para cada valor de *EFT* utilizado nos ensaios.

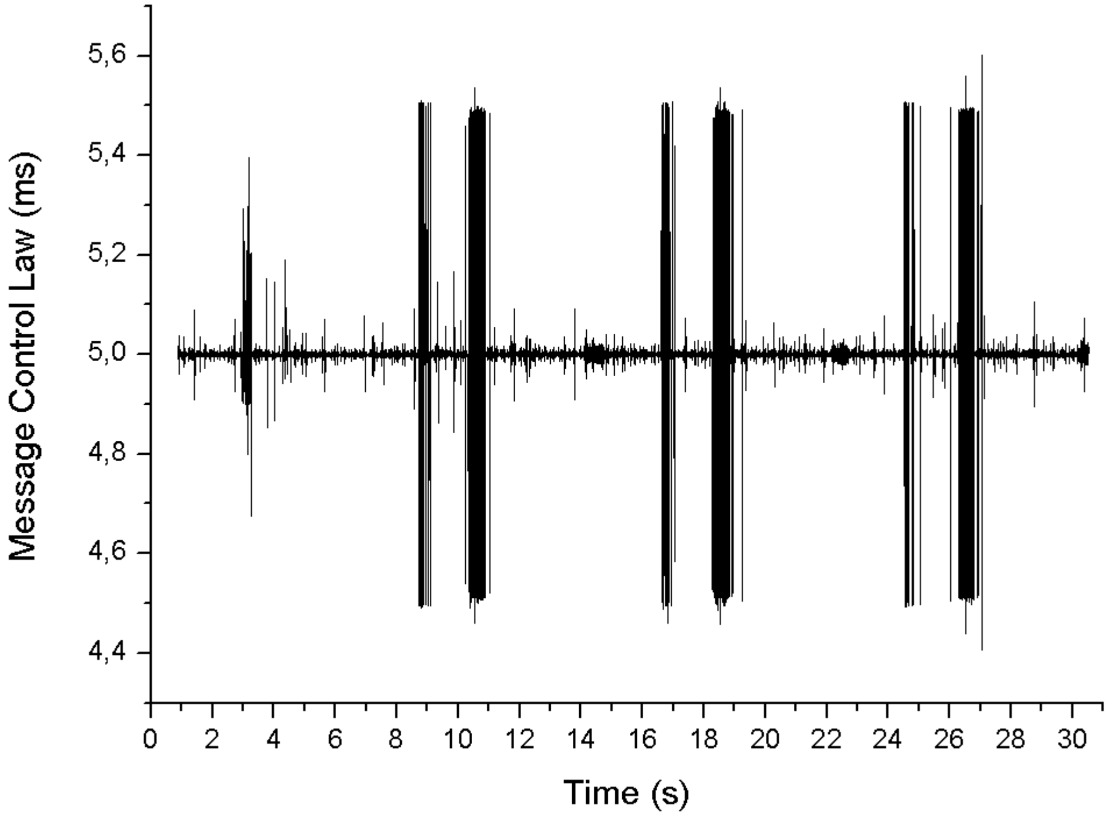
5.3.3 Resultados dos ensaios com protocolo *CAN-FD*

Uma série de ensaios com o protocolo *CAN-FD* foram conduzidos com o objetivo de verificar a susceptibilidade deste protocolo à ruídos do tipo *EFT*. Estes ensaios seguiram os procedimentos já descritos e obedecendo as normas *IEC 62228 e ISO 26262*. As três *ECUs* foram configuradas com os algoritmos de uma malha fechada de controle de suspensão ativa, cujos dados trocados entre estas *ECUs* são mostrados na tebela 8.

Nos ensaios, os dados da comunicação foram capturados pela ferramenta de análise do protocolo *CAN-FD* da *Grid Connect*. Em conjunto com esta ferramenta, foi utilizada a ferramenta de análise e geração de tráfego para o barramento de comunicação do protocolo *CAN-FD* da Vector, o *CANanalyser e o CANoe*.

Os procedimentos de teste consistiram inicialmente no estabelecimento da comunicação entre as *ECUs* da malha de controle, sem a injeção de *EFT*, o que serviu de parâmetro de comparação para os dados a serem coletados quando a comunicação estiver sob injeção. Todas as capturas de dados de comunicação, para efeitos de comparação, tiveram o período setado em 30s. Na Figura 42 pode-se verificar o comportamento da comuinicação sem a injeção de *EFT*.

Figura 42 – Gráfico da comunicação *CAN-FD* sem injeção de *EFT*.

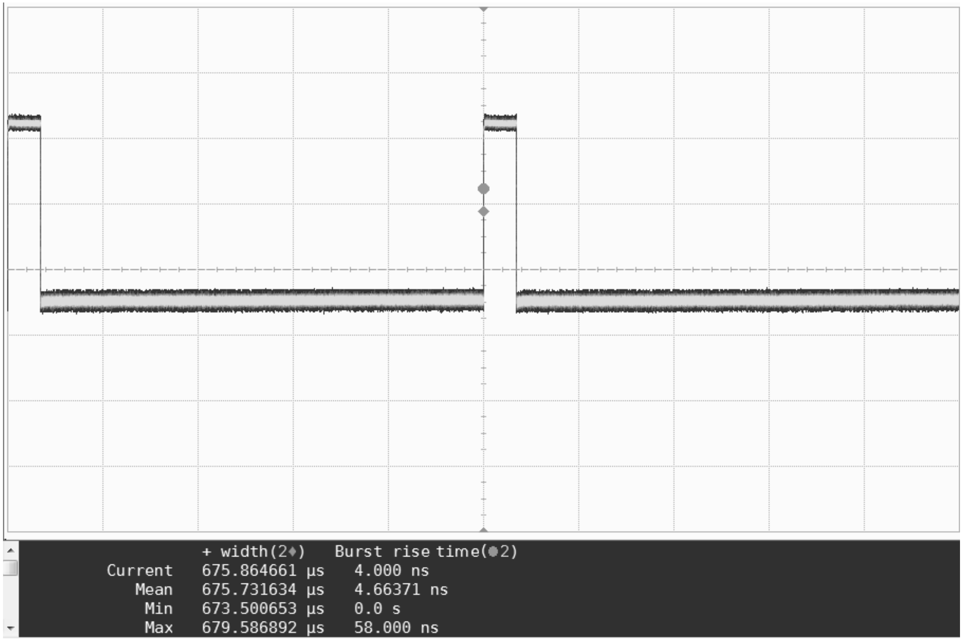


Fonte: Autor.

Neste gráfico pode ser observado no período de captura, que a média dos ciclos de comunicação ficaram entre 4,4 e 5,6 ms. Estas pequenas variações são consideradas normais, uma vez que em uma rede real, as conexões de cabos e conectores, podem gerar pequenos erros e ou atrasos. A razão para essas flutuações é a variação de tempo entre o pacote recebido em um ciclo da *malha de controle* anterior e o pacote enviado no próximo ciclo. Estes pequenos erros são gerados pelo temporizador de software utilizado para gerenciar o ciclo de controle, porém o fato destes pequenos erros de temporização na comunicação acontecerem, não afetam os ensaios, tendo em vista que o objetivo é verificar se estes valores sofrem influência com a injeção de EFT e qual a magnitude desta interferência, e não a temporização da malha em si.

Seguindo a ordem de testes estabelecida na Tabela 9, o segundo ensaio realizado foi com o valor de EFT de 47 Vp e 675μs, cujos pulsos de *BURST EFT* podem ser visualizados na Figura 43. É possível observar neste gráfico que o valor do tempo de subida o pulso está atendendo o exigido pela norma IEC 62228, ou seja, é < *5ns + 30%.*

Figura 43 – Imagen do pulso de *EFT* de 47Vp e 675μs.

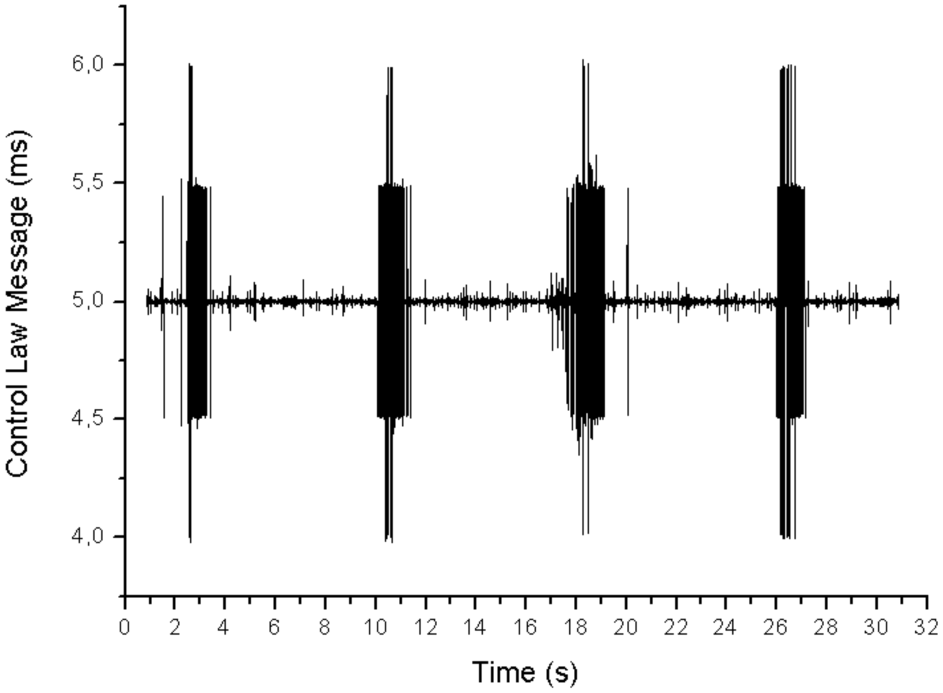


```
              + width(2♦)    Burst rise time(●2)
     Current  675.864661 µs   4.000 ns
        Mean  675.731634 µs   4.66371 ns
         Min  673.500653 µs   0.0 s
         Max  679.586892 µs   58.000 ns
```

Fonte: Autor.

A Figura 44 mostra o gráfico gerado com base na comunicação da malha de controle e a injeção acima.

Figura 44 – Gráfico da comunicação *CAN-FD* com injeção de *EFT* de 47Vp e 675μs.

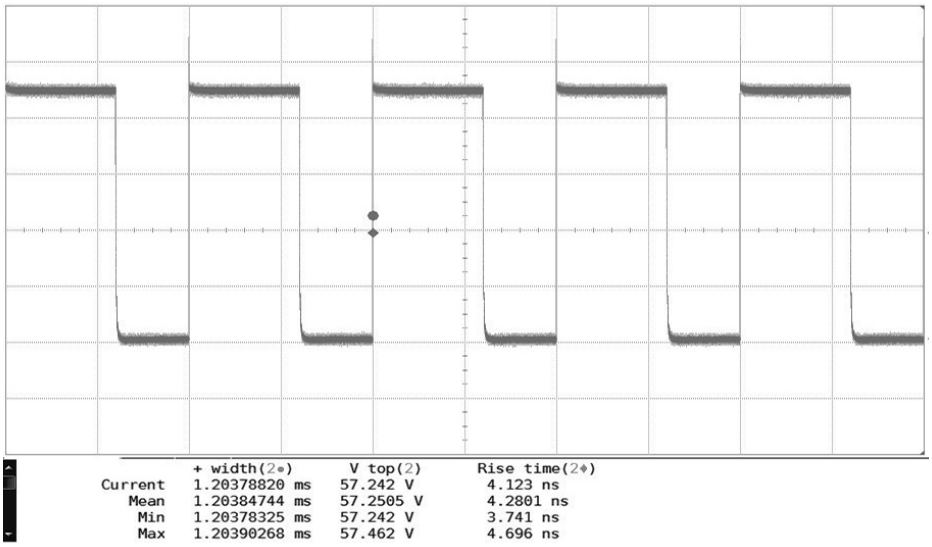


Fonte: Autor.

Em uma análise rápida é possível verificar que a comunicação sofreu impacto quando injetado pulsos de *EFT*, uma vez que o gráfico mostra um aumento nos picos de comunicação apara $\approx$ 6ms, além do aumento da frequência da incidência destes atrasos.

Os pulsos de *BURST EFT* injetados na sequência dos ensaios foram de 57 Vp e 1,2ms. Na Figura 45 pode-se ver este pulso com os valores registrados na tela do osciloscópio, onde o tempo de subida se mantém dentro dos parâmetros exigidos pela norma IEC 62228.

Figura 45 – Imagen do pulso de *EFT* de 57Vp e 1,2ms.



```
               + width(2●)        V top(2)      Rise time(2◆)
Current  1.20378820 ms   57.242 V       4.123 ns
   Mean  1.20384744 ms   57.2505 V      4.2801 ns
    Min  1.20378325 ms   57.242 V       3.741 ns
    Max  1.20390268 ms   57.462 V       4.696 ns
```

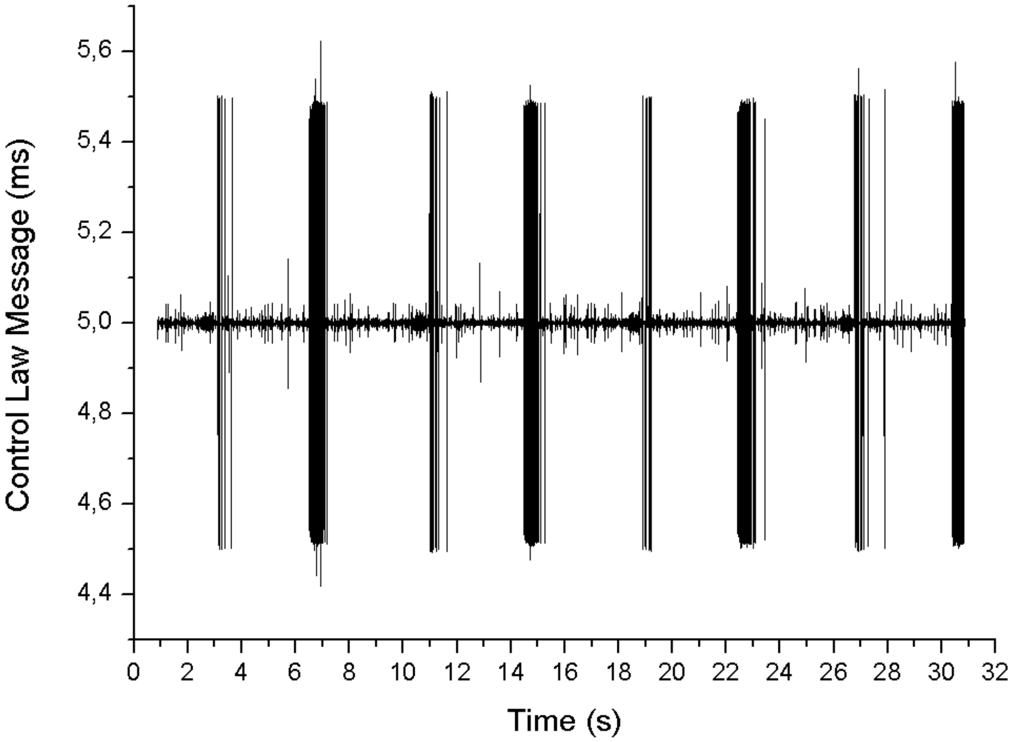
Fonte: Autor.

Com os pulsos mostrados na Figura 45, a comunicação mostrou um impacto superior às injeções anteriores, como pode ser visto na Figura 46, onde os valores dos picos de atraso na comunicação chegaram a 5,8ms, e a incidência das perturbações se mostram mais constantes. O próximo ensaio realizado foi com os pulsos de *BURST EFT* de 63Vp e 500μs. Estes testes foram realizados para verificar o impacto de niveis maiores de tensão nos pulsos, bem como tempos menores. Neste caso a comunicação teve um impacto um pouco maior, como esperado, levando em conta a maior amplitude do sinal aplicado. Na Figura 47, pode-se ver o gráfico de análise da comunicação, com os tempos de atraso na comunicação na casa dos 5,6s, porém com muito mais perturbações afetando o barramento.

No último ensaio realizado, os valores dos pulsos de *BURST EFT* aplicados no barramento de comunicação foram de 67 Vp e 500μs. Com estes pulsos, a comunicação teve um comportamento compatível, ou seja, o aumento da tensão dos ruídos EFT trouxeram consigo o aumento das perturbações no barramento de comunicação. Na Figura 48 pode-se ver o impacto deste ruídos no gráfico de análise da comunicação. De posse dos dados colhidos nestes ensaios, pode-se observar que os valores de atraso de comunicação, quando a injeção dos pulsos de *BURST EFT* tem os valores de 47 Vp e 675μs, são maiores, porém a incidencia destes atrasos são em menor número que ao aumentarmos o valor da tensão de pico destes pulsos. Seguindo esta linha de raciocínio, pode-se observar que ambos fatores, amplitude e duração, impactam na comunicação, porém cada um deles afetam de maneira diferente, sendo a amplitude responsável por aumentar a quantidade de ocorrências das perturbações e a duração dos pulsos responsável pelo aumento dos atrasos na comunicação.

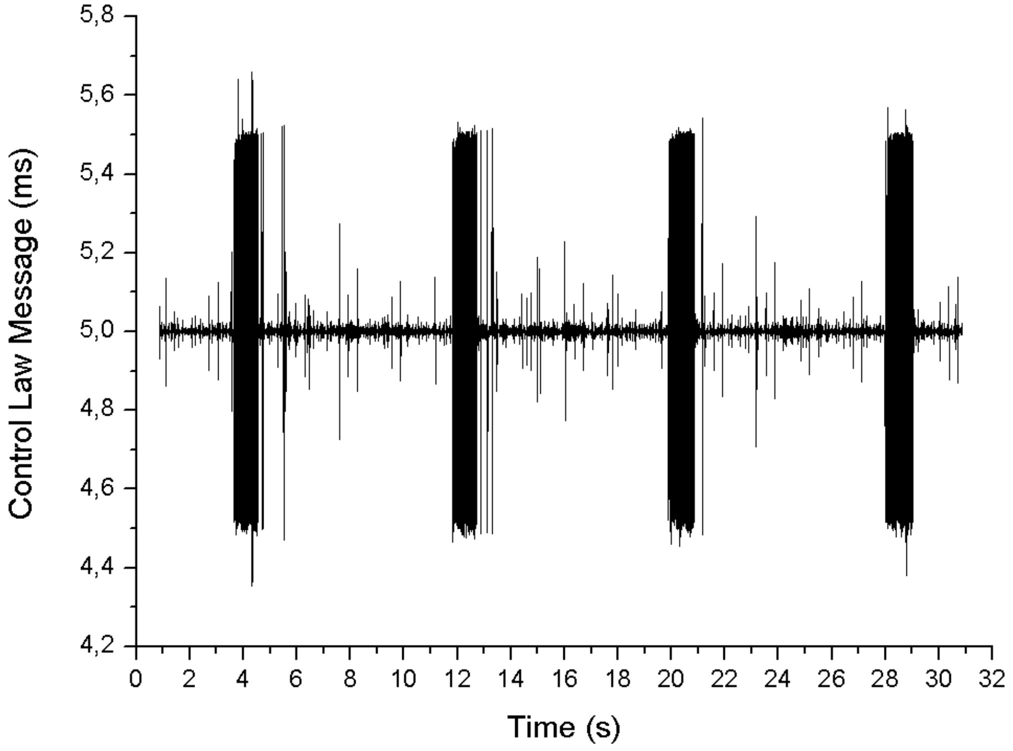
Na Figura 49, é visto a tabela obtida do software de análise de comunicação CAN Analyser, da VECTOR, colhidos durantes o teste com injeção de pulsos com tensão de pico de 67 Vp.

Figura 46 – Gráfico da comunicação *CAN-FD* com injeção de *EFT* de 57Vp e 1,2ms.



Fonte: Autor.

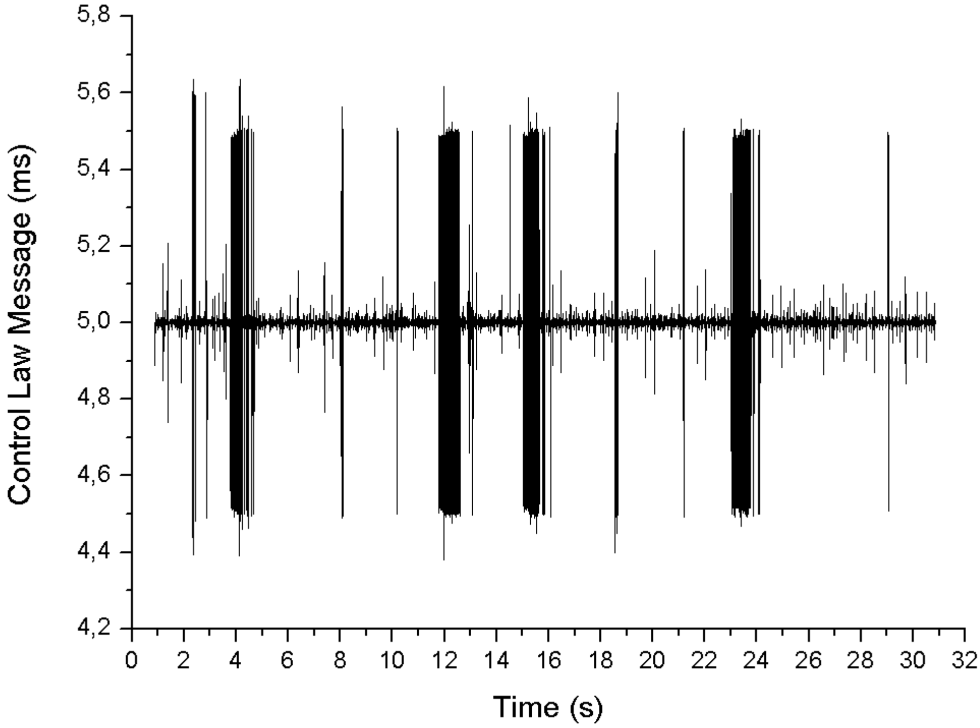
Figura 47 – Gráfico da comunicação *CAN-FD* com injeção de *EFT* de 63Vp e 500μs.



Fonte: Autor.

Todos estes dados foram colhidos em 32s de injeção (a quantidade de dados colhidos foi limitado ao buffer do analisador) e carga do barramento oscilando entre 30 e 60%.

Figura 48 – Gráfico da comunicação *CAN-FD* com injeção de *EFT* de 63Vp e 500μs.

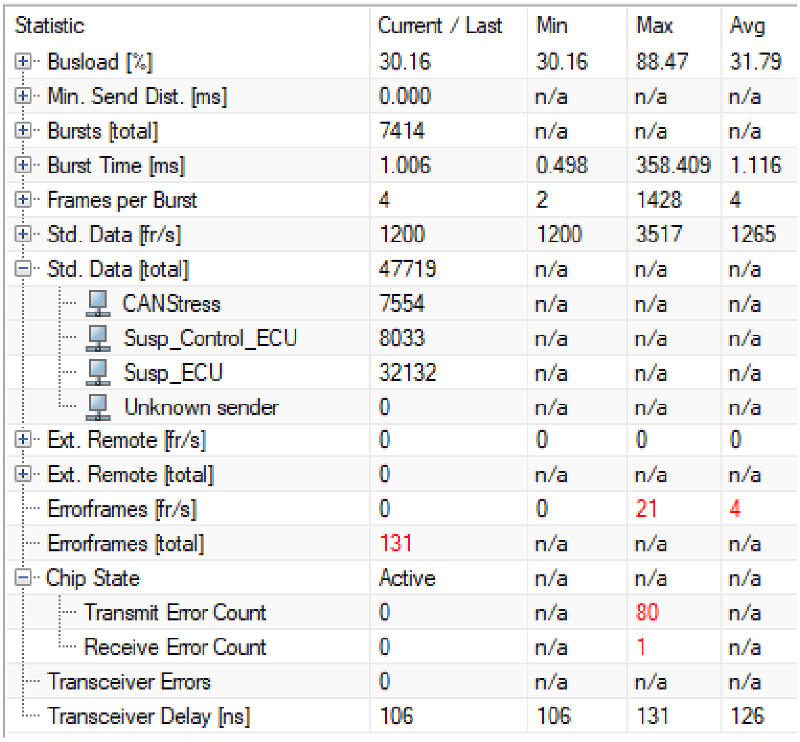


Fonte: Autor.

Com base nestes dados listados, foi possível analisar a performance do protocolo *CAN-FD*. As metricas utilizadas para esta análise foram o *Jitter médio* e o *Jitter diferencial*. O Jitter médio é obtido através do desvio padrão dos valores obtidos nos ensaios, e o Jitter diferencial é obtido subtraindo-se o menor valor de desvio do pior valor de desvio e dividindo por dois, este resultado é subtraído do valor definido como lei de controle. Na Figura 50 pode ser visto o gráfico que mostra as diferenças dos Jitters entre os vários ensaios.

Na Figura 51 pode ser visualizado o gráfico do Jitter médio, calculado através do desvio padrão. Neste caso, o valor do Jitter, se comparado entre o valor sem *EFT* e com a injeção de 47Vp, a diferença é de 29,05%, já com a injeção de 57Vp, a diferença é de 10,41%, com a injeção de 63Vp, a diferença é de 11,56% e por fim, com a injeção de 67Vp, a diferença é de 15,61%. Estes impactos na comunicação, independente dos valores e resultados, afetam diretamente a confiabilidade do protocolo e da rede de comunicação nos sistemas embarcados distribuídos, levando em conta as exigências das normas que regem os sistemas automotivos e as redes intraveiculares, as restrições temporais e a segurança dos condutores. Os resultados encontrados nos ensaios realizados com o protocolo *CAN-FD*, apesar de mostrar valores de atrasos bem menores que com o protocolo *CAN*, não podem ser desconsiderados, tendo em vista que os parâmetros de temporizações entre estes protocolos são de grandezas diferentes, e desta forma, os impactos no protocolo *CAN-FD* observados dentro deste contexto, também são impactantes, e merecem muita análise e trabalho com o foco em atenuá-los ou mesmo eliminá-los por completo.

Figura 49 – Tabela de dados de comunicação CAN-FD.



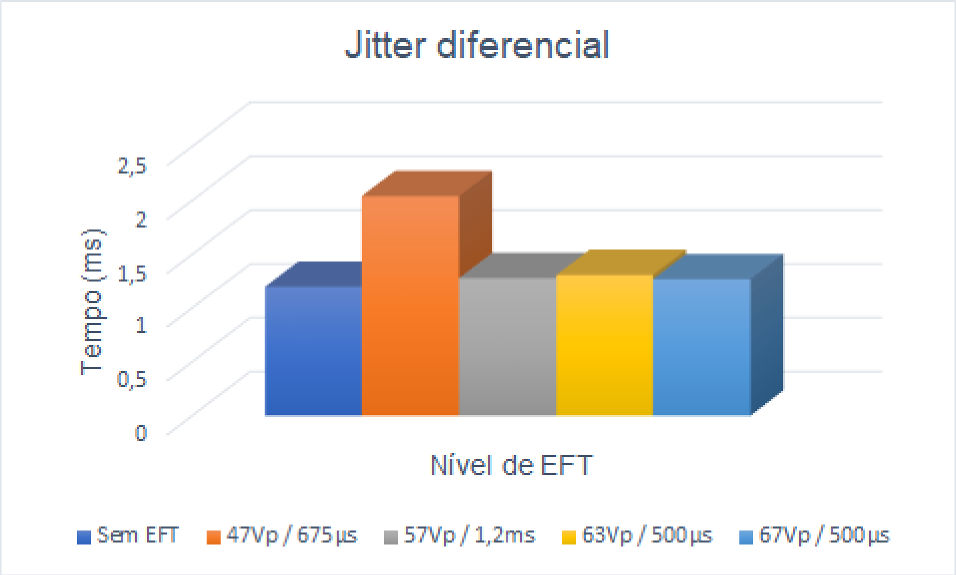
Statistic	Current / Last	Min	Max	Avg
⊞ Busload [%]	30.16	30.16	88.47	31.79
⊞ Min. Send Dist. [ms]	0.000	n/a	n/a	n/a
⊞ Bursts [total]	7414	n/a	n/a	n/a
⊞ Burst Time [ms]	1.006	0.498	358.409	1.116
⊞ Frames per Burst	4	2	1428	4
⊞ Std. Data [fr/s]	1200	1200	3517	1265
⊟ Std. Data [total]	47719	n/a	n/a	n/a
CANStress	7554	n/a	n/a	n/a
Susp_Control_ECU	8033	n/a	n/a	n/a
Susp_ECU	32132	n/a	n/a	n/a
Unknown sender	0	n/a	n/a	n/a
⊞ Ext. Remote [fr/s]	0	0	0	0
⊞ Ext. Remote [total]	0	n/a	n/a	n/a
Errorframes [fr/s]	0	0	21	4
Errorframes [total]	131	n/a	n/a	n/a
⊟ Chip State	Active	n/a	n/a	n/a
Transmit Error Count	0	n/a	80	n/a
Receive Error Count	0	n/a	1	n/a
Transceiver Errors	0	n/a	n/a	n/a
Transceiver Delay [ns]	106	106	131	126

Fonte: Autor.

Nesta tabela pode-se observar dados como:

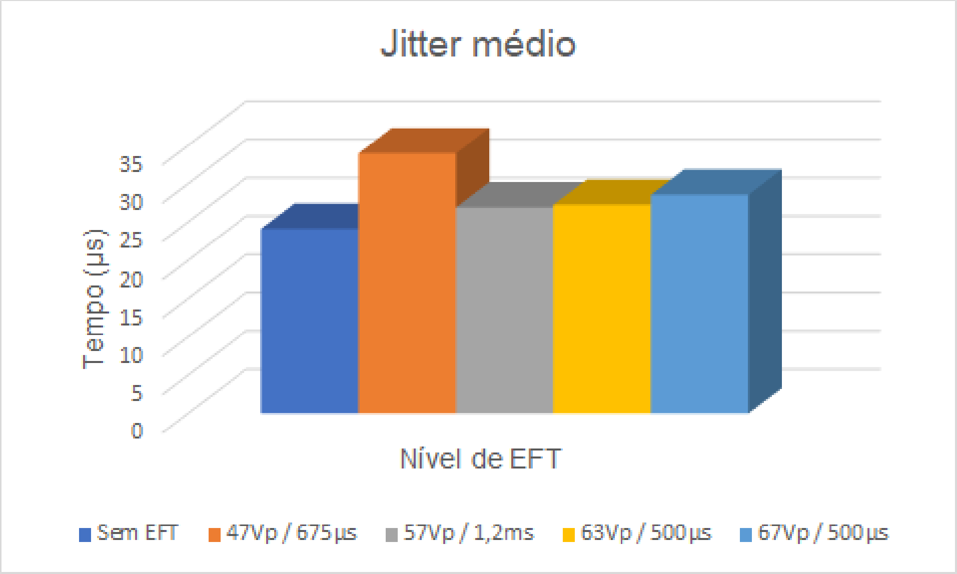
- Número total de frames com erro = 131
- Erros de estado de transmissão = 80
- Média de frames com erros = entre 4 e 21

Figura 50 – Gráfico do Jitter diferencial na comunicação CAN-FD.



Fonte: Autor.

Figura 51 – Gráfico do Jitter médio na comunicação CAN-FD.



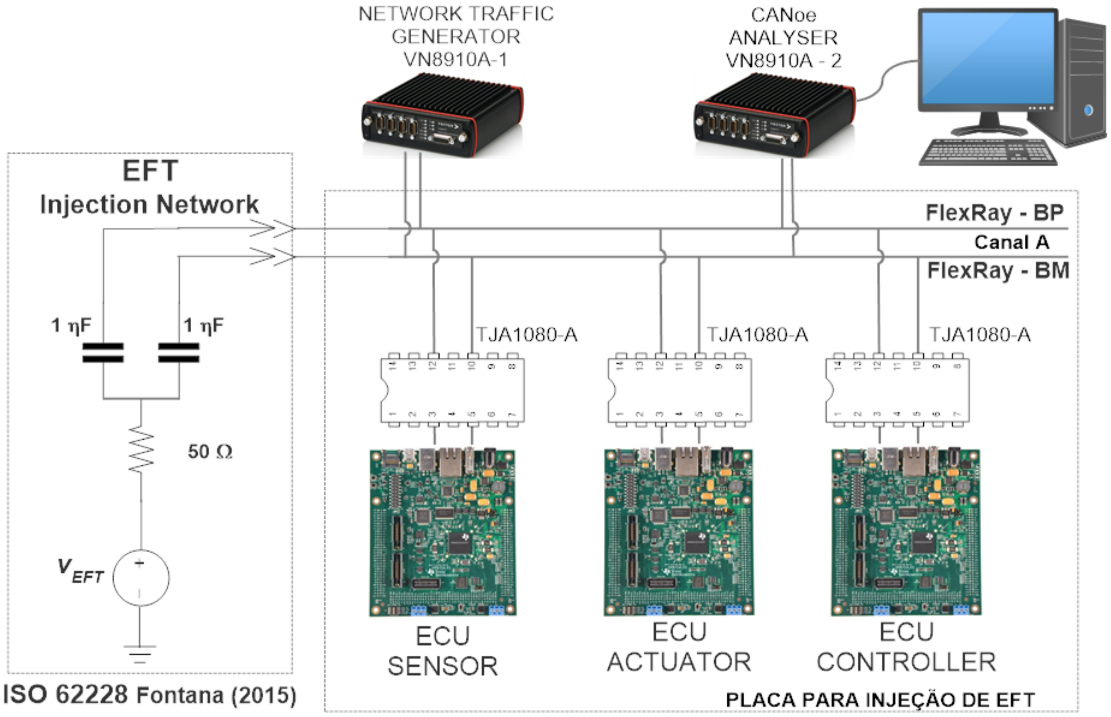
Fonte: Autor.

5.4 Ensaios com protocolo FlexRay

Os últimos ensaios foram realizados com base no protocolo *FlexRay*, com o objetivo de verificar a susceptibilidade deste protocolo aos ruídos do tipo *EFT*. Nos mesmos moldes dos ensaios anteriores, após a rede ter sido configurada, pulsos do tipo *BURST EFT* foram injetados no barramento de comunicação, objetivando a análise dos dados coletados, e levantando de forma prática a influência destes ruídos na comunicação.

Os ensaios também foram baseados na norma IEC 62228 (IEC-62228, 2016), utilizando para esta finalidade, o mesmo setup de hardware já utilizado nos ensaios dos protocolos *CAN e CAN-FD*. O hardware das placas projetadas para a injeção de *EFT* contemplam dois canais de comunicação *FlexRay* (canal A e canal B), sendo que nestes ensaios foram utilizados apenas os canais "A". Para a comunicação *FlexRay* foram utilizados os drivers de comunicação TJA1080A da NXP, montados na placa para a injeção de *EFT*. Nesta placa existem seis drivers TJA1080A, sendo que um conjunto de três drivers formam o canal "A"e os outros três formam o canal "B". A estrutura da placa para a injeção de *BURST EFT* para o protocolo *FlexRay* obedece às exigências da norma ISO 62228. Como a característica do meio físico deste protocolo implica em termos dois canais de comunicação distintos, foram implementados os canais "A"e "B"no hardware da placa de injeção de EFT, porém nos ensaios, foi utilizado apenas o canal "A". Na Figura 52 pode-se observar o esquema da arquitetura utilizada para os ensaios.

Figura 52 – Diagrama do método de injeção de EFT adotado nos ensaios com o protocolo FlexRay.



Fonte: Autor.

5.4.1 Descrição dos procedimentos para os testes com *FlexRay*

Seguindo a mesma metodologia dos ensaios anteriores, para a realização com o protocolo *FlexRay*, foi configurada uma malha de controle de suspensão ativa composta por três nós distintos, sendo eles, *Sensor, Atuador e Controlador*. Estes nós foram programados ns placas *TMS570LS31HDK*, da familia de processadores *HERCULES*™, onde cada placa exerce uma função específica das acima mencionadas, simulando *ECUs* embarcadas no veículo. Na Tabela 10, podem ser visualizados os dados que são trocados entre estas *ECUs* para a efetivação do controle da malha de suspensão ativa. O conjunto de mensagens listadas na Tabela 10 são transmitidas ciclicamente dentro dos tempos estipulados nos algoritmos de controle, ou seja, período de *5ms*. Esta malha de controle, foi configurada para trabalhar na velocidade de *10 Mbps*, e os dados gerados com estes ensaios foram observados em três condições distintas, sendo elas 2%, 30% e 80% de carga do

Tabela 10 – Configuração dos nós da rede da malha tipo "Quater Car Model".

Nó	Função	Mensagens / TX–RX
Sensor	Conjunto *Massa-Mola-Amortecedor*. Parametros da suspensão ativa.	MSG–Velocidade vertical do corpo MSG–Deflexão da suspensão MSG–Deflexão dos pneus
Atuador	Ajuste da posição vertical da suspensão.	MSG–Ajust–Vert–Susp.
Control.	Calculo da posição apropriada da suspensão e ajuste. Lei de controle	MSG–Alg.–Controle

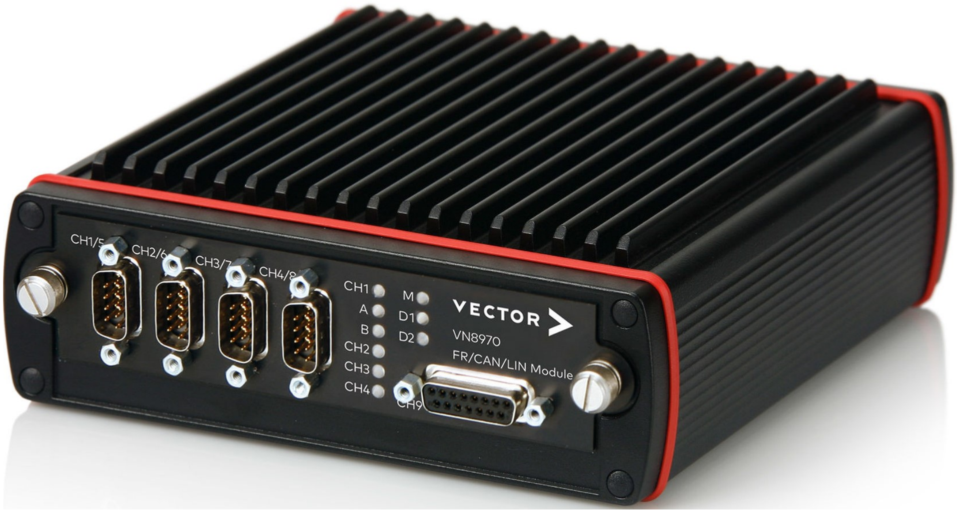
barramento, sendo estas duas últimas obtidas através da injeção de pacotes esporádicos de dados, visando gerar uma carga de comunicação no referido barramento.

Para obter os dados de tempo das transmissões dos pacotes e os respectivos atrasos decorrentes das injeções de ruídos tipo *EFT*, foram utilizados como ferramenta de análise e geração de tráfego na rede dois módulos VN8910A da Vector, sendo o primeiro responsável pela geração de tráfego na rede e o segundo responsável por coletar os dados da comunicação, para que fosse possível utilizá-los na análise do impacto da injeção de ruídos *EFT* através do software CANoe.

A finalidade da coleta destes dados é permitir a análise do mesmos, confrontando os resultados obtidos no cenário sem a injeção de *EFT* e nos demais cenários com as injeções, possibilitando a comparação e o levantamento do real impacto destes distúrbios na comunicação, e principamente sobre as métricas de *Latência e Jitter*.

Para tal coleta, no caso do protocolo *FlexRay*, foi utilizada a ferramenta da Vector CANoe e CAN Analyser e o hardware VN8910A, que pode ser visto na Figura 53. Este módulo ainda é composto da placa de comunicação VN8970, que permite o uso de até quatro canais de comunicação CAN e CAN-FD ou um canal duplo ("A"e "B") para *FlexRay*.

Figura 53 – Hardware da ferramenta CANoe da Vector, utilizada nos ensaios com o protocolo FlexRay.



Fonte: Autor.

5.4.2 Valores de *EFT* utilizados nos testes

Também nos ensaios com o protocolo *FlexRay*, as injeções dos "*BURST*"de *EFT* foram efetuadas de acordo com a Tabela 11, com o barramento de comunicação sendo carregado com dados gerados na ferramenta da Vector. Estes testes foram realizados também de acordo com as normas base deste trabalho, a *IEC 62228 e ISO 26262*.

Tabela 11 – Tabela de sequência de transientes *EFT* para os testes FlexRay

Tensão de pico - Vp	TEMPO de BURST
47 volts	675μs
57 volts	1,2ms
63 volts	500μs

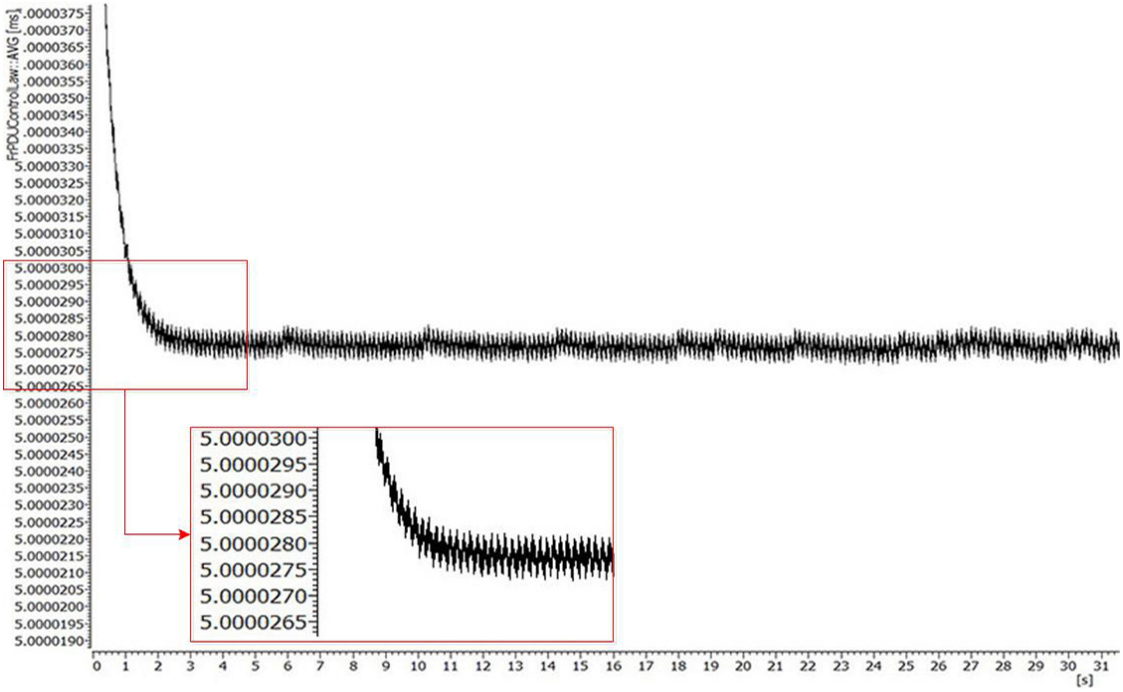
Os mesmos procedimentos utilizados nos ensaios com os protocolos *CAN e CAN-FD* foram aplicados nestes ensaios, ou seja, o valor da tensão de *BURST EFT* aplicado foi ajustado em uma fonte externa, o pulso de trigger para o circuito de injeção do *BURST* é proveniente de um gerador de funções arbitrário também externo. A aferição dos valores, tanto tensão, largura dos pulsos como o tempo de subida (*rise time*) é feita através da leitura destes parâmetros no osciloscópio MSO9104A.

5.4.3 Resultados dos ensaios com o protocolo *FlexRay*

Os ensaios realizados com o protocolo *FlexRay* foram conduzidos com base nas normas *IEC 62228 e ISO 26262* objetivando caracterizar a susceptibilidade deste protocolo perante à ruídos do tipo *EFT*. Para estes ensaios, as três *ECUs* foram configuradas com base nas informações da Tabela 10, cujos dados simulam uma malha de suspensão ativa de uma roda (Quarter Car Model)(AGHARKAKLI; SABET; BAROUZ, 2012).

O ensaio inicial foi realizado considerando a comunicação entre as *ECUs*, sem nenhum tipo de distúrbio injetado na rede, para que fosse possível armazenar os dados de latência e Jitter da comunicação. Com estes dados armazenados, foi possível verificar os tempos de oscilação na comunicação na faixa de 27ns, conforme pode ser visto na Figura 54.

Figura 54 – Lei de controle do protocolo FlexRay sem injeção de *EFT*.

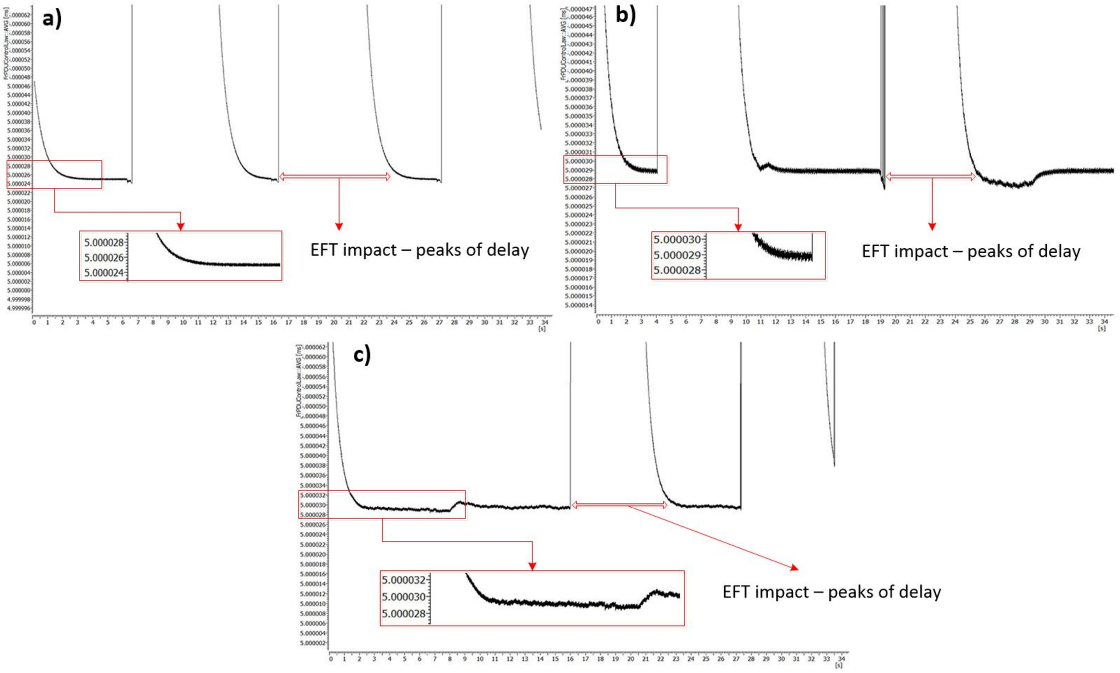


Fonte: Autor.

Os próximos ensaios realizados foram conduzidos com base nos valores contidos na Tabela 11 e com carga de barramento nos valores de 2%, 30% e 80% (cargas geradas através do software CANoe da Vector). Na sequência dos testes, a injeção foi ajustada para os valores de 47Vp e 675μs, sempre obedecendo a lei de controle de 5ms e as cargas de barramento de comunicação de 2%, 30% e 80%.

Nas Figuras 55a, 55b e 55c, o detalhe mostra as oscilações nos tempos de atraso da lei de controle devido à interferência sofrida pelo barramento em consequência da injeção dos *BURST de EFT*.

Figura 55 – Lei de controle do protocolo FlexRay com injeção de *EFT* de 47Vp e 675μs.



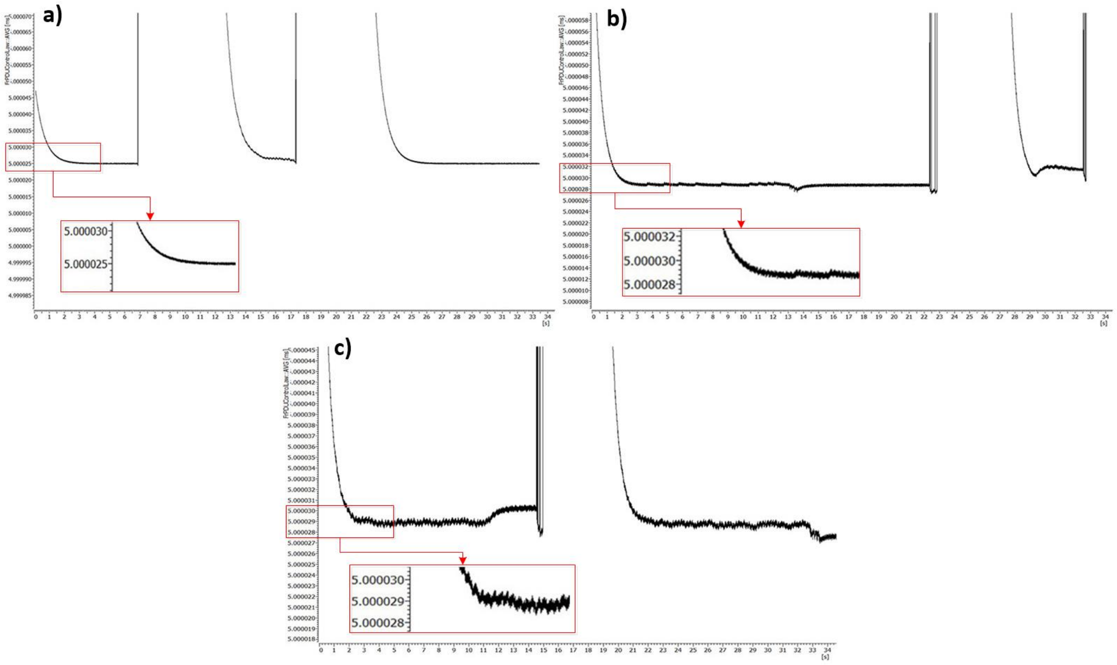
Fonte: Autor.

Nos testes de injeção com EFT de 47Vp e 675μs, observou-se a média de oscilação na lei de controle de 26ns, com carga de 2% (apenas a lei de controle), já com cargas de barramento mais altas (30% e 80%), a oscilação aumenta (evidenciada pelas partes do gráfico realçadas), registrando picos de atraso superiores a 80ns, com maior índice de ocorrências e maior duração.

No segundo ensaio, com injeção de *BURST de EFT* de 57Vp e largura de pulso de 1,2ms, cujos pulsos podem ser visto na Figura 45, o impacto na rede foi semelhante ao ensaio anterior, porém os distúrbios aumentam a média do tempo de atraso da comunicação na ordem de 25 a 30ns. Apesar destes atrasos médios não serem realmente impactantes na comunicação *FlexRay*, os picos que aconteceram decorrentes da injeção, que atingiram a casa de 37μs com a carga do barramento em 2% e 260μs com a carga de 80%, mostra que o impacto é considerável, pois estes tempos realmente são altos para este protocolo. Na Figura 56a podemos ver o gráfico da comunicação com injeção e carga de barramento de 2%, na Figura 56b com carga de 30% e na Figura 56c com carga de 80%. O objetivo do terceiro ensaio era analisar os efeitos na comunicação, quando injetado uma valor maior de tensão, pórém com uma largura menor do pulso de *BURST de EFT*. Neste caso, os resultados mostram que os picos de atraso aumentaram com o aumento do tráfego na rede, enfatizado pelo gráfico da Figura 57. É possível verificar que a média de atraso não retorna ao patamar de normal após transcorridos 27,5s do tempo do ensaio. Ao compararmos com o primeiro ensaio, os resultados mostram um impacto maior com o *BURST de EFT* com largura de pulso menor porém maior amplitude de tensão. Esta situação se reflete na lei de controle com maiores tempos de atraso e aumento nas perdas de pacotes na comunicação. A taxa de erro registrada no software CANoe, aumenta de 33 para 76 pacotes por segundo, respectivamente com as cargas do barramento de 2% e 80%.

Esta sequência de ensaios com as injeções de *BURST de EFT* de 47, 57 e 63Vp, permite uma análise profunda sobre os aspectos negativos que estes distúrbios acarretam no barramento de comunicação do protocolo *FlexRay*. Este protocolo trabalha com uma

Figura 56 – Lei de controle do protocolo FlexRay com injeção de *EFT* de 57Vp e 1,2ms.



Fonte: Autor.

taxa de transmissão de dados bem alta, com slots de comunicação menores, o que permite uma maior largura de banda, que nestes ensaios estavam configurados na casa de 10Mbps.

Como este protocolo tem como prioridades a alta capacidade de taxa de transmissão de dados e a alta confiabilidade na comunicação, as alternativas para mitigar ou eliminar os impactos gerados por elementos externos são de extrema importância. Sistemas de controle focados na segurança do veículo e do passageiro dependem totalmente de um ambiente de comunicação robusta, eficaz e confiável.

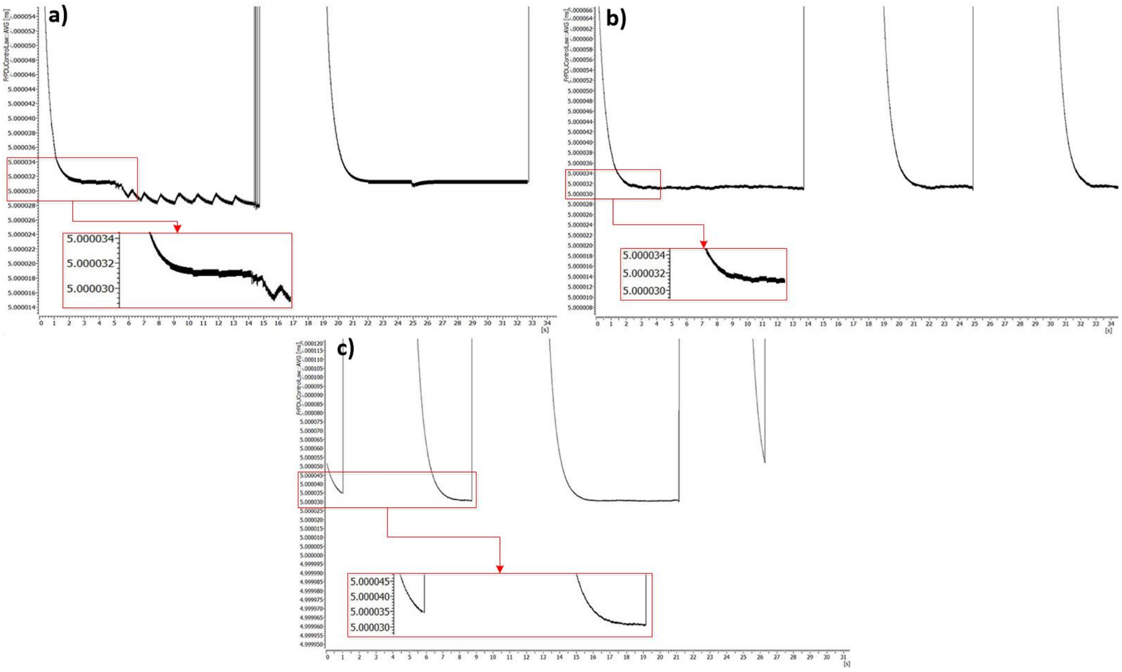
Com o objetivo de evidenciar a degradação da performance gerada pela injeção de ruídos *EFT* no barramento de comunicação do protocolo *FlexRay*, utilizando a metodologia de análise adotada para o experimento, as métricas utilizadas para tal foram o "Diferencial de Jitter"e o "Jitter Médio", cujos dados foram capturados durante os ensaios. Na Tabela 12, são mostrados os valores de tempo da comunicação sem a injeção de *BURST de EFT* e a degradação destes tempos com as respectivas injeções de 47, 57 e 63Vp.

Tabela 12 – Resumo da degradação da comunicação durante os testes com FlexRay

Ensaio	Carga 2%	Carga de 30%	Carga de 80%
SEM EFT	0,0254μs	0,0257μs	0,0259μs
EFT 47Vp - 675μs	5,6μs	13μs	87,6μs
EFT 57Vp - 1,2ms	2,9μs	11,6μs	29,1μs
EFT 63Vp - 500μs	10,1μs	19,9μs	94,5μs

Os dados resultantes da análise com as métricas citadas, mostram os piores efeitos de degradação do desempenho (picos de atraso de 1,2 ms e oscilação média de atraso de até 94,5μs) nos experimentos com 63 volts e 500μs. Observando os dados da Tabela 12, destaca-se o maior efeito de degradação na rede FlexRay com transientes de EFT

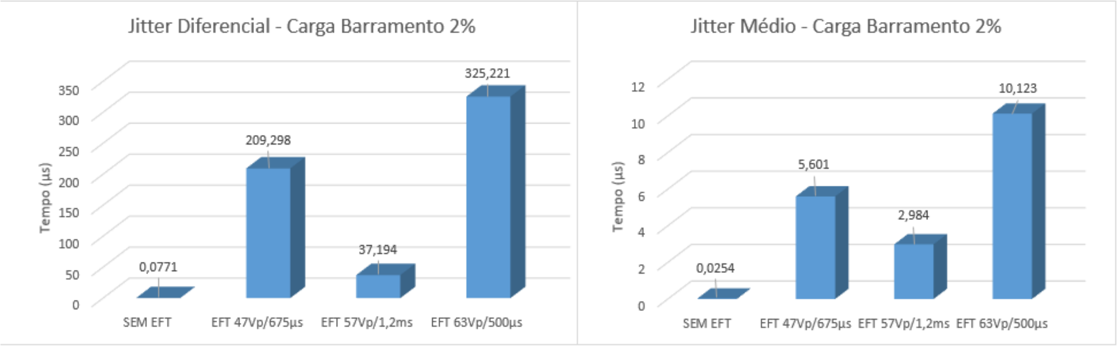
Figura 57 – Lei de controle do protocolo FlexRay com injeção de *EFT* de 63Vp e 500μs.



Fonte: Autor.

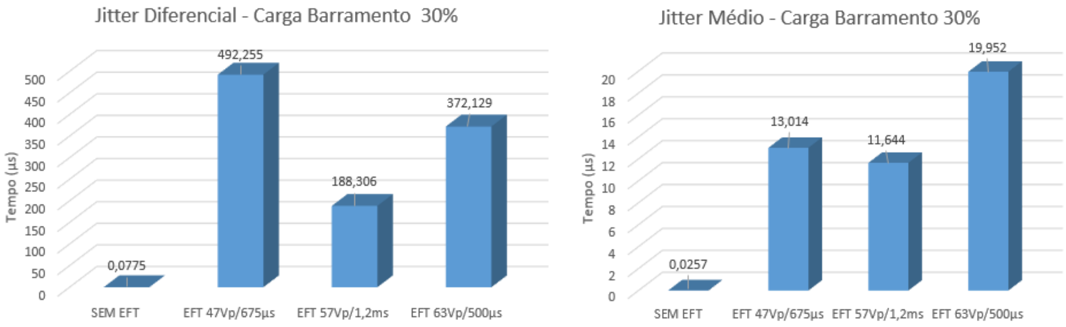
de menor duração do *BURST* e especificamente, com pico mais alto de tensão. Esses valores são justificados pelo fato de que a lei controle utilizada no estudo de caso é de 5ms. Nesse caso, o menor tempo de largura de pulso destes transientes permitem uma chance maior desses pulsos afetarem as mensagens de comunicação entre as *ECUs* com maior frequência. Por outro lado, com uma longa duração de *BURST* (1,2 ms), durante o ciclo da lei de controle, a quantidade de transientes que afetam os dados obtidos da planta do sistema são menores, resultando em menor degradação. É importante destacar o aumento do atraso médio da lei de controle de 397, 774 e 3648 vezes,em todas as cargas de barramento do pior cenário de teste (EFT de 63 volts e 500μs). Vale ressaltar que as análises foram realizadas em um curto período de amostragem, caracterizando análise de susceptibilidade transitória à ruídos do tipo *BURST de EFT*, de acordo com as diretrizes das normas ISO 26262, IEC 61000-4-4 e ISO 7637-3. Nas Figuras 58, 59 e 60 é possivel observar a influência das injeções de *EFT* no barramento de comunicação, com as referidas cargas e valores de tensão e largura de pulsos.

Figura 58 – Grafico das variações de Jitter com carga do barramento de 2%



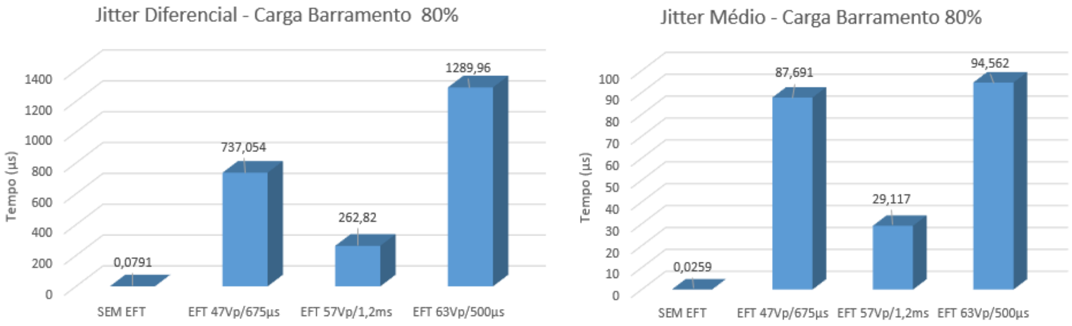
Fonte: Autor.

Figura 59 – Grafico das variações de Jitter com carga do barramento de 30%



Fonte: Autor.

Figura 60 – Grafico das variações de Jitter com carga do barramento de 80%



Fonte: Autor.

As informações obtidas com estes ensaios, enfatizam os efeitos negativos causados no barramento de comunicação *FlexRay* quando submetidos à ruídos do tipo *EFT*, e que este efeito é nocivo aos sistemas críticos de segurança que possuem restrições temporais extremamente rígidas como suspensão ativa, direção assistida, freios ABS, entre outros.

Portanto, monitorar, registrar e analisar estes dados, para que tenhamos conhecimento do comportamento destes ruídos e suas consequências é de extrema importância, seja para uma análise mais criteriosa, seja para a elaboração de processos e sistemas mais robustos e imunes a estes problemas.

6 CONCLUSÕES E TRABALHOS FUTUROS

Estes trabalhos foram motivados tendo como base os problemas gerados por ruídos do tipo *EFT* em protocolos embarcados como o *CAN, CAN-FD e o FlexRay*, principalmente que vários sistemas de segurança instalados nos veículos hoje, utilizam estes protocolos como meio de interface entre os elementos que compôem estes respectivos sistemas.

O fato destes sistemas serem de extrema importância, tanto para segurança dos condutores como do veículo, nos mostra também a importância de entendermos as vulnerabilidades destes protocolos, e como podemos atuar para minimizar ou mesmo mitigar estes efeitos nocivos.

O uso das normas IEC 62228 e ISO 26262 para nortear este trabalho teve como principal objetivo firmar as bases dos testes, para que fosse possível ter parâmetros de comparação e mesmo uma linha de raciocínio concreta e objetiva, pois apesar de serem amplamente utilizados em veículos automotivos, muitas vezes convivendo no mesmo ambiente, estes três protocolos tem características e comportamentos diferentes. Vários ensaios já foram realizados com foco na capacidade destes protocolos, quando submetidos aos ruídos do tipo *EFT*.

Porém, a realidade é que nestes ensaios, as atenções estão focadas nas implicações elétricas dos tranceptores, quando submetidos a ruídos do tipo *EFT* nas linhas de comunicação, alimentação, "wake-up", etc., porém os distúrbios na comunicação, causados por estes ruídos, não são devidamente abordados, bem como soluções para eliminar estas falhas ou ao menos reduzir suas implicações, também não são pesquisadas no mesmo nível de sua importância.

Nestes ensaios o foco foi direcionado para a comunicação, devido a isso, os testes foram moldados observando o uso de situações o mais próximo possível da realidade, com componentes e programações que muito se assemelham às *ECUs* que encontramos instaladas nos veículos hoje, e com as funções respeitando as mesmas restrições temporais que estas *ECUs* respeitam.

Depois de realizar dezenas de ensaios, com os três protocolos, fica evidente o impacto negativo que ruídos gerados de forma espontânea no veículo, por mais simples que seja (ligar o ar condicionado, por exemplo), afetam sistemas críticos como um sistema de freio ABS.

Nos três protocolos os impactos foram consideráveis, porém quanto mais rápido o protocolo, maior o valor de grandeza que afeta os resultados. Ao levarmos em consideração o protocolo *CAN*, os valores de latência e Jitter aumentaram, porém permaneceram na mesma casa de grandeza de tempo, ou seja, milisegundos. Já no protocolo *FlexRay*, com a injeção de ruídos, saímos de latência na ordem de ns para a casa de μs, ou seja, um valor mil vezes maior. Podemos considerar que os valores não afetariam um sistema onde os tempo de latência saem da casa de ns para a casa de μs, mas precisamos avaliar que os projetistas podem ter considerado o tempo de resposta de ns, e neste caso, os atrasos inseridos pelos ruídos comuns do veículos, podem acarretar em prejuízos ou mesmo em risco à segurança.

O fundamento pricipal deste trabalho foi coletar dados para que fosse possível, em um nível superior do estudo, a criação de uma metodologia ou mesmo um sistema que pudesse gerenciar estes dados de forma ativa, e tivesse a capacidade de condensá-los em uma rotina ou algoritmo que pudesse de forma preditiva, identificar estes ruídos na comunicação e agir contra os problemas que ficou evidenciado neste trabalho.

Como parte desta etapa superior, na Tese de doutorado de Alexandre Roque, foi criada uma ferramenta de captura destes dados, visando a continuidade do trabalho, que é a possibilidade de embarcar uma inteligência artificial em conjunto com as *ECUs*, para que estes ruídos possam ser identificados, e medidas pró ativas possam ser adotadas, visando mitigar os problemas aqui descritos.

A continuidade deste trabalho pode focar nesta análise preditiva utilizando a inteligencia artificial, focando em uma plataforma local com capacidade de análise em tempo real e "on line", objetivando aumentar a segurança e a confiabilidade destes sistemas embarcados.

REFERÊNCIAS

AGHARKAKLI, A.; SABET, G. S.; BAROUZ, A. Simulation and analysis of passive and active suspension system using quarter car model for different road profile. **International Journal of Engineering Trends and Technology**, [S.l.], v.3, n.5, p.636–644, 2012.

ARORA, M. **The art of hardware architecture**: design methods and techniques for digital circuits. [S.l.]: Springer Science & Business Media, 2011.

ASHRAE. **Standard 135-2016 – BACnet - A Data Communication Protocol for Building Automation and Control Networks**. [S.l.]: ASHRAE, 2016.

AUTOSAR - Technical Overview. [S.l.]: AUTOSAR–GbR, 2006. 43 p. Disponível em: <https://www.autosar.org/fileadmin/user_upload/standards/classic/2-0/AUTOSAR_TechnicalOverview.pdf>. Acesso em: 26.09.2019.

BAUER, S.; DEUTSCHMANN, B.; WINKLER, G. Prediction of the robustness of integrated circuits against EFT/BURST. In: IEEE INTERNATIONAL SYMPOSIUM ON ELECTROMAGNETIC COMPATIBILITY (EMC), 2015. **Proceedings. . .** IEEE, 2015. p.45–49.

BOSCH, R. CAN with flexible data-rate specification. **Robert Bosch GmbH, Stuttgart**, [S.l.], 2012.

BOSCH, R. et al. CAN specification version 2.0. **Rober Bousch GmbH, Postfach**, [S.l.], v.300240, p.72, 1991.

CENA, G.; DURANTE, L.; VALENZANO, A. Standard field bus networks for industrial applications. **Computer standards & interfaces**, [S.l.], v.17, n.2, p.155–167, 1995.

FENNEL, H. et al. **Achievements and exploitation of the AUTOSAR development partnership**. [S.l.]: SAE Technical Paper, 2006.

FONTANA, M.; HUBING, T. H. Characterization of CAN network susceptibility to EFT transient noise. **IEEE Transactions on Electromagnetic Compatibility**, [S.l.], v.57, n.2, p.188–194, 2015.

GUPTA, R. A.; CHOW, M.-Y. Networked control system: overview and research trends. **IEEE transactions on industrial electronics**, [S.l.], v.57, n.7, p.2527–2535, 2009.

HARTWICH, F. CAN with flexible data-rate. In: INTERNATIONAL CAN CONFERENCE ICC, 2012. **Proceedings. . .** [S.l.: s.n.], 2012. p.1–9.

HESPANHA, J. P.; NAGHSHTABRIZI, P.; XU, Y. A survey of recent results in networked control systems. **Proceedings of the IEEE**, [S.l.], v.95, n.1, p.138–162, 2007.

HUANG, S. et al. Transient fault tolerant control for vehicle brake-by-wire systems. **Reliability Engineering & System Safety**, [S.l.], v.149, p.148–163, 2016.

IEC 60730 and UL 1998 Safety Standard Compliance Made Easier with TI Hercules MCUs. [S.l.]: TEXAS INSTRUMENT, 2013. 6 p. Disponível em: <http://www.ti.com/lit/wp/spny005/spny005.pdf>. Acesso em: 28.09.2019.

IEC-61000/4-4. Electrical Fast Transiente/Burst immunity test. , [S.l.], 2015.

IEC-61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. , [S.l.], 2010.

IEC-62228. EMC evaluation of communication transceivers. , [S.l.], 2016.

ISO-11898/93. Road vehicles–interchange of digital information–Controller Area Network (CAN) for high-speed communication. , [S.l.], 1993.

ISO-14908/1. LonWorks - Local Operating Networks. , [S.l.], 2012.

ISO-17458. FlexRay communications system — General information and use case definition. **Road vehicles-FlexRay communications system**, [S.l.], 2013.

ISO-26262. Draft Road Vehicle - Functional Safety. , [S.l.], 2018.

ISO-7637. Road Vehicles - Electrical disturbances from conduction and coupling. , [S.l.], 2002.

KELKAR, S.; KAMAL, R. Adaptive fault diagnosis algorithm for controller area network. **IEEE transactions on Industrial Electronics**, [S.l.], v.61, n.10, p.5527–5537, 2014.

KER, M.-D.; YEN, C.-C. New transient detection circuit for on-chip protection design against system-level electrical-transient disturbance. **IEEE Transactions on Industrial Electronics**, [S.l.], v.57, n.10, p.3533–3543, 2010.

KUMAR, B. V.; RAMESH, J. Automotive in vehicle network protocols. In: INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATION AND INFORMATICS, 2014. **Proceedings. . .** IEEE, 2014. p.1–5.

LANGE, R. et al. Timing analysis of hybrid FlexRay, CAN-FD and CAN vehicular networks. In: IECON – ANNUAL CONFERENCE OF THE IEEE INDUSTRIAL ELECTRONICS SOCIETY, 2016. **Proceedings. . .** IEEE, 2016. p.4725–4730.

LEE, T.-Y. et al. A Reliability Scheduling Algorithm for the Static Segment of FlexRay on Vehicle Networks. **MDPI - Sensors**, [S.l.], v.18, n.11, p.3783, 2018.

LIU, B.; BAI, W.; ZHEN, G. A prompt retransmission method for in-vehicle network FlexRay. In: IEEE CHINESE CONTROL CONFERENCE (CCC), 2017. **Proceedings. . .** IEEE, 2017. p.7841–7846.

LIXIAN, Z.; HUIJUN, G.; KAYNAK, O. Network-induced constraints in networked control systems—A survey. **IEEE Transactions on Industrial Informatics**, [S.l.], v.9, n.1, p.403–416, 2013.

MAKOWITZ, R.; TEMPLE, C. FlexRay-a communication network for automotive control systems. In: IEEE INTERNATIONAL WORKSHOP ON FACTORY COMMUNICATION SYSTEMS, 2006. **Proceedings. . .** IEEE, 2006. p.207–212.

MARQUES, L. et al. Tolerating transient communication faults with online traffic scheduling. In: IEEE INTERNATIONAL CONFERENCE ON INDUSTRIAL TECHNOLOGY, 2012. **Proceedings. . .** IEEE, 2012. p.396–402.

MARQUES, L. et al. Efficient transient error recovery in FlexRay using the dynamic segment. In: IEEE EMERGING TECHNOLOGY AND FACTORY AUTOMATION (ETFA), 2014. **Proceedings. . .** [S.l.: s.n.], 2014. p.1–4.

MIESTERFELD, F. The Next Generation Vehicle Architecture. **PROGRESS IN TECHNOLOGY**, [S.l.], v.78, p.645–650, 1999.

MODICON. Modbus protocol reference guide. **North Andover, Massachusetts**, [S.l.], p.28–29, 1979.

PANNILA, E.; EDIRISINGHE, M. Power system switching transients in passenger automobiles. In: IEEE INTERNATIONAL CONFERENCE ON INFORMATION AND AUTOMATION FOR SUSTAINABILITY, 2014. **Proceedings. . .** IEEE, 2014. p.1–6.

PATTANAIK, B.; CHANDRASEKARAN, S. Recovery and reliability prediction in fault tolerant automotive embedded system. In: IEEE INTERNATIONAL CONFERENCE ON EMERGING TRENDS IN ELECTRICAL ENGINEERING AND ENERGY MANAGEMENT (ICETEEEM), 2012. **Proceedings. . .** IEEE, 2012. p.257–262.

PIPER, T. et al. Mitigating timing error propagation in mixed-criticality automotive systems. In: IEEE INTERNATIONAL SYMPOSIUM ON REAL-TIME DISTRIBUTED COMPUTING, 2015. **Proceedings. . .** IEEE, 2015. p.102–109.

POHREN, D. H. et al. An Analysis of the Impact of Transient Faults on the Performance of the CAN-FD Protocol. **IEEE Transactions on Industrial Electronics**, [S.l.], v.67, n.3, p.2440–2449, 2019.

RENESAS - In-Vehicle Networking Solutions. Disponível em: <https://www.renesas.com/us/en/solutions/automotive/technology/networking-solutions.html#>. Acesso em: 15.08.2019.

ROQUE, A. S. et al. Communication analysis in CAN networks under EFT injection. In: IEEE INTERNATIONAL CONFERENCE ON AUTOMATICA (ICA-ACCA), 2016. **Proceedings. . .** IEEE, 2016. p.1–6.

ROQUE, A. S. et al. Eft fault impact analysis on performance of critical tasks in intravehicular networks. **IEEE Transactions on Electromagnetic Compatibility**, [S.l.], v.59, n.5, p.1415–1423, 2017.

SCHIFFER, V.; VANGOMPEL, D.; VOSS, R. The common industrial protocol (CIP) and the family of CIP networks. **ODVA**, [S.l.], 2006.

TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks 5th ed.** [S.l.]: Prentice Hall, 1999.

WOO, S. et al. A practical security architecture for in-vehicle CAN-FD. **IEEE Transactions on Intelligent Transportation Systems**, [S.l.], v.17, n.8, p.2248–2261, 2016.

XIA, F.; SUN, Y.-x. **Control and scheduling codesign**: flexible resource management in real-time control systems. [S.l.]: Springer Science & Business Media, 2008.

YIN, S.; HUANG, Z. Performance monitoring for vehicle suspension system via fuzzy positivistic C-means clustering based on accelerometer measurements. **IEEE/ASME Transactions On Mechatronics**, [S.l.], v.20, n.5, p.2613–2620, 2015.

ApêndiceA

A.1 Publicação IEEE - Transactions on Industrial Electronics

An Analysis of the Impact of Transient Faults on the Performance of the CAN-FD Protocol

Daniel Henrique Pohren, *Member, IEEE*, Alexandre dos Santos Roque, *Member, IEEE*, Tiago Antônio Ingracio Kranz, *Member, IEEE*, Edison Pignaton de Freitas, *Member, IEEE*, and Carlos Eduardo Pereira, *Member, IEEE*

***Abstract*—The increasing complexity of distributed real-time control systems in the vehicular area has led to the development of new protocols, such as controller area network with a flexible data rate (CAN-FD), that provides high-bandwidth communication with FD rate. Different topologies are used to interconnect electronic control units in safety-critical applications in the automotive area and the applied communication protocols, such as CAN-FD, must comply with reliability requirements. Moreover, the functional operations must be tested to their limits, since they require appropriate assessment techniques for different application scenarios. Recent research has highlighted that power switching systems cause transient faults that affect the communication network. In light of this concern, this paper explores the IEC/TS 62228:2007 and ISO 26262-3/4/9:2018 standards that can act as guidelines for the development of a test method and testing board for evaluating the impact of electrical fast transients on the performance of a distributed automotive control system. Metrics such as difference jitter, average jitter, and packet loss, are used to determine the fault impact on the control law of a critical vehicular control system. The experiments that were conducted show that during the four test scenarios in which the testing board was used, the average jitter increased from 10.41 to 29.05% in the worst case scenario. These results highlight the importance of carrying out consistent tests to prevent critical situations and that these data can be used in software requirements specification phases to improve reliability in vehicular control systems.**

***Index Terms*—Controller area network with a flexible data rate (CAN-FD), IEC 62228, ISO 26262, reliability, transient faults, vehicular communication protocols.**

I. Introduction

COMMUNICATION protocols are responsible for interconnecting and integrating different control systems in the automotive area by characterizing intravehicular networks [1]. Vehicular communication protocols, such as controller area network (CAN), LIN, and MOST [2], are often employed to interconnect electronic control units (ECUs). Moreover, some of them are responsible for critical control point tasks, for example, traction control systems, active suspension, and brake-by-wire systems, among others [2], [3].

Owing to the increasing complexity of these distributed control systems, the CAN protocol has undergone updating and evolutionary procedures that has led to variations of the original protocol, with the aim of improving reliability and flexibility. With regard to these upgrades and evolutions, the following can be cited: a flexible time-triggered communication system based on CAN (TT-CAN) and a flexible time-triggered communication system based on CAN (FTT-CAN) [4], [5]. According to the reliability goal settings, other automotive protocols designed for safety-critical and fault-tolerant applications have also been developed, such as time-triggered protocol-class C (TTP/C), Byteflight, and FlexRay [2], [6]. By applying the topologies and traits of a physical medium, the FlexRay protocol allows the use of two transmission channels (Channels A and B), where it is possible to configure the transmission rates and bit rates (10, 5, and 2.5 Mbps) and make them more flexible. However, in spite of its ability to achieve high transmission rates, the protocol is not free of faults and often adds high costs to the project [7].

Owing to the increasing demand for higher communication bandwidth in intravehicular networks and the need to meet the requirements of modern vehicular control systems, a new protocol was recently developed by Robert Bosh—GmbH, the CAN with flexible data rate (CAN-FD) [8]. The main innovations of the CAN-FD include an increase in speed (greater than 1 Mbps), and an increase in the amount of transmitted data (from 8 to 64 B). Another important feature is the possibility of increasing the speed of the data packet flow, as long as the transmission has already been started and the network nodes have already been synchronized. By maintaining arbitration mechanisms and the classical CAN message standard, CAN-FD allows an increase in the transmission speed of the other message fields: data length code, data field and checksum (CRC) [8], [9]. Thus, in addition to increasing the baud rate, it is also possible to increase the amount of transmitted data. However, none of these evolved features that are displayed and aggregated by the new CAN-FD protocol, can be included if there is interference or electrical disturbance in the communication protocol.

Manuscript received August 13, 2018; revised November 15, 2018, December 12, 2018, and January 16, 2019; accepted February 1, 2019. Date of publication March 4, 2019; date of current version October 31, 2019. This work was supported by the Electrical Engineering Department of Federal University of Rio Grande do Sul under Grant UFRGS/BRASIL. *(Corresponding author: Daniel Henrique Pohren.)*

The authors are with the Research Group in Control, Automation and Robotics, Electrical Engineering Department, Federal University of Rio Grande do Sul, Porto Alegre, RS 90040-060, Brazil (e-mail: daniel.pohren@ufrgs.br; as.roque@ufrgs.br; tiago.kranz@ufrgs.br; edison.pignaton@inf.ufrgs.br; cpereira@ece.ufrgs.br).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIE.2019.2901639

TABLE I
ACRONYMS

Acronym	Definition
AUTOSAR	AUTomotive Open System ARchitecture
CAN	Controller Area Network
CAN-FD	Controller Area Network With Flexible Data-Rate
CRC	Cyclic Redundancy Check
ECU	Electronic Control Unit
EFT	Electrical Fast Transient
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FTT-CAN	Flexible Time-Triggered communication on CAN
IDS	Intrusion Detection System
IEC	International Engineering Consortium
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport
PCB	Printed Circuit Board
TT-CAN	Time-Triggered Communication on CAN

The results of recent studies [10] and [11] provide evidence that electrical fast transients (EFT) cause disturbance in CAN transceivers. This interference is sporadic and often disrupts the CAN signals, and degrades performance in communication. This increases the number of retransmissions and also completely stops the control system that is embedded in the ECU.

For this reason, the research problem addressed in this paper involves conducting an analysis of performance degradation in the new CAN-FD protocol as a result of faults arising from electromagnetic interference, such as EFT. The research carried out by [12] and [13] provide a brief overview of the fault impact on the performance degradation of the CAN and CAN-FD protocols, but there is a lack of a comprehensive survey that takes account of the electromagnetic compatibility standards. Thus, the objective of this paper is to fill the gap in the test methods described in [12], by focusing on the development of new hardware testing tools that are compliant with IEC 62228 and ISO 26262, as well as conducting new interference tests in the CAN-FD protocol. The choice of this protocol is due to the fact that it is an emerging strategy which has the potential to be widely employed by the vehicular industry although its testing methods have not been explored to determine its vulnerabilities.

The testing approach outlined here allows a communication analysis to be conducted of a critical control system for a transient fault injection and the development of a fault-tolerant mechanism in the future. This analysis is supported by the Vector CANoe/Analyzer (Vector Informatik GmbH) hardware and software platform (VN8970 module), which allows the analysis of the case study set out here.

For the convenience of the readers, Table I was added at the end of this introduction, to provide a list of the main acronyms used in this paper. The rest of this paper is organized as follows. Section II reviews the literature and examines the key-related works. Section III outlines the proposed testing methodology. Section IV describes the case study that is carried out with a specific vehicular control system and the EFT injection method. Section V examines the results of the experiment, and Section VI concludes this paper.

TABLE II
RELATED WORKS SUMMARY

Ref.	Main Approach	Gap / Research opportunities
[10]	Statistics of transient faults in automotive electrical systems	Tests do not consider the impact on communication
[11]	EFT impact analysis in CAN transceiver ports	Tests only consider the susceptibility of EFT and not the system propagation
[12]	Impact analysis of EFT faults on CAN protocol and critical control systems	Tests only in CAN protocol and not using test standards
[13]	Tests comparing the greater data capacity of CAN-FD over conventional CAN	Tests only with simulations and without interferences on communication
[14]	Transient detection circuit for on-chip protection against EFT	The work emphasized the EFT disturbance problem. Lack of network level tests against EFT
[15]	Conducted noise disturbances in power distribution, transient detection circuit for on-chip protection	Test conducted and only based on Fieldbus protocol. The work emphasized the EFT impact in protocols.
[16]	EFT analysis in a small control plant	Test do not consider critical tasks with hard time constraints
[17]	Attacks in the communication network focus on an IDS	The work not evaluate how attacks affect the communication performance
[18]	An adaptive algorithm for fault diagnosis on CAN networks	Correlation between physical faults events and diagnosis process
[19]	Performance analysis of the FlexRay communication	Tests with simulations and without physical systems
[20]	A fault detection method and a performance analysis of the vehicle suspension system	Tests do not consider the communication network and protocols
[21]	Interconnection and the coexistence analysis of different protocols	Performance and noise analysis were not considered
[22]	A security architecture for in-vehicle CAN-FD network	Performance and noise analysis were not considered
[23]	Gateway system for message routing in CAN and CAN-FD mixed networks	Analysis of the routing method under faults was not considered
[This Paper]	Development of a test board according to ISO 62228 for fault impact analysis on CAN-FD protocol	(Covered Gap) Real test scenario for performance analysis of CAN-FD under transient fault injection

II. Related Works

Recently, there have been a number of studies concerned with identifying, mitigating, or even eliminating the damage caused by EFT noise on communication buses, whether these buses are designed to meet these immunity requirements or even older buses without these requirements. In [14], emphasis is laid on the system-level protection against electrical-transient disturbance with the aim of detecting positive and negative electrical transients. As a result of this paper, the transient immunity against EFT is improved by focusing on microelectronic products based on complementary metal oxide semiconductor (CMOS) integrated circuits. The EFT problem is addressed, but it is also worth noting that impact analyses are needed at other levels. In [15], tests are carried out on electromagnetic compatibility and the EFT impact on Fieldbus communication; this provides a new physical layer for industrial Fieldbus networks and improves the immunity system obtained against conducted noise. The test results confirm that there have been improvements against EFT on the sensor/actuator connection side. This paper shows how disturbances caused by EFT degrade industrial systems, but also suggests that these effects could be studied in other industrial applications.

With regard to susceptibility to EFT in the automotive area, in [10], the authors carried out a survey of the transient faults caused by automotive electrical systems. The transient measurement statistics in a real automotive chassis are set out on the basis of three operational systems: ignition, ac, and headlights. The data are shown with a time range duration and peak amplitude in volts. Another research study in the area discussed in [11], which examines the susceptibility of the CAN to EFT transceivers, highlights the impact made on the CAN signals (according to IEC TS 62228). However, neither of these studies states whether or not these faults degrade the performance of the control system in operation, and they fail to take account of the performance metrics of the protocol.

The study carried out in [16] shows the impact analysis of the EFT in a generic plant with a closed-loop control, but without being subject to any specific time constraints. In a different and more extensive way, Roque *et al.* [12] shows a concern about the impact of noise from EFT on a CAN network, and highlights the following factors: this fault type can lead to deviations of communication in mean time (jitter), increase communication delays (latency) and loss of packets, or even damage the CAN communication drivers. However, this paper only focused on ordinary CAN communication, and thus failed to analyze other protocols, such as CAN-FD, as well as not being compliant with the standards.

The accelerated growth of distributed embedded systems, makes the concern with the use of the communication buses increasingly important. Moreover, it has led to the development of other alternatives that are faster, safer, and more reliable, as examined in [13], which focused on the CAN-FD protocol and took into account that it had a greater data capacity than the conventional CAN. However, the tests and results were within the scope of the simulations, since there were no real tests, or any relation to the problem of noise in the communication and its possible impacts.

In the experiment described in [17], attention was paid to attacks in the communication network, which could either be some type of external communication or even failures resulting from lost communication with the nodes themselves. The idea of using an intrusion detection system through time windows can be feasible, but one must analyze this methodology in the real world, where there are not only intrinsic communication problems, but also other external kinds of interference, such as EFT noise. The analysis of this paper did not take into account how these attacks affect communication and the related timing properties (jitter, latency, etc.) as well as whether they would be resistant to EFT noise.

In a similar way, in [18], the authors investigated fault diagnosis techniques to mitigate their impact on a CAN-based distributed system. An adaptive fault diagnosis algorithm was created, to detect faulty nodes in the network and at the same time, allow a new node entry point during a diagnostic cycle. The results of this paper provide evidence of the possibility of making a diagnosis in real time. However, if the diagnosis is correlated with faults and transient events such as EFT, it is possible to make improvements by means of new diagnostic mechanisms.

In [19], a performance analysis was conducted of the FlexRay communications system that requires a deterministic strategy for the tasks carried out by the different nodes. The example in this case was the “quarter-car” model, which was based on two control strategies, and designed to analyze communications between the sensor, the actuator, and the controller. In this paper, all the information provided and collected was obtained through simulations, without the use of physical systems, and also in a “controlled” environment. Moreover, it did not take account of any interference from other embedded systems, such as transient faults.

The work in [20] presents a performance analysis for a vehicle suspension system, based on a method for fault detection and isolation. The method uses data collected from four accelerometers installed in the corners of the vehicle. The computation is made based on a technique that distinguishes fault from nonfaulty data, in this paper the fuzzy positivistic C-means clustering and fault lines algorithm. The performance and effectiveness of the method are demonstrated by simulation on a benchmark. Despite its contributions, the referred work does not consider data from vehicular networks. Conversely, the practical analysis here presented shows the importance of the reliability and safety of these systems.

The study carried out in [21] was based on the growing need for the use of several different elements embedded in vehicles, which may require interconnection between different buses, such as CAN, FlexRay, and CAN-FD, with the assistance of gateways. The use of this type of mix bus, combined with the use of gateways, can increase the susceptibility of communication to noise and the coexistence of delays in the environment where these systems are installed (as well as those included by the new installed components themselves). However, the communication parameters (jitter, latency, packet loss, etc.) and EFT noise were not taken into account in their study, and in addition, the data collected were obtained through simulations.

Another significant study in the area is described in [22] where a security architecture was designed for invehicle CAN-FD, which includes the features of the ISO 26262 Automotive Safety Integrity Level. This paper provided a key management design, data encryption, and authentication protocols for CAN-FD, and conducted a performance analysis of the security architecture based on an attack model. However, this paper evaluated the CAN-FD protocol from a security perspective, but failed to address the question of noise and interference and their effects on the performance of the protocol, which are related to safety factors.

The work in [23] sets out a gateway system for a CAN and CAN-FD mix network based on an effective routing method. This paper analyzes the transmission time and the gateway processing time for each message, with different payloads and in accordance with the state of the CAN-FD network. In addition, a buffer memory was allocated to transmit the CAN-FD data to avoid missing data. Although this paper includes a discussion of CAN-FD routing messages, there is a lack of concern about how the routing algorithm will react to several kinds of interference and transient faults. Table II provides a summary of the main points concerning the gap explored in this paper with regard to what has been found in the literature.

On the basis of these studies, it can be concluded that real control situations with complex and critical applications need proactive and real-time measures. Thus, the behavior of the protocol must be analyzed in fault situations, that can allow the design and development of fault-tolerant systems and hence ensure a greater survival capacity and maximize the system lifetime.

III. Analysis of the Methodology

In distributed embedded vehicular control systems, almost all the tasks are carried out by controllers using data from a number of distributed nodes, which communicate within a network in which these nodes are interconnected. This makes data determinism and control logic important for a satisfactory response to the actuator parts of the overall system [?]. This type of communication network is exposed to external disturbances, such as EFTs, which can disrupt signals by interfering with the parameters of the network, such as latency and jitter. These interferences in real-time systems affect the performance and lead to critical situations that may cause very serious problems. The purpose of these experiments was to determine if the communication networks in embedded vehicular control systems are affected by EFTs. This task involved conducting tests based on the standards of IEC 62228 (EMC evaluation of CAN transceivers) and ISO 26262 (road vehicle functional safety services) and their respective bases, which are the standards of IEC 61000-4-4 (testing and measurement techniques—EFT/burst immunity test) and ISO 7637-3 (electrical transient transmission by capacitive and inductive coupling through means other than supply lines). The experiments were carried out in a communication network using the CAN-FD protocol.

The hardware that was used consists of a board developed by the manufacturer called Texas Instruments Incorporated, which uses a Hercules series processor, the TMS570LS3137, which was designed to address the safety standards for intravehicular systems specified in the IEC 62228 and ISO 61508. These standards serve as the basis for determining if a system is compliant with AUTOSAR. This processor has been designed to handle security and reliability issues, as well as being used in CAN, CAN-FD, FlexRay, and LIN protocols. The second part of the hardware was designed especially for the tests, and complied with the guidelines laid down by the abovementioned standards. In addition to the processor, the transceivers and controllers used for communication must also meet the respective standards. The CAN-FD communication is compliant with ISO 11898-1 and 11898-2 uses the MCP2517FD from Microchip as an external controller, as well as the TCAN332G transceiver from Texas Instruments. The board was prepared for future tests with FlexRay communication, by means of the TJA1080A transceiver from NXP, which complies with ISO 17458-2013.

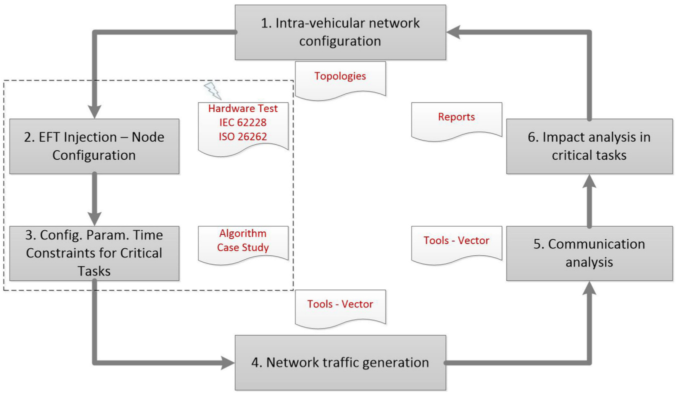
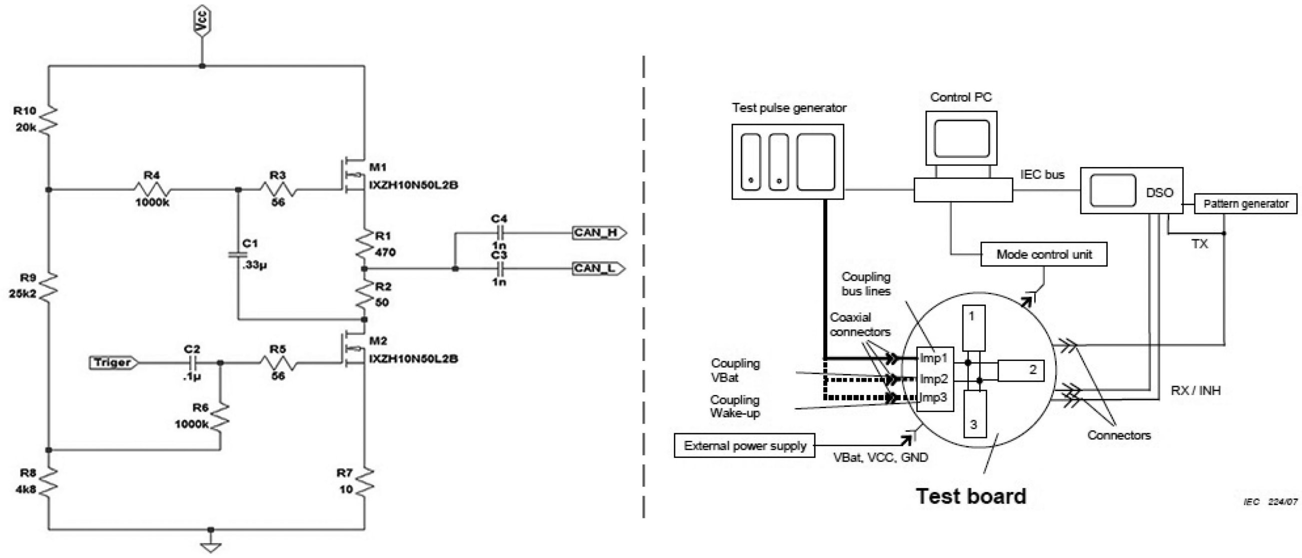

1. Intra-vehicular network configuration
Topologies
Hardware Test
IEC 62228
ISO 26262
Reports
2. EFT Injection – Node Configuration
6. Impact analysis in critical tasks
3. Config. Param. Time Constraints for Critical Tasks
Algorithm Case Study
Tools - Vector
5. Communication analysis
Tools - Vector
4. Network traffic generation

Fig. 1. Flowchart of the applied test method. Based on [12].

The printed circuit board design (PCB) also meets the requirements stipulated in IEC 61000-4-4 [24], [25] and ISO 7637-3 [26], [27]. Fig. 1 shows the flowchart for the test method that is employed in this experimental study. It has benefited from advances made in a previous study described in [12], and also filled the gap that existed with regard to the use of the ISO 62228 standard, which was not included in that study. The dotted lines in Fig. 1 (covering Stages 2 and 3) show to what extent the test method has been updated.

Stage 1 represents the configuration of the networked vehicular system, in which a critical control system was programmed and embedded in the ECU nodes, based on an adaptation of an active suspension system set out in [19] and the quarter-car model developed in [28]. Stage 2 represents the EFT injection that was investigated by means of the developed EFT board. In the case of Stage 3, time constraints and a cycle time were used with regard to the implemented active control system as a setup to define parametrization. In Stage 4, traffic is generated in the network with the aim of observing the network behavior when there is a high bus load. The experimental analysis with vector tools (i.e., the CAN Analyser) is conducted in Stages 5 and 6. This means that the new experiments can be tuned to start a new turn. The next section provides details of the experimental case study and analyzes the performance impact of EFT faults on the CAN-FD protocol.



(a) (b)

Fig. 2. (a) EFT injector power stage schematic. (b) Test Board IEC 62228.

IV. Case Study

As the work is based on the standards IEC 62228 and ISO 26262, both the EFT injection circuit and the board that brings together the transceivers and communication lines CAN, CAN-FD, and FlexRay, must also comply with these standards. Thus, the use of a digital pulse conditioning circuit was designed in conjunction with a power section using the YXIS MOSFET type transistor model IXZH10N50L2B, with low capacitance L-MOS technology for RF applications. This transistor meets the low rise and fall time parameters as well as the ability of high currents and working voltages. Fig. 2(a) shows the schematic diagram of a power stage in the EFT pulse generator that is employed in the tests.

The pulse control circuit consists of a set of inductors, capacitors, and transistors that are mounted to generate very fast pulses. This circuit receives signals from an arbitrary function generator in an external trigger system, that is configured to generate pulses of the "burst" type. Thus, it sends a trigger pulse to the power stage, with a rise and fall time less than 5 ns, while ensuring that this time is repeated during the power output stage, through IXYS MOSFET transistors. This power stage is powered by an external voltage source, which supplies values between 30 and 70 V.

In order to be able to perform all the tests, and to fulfill the various standards that affect the communication in CAN, CAN-FD, and FlexRay, building a dedicated hardware is necessary, considering the premises required by the considered standards. As the TMS570LS3137 processor was adopted, it was possible to meet these standards. The TMS570LS3137 has two FlexRay and four CAN channels apart from three SPI channels, and this enables the FlexRay communication to be submitted both in channel A and in channel B. This flexibility facilitated the implementation of a hardware that allowed three CPU boards to be interconnected, each of which controls a FlexRay node (channel A and channel B) and a CAN-FD node through the CAN-FD external controller. The real-time operating system (FreeRTOS) that was used, was based on the assumptions about time constraints and determinism. This has been endorsed by Texas itself which means it can be used with the Hercules processor family (that comprise the controller nodes, sensor, and actuator used in the case study). Thus, the test board was designed with three 80-pin header connectors, to which each CPU board is connected. EFT injections are carried out directly through a BNC-type connector, where the three CAN-FD transceivers are interconnected at the junction. In the FlexRay communication, where there are six transceivers (three for channel A and three for channel B), the injections are carried out independently in each channel, through a BNC connector for each communication channel. This same scheme is used for the common power supply of the board, which supplies power for all the transceivers and also the CPU cards, as well as complying with the IEC 62228 standard. The basic assembly scheme that is prepared for the EFT injection tests in accordance with IEC 62228 standard, is shown in Fig. 2(b). The test board must contain at least three CAN transceivers, have an external power supply, and include an EFT point attached to a coaxial cable connector. The PCB was built in line with IEC 62228, having its nodes arranged in a "star" topology, as required by the standard, and using three CAN-FD transceivers in the same board.

In Fig. 3, an image is displayed of the entire system assembled for the tests, including the PCB developed for the EFT injections and the Hercules processor boards connected to it.

V. Tests and Results

A. Description of the Test Procedure

The test method followed the stages outlined in Fig. 1, with different fault injection configurations. The configured network

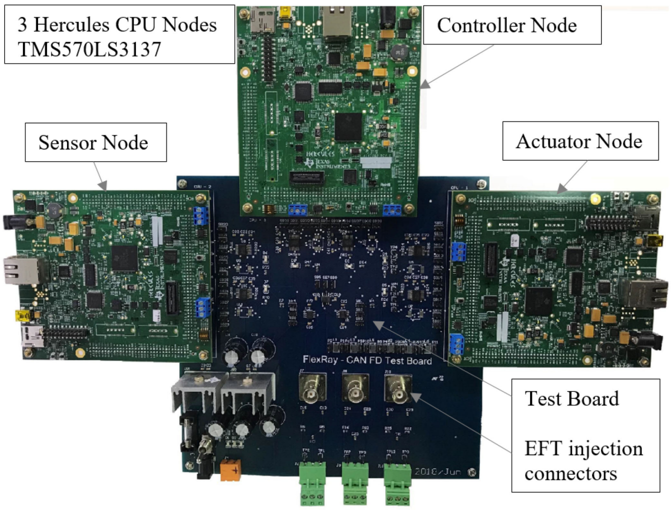


Fig. 3. PCB board developed for the EFT injection with the external CPUs connected on it.

TABLE III
NODES CONFIGURATION

Node	Function	Data / TX–RX messages
Sensor	Mass-spring-damper assemblies. Parameters of the suspension system.	MSG–Body–Vert–Speed MSG–Susp–Deflection MSG–Tire–Deflection
Actuator	Adjustments in the vertical position of the suspension assembly	MSG–Susp–Set–Vert–Speed
Controller	Computation of the appropriate levels of suspension parameter settings. Control Law	MSG–Control–Law

is based on the CAN-FD protocol and represents the normal operating conditions of the implemented distributed control system (active suspension control system) [19] with a sensor node, an actuator, and a controller, running at a regular cycle time of 5 ms. Table III shows details of the configuration used in each node of these vehicular control systems, and is based on the quarter-car model.

The messages defined above are transmitted cyclically, and represent the standard operating conditions of the control system. In accordance with these node parameters, the CAN-FD network was configured to operate with 1 and 4 MBps during the experiments and with five data packets of 8 B each. These packets are linked to the control law for messages and the others are related to the plant behavior (i.e., the sensors and actuators). Different payloads were sent through the CAN-FD network to increase the bus load during the experiment.

Moreover, the bus load was between 30% and 60% because the traffic messages were randomly generated. The tests were designed to determine the influence of EFT and register the communication logs. The tools used in each stage can be listed as follows: Stage 1: the network based on the CAN-FD protocol; Stage 2: EFT injection with the developed hardware based on IEC 62228 and ISO 26262; and Stage 3: traffic generation and communication analysis by means of the Vector CAN Analyzer (based on the registered logs).

TABLE IV
SEQUENCE OF EFT TESTS

Voltage Peak	Burst Time
47 volts	687 us
57 volts	1,2 ms
63 volts	500 us
67 volts	500 us

EFT consists of bursts with variable amplitudes generated in networks from different noise sources (ignition, headlights, air conditioners, and others). The degree of applicability of the test board was determined by injecting a series of disturbances into the network during the control system processing. The pulses were generated by means of an arbitrary waveform generator. Table IV shows the sequence followed by the fault injections.

The following section sets out the measurements that were calculated to check each injected pulse in the CAN-FD network. An Agilent oscilloscope mod. MSO9104A was used to measure the EFT pulses injected in the communication bus. Fig. 4(a) and (b) displays pulses of 47 and 57 of peak voltage, respectively, to show how these pulses were determined during the experiment.

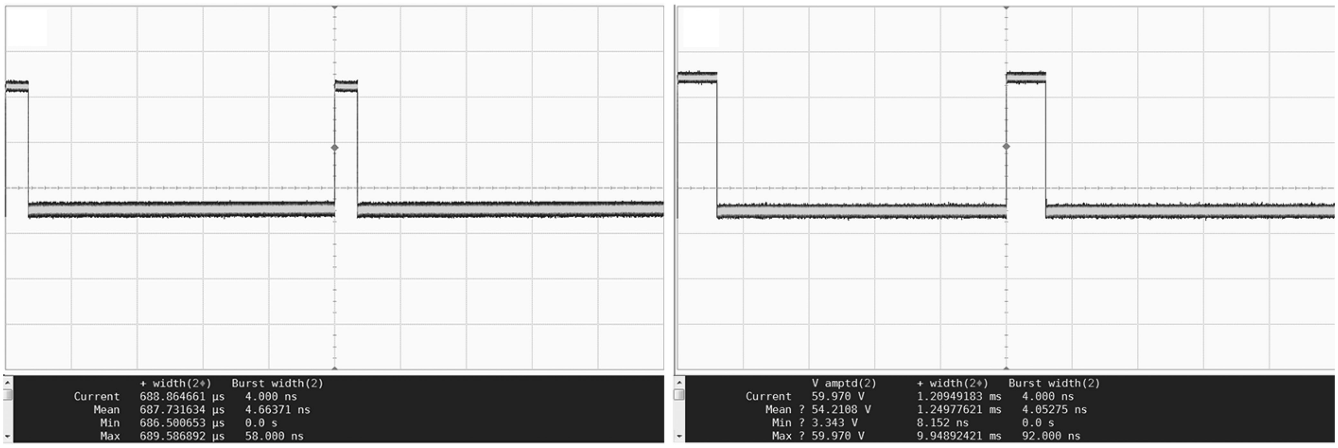
B. Results

A series of communication tests was conducted in accordance with the EFT signals that were generated, so that the control system could be monitored through the transmission of a specific control law message. The message sent through the control law is the result of the control model in computing (i.e., the ECU) after messages have been received from the plant behavior (ECU sensor and ECU actuator), as shown in Table III. Details of the control system that is used are given in [19] and [28].

The experiment checked the communication logs registered by the Vector CAN Analyzer (Vector Informatik GmbH) and then the corresponding graphs were plotted for their analysis. For comparison purposes, before plotting the test sequence, a measurement of network communications was carried out without the EFT injection pulses. All the measurements were based on a 30-s period of stored and analyzed logs. Fig. 5 shows the measurement of the control law without an EFT injection.

The graph in Fig. 5 shows the sampled period of the communication with cycle ranges between 4.4 and 5.6 ms. It should be noted that this is a real network (where the ECUs are connected to CAN-FD cables according to a real automotive application scenario) where fluctuations are normal and very frequent, but with short time variations.

The reason for these fluctuations is the time variation between the received packet in the previous control law and the packet sent in the next control law. The graph in Fig. 6(a) shows the



```
              + width(2♦)     Burst width(2)
    Current   688.864661 µs   4.000 ns
       Mean   687.731634 µs   4.66371 ns
        Min   686.500653 µs   0.0 s
        Max   689.586892 µs   58.000 ns
```

(a)

```
              V amptd(2)      + width(2♦)     Burst width(2)
    Current   59.970 V        1.20949183 ms   4.000 ns
     Mean ? 54.2108 V         1.24977621 ms   4.05275 ns
      Min ? 3.343 V           8.152 ns        0.0 s
      Max ? 59.970 V          9.94892421 ms   92.000 ns
```

(b)

Fig. 4. Measured EFT pulses. (a) 47 V_p and burst of 687 μs. (b) 57 V_p and burst of 1.2 ms.

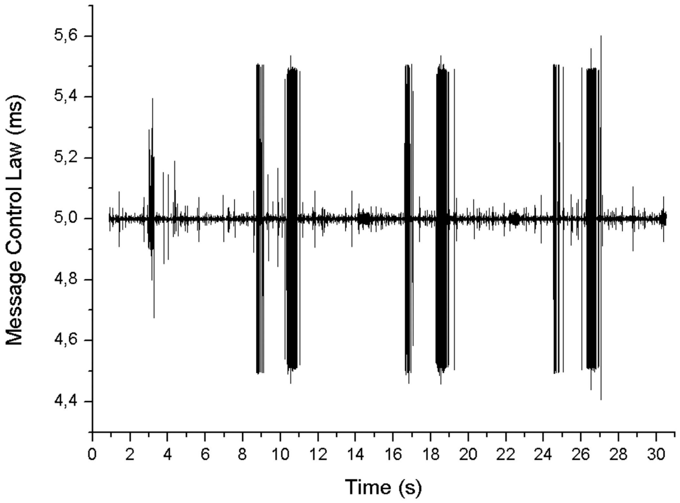


Fig. 5. Control law without EFT injection.

communications performance metrics with 47 V of EFT and 687 μs of burst duration. The graph in Fig. 6(b) shows the communications performance with 57 V of EFT and 1200 μs of burst duration.

Both graphs in Fig. 6(a) and (b) show the impact of the communication cycle on the performance, and highlight the peaks delay that occurs between the messages, and ranges from 4 to 6 ms. It can be seen that there is an increase in the number of messages with a delay of more than 5.2 ms, as well as the frequency of their fluctuations and peaks.

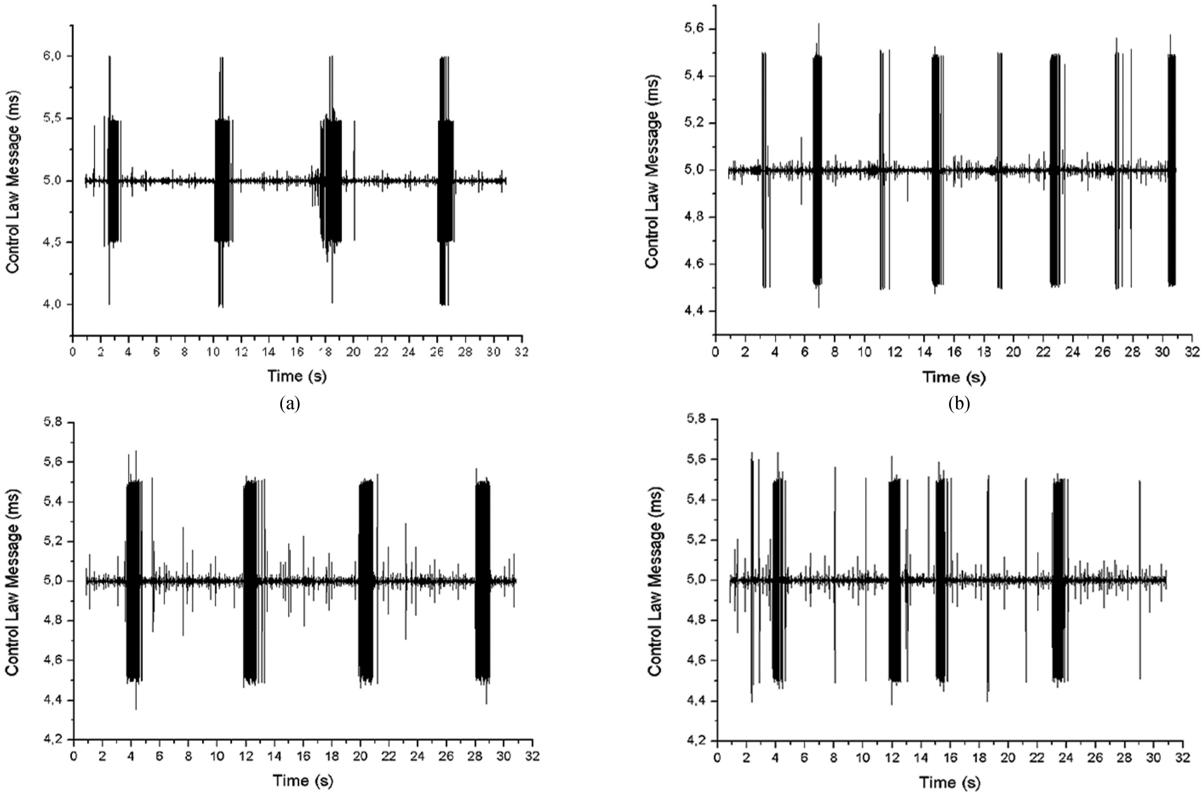
The graphs in Fig. 6(c) and (d) show the records of the control law messages with EFT of 63 and 67 peak voltage and with a burst time of 500 μs. This test was carried out to check the behavior of the control system in the event of a short burst of fault injections, but with higher voltages.

It was observed in the experiments that when there were 47 V and burst injections of 687 μs the effects in terms of delay were higher, but with a lower occurrence frequency. On the other hand, with fault injections with higher voltages and smaller bursts, the effect is not so remarkable, but the occurrence frequency of delays in the control cycles is greater. The reason for this contrast is that with larger bursts, the chance of EFTs generating retransmissions in a given message sequence is greater than with smaller bursts. However, with a higher voltage of EFT injection (i.e., above 65 V), the frequency of delays in control cycles is sporadic, while in larger amounts it can often generate error frames (around 131), as can be seen in the statistics provided by the CAN Analyzer shown in Fig. 7.

Fig. 7 displays a print screen report obtained from the Vector CAN Analyzer during the tests with EFT injections. These statistics provide information about the negative impact of fast transients on the CAN-FD network, and draw attention to the following: 1) the total number of error frames (131); 2) the chip state with detected transmission errors (80); and 3) the average number of error frames (between 4 and 21). All these data were obtained during 32 s of measured time with EFT fault injections and bus loads that fluctuated between 30% and 60%.

On the basis of this analysis, Fig. 8(a) and (b) provides a summary of the CAN-FD network performance for the control system that was used. The assessment metrics were difference jitter and average jitter. The difference jitter is obtained by subtracting the best-case transmission time from the worst-case transmission time and also from the set of measurements from the sample. The average jitter is represented by the standard deviation in the estimated average transmission time for the messages.

In reality, in all the scenarios, stress is laid on the importance of preventing the effects of electrical transients in both CAN transceivers and the control cycle. There is an increasing occurrence of performance degradation which causes delays that can often be critical to control systems, especially in hard real-time message traffic. As can be seen in Fig. 8(b), when compared with the sample set measured without an EFT injection, the average increases in jitter were as follows: 29.05% (EFT of 47 V_p), 10.41% (EFT of 57 V_p), 11.56% (EFT of 63 V_p), and 15.61%



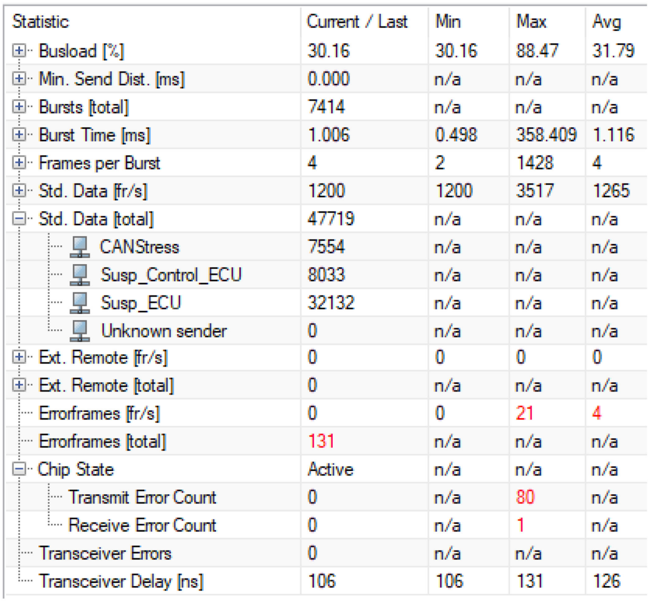
(a)

(b)

(c)

(d)

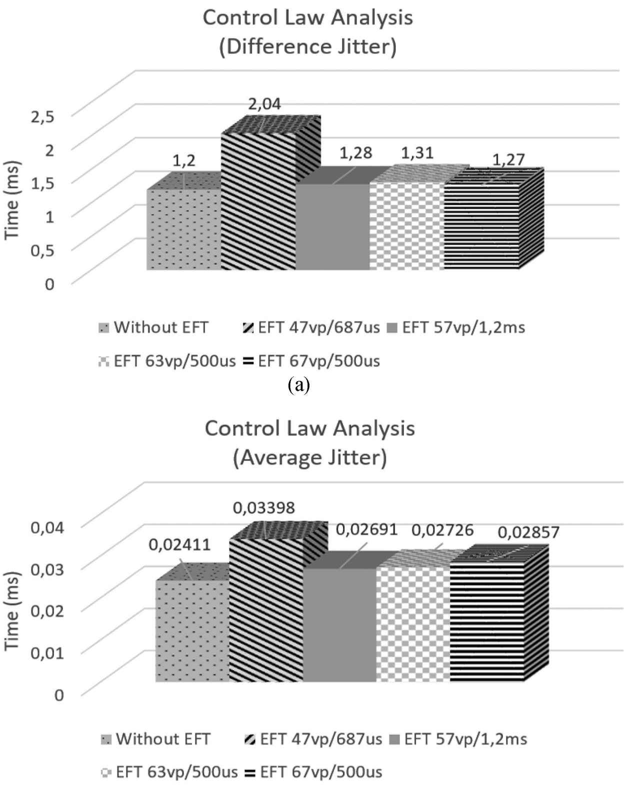
Fig. 6. Control law with EFT injections. (a) EFT 47vp and burst 687 us. (b) EFT 57vp and burst 1,2 ms. (c) EFT 63vp and burst 500 us. (d) EFT 67vp and burst 500 us.



Statistic	Current / Last	Min	Max	Avg
⊞ Busload [%]	30.16	30.16	88.47	31.79
⊞ Min. Send Dist. [ms]	0.000	n/a	n/a	n/a
⊞ Bursts [total]	7414	n/a	n/a	n/a
⊞ Burst Time [ms]	1.006	0.498	358.409	1.116
⊞ Frames per Burst	4	2	1428	4
⊞ Std. Data [fr/s]	1200	1200	3517	1265
⊟ Std. Data [total]	47719	n/a	n/a	n/a
CANStress	7554	n/a	n/a	n/a
Susp_Control_ECU	8033	n/a	n/a	n/a
Susp_ECU	32132	n/a	n/a	n/a
Unknown sender	0	n/a	n/a	n/a
⊞ Ext. Remote [fr/s]	0	0	0	0
⊞ Ext. Remote [total]	0	n/a	n/a	n/a
Errorframes [fr/s]	0	0	21	4
Errorframes [total]	131	n/a	n/a	n/a
⊟ Chip State	Active	n/a	n/a	n/a
Transmit Error Count	0	n/a	80	n/a
Receive Error Count	0	n/a	1	n/a
Transceiver Errors	0	n/a	n/a	n/a
Transceiver Delay [ns]	106	106	131	126

Fig. 7. Statistics provided by CAN Analyser during EFT 67 V_p.

(EFT of 67 V_p). This criticality is highlighted in standards such as ISO 26262, because the effects of performance degradation entails risks and affects the safety and reliability of embedded distributed control systems, such as those in intravehicular networks.



(a)

(b)

Fig. 8. Difference and average jitter in control law messages.

VI. Conclusion

This paper showed the results of a performance analysis of the CAN-FD protocol through a method of EFT injection. The main contribution made in this paper was the development of a new test board based on a test method that met the requirements of the IEC 62228, ISO 7637-3, and ISO 26262 standards. It also addressed the question of the rise and fall times (less than 5 ns) for each EFT injection performed in the experiments. In previous studies [10]–[13] and [16], tests were carried out to measure susceptibility to EFT and its impact on the CAN protocol, either with a nonstandard compliant EFT board or just through simulation, and with a low bandwidth usage of the network. In contrast, this paper complied with the abovementioned standards, increased the network bandwidth usage and showed how EFT degrade performance in a different and emerging vehicular communication protocol (CAN-FD).

Experiments were conducted with a critical control system embedded in the control board and based on FreeRTOS (TMS570LS3137). In addition, the communication system was analyzed with logs generated by Vector CAN Analyzer software. The control law represents a predefined time constraint for all control messages that have a period of 5 ms.

These experiments showed an increase in the difference jitter and average jitter of the control law, with an EFT injection of 47, 57, 63, and 67 peak voltages, and burst time variation ranging between 500 and 1200 μs, to determine the effects on the network performance. It was found that EFT could cause delays in control communications from around 10 to 30%. As in the CAN protocol, transient faults degrade the performance of distributed control systems that are based on the CAN-FD protocol. These transients affect the communication in ways ranging from a simple increase in latency and jitter to severe packet loss. The test method allowed an analysis to be conducted of networked control systems in safe-critical control applications, while also assisting in the design of future fault-tolerant systems. However, the current work had limitations since, for example, it only focused on vehicular communication protocols in one type of fault test, and still lacks to examine other related real-time domains, such as avionic systems.

The obtained results also revealed that delays were significant and could affect the reliability of the CAN-FD protocol. As observed in the experiments, the cause of the degradation was the disruption of CAN signals. Thus, the control law starts and ends at different times, and also results in fault behavior that can lead to more retransmissions and packet losses (Fig. 7).

Future work can be developed aiming at a reliability assessment based on a fault tree analysis employing methods as those recommended in [29], which can be used to detect the main causes of the faults. Other future works could move into the direction of applying the test method to different types of communication protocols and critical real-time control systems as well as other vehicular networks, such as those in avionic systems.

Acknowledgment

The authors would like to thank Vector Informatik GmbH and Vector Brazil for providing the CANoe/CANAnalyser license used to perform the analyses of the experiments in this paper, and DHP Prodepred, that did not measure efforts, providing equipment and infrastructure to carry out the necessary studies.

References

[1] D. Gessner, M. Barranco, A. Ballesteros, and J. Proenza, “sfiCAN: A star-based physical fault-injection infrastructure for CAN networks,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1335–1349, Mar. 2014.

[2] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, “Intra-vehicle networks: A review,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 534–545, Apr. 2015.

[3] T. Piper, S. Winter, O. Schwahn, S. Bidarahalli, and N. Suri, “Mitigating timing error propagation in mixed-criticality automotive systems,” in *Proc. IEEE 18th Int. Symp. Real-Time Distrib. Comput.*, 2015, pp. 102–109.

[4] B. Kumar and J. Ramesh, “Automotive in vehicle network protocols,” in *Proc. IEEE Conf. Comput. Commun. Inform.*, 2014, pp. 1–5.

[5] L. Marques, V. Vasconcelos, P. Pedreiras, and L. Almeida, “Tolerating transient communication faults with online traffic scheduling,” in *Proc. IEEE Conf. Ind. Technol.*, 2012, pp. 396–402.

[6] P. F. do Souto, P. Portugal, and F. Vasques, “Reliability evaluation of broadcast protocols for FlexRay,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 525–541, Feb. 2016.

[7] I. Choi, T. Han, and S. Kang, “Bit transmission error correction scheme for FlexRay based automotive communication systems,” in *Proc. IEEE Global Conf. Consum. Electron.*, 2013, pp. 488–490.

[8] R. Bosch, “CAN with Flexible Data-Rate Specification Version 1.0,” Robert Bosch GmbH, Stuttgart, Germany, 2012.

[9] N. Navet and F. Simonot-Lion, “In-vehicle communication networks–A historical perspective and review,” in *Industrial Communication Technology Handbook*, 2nd ed., vol. 96. Luxembourg: Univ. Luxembourg, 2013.

[10] E. Pannila and M. Edirisinghe, “Power system switching transients in passenger automobiles,” in *Proc. 7th Int. Conf. Inf. Autom. Sustain.*, 2014, pp. 1–6.

[11] M. Fontana and T. H. Hubing, “Characterization of CAN network susceptibility to EFT transient noise,” *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 2, pp. 188–194, Apr. 2015.

[12] A. S. Roque, D. H. Pohren, T. J. Michelin, C. E. Pereira, and E. P. Freitas, “EFT fault impact analysis on performance of critical tasks in intra-vehicular networks,” *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 5, pp. 1415–1423, Oct. 2017.

[13] G. M. Zago and E. P. de Freitas, “A quantitative performance study on CAN and CAN FD vehicular networks,” *IEEE Trans. Ind. Electron.*, vol. 65, no. 5, pp. 4413–4422, May 2018.

[14] M. D. Ker and C. C. Yen, “New transient detection circuit for on-chip protection design against system-level electrical-transient disturbance,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, pp. 3533–3543, Oct. 2010.

[15] A. Menendez, A. Barbancho, E. Personal, and D. F. Larios, “Industrial fieldbus improvements in power distribution and conducted noise immunity with no extra costs,” *IEEE Trans. Ind. Electron.*, vol. 58, no. 7, pp. 2653–2661, Jul. 2011.

[16] A. S. Roque, D. Pohren, C. E. Pereira, and E. P. Freitas, “Communication analysis in CAN networks under EFT injection,” *IEEE Int. Conf. Automatica, XXII Congr. Chilean Assoc. Automat. Control*, vol. 22, 2016, pp. 1–6.

[17] H. M. Song, H. R. Kim, and H. K. Kim, “Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network,” in *Int. Conf. Inf. Netw.*, 2016, pp. 63–68.

[18] S. Kelkar and R. Kamal, “Adaptive fault diagnosis algorithm for controller area network,” *IEEE Trans. Ind. Electron.*, vol. 61, no. 10, pp. 5527–5537, Oct. 2014.

[19] J. M. G. da Silva, C. E. Pereira, and T. J. Michelin, “Performance analysis of distributed control systems using the FlexRay protocol,” *IFAC Proc.*, vol. 47, no. 3, pp. 5252–5257, 2014.

[20] S. Yin and Z. Huang, “Performance monitoring for vehicle suspension system via fuzzy positivistic C-means clustering based on accelerometer measurements,” *IEEE/ASME Trans. Mechatron.*, vol. 20, no. 5, pp. 2613–2620, Oct. 2015.

[21] R. Lange, A. C. Bonatto, F. Vasques, and R. S. de Oliveira, “Timing analysis of hybrid FlexRay, CAN-FD and CAN vehicular networks,” in *Proc. 42nd Annu. Conf. IEEE Ind. Electron. Soc.*, 2016, pp. 4725–4730.

[22] S. Woo, H. L. Jo, I. S. Kim, and D. H. Lee, “A practical security architecture for in-vehicle CAN-FD,” *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2248–2261, Aug. 2016.

[23] H. S. An and J. W. Jeon, "Analysis of CAN FD to CAN message routing method for CAN FD and CAN gateway," in *Proc. IEEE 17th Int. Conf. Control, Automat. Syst.*, 2017, pp. 528–533.

[24] IEC 61000, "Electromagnetic compatibility (EMC)-Part 4-4: Testing and measurement techniques electrical fast transient/burst immunity test," 3rd ed., International Electrotechnical Commission - IEC, Geneva, Switzerland, 2012.

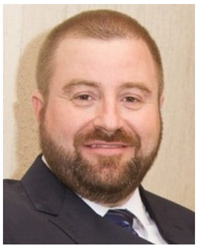
[25] M. Magdowski and R. Vick, "Estimation of the mathematical parameters of double-exponential pulses using the NelderMead algorithm," *IEEE Trans. Electromagn. Compat.*, vol. 52, no. 4, pp. 1060–1062, Nov. 2010.

[26] ISO 7637-3, "Road vehicles electrical disturbances from conduction and coupling Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines," 3rd ed., International Organization for Standardization - ISO, Geneva, Switzerland, 2016.

[27] N. Lambrecht, H. Pues, D. De Zutter, and D. V. Ginste, "A circuit modeling technique for the ISO 7637-3 capacitive coupling clamp test," *IEEE Trans. Electromagn. Compat.*, vol. 60, no. 4, pp. 858–865, Aug. 2018.

[28] C. Poussot-Vassal, "Robust LPV multivariable automotive global chassis control," Doctoral thesis, Inst. Nat. Polytech. Grenoble, Grenoble, France, 2008.

[29] G. R. Biswal, R. P. Maheshwari, and M. L. Dewal, "Cool the generators: System reliability and fault tree analysis of hydrogen cooling systems," *IEEE Ind. Electron. Mag.*, vol. 7, no. 1, pp. 30–40, Mar. 2013.



Daniel Henrique Pohren (M'17) received the B.Sc. degree in electrical engineering from Lutheran University of Brazil, São José, Brazil, in 2014. He is currently working toward the master's degree in electrical engineering with the Federal University of Rio Grande do Sul, Porto Alegre, Brazil.

He is a member of Research Group in control, automation, and robotics. His research interests include automation, communication protocols, distributed real-time control systems, and embedded systems.

Alexandre dos Santos Roque (M'13) received the B.Sc. degree in computer science from Regional Integrated University, Santo Angelo, Brazil, in 2005, and the M.Sc. degree in production engineering with emphasis in automation and control systems from the Federal University of Santa Maria, Santa Maria, Brazil, in 2010. He is currently working toward the Ph.D. degree in electrical engineering with the Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil.

He is a member of Research Group in control, automation and robotics, UFRGS. His research interests include reliability, embedded systems, distributed real-time control systems, and industrial communication protocols.

Tiago Antônio Ingracio Kranz (M'18) received the B.Sc. degree in electrical engineering from the Lutheran University of Brazil, São José, Brazil, in 2014. He is currently working toward the master's degree in electrical engineering at the Federal University of Rio Grande do Sul, Porto Alegre, Brazil.

His research interests include automation, communication protocols, and embedded systems.

Edison Pignaton de Freitas (M'08) received the bachelor's degree in computer engineering from the Military Institute of Engineering, Rio de Janeiro, Brazil, in 2003 the M.Sc. degree in computer science from the Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil, in 2007, and the Ph.D. degree in computer science and engineering from the Halmstad University, Halmstad, Sweden, in 2011.

He is currently an Associate Professor with the UFRGS, affiliated to the Graduate Programs in electrical engineering and computer science, acting as a member of Research Group in control, automation and robotics. His research interests include industry automation, computer networks, and automation and real time systems.

Carlos Eduardo Pereira (M'90) received the B.S. degree in electrical engineering and the M.Sc. degree in computer science from the Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil, in 1987 and 1990, respectively, and the Ph.D. degree in electrical engineering from the University of Stuttgart, Stuttgart, Germany, in 1995.

He is currently a Full Professor of Automation and Real Time Systems with the UFRGS, Porto Alegre, Brazil, and the Director of Operations with the Empresa Brasileira de Pesquisa e Inovação Industrial Brazilian Industrial Research and Innovation Company (EMBRAPII), Brasília, Brazil. He has authored or coauthored more than 400 technical publications on conferences and journals.

Prof. Pereira is an Associate Editor for the Journal *Control Engineering Practice* and *Annual Reviews in Control* from Elsevier and Council Member of *IFAC*. He was the recipient of the Friedrich Wilhelm Bessel research award from the Alexander von Humboldt Foundation—Germany, in 2012.

ApêndiceB

B.1 Publicação SBA - Journal of Control, Automation and Electrical Systems

https://doi.org/10.1007/s40313-019-00483-w

An Approach to Address Safety as Non-Functional Requirements in Distributed Vehicular Control Systems

Alexandre dos Santos Roque[1] · Daniel Pohren[1] · Edison Pignaton Freitas[1] · Carlos Eduardo Pereira[1]

Received: 29 January 2019 / Revised: 27 May 2019 / Accepted: 4 June 2019 / Published online: 21 June 2019

Abstract
Distributed vehicular control systems include several safety-critical processes so that reliability aspects are of growing importance, raising concerns about faults affecting them. Observing this fact, this paper presents a combination of aspect-oriented concepts to model faults in early-design phases of distributed vehicular control systems. A fault modeling approach in communication protocols as non-functional requirements—NFR is proposed, using aspect-oriented modeling (AOM) with the support of the Real-Time From Requirements to Design using Aspects (RT-FRIDA) framework. Following practical experiments about the effect of electrical fast transients in vehicular control systems, a study was performed specifying NFR associated with these faults. Then, an evaluation with a SIG graph using the softgoal weight method and the NFR framework is presented to validate the proposed approach. The results emphasize that early fault modeling could improve the control system modeling mapping fault behaviors in order to mitigate and diagnosis the fault impact in critical tasks. The approach cover gaps related to fault modeling and allow requirements specification with AOM concepts emphasized in the case study by the correlation among network performance degradation and requirements related to faults. The analysis with the softgoal weight method also provides an alternative view of the impact of fault modeling in vehicular critical real-time systems.

Keywords Fault modeling · Aspect-oriented modeling (AOM) · Distributed control systems · NFR framework

1 Introduction

Distributed embedded control systems have increasing importance in the automotive area, mainly because of the growing application of electronic control units (ECU) that are fundamental to safety applications, such as ABS, traction control, AirBags among other systems. Currently, intra-vehicular networks apply communication protocols that are responsible for interconnecting several ECUs, according to a specific topology. Some safety-critical tasks communicate over the network and must timely execute actions that often occur independently of the drivers actions or commands.

With the complexity of distributed embedded control systems, such as the set of systems that compose modern vehicles, the number of faults due to the communication among the components tend to increase significantly. In order to face this problem, some protocols adopted in intra-vehicular networks have been expanded in order to improve the control system reliability, adding fault tolerance capabilities. Additionally, proposed extensions to the CAN protocol, such as TT-CAN (Time-triggered CAN) and FTT-CAN (Flexible Time-triggered CAN) were developed (Tuohy et al. 2015). Another communication protocol specifically designed to the automotive sector and which includes fault-tolerant concepts is the FlexRay protocol (Tuohy et al. 2015).

Although these protocols have features to ensure reliable communications, gaps regarding system reliability and the ability to support faults need to be addressed. Commonly, the adopted fault diagnosis strategies are reactive and generate an excessive number of retransmissions, increasing the channel communication rate and not solving the errors (Brunner et al.

Alexandre dos Santos Roque
as.roque@ufrgs.br

Daniel Pohren
daniel.pohren@ufrgs.br

Edison Pignaton Freitas
edison.pignaton@ufrgs.br

Carlos Eduardo Pereira
cpereira@ufrgs.br

[1] School of Engineering - Campus Centro Graduate Program in Electrical Engineering, Federal University of Rio Grande do Sul - UFRGS, Porto Alegre, Brazil

2017; Marques et al. 2014a; Nakamura et al. 2015). Detecting and diagnosing different fault types is not a simple task and usually requires mechanisms implemented in hardware and software (Nakamura et al. 2015).

In this context, the fault analysis and modeling of typical faults in design phases contribute to the development of more robust systems, consequently improving the performance of real-time applications. Different faults that affect and degrade the performance of vehicular protocols have transverse effects (affect more than one component at the same time). In this sense, the application of aspect-oriented concepts with non-functional requirements (NFR) specification, together with the fault impact analysis in control systems, provides a mechanism for reliable design because the aspect-oriented paradigm can capture and separate crosscutting concerns.

The present work combines NFR specification of faults and aspect-oriented modeling (AOM) strategy in the distributed control system design, allowing the modeling of fault-tolerant and fault-diagnostic mechanisms to improve reliability in communication protocols focusing on intra-vehicular networks. Moreover, this combination also can help to prevent or reduce retransmissions and to enable a diagnostic hardware development and real-time diagnostic.

The research problem is centered on the lack of fault modeling techniques in early-design phases, focusing on in-vehicle communication protocols, which are increasingly subject to faults and interferences due to the complexity demanded by the recent technologies applied in the automotive industry. The research hypothesis addresses the use of aspect-oriented modeling in conjunction with an extended version of the RT-FRIDA framework, in order to map faults that degrade performance, as non-functional requirements, having this feature handled earlier in the distributed embedded control system design. Thus, the main contribution of this paper is the exploration of AOM for fault modeling in earlier design phases, focusing, in particular, in reliability aspects of the communication protocols.

This paper is organized as follows: Sect. 2 presents possibilities for fault modeling according to software engineering approaches; Sect. 3 presents related works regarding modeling approaches for distributed communication networks; Sect. 4 describes the proposed approach for fault modeling, while Sect. 5 presents the developed case study as proof of concept. Section 6 provides the assessment of the results obtained in the case study, while Sect. 7 provides discussions and conclusions related to the obtained results and possibilities of enhancements.

2 Overview of Fault Modeling for Intra-Vehicular Networks

2.1 Aspect-Oriented Modeling: AOM

Over the last years, several approaches to help engineers deal better with complex design tasks have been proposed. These approaches are applied to different areas, as automotive and avionics. Recently, researches have focused on increasing the use of aspect-oriented modeling—AOM (Vyatkin 2013; Wehrmeister et al. 2013).

In distributed real-time embedded (DRE) systems, the requirements specification linked to time constraints compliance, task distribution, and embedded system performance are essential to the project success. These characteristics affect several components of the system in a non-uniform way, which makes them difficult to be handled with traditional development methodologies (Wehrmeister et al. 2013).

AOM can be considered an extension of the object-oriented modeling. According to Kienzle et al. (2010), AOM focuses on the application of techniques based on aspects with the objective of modularizing transversal concepts (crosscutting concerns), using modeling notations and abstraction levels. AOM approaches have been applied in different contexts, based on UML (Unified Modeling Language) models (Iqbal et al. 2012), adding aspects to the development of safer systems (Wimmer et al. 2011) as well as in reusing modeling aspects based on dependability attributes (Alzahrani and Petriu 2015).

Requirements related to power consumption, performance and dependability affect the system transversally. These requirements cannot be addressed only at the final phases of the development, but also in the specification and in the design phases. However, to consider the modeling of transversal characteristics in early-design phases, in particular, due to the higher complexity of current DRE systems, is gaining in importance over the last years. This paradigm proposes the separation of concerns in handling NFR, contributing to system modularization (Wehrmeister et al. 2013; Alzahrani and Petriu 2015).

The work presented in Wehrmeister et al. (2013) highlights the application of software engineering in industrial automation, with the emphasis in using aspect-oriented concepts, that is a trend in developing new embedded systems applications, because of its ability to improve the software lifecycle efficiency and dependability. In traditional software engineering approaches, specific problems related to NFR specification, such as transient faults in communication processes, are not considered, thus representing an open research challenge (Oetjens et al. 2014; Huang et al. 2016).

Modeling based on "Aspects" can be applied in different contexts and is widely used in recent research related to industrial automation. Researches demonstrate that AOM can add robustness to the design of complex systems. In Kienzle et al. (2010) some examples of typical uses of AOM modeling in the industry are presented, such as in health applications, modularizing crosscutting concerns such as architecture validation, caching, auditing, performance monitoring.

Supporting AOM, the aspect-oriented programming—AOP, is characterized by the use of specific notations in the source code that represent crosscutting concerns which affect the system being developed as a whole. Hence, faults can be characterized by crosscutting concerns and represented using AOM. Programming can be done by adapting existing structures of a programming language or using a language that provides support for "aspects", such as AspectJ in Java language. AspectJ extends Java with specific syntax supporting aspects, and these aspects have been embedded in programming frameworks (Apel and Batory 2010).

According to Vyatkin (2013), AOP is a programming paradigm which aims to increase modularity by allowing the separation of crosscutting concerns and forms the basis for aspect-oriented software development. In AOP, the <<crosscut>> stereotype characterizes a crosscutting concern as a parameter passing in the adaptation performed by the modeled aspects, emphasizing that this is a partial view of the application. In AOP the main goal is the application of AOM concepts, represented by features as the pointcut (a part responsible for capturing a joinpoint), joinpoint (a specific point in the program flow responsible for characterizing a point of a crosscutting aspect) and advice (a code block determined by a pointcut and that will be executed when a respective joinpoint is reached). Further details about aspect-oriented programming concepts can be found in Kiczales et al. (1997).

Although these concepts are being applied in different contexts, there are gaps related to fault modeling techniques in early-design phases with the increasing complexity in distributed vehicular control systems.

2.2 Faults in Communication Protocols

Different fault types can affect communication protocols. Faults can be either permanent or transient. According to Marques et al. (2013) faults can be classified by duration as permanent, intermittent or transient. Permanent faults are software and hardware faults that always produce errors when they are fully exercised and temporary faults can be distinguished into external faults (transient) and internal faults (intermittent).

Transient faults are temporary by nature and are due mainly to electromagnetic interference (EMI), radiation or temperature variation for instance. On the other hand, permanent faults are persistent, resulting from physical defects in system parts and lasting until repair or replacement (Mahapatro and Khilar 2013).

Electrical transients affect communication networks in different ways, and even small delays can lead to critical faults in the control system. When these faults occur, messages with hard periodicity constraints can be lost. Some detection approaches check the message bits through a bit error rate (BER), but its possible causes are not identified (Mahapatro and Khilar 2013). This is an important point that needs to be aggregated in modeling techniques for developing more reliable systems.

3 Related Works

Research challenges related to reliability in communication protocols used in the automotive industry have been increasingly studied and need constant attention. This section presents some works that highlight this problem and also research possibilities. An essential point to consider is the main challenge related to the development of networked control systems—NCS (for example, in intra-vehicular networks) because of the degenerative effect caused by the inclusion of this communication network in the closed loop control, as highlighted in Godoy and Porto (2013). The authors present a revision about co-simulation tools for the design and evaluation of NCS. It is evaluated the performance problem of CAN-based NCS and the quality of control under various timing conditions including different transmission period of messages and network delays.

Following this research line, many works have highlighted the problem of interferences and disturbances in intra-vehicular networks. The work presented in Pattanaik and Chandrasekaran (2012) proposes a method to predict the occurrence of faults by analyzing specific control system events, with hard real-time constraints. The analysis verifies if the event repeats with determined periodicity correlating with control system problems. In the same context, the need for injection and fault detection methods, allows new applications that use CAN networks to be tested to their limits. In Gessner et al. (2014) is presented the design and implementation of a physical fault injector for the CAN protocol, which provides testing features and discusses the benefits of a star topology. The work allows a remote and flexible configuration of fault injection and the retrieval of accurate information about the subsequent behavior of the nodes. The work presented in Shah et al. (2016) focuses on algorithms for error handling to replace the native CAN error handling. The methodology is evaluated using a steer-by-wire system of vehicles to analyze the effect of fault occurrences in the CAN protocol. Although the fault impact analysis in network control systems is fundamental, the research does not deal with the possibility of fault modeling and specification of control system requirements.

Protocols that are designed to be more reliable also require fault analysis. In Zeng et al. (2015) the analysis of problems in the FlexRay protocol is presented, specifically regarding the fault detection. Data inconsistency, invalidation, and fault-delayed notification are the main problems identified. The research highlights that FlexRay has a robust communication channel, but lacks mechanisms to detect and notify communication faults. This fact causes the receiver to discard messages without informing the sender. The work presented in Marques et al. (2014b) discusses FlexRay transient faults. The authors propose a mechanism that uses temporal redundancy to recover transient errors in time-triggered messages.

Fault detection and notification always represent a challenge in any industrial system due to the complexity and heterogeneity. In Costa et al. (2014) the work emphasizes this issue proposing and evaluating a new method for fault detection in industrial plants. Instead of using mathematical models, the approach is based on the estimation of the density in the data space. The density is expressed by a kernel function and calculated recursively, making the approaching power efficient and differing from other researches by the fact that could be applied in real-time applications.

These works demonstrate that there are still gaps to be worked on regarding the reliability of the communication protocols. The research works highlight how system faults need to be diagnosed early, particularly considering the growing complexity of the current distributed control systems.

Aspect-oriented modeling—AOM—has been an important ally in mapping systemic aspects in the industry. The work presented in Ali et al. (2012) pointed out that the concepts of AOM can add robustness in industrial systems with the support of state machines. The methodology RUMM (robustness modeling methodology) is presented, emphasizing aspect-oriented concepts to map systems behavior and the possibilities of reducing the system complexity.

In the same way, the work presented in Wasicek et al. (2014) applies aspect-oriented modeling to describe attacks on automotive cyber-physical systems. Safety concepts are developed based on the AOM, providing data about attacks behavior that are used to provide reliability mechanisms in control systems.

In Nguyen et al. (2014) the authors emphasize the Model-Driven Security (MDS) methodology. The paper presents a discussion of the MDS approach based on a set of security standards, supported by aspect-oriented modeling, with the aim of providing a requirements document about system vulnerabilities. However, the work lacks a study about its applicability in fault modeling of communication processes and does not validate the work. Other approaches as FTA could be applied for failure diagnostic. The work presented in Chiremsel et al. (2016) discuss a probabilistic fault diagnosis approach of safety instrumented systems based on fault tree analysis (FTA) and Bayesian networks (BN). Despite this method provide a systematic procedure for identifying system failures, FTA corresponds to a top-down approach based on a known sequence of events, according to causes and effects of failures. However, in unknown scenarios, it is also relevant to focus on the silent degradation effect generated by failures, than on specific failures.

The fault handling that may compromise the temporal requirements in automotive applications is another research field with gaps to be explored. In Piper et al. (2015), the authors present a technique to monitor critical tasks of the control system, verifying if interferences and faults are causing delays, thus seeking to provide execution time guarantee. The proposal presents the differences in the approach comparing to existing tools. This approach highlights the timing requirements violation in communication protocols but does not consider modeling these faults in early-design phases.

A recent work presented in Akkaya et al. (2016) shows how to use aspect-oriented modeling in a Model-Based Design, emphasizing how the approach can manage the system complexity. These concepts are demonstrated with actor-oriented models of an industrial robotic-swarm application. Especially related to fault modeling the work highlights how faults are orthogonal concerns that can be modeled as aspects.

Another work that emphasizes the basis of this research, i.e., the reliability modeling in design phases, is presented in Mo et al. (2017). The work presents a new stochastic model represented by linear discrete-time approach considering data packet transmissions and specific data packet dropout that are neglected in other approaches. In this work, historical behaviors of networked degradations are modeled by multistate Markov chains with uncertainties, releasing the assumption that faults of all periods are independent of each other. The present work aims to handle the non-functional requirements specification related to faults in communication protocols, contributing in a similar way in the reliability of the distributed embedded control systems. In Mo et al. (2017) the authors emphasize that it is necessary to get a model to verify and evaluate the system reliability in the early-design phase, prior to its implementation. Thus, this current paper address this issue, covering this gap, since the RT-FRIDA framework makes it possible to handle these issues.

In this sense, Freitas et al. (2007) presents the RT-FRIDA methodology to specify NFR in real-time systems. The main purpose is the mapping of these requirements from analysis design phases as "aspects". RT-FRIDA elicits NFR related to timing, distribution and embedded concepts as aspects. However, RT-FRIDA does not address different fault types that affect real-time systems, degrading the performance of different parts of a system at the same time, especially those regarding communication protocols. Thus, the work presented in Roque et al. (2017b) proposes an extension of the RT-FRIDA framework to cover this gap, with the classification of faults according to specifics NFR and their model using the aspect-oriented paradigm. For this task, new checklists and templates for fault requirements specification were developed. In addition, in Roque et al. (2018) it is presented a comparison of requirements specification using the extended version of RT-FRIDA with two critical control systems, introducing the softgoal weigh method for requirements evaluation. However, in Roque et al. (2018) the control systems were analyzed after tests, not considering the fault modeling during test phases. The present work differs from both previous ones showing how the fault modeling can be done during the test phases, performing fault injection and collecting data about performance degradation during the typical control system operation. Table 1 presents a summary of the main points and gaps in the literature, emphasizing the contribution of the present work combining recent researches to provide a novel approach for fault modeling.

Combining some of the evaluated related works makes it possible to cover the gaps related to fault modeling that degrade performance in automotive communication protocols. Modeling faults in design phases contribute to reliability enhancement in distributed embedded control systems.

4 Proposed Fault Modeling for Distributed Vehicular Control Systems

According to the state-of-the-art analysis, fault-tolerant handling in intra-vehicular networks have gaps to be explored, specifically related to mechanisms for fault diagnostic and notification, in protocols such as FlexRay and CAN. In order to contribute with solutions to reduce these problems, the present work proposes the integration of the aspect-oriented modeling methodology and RT-FRIDA, with recent works based on AOM to correlate and to model communication faults as aspects. The focus is to provide an approach that allows the modeling of control systems with features as real-time diagnostic capability and adaptability.

RT-FRIDA framework is dedicated to identifying the system functional and non-functional requirements. Use case diagrams and templates are used to elicit those requirements. For this task, checklists, lexicons, and conflict resolution rules are used. A link among classes, actors, and the use cases is created, and the NFR is visually represented in the class diagram. In the end, a source code of classes and aspects (i.e., skeletons for classes and aspects) is generated (Freitas et al. 2007).

This framework does not encompass recent issues related to fault modeling. Some fault behaviors can be previously modeled in early-design phases of embedded system lifecycle with the goal of developing fault-diagnostic mechanisms. In an embedded network, data can be collected and correlated with features and time constraints allowing trigger redundancy mechanisms in hardware and software, checking the impact of the inclusion of these mechanisms in system performance.

Figure 1 shows the approach of a cyclical model for fault modeling with the emphasis in AOM. The interaction illustrates that the present work focuses on protocols used in intra-vehicle networks and different types of faults modeled as NFR using “aspects”. The Fig. 1a is divided into four parts.

Part 1 highlights the growing importance of distributed embedded control systems that have many ECUs interconnected in networks using communication protocols. Part 2 represents the importance in performing a case study to verify the applicability of AOM in this research context, for example, an Active Suspension System has characteristics as hard real-time constraints, with sensors data that are transmitted over the network and represents a critical system.

In part 3, some common faults found in vehicular communication protocols are highlighted. Many of these faults are reactively handled after the problem occurs and for specific situations added to embedded systems, often causing other problems such as increased communication rate on the bus.

Part 4 (in detail on Fig. 1b) shows an important research contribution, going beyond to what was originally presented in RT-FRIDA, with the integration of a fifth dimension related to fault requirement specification. The aspect-oriented modeling (AOM) provides a tool for modeling faults (e.g., transient faults in communication protocols) as NFR. Including this dimension into RT-FRIDA enhances its usefulness, as the original framework considered that all components in the system behaves as expected. With the contribution here presented, this assumption is not valid, thus bringing an additional challenge in the system specification, which is only possible to be addressed with the proposed extension.

In order to achieve an enhanced level of reliability, a study on NFR is necessary. The fault may be described as NFR due to the crosscutting impact on the system overall performance. The crosscutting concerns characterize the base of AOM, in which each requirement may be seen as a “concern” and separately specified. There are several classification approaches of NFR, as proposed in Freitas et al. (2007), Akkaya et al. (2016) and Chung et al. (2012). The present work is based on the classification proposed in Freitas et al. (2007) considering the network performance degradation according to Mo et al. (2017) and Roque et al. (2017a).

The work Freitas et al. (2007) presents different requirements that affect the operation of the real-time system, subdivided four groups: “Time”, “Performance”, “Distribution” and “Embedded”. These requirements groups are directly mapped on properties that guide the execution of tasks in a distributed control system. The group “Time” refers to deadline, period, cost and the worst-case execution time

Table 1 Related works summary

Work	Approach	GAP
Pattanaik and Chandrasekaran (2012)	Redundancy Enabled Collaborative Recovery model	Fault isolation process, imprecise information
Godoy and Porto (2013)	Co-simulation tools for the design and evaluation of NCS	Performance degradation in CAN-based networks, quality of control
Gessner et al. (2014)	sfiCAN—Fault injection in CAN networks	Fault analysis. Test under inconsistency scenarios
Shah et al. (2016)	Algorithm for effect analysis of faults in CAN-based networked control systems	Fault modeling and fault analysis in automotive systems
Zeng et al. (2015)	A qualitative study of FlexRay and Ethernet protocols for in-vehicle communication	Data inconsistency. Lack of fault notification mechanisms
Marques et al. (2014b)	Scheduling message retransmissions dynamically in FlexRay protocol	Fault notification. Transient error recovering
Costa et al. (2014)	Real-time fault detection in industrial plants analyzing control and error signals	Data density analysis in fault detection. Highly complex algorithms
Ali et al. (2012)	AOM to reduce model efforts and modeling robustness behaviors with state machines	Modeling robustness in complex industrial systems
Wasicek et al. (2014)	AOM to describe attacks in automotive systems	The vulnerability of safety-critical systems to attacks
Nguyen et al. (2014)	Aspect-oriented design patterns to model secure systems	Lack of design methodologies for early stages
Chiremsel et al. (2016)	Fault diagnosis approach of safety instrumented systems	The vulnerability of critical control systems to performance degradation
Piper et al. (2015)	Monitor tasks that constitute a potential source of errors. AUTOSARs timing protection	Protection of critical tasks from interferences
Akkaya et al. (2016)	AOM techniques with a model-based design. Integration of modeling methods	Modeling complexity of industrial cyber-physical systems
Mo et al. (2017)	Reliability with a stochastic model represented by a linear discrete-time approach	Modeling reliability aspects in DNCS considering data packet transmissions and data packet dropout
Freitas et al. (2007)	Framework for requirements specification using aspects. Templates and checklist for a systematic specification	Lack of fault modeling as system requirements
Roque et al. (2017b)	RT-FRIDA extension for fault modeling	Lack of tests of the framework with a Case Study and after real tests of fault injection
Roque et al. (2018)	Requirements specification after tests for critical control systems	Lack of requirements analysis during test phases Fault analysis during control system operation
The present work	AOM and RT-FRIDA framework extended applied for fault modeling. NFR requirements and a test-based approach	Fault modeling and specification in early-design phases of distributed vehicular control systems

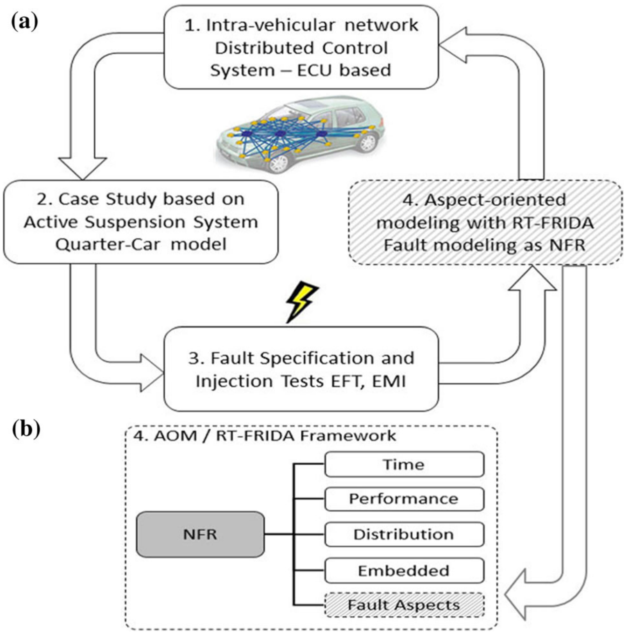

(a)
1. Intra-vehicular network Distributed Control System – ECU based
2. Case Study based on Active Suspension System Quarter-Car model
3. Fault Specification and Injection Tests EFT, EMI
4. Aspect-oriented modeling with RT-FRIDA Fault modeling as NFR
(b)
4. AOM / RT-FRIDA Framework
NFR
Time
Performance
Distribution
Embedded
Fault Aspects

Fig. 1 **a** Fault modeling approach. **b** AOM/RT-FRIDA framework extended

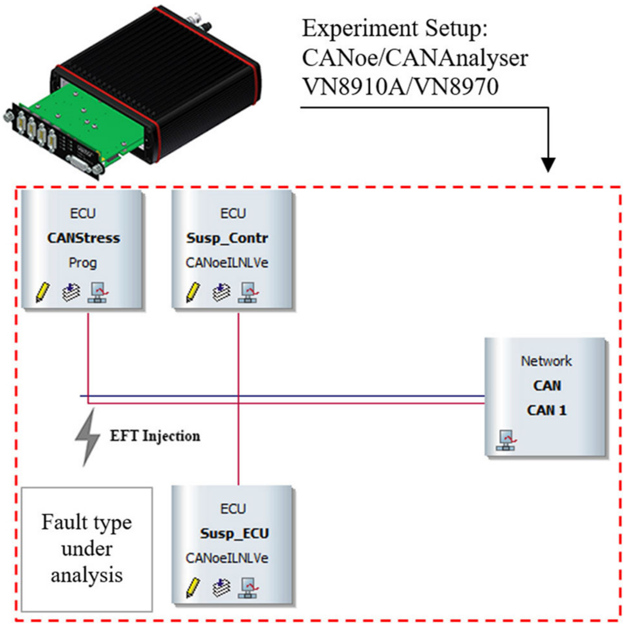


Fig. 2 Vector tools and the CAN network topology used in the experiments

of tasks on the system. “Performance” refers to the rate at which a resource must perform its function (flow rate) and the time it takes for the system to return a final response (response time). “Distribution”, handle the task allocation that is related to distribution and scalability in different processing units. “Embedded” can refer to power consumption constraints of system components and the system memory usage.

Moreover, some faults affect the system in general, degrading performance of different system parts at the same time. Faults may affect the classification proposed in Freitas et al. (2007) changing many NFR at the same time. For example, a transient fault that affects a period of a task of causing a delay or jitter, impacting the response time of a communication between the stations (ECUs) as well as the power consumption. Therefore, it is important to model fault-diagnostic mechanisms relating their crosscutting concern that can affect the safety of the overall system. In intra-vehicular networks, it is required the analysis of requirements related to the vulnerabilities of their protocols and which faults can reduce the data transmission reliability.

An intra-vehicular network has several NFR that affect the safety of this distributed system. The framework RT-FRIDA focuses on real-time requirements with a new part “Faults Aspects” considering different fault types that can be specified using AOM. These features are the reasons behind the choice for this framework, in detriment of others, applied to the control system fault modeling. The following section presents the proposed method and the extended framework to illustrate how this method can improve the early-design of control systems considering degradation in communication protocols.

5 Case Study of Fault Modeling with RT-FRIDA Extended

According to the model presented in Fig. 1, for the part 1 and 2 an active suspension system, based on Quarter-Car-Model developed in Poussot-Vassal (2008), running on ECUs interconnected via a CAN network was selected as a real scenario of a case study. The study was performed in the university research laboratory (Control Automation and Robotics Group—GCAR, UFRGS), with that specific developed control plant. For this case study, the Vector CANoe/CANAnalyser platform (Vector Informatik GmbH) was used with two specific hardware tools, the VN8910A, and the VN8970 hardware module. In each hardware, an ECU function was programmed, one for the ECU suspension plant and another for the ECU control system. Figure 2 shows the hardware and the CAN network configured to monitoring and logging the message traffic between the ECUs.

As can be observed in Fig. 2, an extra ECU (CAN Stress) was created in the specific purpose of generating traffic on the bus because this study also considers the fault impact analysis during the bus overload. In fact, the source of the fault is not the kernel of this investigation; the core is the ability in handling faults, independent of their source.

For part 3, the possibilities of fault modeling based on NFR related to Electrical Fast Transients (EFT) faults were

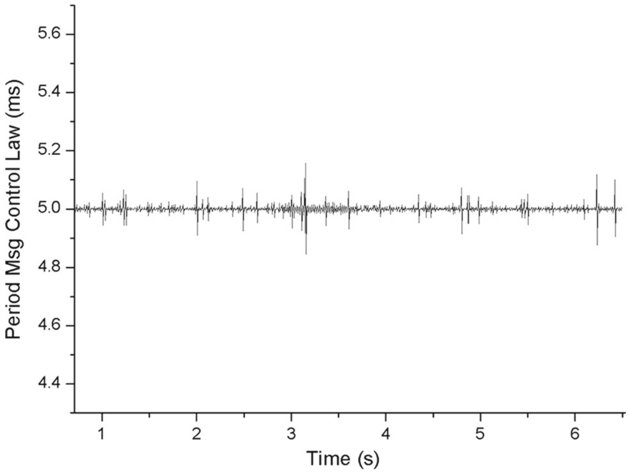


Fig. 3 Control law messages without EFT injection

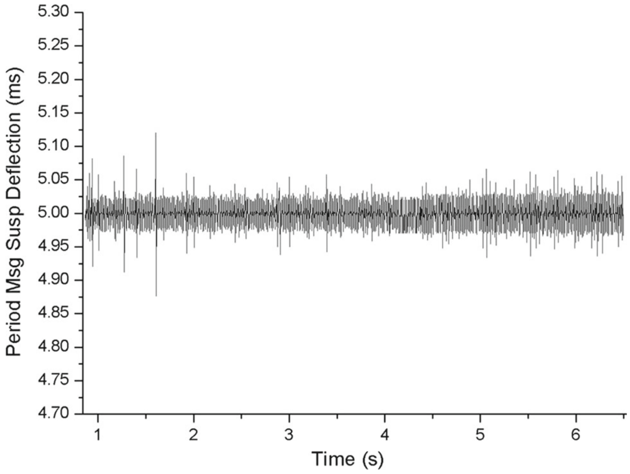


Fig. 4 Suspension deflection messages without EFT injection

investigated (fault type under analysis in Fig. 2). The information used in the current experiment was based on Roque et al. (2017a) but all tests were performed again by registering logs, and differing mainly because the system behavior under faults was registered and mapped based on the specified aspect-oriented requirements. Another difference is the logging of delays between control messages, with high bandwidth usage, during all EFT injections with the Vector CANoe implementation, a task that was not developed in the previous works (Roque et al. 2018, 2017a). In the present work, as an example, the EFT injection with 57 volts of peak was used to observe the bus behavior and to analyze how this fault increases the jitter and the average delay, degrading the control system performance.

Figures 3 and 4 show the data acquired by monitoring the control law messages and the suspension deflection messages on the bus without EFT injection. Figures 5 and 6 show the same type of data related to the monitoring of control law and the suspension deflection messages, but with EFT injection, traffic and error messages inserted by ECU CANStress.

Figures 7 and 8 present results related to the delay analysis in the messages of the Control Law (ECU controller) and the Suspension Deflection (ECU suspension plant) with and without EFT injection.

The analysis of this fault type was made verifying two delay metrics: the difference jitter obtained by subtracting the best-case transmission time from the worst-case transmission time out of the measurements in the sample set; and the average jitter represented by the standard deviation in the same sample set of message transmissions. As can be seen in Figures 7 and 8, the three columns represent the CAN bus network analysis in which, the first without EFT injection, the second with EFT injection and the third column shows the effect of error frames and retransmissions occurred during

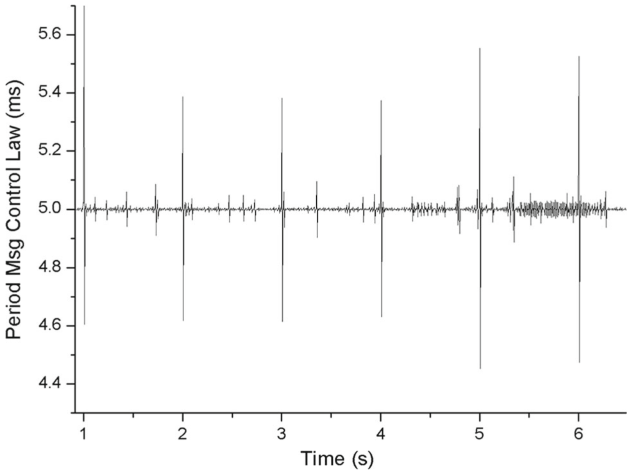


Fig. 5 Control law with EFT injection bursts approximately each second

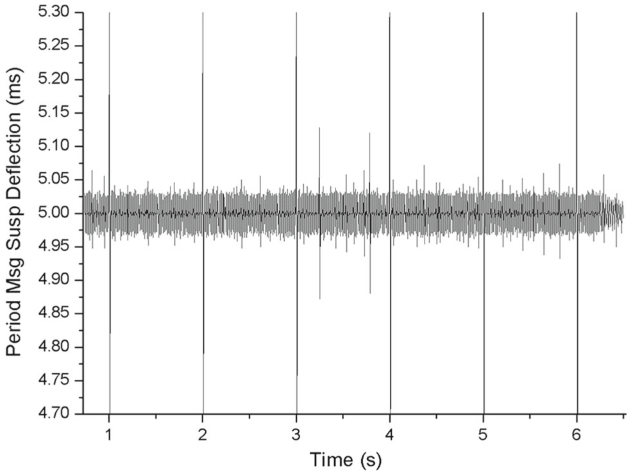


Fig. 6 Suspension deflection with EFT Injection bursts approximately each second

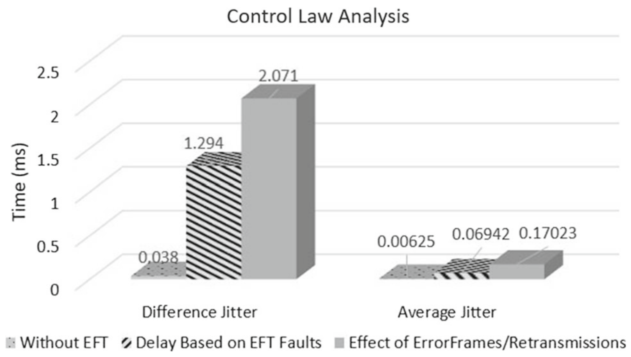


Fig. 7 Jitter and average jitter in control law messages

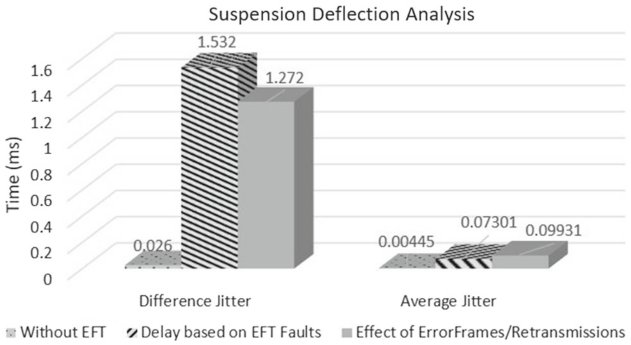


Fig. 8 Jitter and average jitter in suspension deflection messages

the EFT injection. These data were collected by the Vector CANoe software using its log files.

During this case study, the busload of the CAN network was defined as 60% in order to allow an analysis of the impact of this fault type in a real CAN network with high bandwidth usage. The study allowed the verification of how different fault types, like EFT, commonly can be silent and remain unnoticed by the control systems, but its effects can degrade the system performance.

Based on the analysis of the results obtained in this case study, it is possible to define the specific system requirements for diagnostic fault situations and thus, be proactive in handling them. Taking this into account, in part 4 of this fault modeling method, the aspect-oriented modeling approach is applied to support NFR specification. This task was performed according to the first phase of RT-FRIDA that includes a template for requirements identification. This phase is subdivided into two steps: I. Identification/specification of the functional requirements; and II. Identification and specification of the NFR. Figure 9 presents the developed use case for the addressed case study scenario.

For step I, the goal is the identification of the desired system functionalities and the development of a use case diagram. Then, a template for non-functional requirements that details the features presented in the use case diagram must be filled in. As the paper focus is on fault modeling as NFR, the step I considering the previous scenario for an active suspension control system is no further detailed.

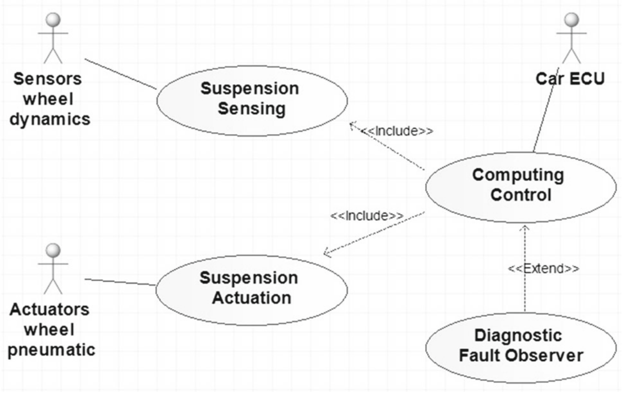


Fig. 9 Use case developed for the case study scenario

The study was performed with a control message cycle of 5 ms and according to the EFT injection delays registered in recent works, between 500 us and 1.6 ms (Roque et al. 2017a). Thus, based on these experiments, it was observed how transient faults may degrade the performance of intra-vehicular control systems. For example, the average jitter increased six times in the Suspension Deflection messages and increased nine times in Control Law messages. This information obtained by the extensive tests are represented by questions in the checklists and the designer could decide what specific NFR could be aggregated in the control system to detect or mitigate the problem. In the present work, it is proposed the use of real-time triggers for fault diagnosis (integrated into a fault observer), features that must be added during the system modeling.

The use case presented in Fig. 9 highlights that in intra-vehicular networks, different types of embedded control systems are used and each one can be affected by faults. A "fault observer" mechanism to monitor the Active Suspension control system is proposed. As an example, the case study focuses on the effect of EFT faults and shows how AOM can contribute to fault modeling.

For step II, the identification of NFR, RT-FRIDA framework uses a set of questions designed for the domain under concern composing a checklist. For each of the four NFR handled by the framework, a checklist was developed. In addition to them, a new checklist for the fifth set of NFR, related to faults in communication protocols, was developed. Table 2 presents an example with a subset of the proposed checklist, which is composed of several questions related to faults, and that after will compose several templates of NFR. The checklist is based on the experiment related to EFT faults, specifying questions about different priorities that compose this fault modeling example. It allows a systematic specification of the application requirements, as well as

Table 2 Checklist for NFR related to faults

Faults/source/effect	P	Restrictions/description
Is there a specific fault type that could degrade the system?	H	Electrical fast transients - EFT
If there is a known fault, are there standards for testing and verifying the disturbances caused by such fault?	H	Yes. Tests following the fault injection standard defined in IEC 62228, ISO 7637
Is there a known source or cause of the fault type?	M	Power System Switching Transients, generated by different component in the car
Are there any possible ways to detect this fault type?	L	The addition of sensors or chips with tolerance and detection capability is possible, but costs can be prohibitive
Are there routines for register performance degradation of the communication network?	H	Registration of logs for further analysis. Registration of the components and ECUs related
Are there specific performance metrics monitored in real time?	H	Yes. Busload, Throughput, Average Jitter and Difference Jitter (worst case)
Are there defined tolerance limits for these metrics?	H	Yes. Based on tests performed, a tolerance of 10% in the throughput and 25% in the jitter was defined
Are there notification triggers using messages in case of frequent communication disturbances?	M	Yes. Through overhead analysis in communication. Or just log registration for further analysis

Legend *P* priority, *H* high, *M* medium and *L* low

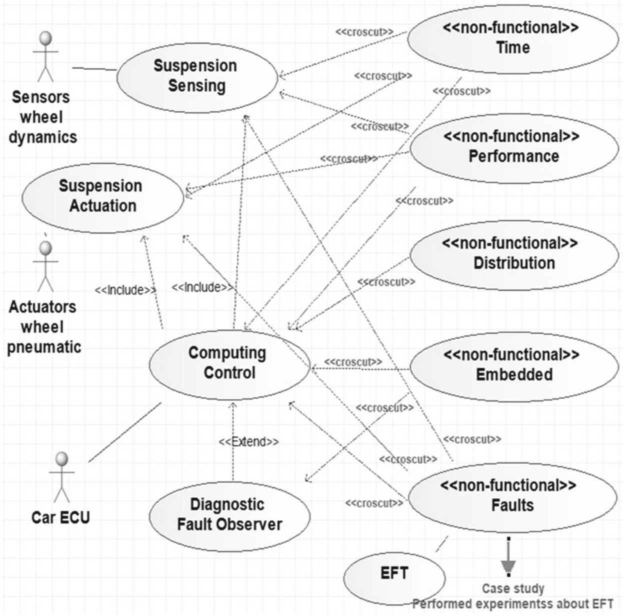

Sensors wheel dynamics
Suspension Sensing
<<non-functional>> Time
<<non-functional>> Performance
Suspension Actuation
Actuators wheel pneumatic
<<non-functional>> Distribution
<<Include>>
<<Include>>
Computing Control
<<non-functional>> Embedded
<<Extend>>
Car ECU
Diagnostic Fault Observer
<<non-functional>> Faults
<<croscut>>
EFT
Case study
Performed experimentss about EFT

Fig. 10 Use case updated with the AOM stereotypes and the level designed for fault modeling with the RT-FRIDA framework

the customization of other issues that are essential to describe faults (Fig. 1b) “Fault Aspects”).

After the specification of these requirements, the use case diagram is updated including “aspects” stereotypes that represent the additional part of NFR modeled. This model is aggregated into RT-FRIDA framework extending capabilities for modeling specifics fault types in communication protocols. Figure 10 presents the use case updated.

A common weakness of this system modeling is that most of the proposed approaches do not consider the association between requirements and design elements (Freitas et al. 2007; Wehrmeister et al. 2013). This research contributes to mitigating this problem by integrating different modeling techniques. Thus, RT-FRIDA is applied for NFR fault specification based on AOM, and UML MARTE complements this process by providing specific stereotypes to clarify the development. The UML MARTE profile provides support for the design and the model-driven development of real-time embedded systems (RTES) (Khakhar and Nayak 2018).

Therefore, by mapping NFR related to EFT faults and updating the use case diagram, a class diagram for the active suspension system was developed. For this task, the specification based on the UML MARTE profile was used to map non-functional properties and to characterize the system classes. The stereotypes *deviceResource* and *allocated* are used to represent the resources used and allocated by the control system, in this study the system plan. Another stereotype used is *computingResource* which represents any virtual or physical processing resource that runs programs. In this case, this stereotype is used to represent the control system ECU, which performs the computation of the control law. The *saSharedResource* stereotype is related to shared resource and communication analysis, commonly used in real-time systems. This stereotype is used in conjunction with *computingResource* to represent the diagnostic system that was added to the project.

These parameters characterize the adaptation performed by the modeled aspects, emphasizing that this is a partial view of the case study. The diagram shows the aspects and

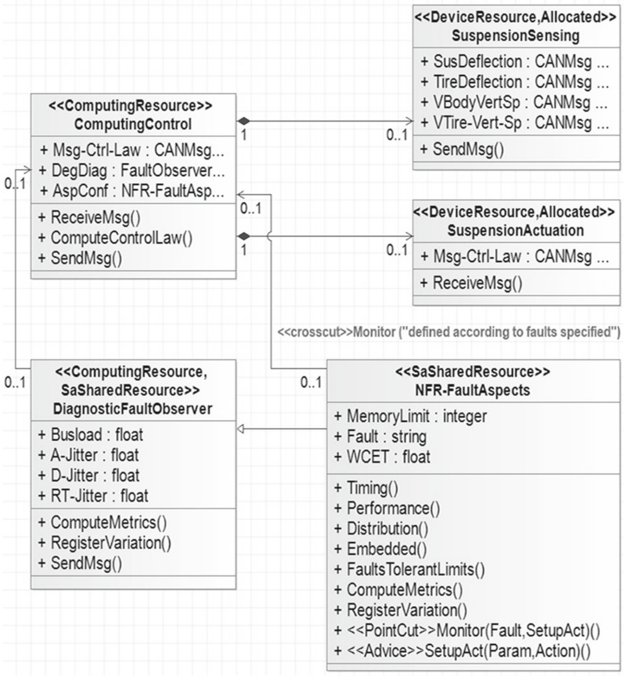


Fig. 11 Class diagram according to faults specification and crosscutting aspects

the applied concepts from AOM. The proposed updated class diagram is shown in Fig. 11.

The diagram is an example that emphasizes the main critical points of the control system and can be adjusted as needed. In order to represent the interaction dynamics between the aspects and the classes, it is necessary to present the point where one or more aspects affect them, called *joinpoints*, which define the places where the interlacing occurs (*pointcuts*). In this study is highlighted a point that represents all aspects, in order to make the diagram clearer and not spread through the system the treatment of each aspect, which facilitates development and maintenance. This point is highlighted in the class "NFR-FaultAspects", by means of the <<*pointcut*>> element where the interlacing occurs. The stereotype <<*crosscut*>> represents the crosscutting relationship between the NFR faults specified and integrated into the control system. The relationship between the NFR-FaultAspects class is aggregation by association.

Then, there is the *joinpoint* "Monitor", responsible for performing the operations of data recording, disturbance reporting, and variation identification in the performance metrics, according to the previously defined parameters, after the fault study and specification. This specific point is responsible for a call to another element named *advice*, in that representation identified by "SetupAct", which is responsible for specifying which parameters/metrics and limits will be observed. By failing to meet these operating limits or sudden fluctuations in performance metrics, diagnostic triggers can be applied, both for logging in local memory, and for sending notification messages.

After this modeling, the checklist and the proposed diagrams serve as the basis for the development of a new embedded vehicular control system. In this sense, it is essential to mention that this study aims to show the importance of fault modeling in design phases. Thus, with the RT-FRIDA framework and applying the model represented by the steps in Fig. 1, it is possible to model the system taking into account fault aspects. The use of aspect-oriented concepts combined with the RT-FRIDA framework extended contributes to the specification of NFR related to the domain under concern, allowing the representation of these aspects in adapted UML models.

This modeling method supported by early fault analysis, templates and checklists of RT-FRIDA framework can be reused in different distributed embedded systems, in design phases, maintaining the link between test phases, requirements, and design, promoting the traceability and system maintenance. Following the steps presented in Fig. 1 and correlating them with this case study, it is possible to evidence the benefits of the proposed method and the framework capabilities, allowing the requirements specification related to performance degradation caused by faults in intra-vehicular networks.

6 NFR Evaluation Using the Softgoal Weight Method

The NFR approach is a goal-oriented technique that can help to determine the extent to which objectives are achieved by a specific design. This feature is fundamental to evaluate the present research because it considers the properties of a system, such as reliability, maintainability, flexibility, and it can emphasize objectives and constraints for a distributed system. Different types of goal decomposition tree can be used in software engineering. The Softgoal Interdependence Graph (SIG) can be used to represent NFR (Chung et al. 2012); the Fault Tree Analysis can be applied to decompose faults in subsequent causes, according to a tree structure (Ruijters and Stoelinga 2015); and the Goal Structuring Notation can be used to represent the system assurance decomposing a top goal in subgoals which are supported by evidence (Spriggs 2012). According to Ruijters and Stoelinga (2015) the Fault Tree Analysis—FTA, with qualitative or quantitative analysis, considers a known fault tree structure and also computes values based on failure probabilities.

These techniques of goal decomposition could be applied in many scenarios, but in essence, they do not consider the crosscutting effects of faults in unknown events. This issue is a contribution of the RT-FRIDA framework application boosted by the aspect-oriented concepts and also highlighted

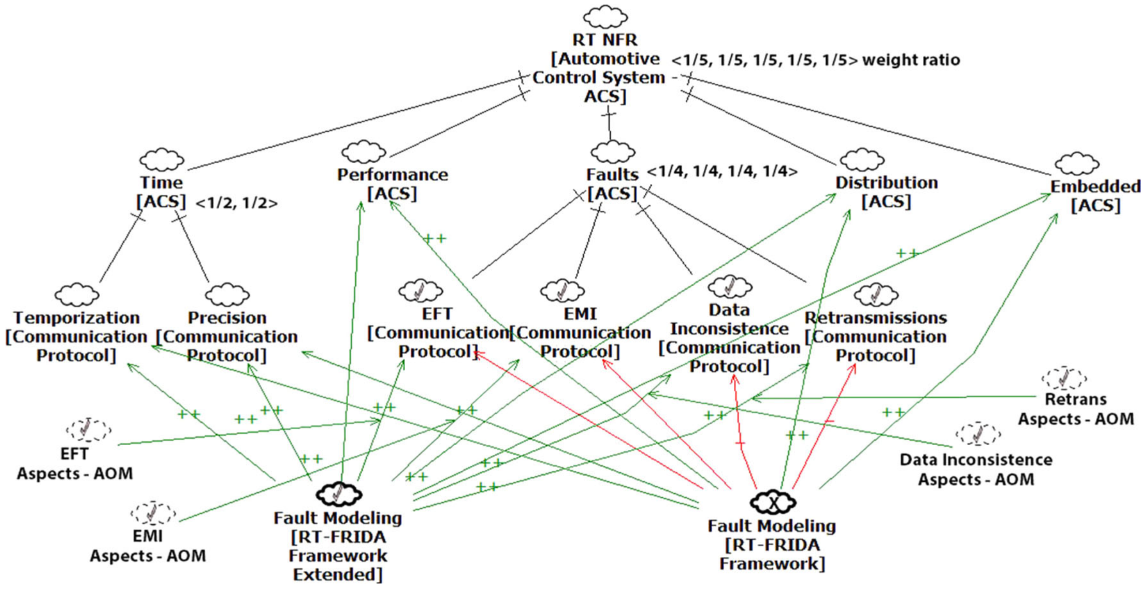


Fig. 12 SIG for evaluating the fault modeling using RT-FRIDA extended

in the SIG evaluation. In addition, most approaches in the literature are qualitative. SIG, on the other hand, can quantitatively represent how different fault types can impact on requirements specification (Subramanian and Zalewski 2016). This evaluation contributes to rapidly identify the design effort associated with a group of specific requirements.

6.1 The NFR Approach and Softgoal Weight Method

In order to develop the SIG to represent non-functional requirements evaluation, it is necessary to obtain quality properties of the system under analysis (Subramanian and Zalewski 2016). These requirements are decomposed in softgoal and sub-softgoals. In the SIG, the representation of operationalization softgoals must comply with parent softgoals, then a SIG graph contributes to helping engineers with decisions about the system design.

As presented in Chung et al. (2012), the NFR approach uses a specific ontology represented by NFR softgoals, operationalizing softgoals, claim softgoals, contributions, and propagation rules. According to Kobayashi et al. (2016), these rules are applied to evaluate a set of specified requirements. The concept of the softgoal weight method is defined as follows:

The SIG “G” is defined as,

$$< g0, S, O, D, Pw, Cw, Aw > \qquad (1)$$

where S is a set of softgoals of “G”, the root goal g0 is a special element of S, O is a set of operationalization softgoals and D represents the dependency relationship between S and O. Pw is a priority weight for softgoals decomposition, Cw defines the contribution weight between the parent and child softgoals. There are negative and positive contributions in the SIG that are represented by solid and dotted lines. Finally, Aw indicates the achievement weights of operationalization softgoals. According to Yamamoto (2015), the achievement weight of upper levels of softgoals Aw(g) is calculated as follows:

$$Aw(g) = \sum_{h_{inChild(g)}} Pw(h) * Cw(h) * Aw(h) \qquad (2)$$

where Child(g) is the set of sub-softgoals of a goal g.

In the sequence, the softgoal weight method is applied to highlight the contribution of fault modeling with RT-FRIDA.

6.2 SIG Evaluation for Fault Modeling with RT-FRIDA

Based on concepts of NFR framework introduced in Chung et al. (2012) and recent works related to the quantitative assessment of NFR (Subramanian and Zalewski 2016; Yamamoto 2015), a softgoal interdependence graph (SIG) was developed to represent and evaluate the real-time NFR modeled for a vehicular fault-diagnostic system. The evaluation shows the contributions of this proposed fault modeling framework based on RT-FRIDA. Figure 12 presents the SIG.

The SIG represents the contributions of the extended fault modeling framework based on RT-FRIDA with the emphasis in “fault aspects”.

The main NFR softgoal is decomposed into Time Aspects, Performance Aspects, Distribution Aspects, Embedded Aspects, and the most important, the Fault Aspects. The sub-

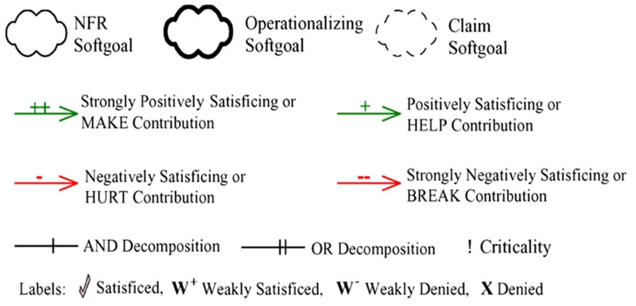

NFR Softgoal
Operationalizing Softgoal
Claim Softgoal
++ Strongly Positively Satisficing or MAKE Contribution
+ Positively Satisficing or HELP Contribution
- Negatively Satisficing or HURT Contribution
-- Strongly Negatively Satisficing or BREAK Contribution
AND Decomposition
OR Decomposition
! Criticality
Labels: Satisficed, W+ Weakly Satisficed, W- Weakly Denied, X Denied

Fig. 13 A brief part of the ontology of the NFR approach. Based on Subramanian and Zalewski (2016)

softgoals form the weight ratio of the parent softgoal (for example, the weight ratio for the parent softgoal "RT NFR" in the SIG of Fig. 12 is 1/5 for each sub softgoal).

According to (1) and (2), and the requirements impact values (weight ratio) defined in the SIG graph developed, is possible to evaluate the impact of fault requirements on the system design. Thus, the quality impact value of requirements specification with extended RT-FRIDA is calculated as:

$$(1/2 + 1/2)/5 + (1)/5 + (1/4 + 1/4 + 1/4 + 1/4)/5 \\ +(1)/5 + (1)/5 = 1$$

The quality impact value of requirements specification with RT-FRIDA original is calculated as:

$$(1/2 + 1/2)/5 + (1)/5 - (1/4 + 1/4 + 1/4 + 1/4)/5 \\ +(1)/5 + (1)/5 = 3/5$$

In Fig. 13 a brief summary of the ontology used in the NFR approach is presented. There are different types of clouds that represent NFR, Operationalizing and Clain softgoals. More details can be seen in Subramanian and Zalewski (2016).

According to Fig. 12, it is possible to observe the contributions with each of the four claimed softgoal (dotted clouds representing the softgoal that captures the design decision about aspects) related to requirements associated to the fault types, below the NFR "faults". This contribution allows operationalizing the extended RT-FRIDA. Comparing this quantitative result for the extended and original RT-FRIDA, 1 and 3/5, respectively, it is verified how the addition of NFR specification with aspect-oriented concepts can contribute to fault modeling and consequently contributing to improving the system reliability.

6.3 Results Analysis

This study presents an analysis of how faults can be studied in the early stages of design, and how their degradation effects can be mapped in order to provide a proactive mechanism. After experiments of fault susceptibility analysis in vehicular networks, the extended RT-FRIDA framework allows by specific checklists and NFR templates to detail the type, cause, and effects of fault degradation. This information is part of new non-functional requirements of the control system (example presented in Table 2). A contribution in the present work is the correlation between test phases and data collected with these tests, with the proposed modeling approach based on aspect-oriented modeling and non-functional specification. This improvement occurs due to the analysis of the system under test and fault injections, observing the system behavior and collecting a fault risk information to add in the control system design. Another contribution of this fault modeling approach is the possibility of a real-time correlation between retransmission message increase and performance degradation with faults injected and analyzed during the ordinary network operation. These issues are examples of how the present approach can improve the control system design with early fault modeling.

The fault modeling approach (Sect. 4) has as basis the fault impact analysis according to previously performed experiments. Therefore, the developed case study shows how the extended RT-FRIDA framework could be applied to fault specification as NFR. Additionally, the presented quantitative study (Sect. 6), shows with the SIG graph and the softgoal weight method, that the approach contributes to covering gaps about early fault modeling in vehicular control systems.

This study allows a fault-diagnostic mechanism development that can be added to the distributed network to detect and notify the fault disturbance on the performance of critical real-time control systems. In this sense, the "fault observer" is proposed (Figs. 10 and 11) and integrated into the active suspension control system based on the fault modeling performed using the RT-FRIDA framework and aspect-oriented concepts. The goal of the "fault observer" is to detect anomalies in the network. For this task and according to the case study, oscillations in performance metrics as average jitter, difference jitter, busload, and throughput are registered in local memory and are designed to trigger fault detection and notification mechanisms. The trigger parameters are based on the performed tests and checklists that specifies the operation limits of the system under different faults or interference. During the practice tests presented in the case study (Figs. 3 to 6), the measured metrics difference jitter and average jitter contributed to assessing the negative fault impact on performance. These capabilities are also observed combining previous experiments of fault injection and analysis presented in the literature (Nakamura et al. 2015; Shah et al. 2016; Roque et al. 2017a).

The presented study also contributes showing the advantage of the evaluation approach using a SIG graph in facilitating the requirements analysis. According to Subramanian and Zalewski (2016), the different types of relationships among softgoals, and between softgoals and operationalization in a SIG, bring the opportunity to conduct a systematic analysis by propagating the impact of decisions along with the relationships. Thus, combined with the applied softgoal weight method, it is possible to observe the contribution of the fault specification as NFR and the fault modeling in the design phases. This type of analysis is relevant, since it validates the analysis and requirements specification, showing to the designer the impact of the changes in the designed system.

6.4 Threats to Validity

Despite the results presented in the case study be general enough to support the claims about the validity of the proposed approach, it has limitations associated with the application scope, for example, focused on the faults that affect vehicular systems and its communication protocols. Thus, in the present study, the threats to validity are specified in three aspects: internal validity, external validity and construct validity (Runeson and Höst 2009; Feldt and Magazinius 2010).

The internal validity could be jeopardized by factors related to the test and instrumentation process before the requirements specification. The tools for analysis need to be carefully parametrized and configured to monitor the vehicular network during fault injections. This configuration could affect the obtained network information and consequently affect the requirement specification about the fault under analysis.

The external validity is related to the difficulty of to generalize the approach to different applications, due to the specific conditions of tests and also the fault modeling for an specific vehicular control system. Nevertheless, with the correct framework parametrization, this approach can contribute even in different scenarios.

The construct validity is related to the obtained results' impact and their relevance in the analyzed context, also considering the performance degradation under concern. The EFT fault effect may not be the same in different control systems, and the results obtained from the requirements specification must be re-evaluated.

Thus, for applications in different domains, the fault modeling and the NFR specification with the RT-FRIDA framework must be adapted considering the typical faults that affect the specific control system under concern for the considered domain.

7 Conclusions and Future Work

Solutions usually proposed for fault-tolerant or fault-diagnostic systems are very specific and can be considered as reactive because faults are usually not considered during the design phase of the distributed embedded control systems and are handled only during runtime. Intra-vehicular networks use many ECUs for critical tasks and control situations. Modeling faults in early-design phases are essential to improve reliability and maintainability. Recent research results highlight gaps in fault modeling focused on communication protocols, and to cover this gap, the present work proposes the fault modeling using aspect-oriented concepts.

The RT-FRIDA framework that was extended for fault modeling provides an approach to model the effect of different fault types as NFR. Thus, it is possible to implement a fault observer based on the proposed method in intra-vehicular networks to detect standard faults and performance degradation. The present work shows a specific case study to model electrical fast transients that can degrade an Active Suspension System in an intra-vehicular network. Experiments in a real CAN bus network were performed to verify the effect of EFT faults in the performance of the critical control system. These experiments show how EFT faults affect the system in terms of timing performance, significantly increasing the jitter during control messages on the network. After that, analyzing the fault behavior, the aspect-oriented modeling was applied to specify requirements to identify the fault impact on the system.

The checklist and models aggregated in the RT-FRIDA framework represent the possibilities of mapping fault effects after its analysis and the specification of suitable NFR. The approach contributes to improving fault modeling in the design phases. The validation process based on a SIG graph, with softgoal weight method and requirements elicitation, quantitatively demonstrated the design possibilities of the proposed modeling method. The fault modeling method also contributes to the system modularity, allowing the modeling of faults as "aspects" that represent crosscutting concerns in the distributed real-time embedded system. Future work indicates the application of the method for mapping other faults types and also its implementation in a real intra-vehicular network, analyzing the performance and possibilities for improvements.

References

Akkaya, I., Derler, P., Emoto, S., & Lee, E. A. (2016). Systems engineering for industrial cyber-physical systems using aspects. *Proceedings of the IEEE*, *104*(5), 997–1012.

Ali, S., Briand, L. C., & Hemmati, H. (2012). Modeling robustness behavior using aspect-oriented modeling to support robustness testing of industrial systems. *Software & Systems Modeling*, *11*(4), 633–670.

Alzahrani, N. A. M., & Petriu, D. C. (2015). Modeling fault tolerance tactics with reusable aspects. In *Proceedings of the 11th international ACM SIGSOFT conference on quality of software architectures* (pp. 43–52). ACM.

Apel, S., & Batory, D. (2010). How aspectj is used: An analysis of eleven aspectj programs. *Journal of Object Technology*, *9*(1), 117–142.

Brunner, M., Huber, M., Sauerwein, C., & Breu, R. (2017). Towards an integrated model for safety and security requirements of cyber-physical systems. In *Software quality, reliability and security companion (QRS-C), 2017 inter. conf. on* (pp. 334–340). IEEE.

Chiremsel, Z., Said, R. N., & Chiremsel, R. (2016). Probabilistic fault diagnosis of safety instrumented systems based on fault tree analysis and Bayesian network. *Journal of Failure Analysis and Prevention*, *16*(5), 747–760.

Chung, L., Nixon, B. A., Yu, E., & Mylopoulos, J. (2012). *Non-functional requirements in software engineering* (Vol. 5). New York, NY: Springer.

Costa, B. S. J., Angelov, P. P., & Guedes, L. A. (2014). Real-time fault detection using recursive density estimation. *Journal of Control, Automation and Electrical Systems*, *25*(4), 428–437.

Feldt, R., & Magazinius, A. (2010). Validity threats in empirical software engineering research-an initial survey. In *Seke* (pp. 374–379).

Freitas, E. P., Wehrmeister, M. A., Pereira, C. E., Wagner, F. R., Silva, E. T., & Carvalho, F. C. (2007). Using aspect-oriented concepts in the requirements analysis of distributed real-time embedded systems. In *Embedded system design: Topics, techniques and trends* (pp. 221–230). Springer.

Gessner, D., Barranco, M., Ballesteros, A., & Proenza, J. (2014). Sfi-can: A star-based physical fault-injection infrastructure for can networks. *IEEE Transactions on Vehicular Technology*, *63*(3), 1335–1349.

Godoy, E. P., & Porto, A. J. (2013). Co-simulation tools for networked control systems: Revision and utilization. *Journal of Control, Automation and Electrical Systems*, *24*(6), 816–830.

Huang, S., Zhou, C., Yang, L., Qin, Y., Huang, X., & Hu, B. (2016). Transient fault tolerant control for vehicle brake-by-wire systems. *Reliability Engineering & System Safety*, *149*, 148–163.

Iqbal, M. Z., Ali, S., Yue, T., & Briand, L. (2012). Experiences of applying uml/marte on three industrial projects. In *international conference on model driven engineering languages and systems* (pp. 642–658). Springer.

Khakhar, D., & Nayak, A. (2018). Capturing performance requirements of real-time systems using uml/marte profile. In *Soft computing: Theories and applications* (pp. 703–714). Springer.

Kiczales, G., Lamping, J., Mendhekar, A., Maeda, C., Lopes, C., Loingtier, J. M., et al. (1997). Aspect-oriented programming. In *European conference on object-oriented programming* (pp. 220–242). Springer.

Kienzle, J., Al Abed, W., Fleurey, F., Jézéquel, J. M., & Klein, J. (2010). Aspect-oriented design with reusable aspect models. In *Transactions on aspect-oriented software development VII* (pp. 272–320). Springer.

Kobayashi, N., Morisaki, S., Atsumi, N., & Yamamoto, S. (2016). Quantitative non functional requirements evaluation using softgoal weight. *Journal of Internet Services and Information Security*, *6*(1), 37–46.

Mahapatro, A., & Khilar, P. M. (2013). Fault diagnosis in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2000–2026.

Marques, L., Vasconcelos, V., Pedreiras, P., & Almeida, L. (2013). Error recovery in time-triggered communication systems using servers. In *Industrial embedded systems (SIES), 2013 8th IEEE international symposium on* (pp. 205–212) IEEE.

Marques, L., Vasconcelos, V., Pedreiras, P., & Almeida, L. (2014a). Comparing scheduling policies for a message transient error recovery server in a time-triggered setting. In *Emerging technology and factory automation (ETFA)* (pp. 1–6). IEEE.

Marques, L., Vasconcelos, V., Pedreiras, P., Silva, V., & Almeida, L. (2014b). Efficient transient error recovery in flexray using the dynamic segment. *Emerging tech* (pp. 1–4). IEEE: Factory Automation (ETFA).

Mo, H., Wang, W., Xie, M., & Xiong, J. (2017). Modeling and analysis of the reliability of digital networked control systems considering networked degradations. *IEEE Transactions on Automation Science and Engineering*, *14*(3), 1491–1503.

Nakamura, M., Ohara, M., Saysanasongkham, A., Arai, M., Sakai, K., Fukumoto, S., et al. (2015). Testbeds of a hybrid-arq-based reliable communication for cans in highly electromagnetic environments. In *Future energy elect. conf. (IFEEC), 2nd Int* (pp. 1–6). IEEE.

Nguyen, P. H., Klein, J., & Le Traon, Y. (2014). Model-driven security with a system of aspect-oriented security design patterns. In *Proceedings of the 2nd workshop on view-based, aspect-oriented and orthographic software modelling* (p. 51). ACM.

Oetjens, J. H., Bannow, N., Becker, M., Bringmann, O., Burger, A., Chaari, M., et al. (2014). Safety evaluation of automotive electronics using virtual prototypes: State of the art and research challenges. In *Proceedings of the 51st annual design automation conference* (pp. 1–6). ACM.

Pattanaik, B., & Chandrasekaran, S. (2012). Recovery and reliability prediction in fault tolerant automotive embedded system. In *Emerging trends in electrical engineering and energy management (ICETEEEM), 2012 international conference on* (pp. 257–262). IEEE.

Piper, T., Winter, S., Schwahn, O., Bidarahalli, S., & Suri, N. (2015). Mitigating timing error propagation in mixed-criticality automotive systems. In *2015 IEEE 18th international symposium on real-time distributed computing (ISORC)* (pp. 102–109). IEEE.

Poussot-Vassal, C. (2008). Robust lpv multivariable automotive global chassis control. Ph.D. thesis, Institut National Polytechnique de Grenoble-INPG.

Roque, A. S., Pohren, D., Michelin, T. J., Pereira, C. E., & Freitas, E. P. (2017a). Eft fault impact analysis on performance of critical tasks in intravehicular networks. *IEEE Transactions on Electromagnetic Compatibility*, *59*(5), 1415–1423.

Roque, A. S., Steinmetz, C., Freitas, E. P., & Pereira, C. E. (2017b). Modeling faults in communication protocols based on an aspect-oriented method. In *Industrial informatics (INDIN), 15th int conf on* (pp. 732–737). IEEE.

Roque, A. S., Nunes, G. L., Freitas, E. P., & Pereira, C. E. (2018). Requirements specification and evaluation for transient faults in communication protocols based on rt-frida framework. *IFAC-PapersOnLine*, *51*(10), 76–81.

Ruijters, E., & Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review*, *15*, 29–62.

Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, *14*(2), 131.

Shah, M. B. N., Husain, A. R., Aysan, H., Punnekkat, S., Dobrin, R., & Bender, F. A. (2016). Error handling algorithm and probabilistic analysis under fault for can-based steer-by-wire system. *IEEE Transactions on Industrial Informatics*, *12*(3), 1017–1034.

Spriggs, J. (2012). *GSN-the goal structuring notation: A structured approach to presenting arguments*. London: Springer.

Subramanian, N., & Zalewski, J. (2016). Quantitative assessment of safety and security of system architectures for cyberphysical systems using the nfr approach. *IEEE Systems Journal*, *10*(2), 397–409.

Tuohy, S., Glavin, M., Hughes, C., Jones, E., Trivedi, M., & Kilmartin, L. (2015). Intra-vehicle networks: A review. *IEEE Transactions on Intelligent Transportation Systems*, *16*(2), 534–545.

Vyatkin, V. (2013). Software engineering in industrial automation: State-of-the-art review. *IEEE Transactions on Industrial Informatics*, *9*(3), 1234–1249.

Wasicek, A., Derler, P., & Lee, E. A. (2014). Aspect-oriented modeling of attacks in automotive cyber-physical systems. In *Design automation conference (DAC), 2014 51st ACM/EDAC/IEEE* (pp. 1–6). IEEE.

Wehrmeister, M. A., Pereira, C. E., & Rammig, F. J. (2013). Aspect-oriented model-driven engineering for embedded systems applied to automation systems. *IEEE Transactions on Industrial Informatics*, *9*(4), 2373–2386.

Wimmer, M., Schauerhuber, A., Kappel, G., Retschitzegger, W., Schwinger, W., & Kapsammer, E. (2011). A survey on uml-based aspect-oriented design modeling. *ACM Computing Surveys (CSUR)*, *43*(4), 28.

Yamamoto, S. (2015). An approach for evaluating softgoals using weight. In *Information and communication technology* (pp. 203–212). Springer.

Zeng, W., Khalid, M., Chowdhury, S. (2015). A qualitative comparison of flexray and ethernet in vehicle networks. In *Electrical and computer eng. (CCECE), 28th Canadian conf. on* (pp. 571–576). IEEE.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

ApêndiceC

C.1 Publicação IEEE - Transactions on Electromagnetic Compatibility

EFT Fault Impact Analysis on Performance of Critical Tasks in Intravehicular Networks

Alexandre S. Roque, Daniel Pohren, Thiago J. Michelin, Carlos Eduardo Pereira, and Edison Pignation Freitas

Abstract—**Electrical fast transients (EFT) represent an important problem to intravehicular networks. Concerning this problem, this paper reports a study about the impact of EFT to the performance of communication protocols used in intravehicular networks. A method of fast transient injection has been applied to an experimental CAN network with the objective of verifying the EFT impact on jitter and how it influences the communication process. An experiment with a simulated control system distributed over a real CAN network was carried out. For this experiment, an active suspension system was chosen as a case study and a sequence of EFT injections was performed. As a result, it was verified that injected EFT bursts increase jitter of safety-critical control messages and may effectively influence and produce faults during the communication process.**

Index Terms—**Automotive electromagnetic compatibility (EMC), CAN protocol, jitter/noise modeling and analysis, safety-critical systems, transmission analysis and testing.**

I. Introduction

RECENT advances in automotive technologies increasingly demand reliability in communication processes, which is an important feature of the main protocols used in this area. In-vehicle electronic systems are rapidly advancing in complexity and diversity. A variety of sensors and processors are employed in different parts of a vehicle for various functions that are responsible for monitoring the vehicle performance and safety aspects. It is possible to consider other technologies, such as camera, radar, and ultrasonic sensors, which have been used to sense the environment surrounding the vehicle, providing relevant information so that in the future vehicles can become more intelligent and autonomous.

Communication protocols used in intravehicular networks are responsible for interconnecting several electronic control units—ECUs according to a specific topology. Some safety-critical tasks communicate over the network and must timely execute their actions. Protocols adopted by intravehicular networks are developed or modified, in order to increase the reliability in the communication processes.

In line with this goal of increasing reliability, some extensions to the CAN protocol have been developed and others automotive protocols aiming at safety-critical systems and fault tolerant concepts have also been developed, such as TTP/C, Byteflight, and FlexRay [1], [2].

Each node in a vehicular network includes one or more transceivers. Transceivers are the interface between the physical media and the host node processor unit, and are also responsible for implementing physical layer specifications [3], [4]. Communication protocols may be affected by several sources of electromagnetic interference that can couple transient energy to circuits through data cables and cause different types of disturbances on ECUs.

Different types of fault situations can be generated by electrostatic discharge, such as power switching transients, defined as electrical fast transients (EFTs) [5]. According to [6] electromagnetic immunity problems may be caused by a variety of mechanisms and system designers are increasingly applying rigorous immunity testing, with the objective to prevent these problems before they occur.

In this context, EFTs play an important role. An EFT is the outward manifestation of a sudden change in circuit conditions and are usually very small and unpredictable [7]–[9]. Represented by either a single pulse or a burst of spikes, EFTs may disrupt differential signaling causing transmission failures. According to [10], electromagnetic disturbances such as low energy EFTs pulse trains generated by switching phenomena in low and medium voltage networks are a present and an ongoing challenge for electrical and electronic equipment.

Many factors make this fault type difficult to measure and constitute potential sources of critical faults. Therefore, very accurate measures to understand these events and their periodicity are essential for reliability of the communication process. Measuring techniques may be applied to experiments with the aim of detecting and registering transients occurrences, in order to after understanding and analyzing them, design solutions to mitigate the problems.

In order to correlate transient faults with performance degradation of critical real-time tasks, the work reported in [11] introduced the first steps toward a method of analysis to perform this desired correlation. This current paper extends this seminal work deeply describing it and applying the method in experiments to evaluate the impact of EFTs not only on ECU transceivers, but also on error propagation in intravehicular

Manuscript received January 8, 2017; revised February 8, 2017; accepted March 14, 2017. Date of publication April 6, 2017; date of current version May 25, 2017.

A. S. Roque, D. Pohren, and T. J. Michelin are with the Department of Electrical Engineering, Federal University of Rio Grande do Sul, Porto Alegre 90040-060, Brazil (e-mail: as.roque@ufrgs.br; daniel.pohren@ufrgs.br; thiago.michelin@ufrgs.br).

C. E. Pereira and E. P. Freitas are with the Federal University of Rio Grande do Sul, Porto Alegre 90040-060, Brazil (e-mail: cpereira@ece.ufrgs.br; edison.pignaton@ufrgs.br).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEMC.2017.2686343

networks. Thus, this study provides an experimental analysis, to include in future works types of transient failures in the modeling phases of control systems, allowing the system survival in critical situations.

This paper is organized as follows: Section II explores related works with emphasis in the gap related to EFT impact analysis. Section III presents the method applied for EFT impact analysis with an overview of the network configuration and the EFT injection. Section IV describes the performed case study to validate the method. Section V presents the test results and EFT analysis on performance of critical tasks defined in the case study. Section VI presents conclusions and future work directions.

II. Related Work

It is possible to find in the literature recent works highlighting the importance of mechanisms that can reduce the impact of transient faults in embedded systems. The development of intravehicular networks presents interest in this topic, as it is the specific protocols used in this domain can be affected by transient faults.

The work reported in [12] discusses an approach of task monitoring aiming at protecting critical tasks from interference with temporal performance guarantees. The approach is based on the ISO 26262 standard (Road Vehicles), risk-based standard. The proposal seeks to highlight the differences compared to existing tools, such as the use of automotive open system architecture, which also allows this monitoring. However, it does not consider monitoring less critical tasks that can propagate errors. The time guarantee is performed by means of pre-emptive monitoring of critical tasks (according to preemption budget).

In [13], a work using flexible time-triggered communication on CAN (FTT-CAN) protocol is presented. This work proposes an online traffic scheduling approach in which retransmissions are scheduled with the remaining time-triggered traffic. Fault detectors are added in FTT-CAN protocol to monitor bus activity and to retransmit omitted messages, with the only focus on temporal redundancy, aiming to handle communication errors in time-triggered systems.

Another relevant work in the area is reported in [14], also based in FTT-CAN, presenting an approach in which the network transmits its messages in specified time instants combining a TT approach with online traffic scheduling. This feature allows using temporal redundancy with message retransmissions triggered by the occurrence of errors.

Following the same principles of the works aforementioned, the work proposed in [15] presents a model for recovery and reliability prediction in automotive embedded systems based on CAN protocol. The model focuses on interaction of different software modules that are responsible for critical tasks. Calculations define the probability of failure according to the record of specific events. The model considers several fault sources that are indexed and analyzed with a prediction algorithm. The mechanism is evaluated by verifying the periodic activation of different redundancy modules.

Among the technologies used in intravehicular networks, FlexRay is a protocol that can be affected by permanent or transient faults. Aiming at addressing the problem, the work presented in [16] proposed a mechanism that uses temporal redundancy to recover transient errors in time-triggered messages of the FlexRay protocol. This mechanism uses dynamic segment of FlexRay frame to implement retransmissions messages. The results shown that this method significantly reduces the use of channel bandwidth and provides faster recovery of a set of faults.

The literature review allowed to finding works proposing different mechanisms and time-triggered message scheduling methods in communication protocols, with the main objective of mitigating faults. However, the relationship between some type of faults and their impact in time constraints of critical tasks and on system performance are not considered.

Related works exist focusing on specific types of faults, as the work presented in [17], which studies the susceptibility of CAN protocol to electrical fast transients (EFT), specifically in signals of transceiver ports. The EFT impact is verified according to IEC TS 62228 [18] with possibilities of rejections and failures in CAN signals. Experiments are performed to verify the EFT susceptibility and a mechanism for immunizing transceivers is proposed. However, the impact in protocol time constraints and in the overall performance is not investigated.

The work presented in [19] reports an extensive survey of transient faults carried out at a constant location within an automobile electrical system. The measured transient parameters were compared to the sensitivity of several standard automotive electronic devices to identify their immunity to the conducted transients. Statistics of the measured transients over three main operations (Ignition, AC, Headlight) are presented with a time range duration and amplitude peak in volts. Despite the value of these data, they are not related to the protocol performance (jitter, lost packets) and their impact in time constraints of critical tasks.

The work in [20] presents a specific application related to transient faults. It presents a proposal of a hierarchical transient fault tolerant scheme with embedded intelligence and resilient coordination for a brake-by-wire (BBW) system. It is based on the analysis of transient fault propagation characteristics. An experiment is conducted to evaluate the system performance for the BBW system with a communication bus based on TT-CAN protocol and also with a simulation using a CAN Analyzer platform. In this experiment, the transient faults are simulated; they are not injected in the real system. Thus, it is possible to combine the approaches presented in [17], [19], and [20] to verify by other perspective the impact in time constraints and performance of different critical tasks.

Table I summarizes the main features of the analyzed related works.

Based on these researches, the next section presents an experimentation method to verify EFT effects in communication performance. In sequence, a case study with focus on CAN network to active suspension system is conducted.

III. Method for EFT Analysis

The initial proposal of the described method was presented in a recent work reported in [11], in which an experiment was conducted injecting EFT noise in a CAN network with three nodes,

TABLE I
RELATED WORKS SUMMARY

Ref.	Main focus	Result	FIPCT*
[12]	Monitoring of less critical tasks that can propagate errors.	temporal performance guarantees	-
[13]	Fault detectors in FTT-CAN to monitor bus activity	online traffic scheduling	-
[14]	FTT-CAN with on-line traffic scheduling	message retransmission triggered by errors	
[15]	Fault sources are indexed and analyzed with a prediction algorithm	model for recovery and reliability prediction	-
[16]	Dynamic segment of FlexRay to implement retransmissions messages	mechanism/temporal redundancy to recover trans. errors	-
[17]	EFT impact in signals of CAN transceiver ports	susceptibility of CAN protocol to EFT	-
[19]	Survey of transient faults within an automobile electrical system	statistics of measured transients over three main operations	X
[20]	"Simulated" transient faults and analysis of propagation characteristics.	hierarchical transient fault scheme for BBW	X
This Work	EFT "injection" in industrial network protocols	Impact analysis in time constraints of critical tasks	X

*FIPCT – Fault impact in performance of communication protocols and critical tasks.

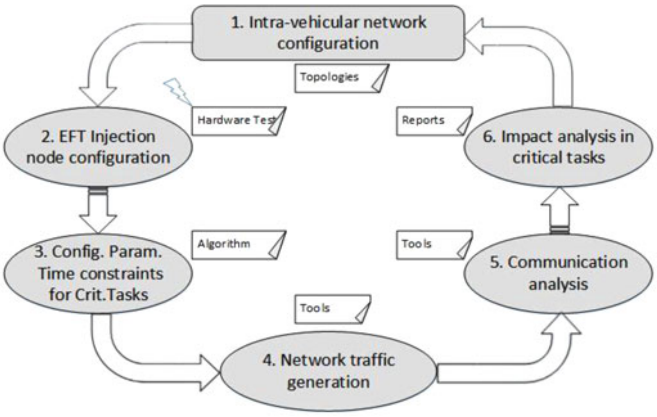

1. Intra-vehicular network configuration
Topologies
Hardware Test
Reports
2. EFT Injection node configuration
6. Impact analysis in critical tasks
Algorithm
Tools
3. Config. Param. Time constraints for Crit.Tasks
5. Communication analysis
Tools
4. Network traffic generation

Fig. 1. Overview of the applied test method.

but without a specific vehicular control system. The present work extends and complements the previous work presented in [11] by deeply describing the method, besides applying and testing the method in a specific vehicle control system, in order to analyze the impact of EFTs in the control system, thus providing more consistent and solid results.

In order to verify the impact of EFTS in industrial communication protocols, network disturbances are generated and were evaluated according to a hardware test developed. Fig. 1 illustrates an overview of applied test method.

The method must be cyclically performed in order to change some parameters and to perform refinements that are necessary to increase the precision and the reliability in data measurements. This method is applied following six steps, as described in the following. In Step 1, the network topology is configured as well as the method of node interconnection for the experiment in order to characterize critical control situations. Step 2 implements a hardware model for EFT injection inspired on IEC TS 62228 test standard, but with focus on the burst injection specification, applied in a real CAN network on a development platform. In this case, a function generator can be used to inject transients with different amplitudes. The main difference in relation to the described in the standard is that it did not use a full EFT board with CAN nodes, but a real CAN network. Thus, it is possible to analyze the impact of this type of fault based on a real vehicle control system. This decision allows this work not only to apply the test suggested in the standard, but also to extend it showing from another perspective how the fault can be analyzed. This new perspective in the analysis can support future techniques to mitigate this fault in control systems. According to IEC TS 62228, it is necessary to attend seven test requirements for this fault injection type: 1) Test pulse generator; 2) test board; 3) oscilloscope bandwidth $> = 500$ MHz; 4) pattern generator; 5) external power supply; 6) mode control unit; and 7) a PC. Only the requirement 2 is modified. Fig. 2 illustrates this interconnection topology and how the EFT injection is introduced.

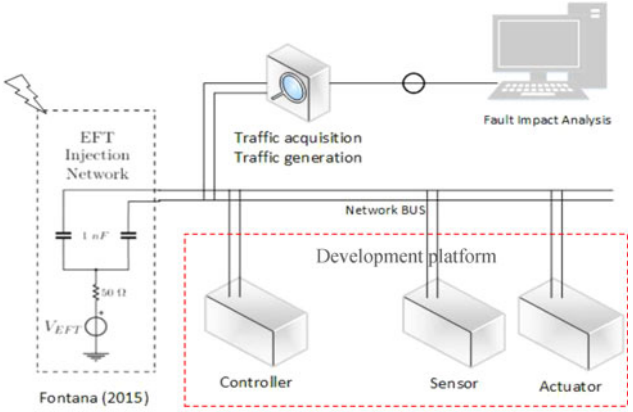


Fig. 2. Overview of the EFT injection method applied.

In step 3, several parameters related to time constraints of some types of critical tasks that use communication protocols are configured (for example, brake and traction control system). Three nodes are specified as sensor, controller, and actuator, with their behavior programmed in an embedded algorithm. After network and hardware configuration, step 4 defines a tool for traffic acquisition. Step 5 defines the usage of another tool to analyze communication and to detect disturbances. Finally, in step 6 reports about the EFT impact on critical tasks defined in step 1 are generated. For future design projects, this feedback must be used to reconfigure the parameters related to time constraints and verified hardware requirements for fault tolerance.

In the following, Section IV presents the details of a case of study and the performed experiments applying this method.

IV. EFT IMPACT ANALYSIS ON CAN PROTOCOL

A. Description of the Test Procedure

The test method was applied following the six steps presented in Fig. 1, with specific configuration and specific tools. The

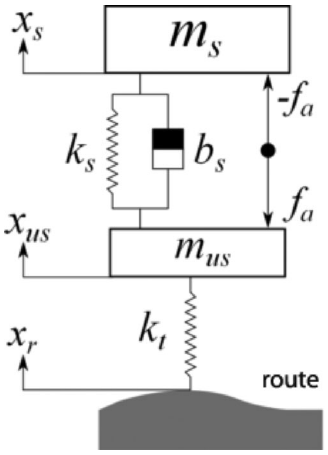


Fig. 3. Quarter-car model [21].

configured network is based on CAN protocol and simulate similar conditions related to a typical part of communication between nodes in a CAN network. The case study aims to verify specifically the influences of EFT and registering logs of the communication process.

The tools and settings used in each step are listed in the following:

1) *Step 1:* Network based on CAN protocol;
2) *Step 2:* EFT injection with a hardware test developed;
3) *Step 3:* Time constraints for active suspension control;
4) *Step 4:* Traffic generation with Vector CANoe tool and VN8900 with VN8970 hardware module;
5) *Step 5:* Communication analysis with Vector CAN Analyzer; and
6) *Step 6:* Graphical results and impact analysis on communication performance;

B. CAN Network Configuration for Active Suspension System

To study the effects of EFT injection on a CAN network, an active suspension system was chosen, as presented in [21]. This task composes the step 1 of test method illustrated on Fig. 2. Such system was selected because it is a safety-critical system, and relies on the underlying communication protocol to meet its time constraints. Fig. 3 illustrates the suspension (plant) model. This model is very well known in the literature, and is known as the quarter-car model.

The plant model is described by many parameters. For this test, the suspension deflection $X_{\rm def}$ is the one considered to evaluate control performance. Suspension deflection is defined as the difference between the vehicle's body vertical position X_s and the suspension set baseline position X_{us} Thus, suspension deflection is defined by:

$$X_{\rm def} = X_{s-}X_{us}.$$

The control applied to this system is a simple state-feedback controller. The first controller developed in [21] is applied.

For experimental evaluation of this case study, two Vector VN8910A devices equipped with a VN8970 plug-in module were employed. One device is responsible for simulating the plant and logging communication data. The other device operates in stand-alone mode and implements the controller.

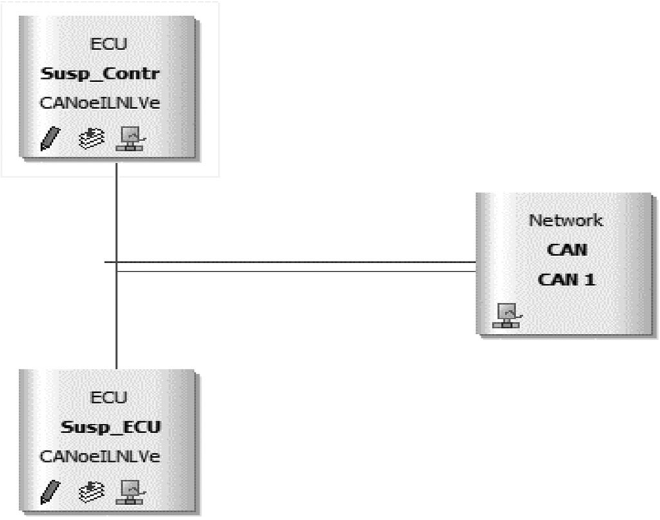


Fig. 4. CAN network topology used in the performed tests.

The CAN network was modeled using the Vector CANoe platform. Within the CANoe environment, two ECUs were configured, as depicted by Fig. 4.

The ECU "Susp_ECU" implements the quarter-car model, whereas ECU "Susp_Contr" implements the controller.

The main objective of this test is to analyze the susceptibility of a CAN network in the presence of EFT injection by verifying the impact it produces on the critical system messages timing. Consequently, its effect on control performance due to higher message latency or, in the worst case, package loss, should also be verified. For the EFT injection part of the experiment, a specific circuit was designed.

C. EFT Injection Circuit

EFTs consist of bursts with variable amplitudes generated in CAN networks by different noise sources (ignition, headlight, air conditioner). In order to verify if disturbances were produced, this test is performed according to step 2 of the test method (see Fig. 1). A specific circuit has been designed for the EFT injection and is presented in Fig. 5.

The circuit of EFT injection consists of a booster voltage amplifier using an operational amplifier model TL071, supplied with -15 and 60 V dc. The strategy to allow the op-amp run with this voltage range is the usage of a voltage divider by 10 at output, together with a noninverter configuration and gain 10. Fig. 6 shows the EFT Injection board highlighting some main components.

In order to guarantee that the voltage will be at the correct value, a zener diode was used to fix this value at 12 V dc at the positive terminal of the op-amp. This allows this system to use an input signal from 15 Vpeak and gives the output until 55 Vpeak. The original signal came from an arbitrary wave generator configured to supply peaks with duration from 15 us to 2 ms and delay about 5–10 ms.

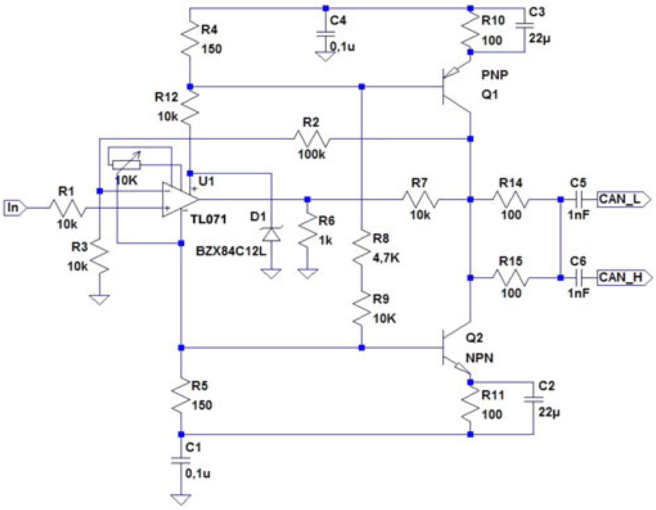


Fig. 5. EFT injection circuit.

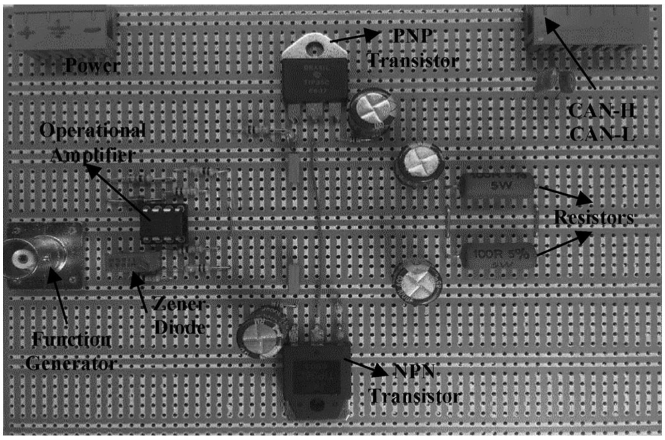


Fig. 6. EFT injection board.

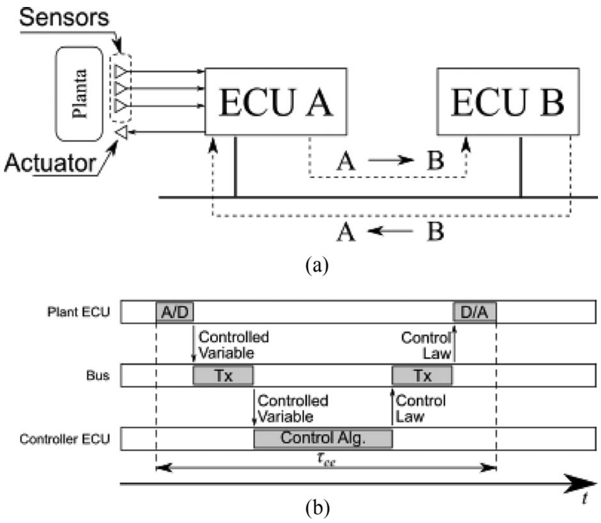


Fig. 7. (a) CAN network control plant with ECUs. (b) Event time evolution that occurs during on cycle of the control application [22].

The circuit rise and fall times are about 20 ns according the transistors applied (TIP35C and TIP36C), but the same circuit can be updated using faster transistors. Thus, it is possible to achieve 5 ns of rise/fall times, according to specification of IEC 61000 standard. On the other hand, the IEC TS 62228 standard does not specify rise and fall times, only emphasizes how the test method can be performed and how the measurement should be, a task that was carried out successfully on this experiment. The main point of this experiment is to show how the EFT injection can be performed allowing fault impact analysis in CAN networks and the study of mechanisms to mitigate this problem. The developed circuit is similar to the circuit proposed in recent work presented in [17] that also is based on the same standard, but with EFT susceptibility test in a two-node PCB CAN network.

The differences between the developed test circuit and the referred IEC 61000-4-4 and IEC TS 62228 standards do not affect the objectives and results of this study, but they allow the analysis of the electric transients and the subsequent verification at the control system level. As presented in [19], EFT failures do not have a specific pattern, they are sporadic, and may have varied rise and fall times. These standards suggest test specifications, but it does not mean that they have to be strictly followed without changes, because they do not always meet the specific criteria of all test scenarios. In this sense, the changes made in this experiment allowed the fault injection to be performed in a real intravehicular network, with a typical vehicular control system, with critical time constraints and using a vehicular development platform. This analysis also allowed verifying the previous modeling of this fault type in vehicle-embedded systems.

To determine the immunity and susceptibility of the communication against EFT noise, disturbances were injected into the network with amplitudes that 19, 39, and 57 Vp to represent faults registered in [19]. Communication data were logged for later analysis.

D. Configuration of the Time Constraints and Traffic Generation for Network Analysis

This section characterizes steps 3–5 of the test method applied. As specified previously, according to the active suspension case study, a specific control system with specific time constraints is configured. The main objective of an active suspension system is to isolate the vehicle chassis from disturbances generated by path irregularity. By means of an external actuator, this system is employed to control the vehicle's body vertical movement. Fig. 7(a) presents the flow of information among the system components, whereas Fig. 7(b) illustrates the end-to-end delay of the control loop, when there is no contention among nodes for bus access.

In this scenario, a simple state-feedback controller was employed. Messages which transmit control law information are cyclic and have a period of 5 ms. This time interval is a constraint for the control system, since longer periods may bring the system to an unstable condition. Therefore, this constraint will be analyzed after EFT injection. The applied test method requires the communication process between nodes to be

Fig. 8. Vector VN8900 with VN8970 module.

TABLE II
TRANSIENT TESTS

Parameter	Operation	Range
Burst duration	Ignition	1.2 ms
	AC	687 us
	Headlight	198 us
Amplitude	Ignition	57 V
	AC	37 V
	Headlight	19 V

Adapted from [19].

logged. Hence, all communication traffic is monitored by Vector VN8900, which is the bus interface employed during this experiment.

Fig. 8 shows the Vector VN8900 tool used for CAN communication.

This tool supports CAN 2.0b and ISO 11898-2 (high-speed CAN with transmission rates up to 1 Mbit/s). For EFT injection terminals, CAN-H and CAN-L are connected to the EFT board using a standard CAN cable with termination of 120 Ω.

V. Results

For the impact analysis on time constraints (step 6 of the applied method), the results about a sequence of performed tests are presented. The tests were performed following the statistics of transient faults listed in [19] for a sequence of EFT injection with burst of 1, 2 ms, 687 and 198 μs. A respective sequence of EFT injection with amplitudes of 57, 37, and 19 V were generated using an arbitrary wave generator. Table II presents the sequence of the generated fast transients.

In order to verify the interconnection between the function generation and the EFT circuit, a prior measurement of the generated pulses was performed. Figs. 9–11 present the measurement sequence of these generated pulses by the oscilloscope.

After checking the generated EFT signals, a sequence of communication tests related to the active suspension control law (suspension deflection parameter and plant actuating) with 5 ms of EFT burst interval was executed. Communication logs were registered by Vector CAN Analyzer and then the corresponding graphs were plotted in MATLAB for their analysis. For comparison purposes, before performing the test sequence, a network communication measurement was performed without the EFT pulses. The sampling interval for the logs recording

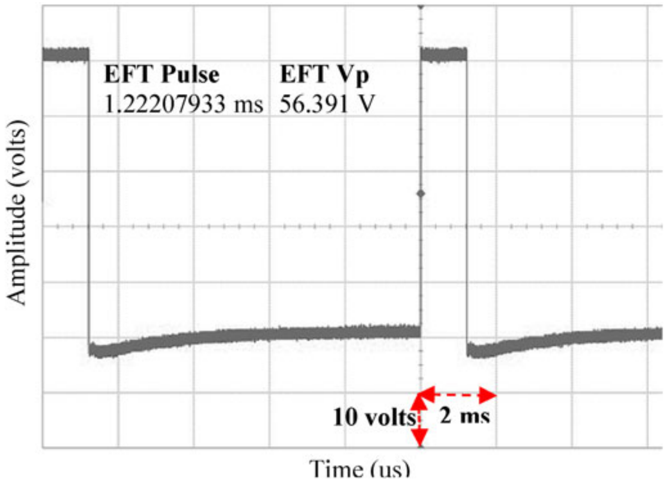


Fig. 9. EFT burst with 57 Vp and 1.2 ms.

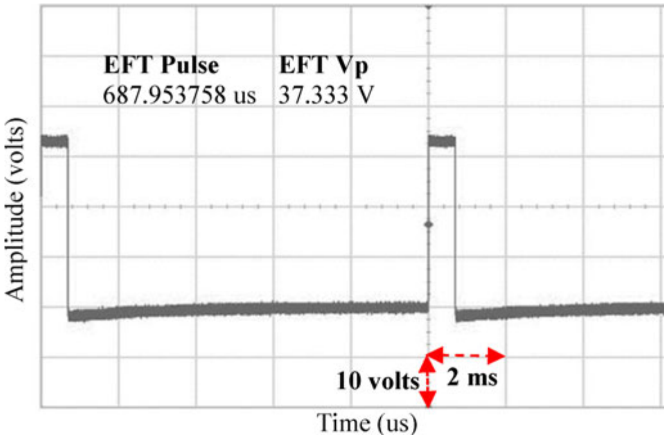


Fig. 10. EFT burst with 37 Vp and 687 us.

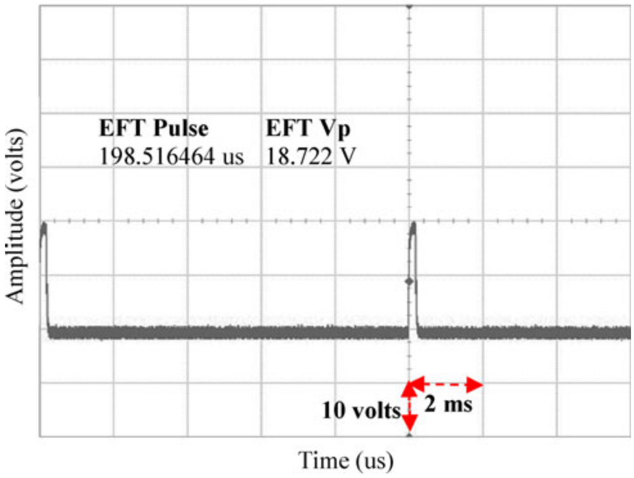


Fig. 11. EFT burst with 19 Vp and 198 us.

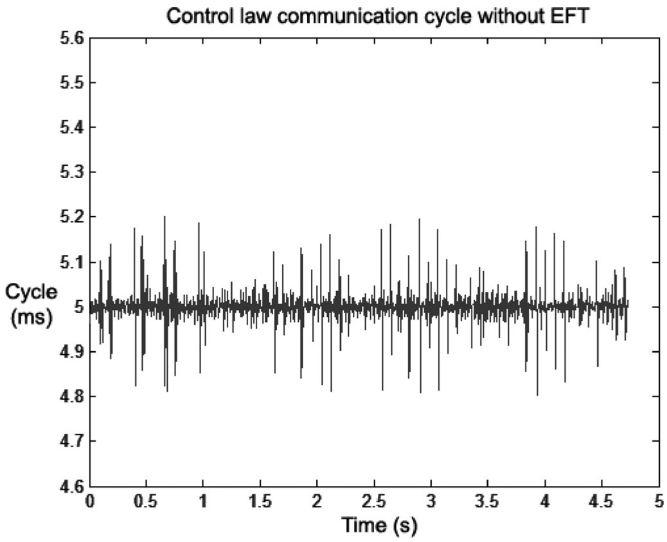


Fig. 12. Communication cycle without EFT Injection.

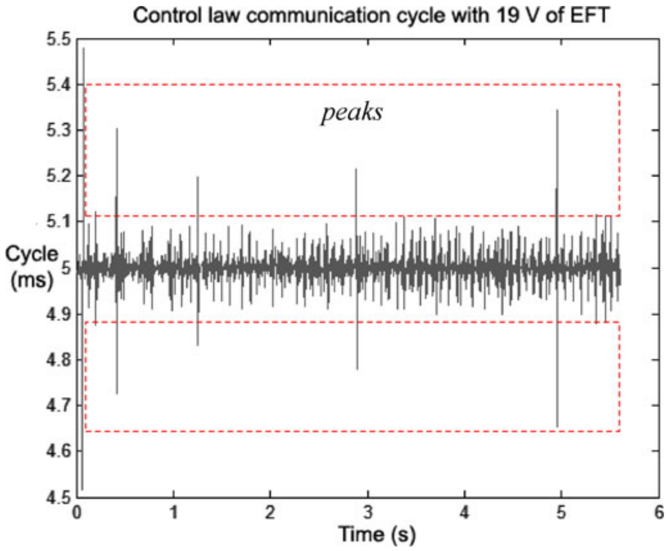


Fig. 13. Performance graph generated with 19 V of EFT.

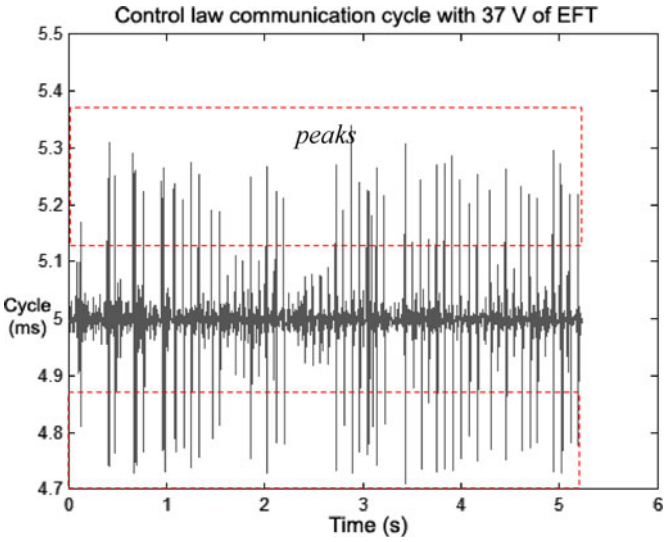


Fig. 14. Performance graph generated with 37 V of EFT.

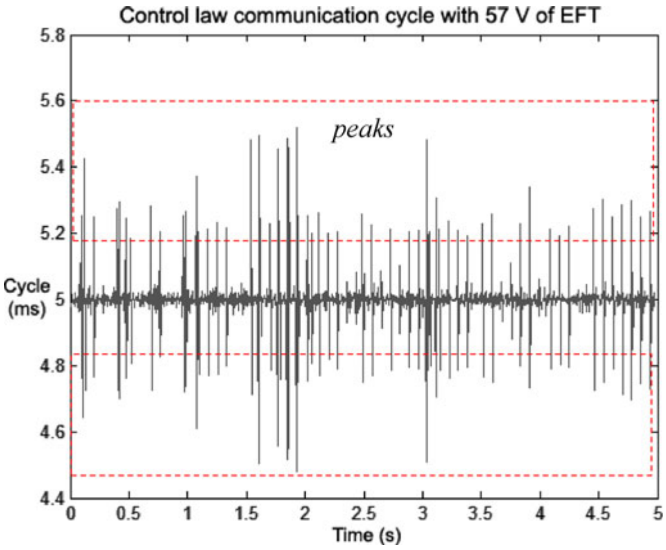


Fig. 15. Performance graph generated with 57 Vp of EFT.

is of 5 s. Fig. 12 presents the performance graph without EFT injection.

According to the graph presented in Fig. 12, for the sampled period, the communication cycle measured ranges between 4.8 and 5.2 ms. This oscillation occurs due to the time variation of the received packet in the previous control law and the packet sent in next control law. The next graph at Fig. 13 shows the performance of the communication process with 19 V of EFT with 198 μs of burst duration.

Fig. 13 shows that the impact on the bus to communicate with 19 V of EFT injection is not significant, but it is possible to verify the increase of delay peaks in communication between 4.7 and 5.5 ms. Fig. 14 presents the performance of the communication process with 37 V of EFT with 687 μs of burst duration.

It can be observed in Fig. 14, according to dotted area, that several communication cycles are affected by EFT injection and that the delay peaks were increased more frequently. Fig. 15 presents the performance of communication process with 57 V of EFT with 1.2 ms of burst duration.

In the communication tests with EFT injection of 57 V, it is possible to observe an increase in communication delays in a greater number of data communication cycles between 4.5 and 5.6 ms. In Fig. 15, it is possible to verify that the amount of peaks is smaller when compared to Fig. 14, but with greater amplitude and impact on performance. These results indicate the susceptibility of CAN communication to EFT noise on the perspective of control cycle.

In order to correlate the experiments, a summary with the difference jitter, average jitter in the communication cycles, is presented. Fig. 16 shows the graphs of the tests evolution.

The difference jitter is obtained by subtracting the best-case (minimum) transmission time from the worst-case (maximum)

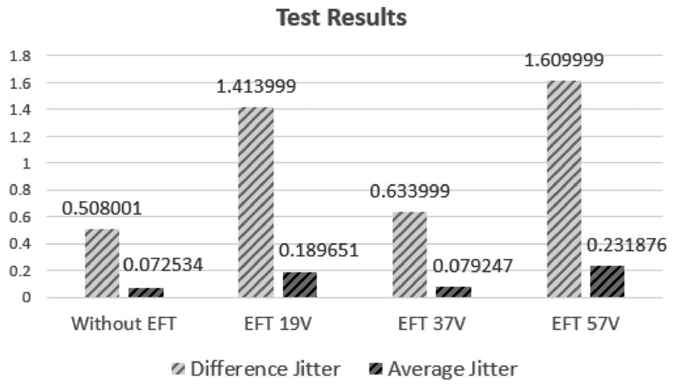


Fig. 16. Graph of jitter in the communication tests.

transmission time from the measurements in the sample set. The average jitter is represented by the standard deviation in the measure of average message transmission time.

After defining the time constraints and performing several tests, it was verified that the delays are significant and can affect the reliability of the communication protocol. Results demonstrated an increase in average jitter of 161% with 19 Vp, 9.25% with 37 Vp, and 219% with 57 Vp. These results may fluctuate somewhat because during the tests, the EFT burst can coincide more or less times with specific control cycles. However, this fact does not affect the conclusions, because these results demonstrated the EFT fault susceptibility of the CAN protocol. These numbers are significant to consider degradation in the communication reliability. Moreover, it is important to highlight that the tests were performed with low-bandwidth usage and with a periodic EFT injection, which suggests an even worst scenario with high-bandwidth usage.

It is important to highlight that this study focuses on impact analysis of EFT fault on network jitter. The results presented show a significant increase in the jitter in several communication cycles of active suspension control law. Thus, critical tasks are affected by EFTs, which may take part of requirements in the embedded system design.

VI. Conclusion

This paper detailed a test method demonstrating that transient faults can affect the communication process of CAN networks. Recent studies are focused on measuring and testing the EFT susceptibility of CAN transceivers, but tests focusing these effects on specific communication processes should be investigated. The experiments performed in this study make possible to assess that the proposed fault injection method worked properly being possible to observe an increase and more variation in jitter between several communication cycles.

The experiment was performed in an Active Suspension system with a quarter-car model control implemented on the Vector CANoe platform. The control law represents a specific safety critical control situation with predefined time constraints. For this task, messages transmit the control law information cyclically having a period of 5 ms. This time interval is a constraint for the control system, since longer periods may bring the system to an unstable condition and this constraint was analyzed after the EFT injection.

Regarding the communication performance, it was verified that the delays are significant and can affect the reliability of the communication protocol. Results demonstrated that the EFT faults can seriously degrade the communication reliability.

Future works drive to the direction of applying the method to other types of communication protocols and conducting tests with higher bandwidth usage.

References

[1] S. C. Talbot and S. R. S. Ren, "Comparision of fieldbus systems CAN, TTCAN, flexray and LIN in passenger vehicles," in *Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Work.*, 2009 pp. 26–31.

[2] S. Tuohy *et al.*, "Intra-vehicle networks: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 534–545, Apr. 2015.

[3] B. Galloway, G. P. Hancke, and S. Member, "Introduction to industrial control networks," *IEEE Commun. Surveys Tut.*, vol. 15, no. 2, pp. 860–880, 2nd Quarter 2013.

[4] C. E. Pereira and P. Neumann, "Industrial communication protocols," in *Springer Handbook of Automation*. Berlin, Germany: Springer, 2009, pp. 981–999.

[5] I. S. IEC 61000, Electromagnetic compatibility (EMC) - Part 4-4: Testing and Measurement Techniques—Electrical Fast Transient/Burst Immunity Test, 2004.

[6] J. Zhang *et al.*, "Modeling injection of electrical fast transients into power and IO pins of ICs," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 6, pp. 1576–1584, Dec. 2014.

[7] D. Gies, "Transients and surge protection considerations in electrical equipment – offense and defense," in *Proc. IEEE Symp. Product Compliance Eng.*, 2013, pp. 1–6.

[8] B. J. A. M. Van Leersum, F. J. K. Buesink, J. G. Bergsma, and F. B. J. Leferink, "Ethernet susceptibility to electric fast transients," in *Proc. Int. Symp. Electromagn. Compat.*, 2013, pp. 29–33.

[9] S. Bauer, B. Deutschmann, and G. Winkler, "Prediction of the robustness of integrated circuits against EFT / BURST," in *Proc. IEEE Int. Symp. Electromagn. Compat.* , 2015, pp. 45–49.

[10] C. Ursachi and E. Helerea, "Immunity to electrical fast transient pulses of computer systems," in *Proc. IEEE Int. Conf. Appl. Theor. Elect.*, 2014, pp. 14–17.

[11] A. S. Roque, D. Pohren, C. E. Pereira, and E. P. Freitas, "Communication analysis in CAN networks under EFT injection," in *Proc. IEEE Int. Conf. Automatica, XXII Congr. Chilean Assoc. Automat. Control*, 2016, vol. 22 pp. 1–6.

[12] T. Piper, S. Winter, O. Schwahn, S. Bidarahalli, and N. Suri, "Mitigating timing error propagation in mixed-criticality automotive systems," in *Proc. IEEE 18th Int. Symp. Real-Time Distrib. Comput.*, 2015, pp. 102–109.

[13] L. Marques, V. Vasconcelos, P. Pedreiras, and L. Almeida, "Tolerating transient communication faults with online traffic scheduling," in *Proc. IEEE Int. Conf. Ind. Technol.*, 2012, pp. 396–402.

[14] L. Marques, V. Vasconcelos, P. Pedreiras, and L. Almeida, "Comparing scheduling policies for a message transient error recovery server in a time-triggered setting," in *Proc. 19th IEEE Int. Conf. Emerging Technol. Factory Autom.*, 2014, pp. 1–6.

[15] B. Pattanaik and S. Chandrasekaran, "Recovery and reliability prediction in fault tolerant automotive embedded system," in *Proc. Int. Conf. Emerging Trends Elect. Eng. Energy Manage.*, 2012, pp. 257–262.

[16] L. Marques, V. Vascóncelos, P. Pedreiras, V. Silva, and L. Almeida, "Efficient transient error recovery in FlexRay using the dynamic segment," in *Proc. 19th IEEE Int. Conf. Emerging Technol. Factory Autom.*, 2014, pp. 1–4.

[17] M. Fontana and T. H. Hubing, "Characterization of CAN network susceptibility to EFT transient noise," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 2, pp. 188–194, Apr. 2015.

[18] IEC/TS-62228, EMC Evaluation of CAN Transceivers. 2007.

[19] E. Pannila and M. Edirisinghe, "Power system switching transients in passenger automobiles," in *Proc. 7th Int. Conf. Inf. Autom. Sustain.*, 2014, pp. 1–6.

[20] S. Huang, C. Zhou, L. Yang, Y. Qin, and X. Huang, "Transient fault tolerant control for vehicle brake-by-wire systems," *Rel. Eng. Syst. Safety*, vol. 149, pp. 148–163, 2016.

[21] T. J. Michelin, "Análise do impacto da comunicação via rede flexray em sistemas de controle," dissertation, Programa de Pós-Graduação em Engenharia Elétrica, Escola de Engenharia, Federal Univ. Rio Grande do Sul, Porto Algere, Brazil, 2014.

[22] A. Albert, "Comparison of event-triggered and time-triggered concepts with regard to distributed control systems," in *Proc. Embedded World*, 2004, pp. 235–252.

Alexandre S. Roque received the B.Sc. degree in computer science from Regional Integrated University in 2005 and the M.Sc. degree in production engineering with emphasis in automation and control systems from Federal University of Santa Maria, Santa Maria, Brazil, in 2010. He is currently working toward the Ph.D. degree in electrical engineering at Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, Brazil.

He is a Member of Research Group in Control, Automation and Robotics – GCAR, UFRGS. His research area is focused on embedded systems, digital systems, and industrial communication protocols.

Daniel Pohren received the B.Sc. degree in electrical engineering from Lutheran University of Brazil in 2014. He is currently working toward the Master's degree in Electrical Engineering at Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, Brazil.

He is a Member of Research Group in Control, Automation and Robotics – GCAR. His research area includes automation, communication protocols, and embedded systems.

Thiago J. Michelin received the B.Sc. degree in electrical engineering from UNESP, São Paulo, Brazil, in 2009, and the M.Sc. degree in electrical engineering in 2014 from Federal University of Rio Grande do Sul, Porto Alegre, Brazil, where he is currently working toward the Ph.D. degree in electrical engineering.

He is a Member of the Control, Automation and Robotics Research Group – GCAR.

Carlos Eduardo Pereira received the Dr-Ing degree in electrical engineering from the University of Stuttgart, Germany in 1995 and the B.S. degree in electrical engineering and the M.Sc. degree in computer science both from Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil.

He is a Full Professor at UFRGS and the Director of Operations at EMBRAPII, Asa Norte, Brazil. He has more than 400 technical publications on conferences and journals. He is an Associate Editor of the Journal *Control Engineering Practice* and *Annual Reviews in Control* from Elsevier and Council Member of IFAC.

Dr. Pereira received in 2012 the Friedrich Wilhelm Bessel Research Award from the Alexander von Humboldt Foundation - Germany.

Edison Pignaton Freitas received the Bachelor's degree in computer engineering from Military Institute of Engineering, Rio de Janeiro, Brazil, 2003, the M.Sc. degree in computer science from Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil, in 2007, and the Ph.D. degree in computer science and engineering from Halmstad University, Halmstad, Sweden, 2011, in the area of wireless sensor networks.

He is currently an Associate Professor at UFRGS, affiliated with the Graduate Programs in Electrical Engineering and Computer Science, acting as a Member of Research Group in Control, Automation and Robotics – GCAR, working in several research areas such as industry automation, computer networks, and real-time systems.

ApêndiceD

D.1 Publicação IEEE - 2016 International Conference on Automatica (ICA-ACCA) - Curicó/Chile

Communication Analysis in CAN Networks under EFT Injection

Alexandre S. Roque, *Member, IEEE*, Daniel Pohren, *Member, IEEE,* Carlos E. Pereira, *Member IEEE,*
Edison P. Freitas*, Member IEEE*

Abstract— **This paper describes a study about the impact of electrical fast transients (EFT) on performance of communication protocols. A method of fast transient injection is applied in an experimental CAN network with the objective of verifying an impact on jitter and how it influences the communication process. An experiment was conducted in laboratory with a model of typical CAN network configuration with three nodes to verify the time delays. As result, was verified that EFT increases peak delay between data control cycles and can effectively influence and generated faults in communication process.**

***Index Terms*— Electrical fast transient; CAN protocol; safety-critical systems.**

I. Introduction

Recent advances in embedded systems and industrial network protocols have led to many innovations in automotive environment. In-vehicle electronic systems are rapidly advancing in complexity and diversity. A variety of sensors and processors are used in different parts of the vehicle for various functions. For example, antilock braking system (ABS), traction control, active suspension and others systems that monitor a vehicle performance and safety. It is possible to consider other technologies as camera, radar, and ultrasonic sensors that have been used to sense the environment around the vehicle and provide information so that in the future vehicles become more intelligent and autonomous.

Intra-vehicular networks apply communication protocols that are responsible for interconnecting several electronic control units - ECUs via a BUS and according to specific topology. Some safety-critical tasks communicate over the network and must timely execute actions.

Some protocols adopted in intra-vehicular networks are developed or modified in order to increase reliability in communication processes. In addition, some extensions to the CAN protocol were developed, such as TT-CAN (Time-triggered CAN) and FTT-CAN (Flexible Time-triggered CAN), and another communication protocol conceived for the automotive sector which includes fault-tolerant concepts, i.e. the FlexRay protocol (FlexRay Consortium) [1] [2].

Communication protocols compose networks where each node include transceivers, the interface between the bus and the digital processors, that implements physical layer specifications and allow communication between different critical functions [3]. Communication protocols can be affected by several sources of electromagnetic interference that can couple transient energy to circuits through data cables and cause different types of disturbances on ECUs.

These fault situations can be generated by electrostatic discharge (ESD) or man-made, such as power switching transients, defined as electrical fast transients (EFTs) [4]. An electrical transient is the outward manifestation of a sudden change in circuit conditions and usually also are very small and unpredictable [5] [6]. Represented by either a single pulse or a burst of spikes, EFTs may disrupt differential signaling causing transmission failures. According to [7] the electromagnetic disturbances as low energy electrical fast transients pulse trains generated by switching phenomena in low and medium voltage networks are a present and an ongoing challenge for electrical and electronic equipment.

These factors make them very hard to measure and constitute potential sources of critical faults. Therefore, very accurate measures to understand these events and their periodicity is essential for reliability of the communication process. Experiments can be performed together with measuring techniques aiming at detecting and registering transients, in order to after understand and analyzing them, sometimes manage to provide solutions to mitigate the problem.

In order to correlate transient faults with performance losses in critical real-time tasks, this paper proposes a method of analysis with experimentation in order to analyze the impact of electrical fast transients not only in their transceivers, but also the error propagation in intra-vehicular networks. Thus, this study provides an experimental analysis for in future works to include types of transient failures in the modeling phases of control systems, allowing the system survival in critical situations.

This paper is organized as follows: Section II explores related works with emphasis in the gap related to EFT impact analysis;

A. S. Roque, PhD Student in Electrical Engineering, Federal University of Rio Grande do Sul, UFRGS, RS, Brazil (e-mail: as.roque@ufrgs.br).

D. Pohren, MSc Student in Electrical Engineering, Federal University of Rio Grande do Sul,, UFRGS, RS, Brazil (e-mail: daniel.pohren@ufrgs.br).

C. E. Pereira, Full Professor, Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, RS, Brazil (e-mail: cpereira@ece.ufrgs.br).

E. P. Freitas, Associate Professor, Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, RS, Brazil (e-mail: edison.pignaton@ufrgs.br).

9781509011476/16/$31.00©2016IEEE

Section III presents the proposed method for EFT impact analysis with an overview about the network configuration and the EFT injection; Section IV describes the performed case study to validate the method. Section V presents the test results and the impact analysis on the performance of critical tasks defined in the case study; Section 6 presents the conclusions and future work directions.

II. Related Works

Recent works have highlighted the importance of mechanisms that reduces the impact of transient faults in embedded systems. Intra-vehicular networks use specific protocols which can be affect by transient faults.

In [8] a new approach of task monitoring is discussed. It aims at protecting critical tasks of interference with temporal performance guarantees. The work is based on the ISO 26262 standard (Road Vehicles), standard risk-based. The proposal seeks to highlight the differences compared to existing tools, such as the use of AUTOSAR (Automotive Open System Architecture), which also allows this monitoring, but do not consider monitoring less critical tasks that can propagate errors.

The time guarantee is performed by means of pre-emptive monitoring of critical tasks (according to preemption budget). It is important to consider that the tasks' communication may occur by means of different network protocols, thus critical tasks and time constraints can be handled according to each protocol. The work presented in [9] uses FTT-CAN (Flexible time-triggered communication on CAN) protocol and it proposes an online traffic scheduling approach in which retransmissions are scheduled with the remaining time-triggered traffic. Fault detectors are added in FTT-CAN protocol to monitor bus activity and to retransmit omitted messages, with the only focus on temporal redundancy, aiming to handle communication errors in time-triggered systems.

Likewise, the work proposes in [10] presents a model for recovery and reliability prediction (R&R) in automotive embedded systems based on CAN protocol. The model focuses on interaction of different software modules that are responsible for critical tasks. Calculations define the probability of failure according to the record of specific events. Several fault sources are indexed and analyzed with a prediction algorithm. The mechanism is evaluated by verifying the periodic activation of different redundancy modules.

Automotive networks use different communication protocols. Among them, FlexRay is a protocol that can be affected by permanent or transient faults. The work presented in [11], proposed a mechanism which uses temporal redundancy to recover transient errors in time-triggered messages of FlexRay protocol. This mechanism uses dynamic segment of FlexRay frame to implement retransmissions messages. This method significantly reduces the use of the channel bandwidth and provides faster recovery of a set of faults.

These previous works are related to different mechanisms and time-triggered message scheduling in communication protocols, with the main objective of mitigating faults. However, the relationship between some type of faults and their impact in time constraints of critical tasks and how impacts on system performance are not considered.

Nevertheless, others works focus on specific types of faults, for example, in [12] the susceptibility of CAN protocol to fast electrical transients (EFT) is handled, specifically in signals of transceiver ports. The EFT impact is verified according to IEC 62228 with possibilities of rejections and failures in CAN signals. An experiment is realized to verify the EFT susceptibility and a mechanism for immunizing transceivers is proposed. However, the impact in protocol time constraints and performance are not investigated. This mechanism uses a fault injection method that is used in the present work to generates a transient pulse in order to verify the impact in protocol performance.

In recent work present in [13] an extensive survey of transient faults is carried out at a constant location within the automobile electrical system. The measured transient parameters were compared to the sensitivity of several standard car electronic devices to identify their immunity to the conducted transients. A brief statistic of measured transients over three main operations (Ignition, AC, Headlight) is presented with a time range duration and amplitude peak in volts. Despite the value of these data, they are not related to the protocol performance (jitter, lost packets) and their impact in time constraints of critical tasks.

Thus, the present work contributes combining and extending the approach presented in [13] to verify by other perspective the impact in communication performance of CAN protocol.

Based on these researches, the next section presents an experimentation method to verify EFT effects in communication performance.

III. Proposal Method for EFT Analysis

In order to investigate the immunity of industrial communication protocols of electrical fast transients – EFT, network disturbances are generated and were evaluated according to the IEC/TS 62228 test method [15]. According [12], this test standard is a standardized common scale for EMC evaluation of transceivers, where EFT disturbances are capacitive coupled to the ports and the susceptibility is characterized in terms of the voltage amplitude of the EFT causing a failure. Fig. 1 illustrates an overview of test method.

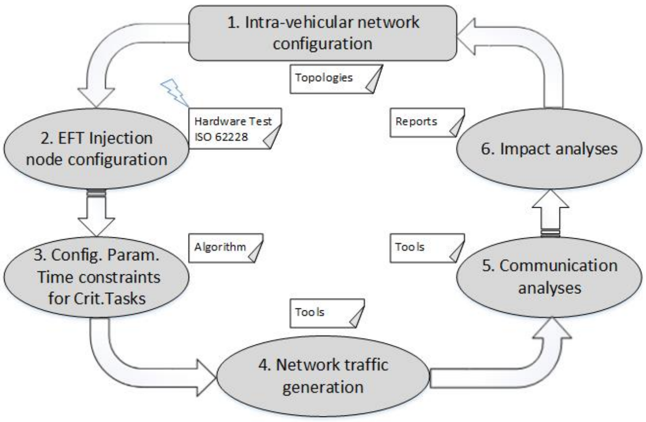

1. Intra-vehicular network configuration
Topologies
Hardware Test ISO 62228
Reports
2. EFT Injection node configuration
6. Impact analyses
Algorithm
Tools
3. Config. Param. Time constraints for Crit.Tasks
5. Communication analyses
Tools
4. Network traffic generation

Fig. 1. Overview of test method applied.

The method must be cyclically performed in order to change some parameters and to perform refinements that are necessary to increase the precision and the reliability in data measurements. This method is applied following six steps, as described in the following. In Step 1 the network topology is configured as well as the method of node interconnection for the experiment in order to characterize control critical situations. Step 2 implements a hardware model for EFT injection based on ISO 62228 test standard. In this case a function generator can be used to inject transients in different amplitudes. Fig. 2 illustrates this interconnection topology and how the EFT injection is inserted.

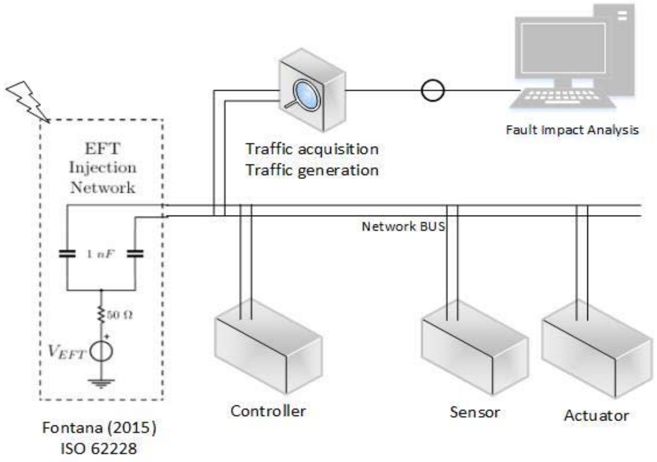


Fig. 2. Overview of EFT Injection method applied.

In step 3, several parameters related to time constraints of some types of critical tasks that uses communication protocols are configured (for example, brake and traction control system), and three nodes are specified as sensor, controller and actuator, with their function programed in an embedded algorithm. After the network and hardware configuration, step 4 defines a tool for traffic acquisition and traffic generation to increase network bandwidth usage. Step 5 defines the usage of another tool to analyze communication and to detect disturbances. Finally, in step 6 reports about the EFT impact on critical tasks defined in step 1 are generated. This feedback must be used to reconfigure the parameters related to time constraints and verified hardware requirements for fault tolerance. Next, Section IV presents the details of a case of study and the performed experiments to validate this method.

IV. EFT Impact Analysis on CAN Protocol

A. Description of the test procedure

The test method was applied following the six steps presented in Fig. 1, with specific configuration and specific tools. The network configured is based on CAN protocol and simulate similar conditions related to a typical part of communication between nodes in a network. The case study aim at only verifying the influences of EFT and registering logs of the communication process. In future other tests with specific time constraints in other scenarios will be performed.

The tools and settings used in each step are listed in the following:

- Step 1: Network based on CAN protocol;
- Step 2: EFT injection method based on ISO 62228 and test used in [12];
- Step 3: Time constraints for active suspension control;
- Step 4: Traffic generation Microchip CAN BUS Tool;
- Step 5: Communication analysis with Microchip CAN Analyzer;
- Step 6: Graphical results and impact analysis in communication performance;

B. CAN Node Configuration

In order to investigate the immunity of CAN Network under EFT injection method, a scenario with three CAN Nodes are configured following the method illustrated on Fig. 2. Each CAN node has been programmed with specific functions. Node 1 operated as a transmitter (sensor) sending data every 25 ms. Node 2 operated as receiver event triggered (controller) sending control data after packet received. Node 3 operated as a receiver (actuator) performing a control plant action and sending an ACK packet to controller node. The Fig. 3 illustrates the implemented control algorithm.

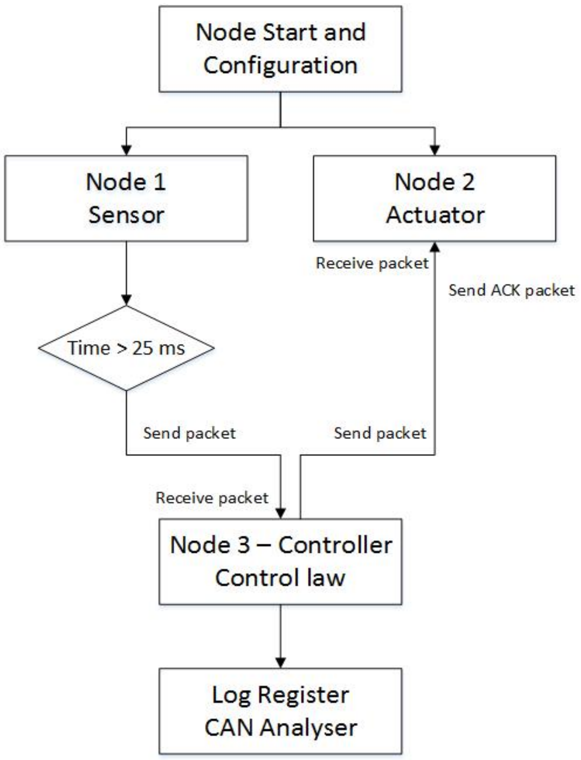


Fig. 3. Control Algorithm applied for Tests.

This test focuses on a network with low traffic to register the impact of transient faults in delay between specific communications (jitter). This test is important to analyze the susceptibility of CAN network and if these faults can affect some type of control. Fig. 4 presents the hardware used in tests.

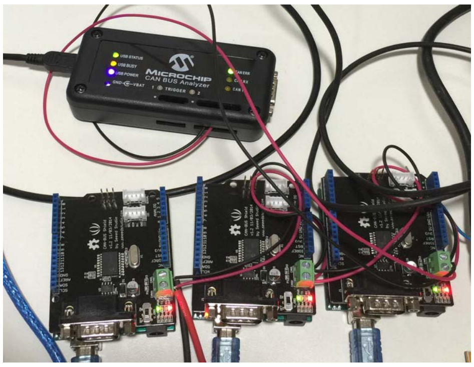


Fig. 4. Three CAN node network configuration.

For the objective of bus network monitoring a sequence of communication tests among the three nodes were performed. After the network configuration a specific circuit for EFT injection was designed.

C. *EFT Injection*

Electrical Fast Transients consist in bursts with variable amplitudes generated in CAN networks by different noise sources (Ignition, Headlight, Air conditioner). In order to verify if disturbances were generated, this test is performed according to the IEC 62228. For the EFT injection, a specific circuit has been designed which is presented in Fig. 5.

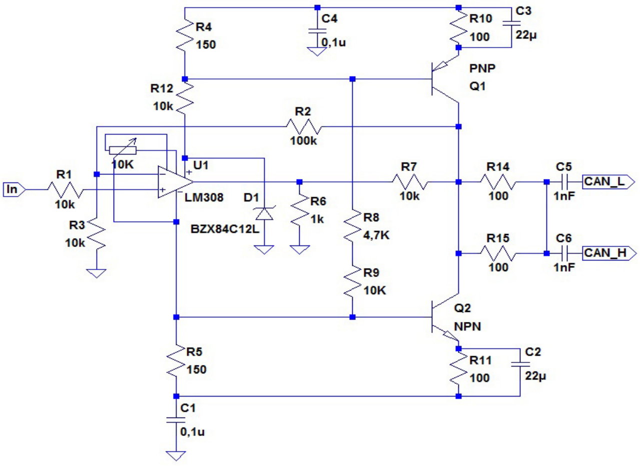


Fig. 5. EFT Injection Circuit

The circuit for EFT injection consist in a booster voltage amplifier using an operational amplifier model TL071, supplied with -15 and 60 volts dc. The strategy to allow the amp op run with this big range of voltage is the usage of a voltage divider by ten at output, together with a non inverter configuration and gain 10. To guarantee that the voltage will be at the correct value, a zener diode was used to fix this value at 12Volts dc at the positive terminal on amp op. This allows this system to use a input signal from 1,5 Vpeak and gives the output until 55Vpeak. The original signal came from an arbitrary wave generator configured to supply peaks with duration from 15us until 2ms and delay about 5 to 10 ms. Fig. 6 illustrate the EFT Injection method.

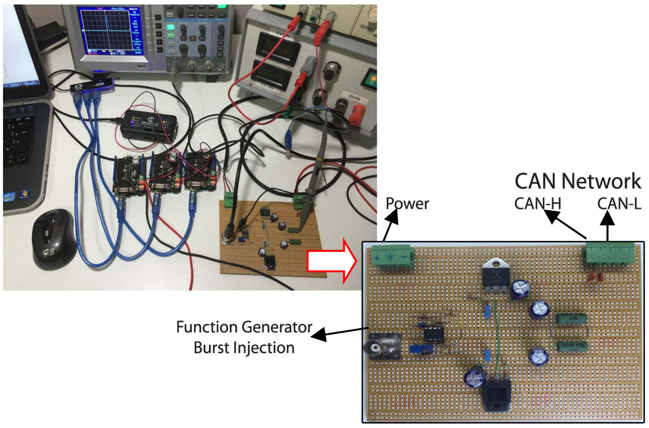


Fig. 6. EFT Injection on Can Network

To determine the immunity of communication against EFT noise, disturbances were injected into the network with amplitudes starting from 19V, 37V and 57V and registering logs of communication for analysis.

D. *Traffic generation and logging*

The applied test method requires that the communication process between nodes be registered. For this task there are several tools that can be used, but as this test has reduced complexity and focuses on fault injection method, a low-cost tool was used. The monitoring tool CAN Bus Analyzer, from Microchip, was used to register (logging) de communication process between nodes. Fig. 7 shows the CAN Bus tool.

Fig. 7. Microchio CAN Bus Tool.

This tool supports CAN 2.0b and ISO 11898-2 (high-speed CAN with transmission rates of up to 1 Mbit/s). The tool is connected to CAN network through a screw terminal interface.

V. Results

According to previous specification a sequence of EFT injection with burst of 198, 688 microseconds and 1,2 milliseconds was performed. A respective sequence of EFT injection with amplitudes of 19, 37 and 57 volts were generated using an arbitrary wave generator. The results of this sequence tests are presented in the following.

For the purpose of verification of function generation interconnection with EFT circuit, a prior measurement of generated pulses is performed. Fig. 8 presents one of these pulses generated with 37 volts of amplitude.

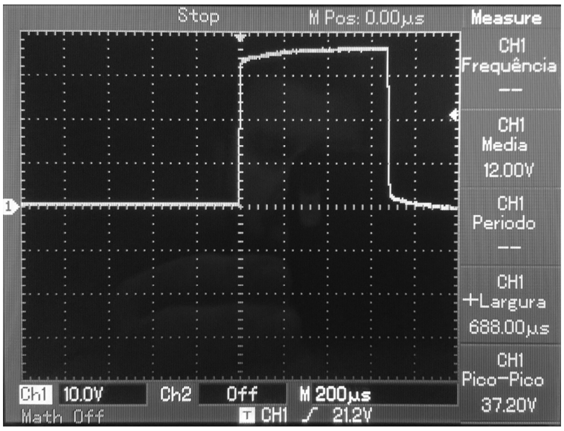


Fig. 8. EFT wave form with 37 Vp.

After checking the generated EFT signals, a sequence of communication tests based on 5 milliseconds of burst period was performed. For comparison purposes, before performing the test sequence, a network communication measurement was performed without EFT pulses. The sampling interval and logs record is about 1000 control cycles. Fig. 9 presents the performance graph without EFT injection.

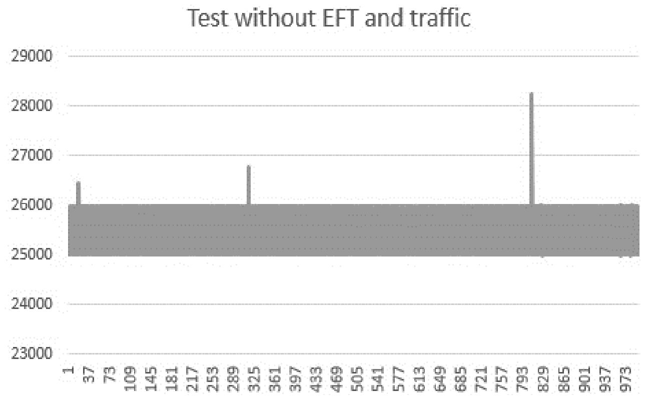


Fig. 9. Performance graph generated without EFT Injection.

According to the graph of Fig. 9 for the period measured jitter ranges below 25 milliseconds with few spikes above this value. The next three graphs at Fig. 10, 11 and 12 shows the performance of the communication process with 19 volts of EFT with 198 microseconds of burst duration.

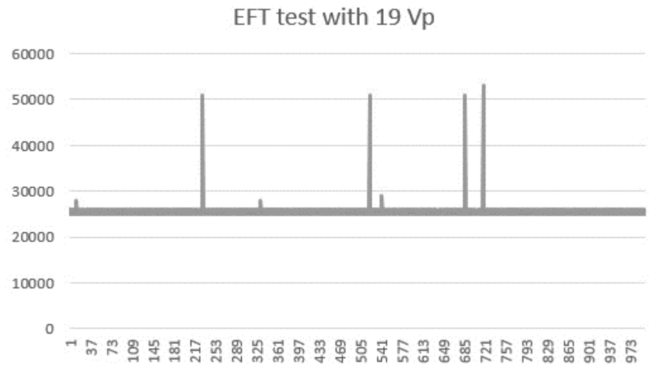


Fig. 10. Performance graph generated with 19V of EFT.

Fig. 10 shows that the impact on the bus to communicate with 19 volts of EFT injection is not significant, but it is possible to verify the increase of delay peaks cycle communication process. Fig. 11 presents the performance of communication process with 37 volts of EFT with 688 microseconds of burst duration.

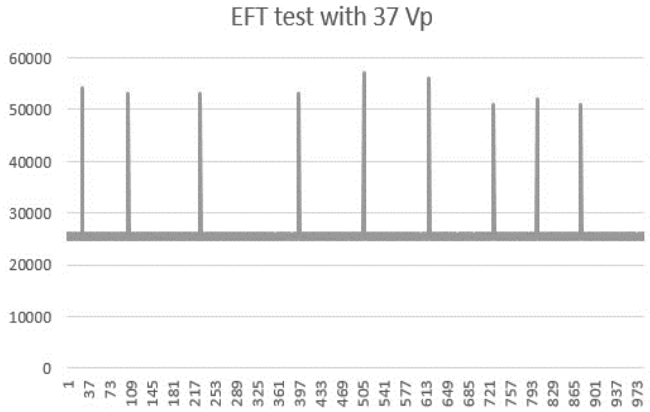


Fig. 11. Performance graph generated with 37V of EFT.

It can be observed in Fig. 11 that several communication cycles are affected by EFT injection and that the delay was increased. Fig. 12 presents the performance of communication process with 57 volts of EFT with 1200 microseconds of burst duration.

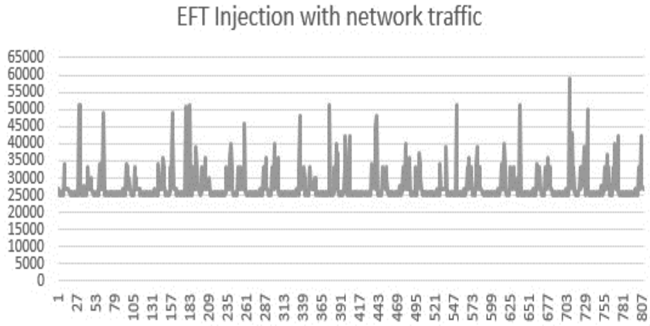


Fig. 11. Performance graph generated with 57Vp of EFT.

In communications tests with EFT injection of 57 volts it is possible to observe an increase in communication delays in a greater number of data communication cycles. Table 2 presents a summary of the difference jitter and the average jitter of communication tests performed.

TABLE 1 – TESTS SUMMARY.

	Difference Jitter	*Average Jitter*
Test without EFT	484.57 us	446.14 us
EFT injection 19 Vp – 188us	1714.34 us	543.24 us
EFT injection 37 Vp – 688us	2685.61 us	683.61 us
EFT injection 57 Vp – 1200us	5010.56 us	1429.62 us

The presented data show that there is a significant increase in generated delay in several communication cycles. It is important to highlight that these results are related to low CAN network bandwidth usage.

VI. Conclusions

The test method presented in this paper demonstrate that transient faults can affect the communication process of CAN networks. Recent studies are focused on measuring and testing of CAN transceivers EFT susceptibility, but testing with a focus on the effects that can have on specific communication processes should be investigated. According to the experiment performed in this work the fault injection method worked properly and it was possible to observe a slight increase in peak delays between several communication cycles. Regarding the communication process performance, these delays are significant and can decrease communication protocol reliability. In addition, more tests with greater variability of fault injection and greater use of CAN network bandwidth will be performed as future work.

References

[1] S. C. Talbot and S. R. S. Ren, "Comparision of FieldBus Systems CAN, TTCAN, FlexRay and LIN in Passenger Vehicles," *2009 29th IEEE Int. Conf. Distrib. Comput. Syst. Work.*, 2009.

[2] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-Vehicle Networks: A Review," *Ieee Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 534–545, 2015.

[3] B. Galloway, G. P. Hancke, and S. Member, "Introduction to Industrial Control Networks," vol. 15, no. 2, pp. 860–880, 2013.

[4] I. IEC International Standard, *EMC: Testing and MeasurementTechniques— Electrical Fast Transient/Burst Immunity Test*. 2004.

[5] D. Gies, "Transients and Surge Protection Considerations in Electrical Equipment – Offense and Defense," in *IEEE Symposium on Product Compliance Engineering (ISPCE)*, 2013, pp. 1 – 6.

[6] B. J. A. M. Van Leersum, F. J. K. Buesink, J. G. Bergsma, and F. B. J. Leferink, "Ethernet Susceptibility to Electric Fast Transients," in *Proc. of International Symposium on Electromagnetic Compatibility (EMC Europe)*, 2013, pp. 29–33.

[7] C. Ursachi and E. Helerea, "Immunity to Electrical Fast Transient Pulses of Computer Systems," in *IEEE International Conference on Applied and Theoretical Electricity (ICATE)*, 2014, pp. 14–17.

[8] T. Piper, S. Winter, O. Schwahn, S. Bidarahalli, and N. Suri, "Mitigating Timing Error Propagation in Mixed-Criticality Automotive Systems," in *IEEE 18th International Symposium on Real-Time Distributed Computing - ISORC*, 2015, pp. 102–109.

[9] L. Marques, V. Vasconcelos, P. Pedreiras, and L. Almeida, "Tolerating transient communication faults with online traffic scheduling," in *IEEE International Conference on Industrial Technology, ICIT*, 2012, pp. 396–402.

[10] B. Pattanaik and S. Chandrasekaran, "Recovery and reliability prediction in fault tolerant automotive embedded system," in *International Conference on Emerging Trends in Electrical Engineering and Energy Management - ICETEEEM*, 2012, pp. 257–262.

[11] L. Marques, V. Vascóncelos, P. Pedreiras, V. Silva, and L. Almeida, "Efficient transient error recovery in FlexRay using the dynamic segment," in *19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, 2014, pp. 1–4.

[12] M. Fontana and T. H. Hubing, "Characterization of CAN network susceptibility to EFT transient noise," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 2, pp. 188–194, 2015.

[13] E. Pannila and M. Edirisinghe, "Power System Switching Transients in Passenger Automobiles," in *7th International Conference on Information and Automation for Sustainability (ICIAfS)*, 2014, pp. 1–6.

[14] IEC/TS-62228, *EMC Evaluation of CAN Transceivers*. 2007.

Alexandre S. Roque received a BSc degree in Computer Science and Master in Automation and Control Systems. Currently is PhD student in Electrical Engineering at Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, Brazil. Member of Research Group in Control, Automation and Robotics – GCAR, UFRGS. Research area focused on embedded systems, digital systems and industrial communication protocols.

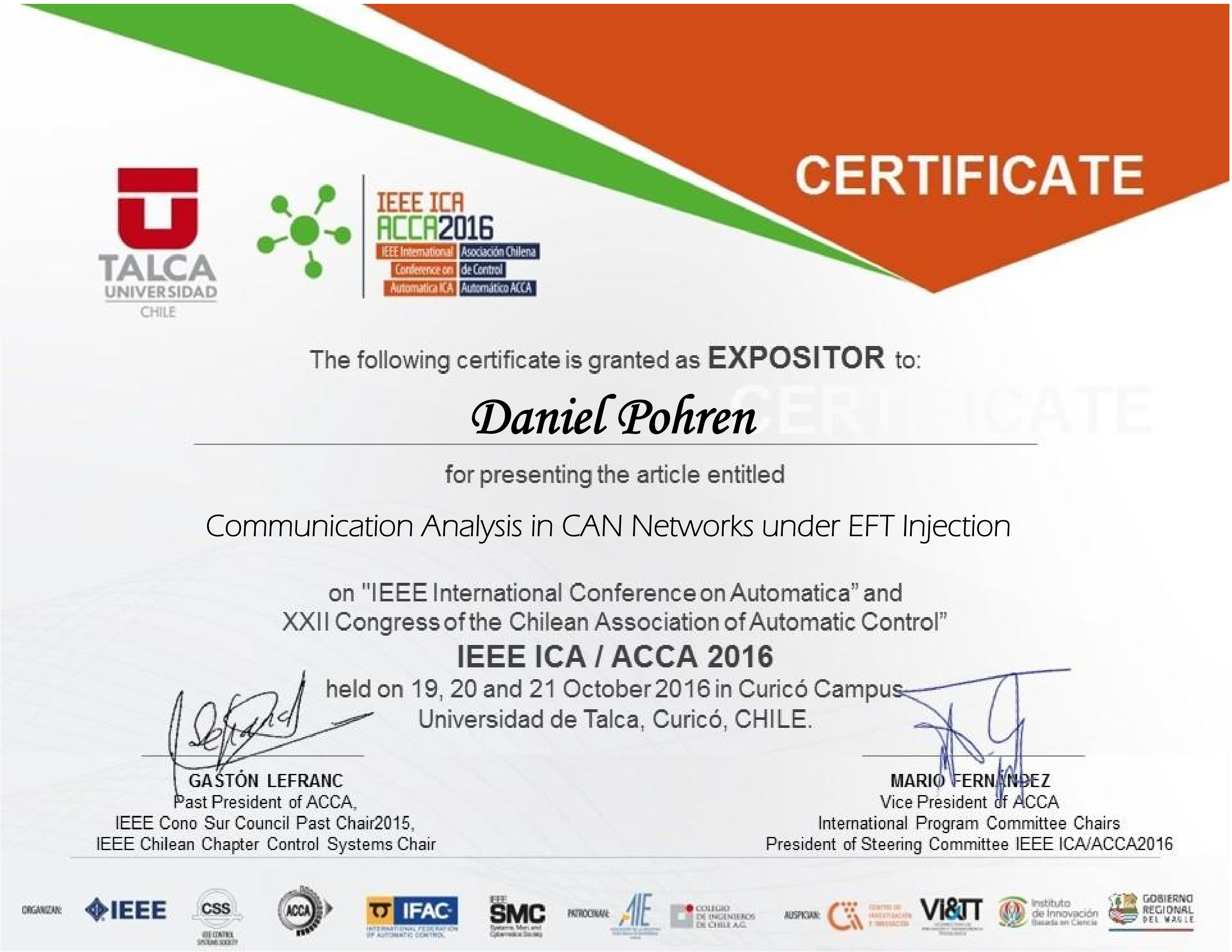
Daniel Pohren received a BSc degree in Electrical Engineering from Lutheran University of Brazil (2014). Currently is Master student in Electrical Engineering at Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, Brazil. Member of Research Group in Control, Automation and Robotics – GCAR, UFRGS. Research area focused on automation and control, communication protocols and embedded systems.

Dr. Carlos Eduardo Pereira received a BSc degree in Electric Engineering from Escola de Engenharia (1987), Brazil, and an MSc degree in Computer Science from UFRGS in 1990. He received a PhD degree in Electrical Engineering from Technische Universitat Stuttgart, Germany, in 1995. He is a professor in the Department of Electrical Engineering and Science Computing at UFRGS and since 2009 he is the Deputy Director of the Engineering of UFRGS. He is a senior member of the IEEE and IFAC Technical Committee on Real-Time Programming.

Dr. Edison Pignaton Freitas has a PhD in Computer Science and Engineering by Halmstad University in Sweden, 2011, in the area of wireless sensor networks, MSc in Computer Science by Federal University of Rio Grande do Sul (UFRGS), Brazil, in 2007 and Bachelor degree in Computer Engineering by Military Institute of Engineering, Brazil, 2003. Currently he holds an associate professor position at UFRGS, affiliated to the Graduate Programs in Electrical Engineering and Computer Science, acting as a member of Research Group in Control, Automation and Robotics – GCAR, working in several research areas such as Industry Automation, Computer Networks and RT Systems.

ApêndiceE

E.1 Apresentação - International Conference on Automatica (ICA-ACCA) - Curicó/Chile - 2016



CERTIFICATE

TALCA UNIVERSIDAD CHILE

IEEE ICA ACCA2016
IEEE International Conference on Automatica ICA
Asociación Chilena de Control Automático ACCA

The following certificate is granted as **EXPOSITOR** to:

Daniel Pohren

for presenting the article entitled

Communication Analysis in CAN Networks under EFT Injection

on "IEEE International Conference on Automatica" and
XXII Congress of the Chilean Association of Automatic Control"

IEEE ICA / ACCA 2016

held on 19, 20 and 21 October 2016 in Curicó Campus
Universidad de Talca, Curicó, CHILE.

GASTÓN LEFRANC
Past President of ACCA,
IEEE Cono Sur Council Past Chair2015,
IEEE Chilean Chapter Control Systems Chair

MARIO FERNÁNDEZ
Vice President of ACCA
International Program Committee Chairs
President of Steering Committee IEEE ICA/ACCA2016

ORGANIZAN: IEEE CSS ACCA IFAC SMC PATROCINAN: AIE COLEGIO DE INGENIEROS DE CHILE A.G. AUSPICIAN: VI&TT Instituto de Innovación Basada en Ciencia GOBIERNO REGIONAL DEL MAULE

ApêndiceF

F.1 Submissão - Transactions on Electromagnetic Compatibility - 2019

Impact Analysis of Electrical Fast Transients on FlexRay protocol according to IEC 62228

***Abstract*—Distributed vehicular control systems are responsible for safety-critical applications, depending on communication protocols. In this context, the FlexRay protocol is frequently applied for ECU interconnection in critical applications. Thus, it must be tested in different fault scenarios to verify if the protocol could comply with hard timing constraints. Typical faults that have been studied are Electrical Fast Transients (EFT), in which power switching systems can generate transients that degrade in-vehicle communication. Recent efforts focus on the specification of test methods for electromagnetic compatibility in communication transceivers, but without considering the negative impact on critical control system messages and its periodicity. This work presents a contribution by exploring the IEC 62228 standard to guide the application of a test method with a specific test board to evaluate the impact of these faults on the control law performance of critical automotive control systems based on FlexRay protocol. The results show that during the test scenarios using the fault injection method, the transients cause performance degradation peaks between 2.9 and 94.5 microseconds, much higher compared to a typical FlexRay delay. The results emphasize that critical control systems must be stressed with consistent tests to map fault behaviors, observing the operation limit under faults.**

***Index Terms*—Automotive EMC, Jitter/noise modeling and analysis, IEC 62228, Electrical Fast Transients.**

I. Introduction

IN-VEHICLE communication protocols are responsible for interconnecting electronic control units - ECUs. Typically, most modern cars count with over 80 ECUs distributed according to a specific topology. Safety-critical control systems communicate through messages in this network and must perform their actions on time, complying with hard timing constraints. Besides, each node in a vehicular network includes one or more transceivers which represent the interface between the physical medium and the host node's processing unit. They are also responsible for implementing the physical layer specifications [1] [2].

Due to the increasing complexity of in-vehicle networks, the communication protocol has undergone updates and evolutions creating variations of the original protocol to improve reliability and flexibility. In line with this goal, safety-critical applications apply more robust protocols to perform its functions, and the FlexRay protocol is frequently chosen [3] [4].

According to the main topologies (passive Linear bus, active star, hybrid) and characteristics of the physical medium, the FlexRay protocol allows the use of two redundant transmission channels (channels A and B), in which it is possible to configure and adjust transmission rates. Thus, the protocol allows setting the transmission bit rates, reaching, for example, 10 Mbps with 100 ns of a bit time. Without channel redundancy, up to 20 Mbps can be achieved. The FlexRay protocol implements these features in an enhanced form, also having the flexibility to transmit at predefined time windows event-triggered messages (in the dynamic segment) and time-triggered messages (in the static segment). The main goal of the protocol is to address the current high demands for bandwidth, reliability, and determinism, which are of great importance in automotive X-By-Wire systems [5].

However, in spite of achieving high transmission rates and a good level of reliability, the protocol is not free of faults, and typically the fault handling adds extra costs to the project [6] [7]. Typically, the adopted fault diagnosis strategy is reactive and usually generates an excessive number of retransmissions, therefore, increasing the channel communication rate and replicating communication errors [8] [9] [10].

In this context, the present research emphasizes the study of problems related to performance degradation in the FlexRay protocol. According to recent studies of electrical transients, these faults occur, for example, by Electromagnetic Interference (EMI), radiation, temperature variation, or buck converters [11]. EFT faults affect in-vehicle communication networks in different ways, and even small delays lead to critical faults in control systems [12] [13]. When these faults occur, important messages with hard constraints on periodicity are lost due to bit errors. The correct test and analysis is an important task during test phases of distributed control systems, and to achieve this goal, different standards are applied in the industry to guide conformity tests. The present work focuses on the standard IEC 62228 [14] (and its bases) to develop a test board for EFT susceptibility analysis on FlexRay protocol, considering as case study, the fault impact analysis in periodical messages of an active suspension system.

Based on the developed EFT board, the present work covers gaps related to EFT fault susceptibility in the FlexRay protocol. Thus, experiments are conducted with three EFT injection configurations and in different network busloads. The performance analysis measures the average jitter and the difference jitter as the main metrics, checking the oscillation based on peaks and the average delay in the sample analysis period. The subsequent data analysis is performed with the Vector CANoe software, which allows network monitoring and data analysis during the experiments.

This paper is organized as follows: Section II reviews the literature with relevant related works; Section III presents the applied test methodology; Section IV describes the case study with the developed EFT board, and the control system for analysis; Section V presents the results of the EFT injection in the FlexRay protocol, and Section VI presents conclusions and future perspectives based in this work.

II. Related Works

Problems in protocols used in the automotive industry have been increasingly studied and need constant attention. Recently, researches are focused on identifying and mitigating the damage caused by EFT noise on communication buses. This section discusses works that highlight this problem and also research possibilities.

In [15] a FlexRay communication performance analysis focused on a control system that demands determinism for its tasks is presented. The used case study was an active suspension system based on a "quarter-car" model, which was modelled based on control strategies, to analyze the communication between the sensor, the actuator, and the controller. All the provided information was acquired through simulations, without the use of physical systems, in a controlled environment, and without any external interference, such as transient faults. In the present paper, the same control system is used as a case study, but with EFT fault injection and tested in a real FlexRay network.

The works presented in [16] and [17] report important results about the fault impact of electrical fast transients on both CAN and CAN-FD networks. Experiments show that this type of fault generates deviations in control systems, specifically according to the average delay in control law messages. The average jitter and difference jitter metrics are used to highlight network degradation. However, these works focused only on CAN-based communication, leaving gaps related to FlexRay analysis according to test standards.

The work in [18] presents a prompt retransmission mechanism (PRTM) to recovery from transient errors in safety-critical time-triggered messages in a FlexRay network. The work uses a statistical method of failure probability analysis, and retransmission is determined with a timing analysis. The authors emphasize that with transient faults, bit errors are inevitable in the current twisted wire cables, generating communication errors. Despite the contributions, the work does not consider transient faults specifically in critical messages, and it does not address EFT faults. Another relevant work in this area is [19], which presents a reliability scheduling algorithm (FRSA) to improve the FlexRay communication. The method reduces the probability of transient faults in one clock cycle by using a retransmission mechanism to improve computational complexity using the lookup table method to ensure system reliability. However, the tests do not consider real transient fault injection and lack an analysis of real in-vehicle networks.

In [20] it is presented an analysis based on the FMEDA (Failure Mode Effect and Diagnostic Analysis) using a fault injection and data analysis framework, in compliance with the functional safety standard ISO-26262, for an automotive safety-critical SoC. The work highlights the risks of faults in automotive networks contributing to fault report generation, improving the designer analysis about the hardware weakness. The work and the standard emphasize the risk of faults, demonstrating the importance of tests in design phases. The present paper also contributes in this direction, proposing a method and hardware for transient fault analysis.

The approaches presented in [21] and [22] focuses on the design of secure and dependable automotive cyber-physical systems (CPS), with a case study about a steer-by-wire (SBW) application, in a CAN network. The work emphasizes the vulnerability of recent modern cars related to many fault types (including transient faults), and also malicious attacks that induce faults. The research also discusses the early investigation of faults, and threats to security in automotive applications. These contributions are very important, but the work leaves gaps related to other fault type analysis on FlexRay networks.

The work in [23] presents a study about intermittent connection (IC) fault, a connectivity problem with short duration, occurring in the CAN network causing performance degradation. The work proposes a novel tree-based IC fault diagnosis method to identify the fault locations in the CAN network. Experiments are conducted in a laboratory to demonstrate the feasibility of the approach. Results show that the IC fault locations are diagnosed by the proposed framework. The work emphasizes the future necessity of application in a real and more complex network, extending the analysis. The work does not consider the fault impact in distributed control systems.

Although the reviewed works present important contributions, lacks related to testing methods considering the IEC 62228 and real in-vehicle networks need to be addressed. The EFT fault impact analysis in critical control systems also is an important gap to consider, specifically in the FlexRay protocol. Table I presents a summary of the main aspects of the related works associated with the gap explored in the present paper.

TABLE I: Related Works Summary

Ref.	Main Approach	Gap
[15]	Performance analysis of the FlexRay communication	Tests with simulations, without real network and interference.
[16], [17]	EFT impact analysis on CAN and CAN-FD protocol. Critical control system analysis.	Lack of tests on FlexRay protocol and test standards.
[18]	Retransmission approach in the FlexRay protocol considering transient faults	Tests do not consider EFT and the effect on periodical messages.
[19]	An scheduling algorithm for FlexRay communication using a retransmission mechanism	The work is not evaluated under real tests and transient fault injection method
[20]	A framework for fault analysis based on ISO 26262	Needs an analysis considering the transient fault impact and with IEC 62228
[21], [22]	Design of secure and dependable automotive cyber-physical systems	Analysis focused in CAN networks and security aspects
[23]	Study about intermittent connection IC faults	Lack of fault analysis in FlexRay and control systems
[This Work]	Development of a test board according to ISO 62228. EFT Fault injection in network control systems	(Covered Gap) EFT fault impact analysis in FlexRay protocol. Analysis in critical control systems

Based on these works, it is emphasized the negative impact of transient faults in communication protocols and the lack of fault analysis in FlexRay networks. Thus, this paper contributes with a test method and test board based on IEC 62228, supplying an alternative to handle this issue.

III. Analysis Methodology

Due to recent advances and technologies applied to in-vehicle distributed control systems, the effective test and reliable EMC evaluation of communication transceivers are of great concern. Control systems (traction control, active suspension, obstacle avoidance, X-By-wire systems, and others) are applied to perform critical control tasks, using distributed controllers embedded on ECUs, composing specific network nodes. The determinism of periodic control messages is extremely important for the effective control logic, according to information obtained by sensors and the response time of actuators in the system [2] [9].

Typically the in-vehicle communication network is exposed to different disturbances, which can disrupt signals, generating more error-handling, interfering in the network reliability. Electrical fast transients are an example of faults generated by many components inside the car, as buck converters. According to EFT susceptibility analyzes carried out in the previous CAN and CAN-FD studies [16] [17], the present work fills the gap of checking the effects of EFT transients on an in-vehicle network using the FlexRay protocol. Experiments of this type are important for verifying the effects of fast electrical transients even on more robust protocols designed with fault-tolerant features, higher bandwidth, and the ability to communicate on redundant channels.

The interference in real-time systems affect the performance and lead to critical situations that may cause catastrophic problems. Thus, this research is applied to a fault injection test method, focused on verifying if the FlexRay communication network, in embedded vehicular control systems, is affected by EFTs. For this task, tests are conducted based on the standards IEC 62228 (EMC evaluation of CAN transceivers) and ISO 26262 (Road vehicles Functional safety) and their respective bases, IEC 61000-4-4 (Testing and measurement techniques - Electrical fast transient/burst immunity test) and ISO 7637-3 (Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines).

The used EFT injection hardware was developed specifically for the fault susceptibility analysis on CAN, CAN-FD, and FlexRay protocols. The design consists of a board developed by the manufacturer Texas Instruments, which uses a Hercules series processor TMS570LS3137, taking into account the safety standards for in-vehicle systems on its construction, according to IEC 62228 standard. This processor has been developed considering security and reliability issues, as well as its use in all in-vehicle communication protocols.

Another hardware part was specially developed for the fault injection test, according to the guidelines specified by the above-mentioned standards. In addition to the processor, the transceivers and controllers used for communication also comply with the respective standards. The designed hardware could perform a control loop communication, composed of a sensor node, an actuator node, and a controller node, besides allowing an external connection with other buses. The FlexRay communication is established through the NXP TJA1080A transceiver [24], which conforms to ISO 17458-2013 [3] and defines the communication system pattern with the FlexRay protocol.

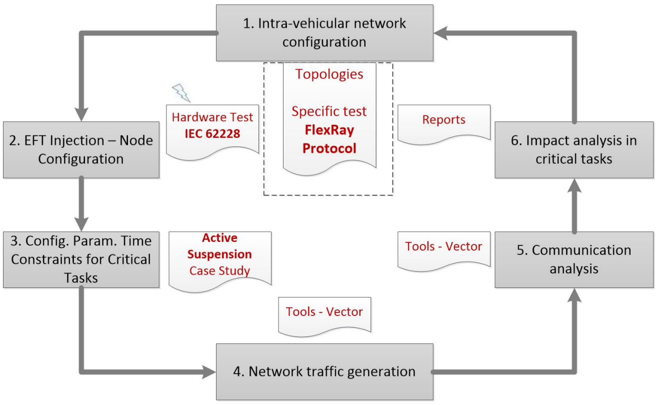

1. Intra-vehicular network configuration
2. EFT Injection – Node Configuration
Hardware Test
IEC 62228
Topologies
Specific test
FlexRay
Protocol
Reports
6. Impact analysis in critical tasks
3. Config. Param. Time Constraints for Critical Tasks
Active
Suspension
Case Study
Tools - Vector
5. Communication analysis
Tools - Vector
4. Network traffic generation

Fig. 1: Test method applied for FlexRay analysis. Adapted from [17].

Fig. 1 presents the flowchart for the test method applied in this study. This test method was already applied in a previous work [17], and in the present work, it was adapted for the FlexRay communication analysis.

In step 1, a critical control system based on the active suspension system proposed in [15] was programmed and embedded in the ECU nodes. Step 2 is composed of the EFT developed board according to IEC 62228. For step 3, it was used the time constraints and the periodical messages of the active suspension control system, with a control law cycle of 5 milliseconds. In step 4, traffic was generated in the network with the main goal of observing the network behavior under different busloads, in this case, observing only the control system operation and also with high busload in the network. The traffic messages were generated by two traffic nodes configured with dummy messages. Step 5 and Step 6 compose the experiment analysis with Vector CANoe/CANAnalyser. The tool allows the registration of graphs and logs data from each performed experiment. These steps provide, in a systematic way, the EFT fault susceptibility analysis, checking specifically the delay in the control law message.

The next section presents details of the performed experiments, detailing the network topology, the case study and analyzing the EFT fault impact in the FlexRay communication performance.

IV. Case Study

For evaluation of the EFT injection method and the FlexRay communication analysis, experiments were performed according to an EFT circuit board design following the recommendations of the IEC 62228 standard. Both EFT injection circuit and board with FlexRay communication transceivers comply with this standard. For this task, an important aspect is the use of a digital pulse conditioning circuit, designed in conjunction with a power section using the ST-ANALOG DEVICES MOSFET type transistor model BSZ900N20NS3, with low capacitance L-MOS technology high-speed applications. This transistor meets the rise and fall time parameters, as well as the requirement of high currents and working voltages.

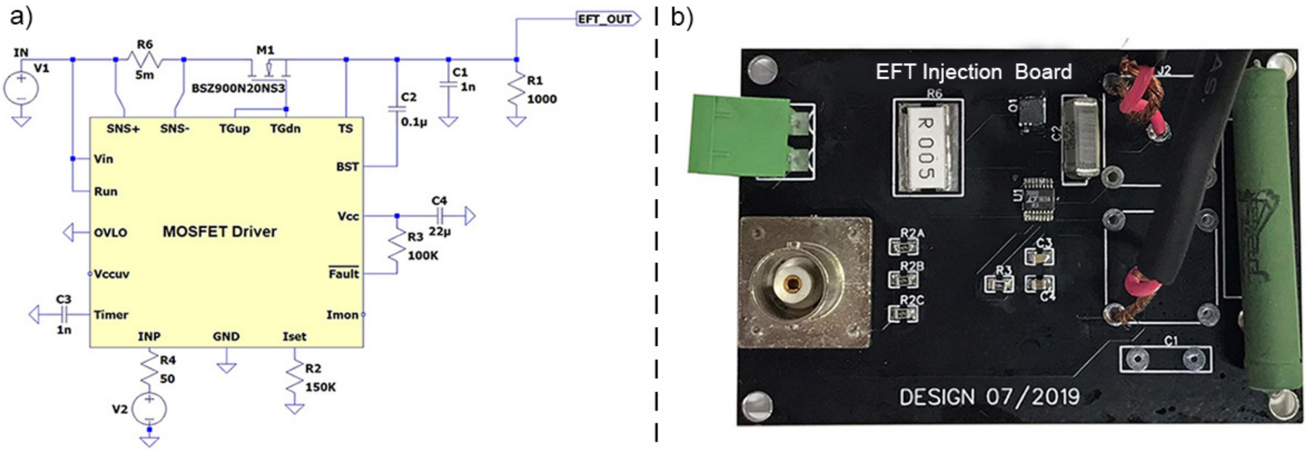


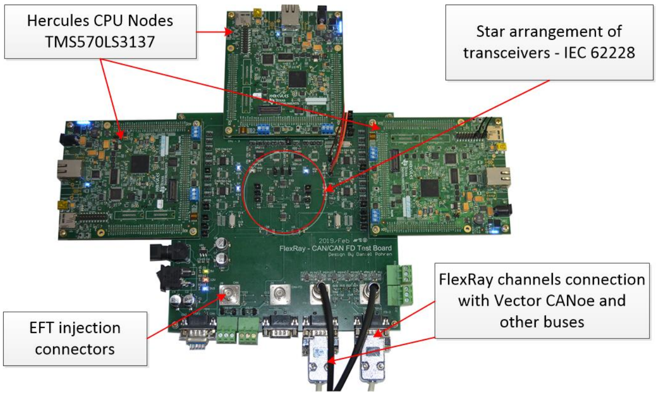
Fig. 2: a) New EFT injector power stage schematic. b) Power Stage board developed.

Fig. 2a shows the new power stage schematic diagram for the EFT pulse generator applied in the tests. In IEC 62228, the basic assembly scheme suggested for EFT injection is shown in Fig. 2b. The test board must contain at least three transceivers, having an external power supply, and having a point of EFT through a coaxial cable connector.

In this work, the pulse control circuit was updated to supply more consistent tests, compatible with the most used in-vehicle communication protocols. The circuit was designed with an arrangement of inductors, capacitors, resistors, and an LTC7000 gate driver mounted to generate fast pulses. This circuit receives external triggers from an arbitrary function generator, configured to generate pulses of different "burst" times. According to IEC 62228, the pulses must comply with rising and fall times less than 5 nanoseconds. The circuit meets this requirement, sending a trigger pulse to the power stage, ensuring that this time is repeated through the power output stage, through ST-ANALOG DEVICES MOSFET transistors. This power stage is powered by an external voltage source, which supplies values between 10 and 120 volts.

For the EFT injection tests it is necessary to build dedicated hardware, according to the already mentioned standards. Addressing this goal, it was adopted the Texas Instruments TMS570LS3137, that is an ARM-Cortex-R4F based high-performance 32-bit RISC Microcontroller, specifically designed for safety-critical applications. The TMS570LS3137 has two FlexRay, four CAN, and three SPI channels, providing the possibility of FlexRay communication. This flexibility eases the hardware implementation that allowed the interconnection of three CPU boards, in which each one controls a FlexRay node (with a channel A and channel B). Addressing the requirements of temporal constraints and determinism, the real-time operating system FreeRTOS was used for the three on-board nodes.

The connection of the CPU nodes on the test board is made by three eighty-pin header connectors. EFT injections occur directly through a BNC-type connector, directly interconnected in the junction of the three FlexRay transceivers. In the FlexRay communication, considering that it has six transceivers, three for channel A and three for channel B, the injections are independently performed in each channel. This same scheme is used for the common power supply of the board, which supplies power for all transceivers and also the CPU cards, complying with the IEC 62228 standard.


Hercules CPU Nodes TMS570LS3137

Star arrangement of transceivers - IEC 62228

EFT injection connectors

FlexRay channels connection with Vector CANoe and other buses

Fig. 3: Updated PCB Board made for EFT Injection and FlexRay susceptibility analysis.

As shown in Fig. 3, the PCB has nodes organized in a "star" topology, using three FlexRay transceivers on the same board. It is possible to observe the entire designed board assembled for the EFT injections tests, and the connected Hercules processor boards. The board was based on the previous work [17], but with an updated in the design specifically for the present study, meeting the most recent specifications for FlexRay protocol and covering the gap of FlexRay communication analysis under EFT interference. The main updated features compared to the original board presented by those authors in [17] were the individual's EFT injection connectors for each FlexRay channel, the standard FlexRay cable connectors, and the power stage schematic circuit updated with MOSFET L-MOS transistors. These changes were necessary because in their work [17] the focus was the CAN-FD protocol analysis, and the FlexRay was out of their scope.

After this specification, the EFT board was connected with the VN8910A hardware module and the software CANoe for traffic and communication analysis.

V. Tests and Results

A. EFT injection test procedure

The test procedures on FlexRay protocol follow the definition of an active suspension system message group, according to the case study performed in [17]. The main messages are vehicle vertical motion-sensing data (sensor node), signals of vehicle vertical position adjustments (actuator), and the computation of the appropriate adjustment levels in the control system parameters, which characterize the Control Law. The test method was applied following the steps depicted in Fig. 1, with different fault injection parameters.

According to the node's settings, the FlexRay network has been configured to operate at 10 Mbps. Due to the greater robustness of the FlexRay protocol and operating with higher bandwidth, the usual average control cycle time is about a few nanoseconds. According to [15], which is the reference of this study on FlexRay protocol, information observed in experiments showed an average variation of approximately 25 nanoseconds, having an upper limit of around 70 nanoseconds. In the present work, as the goal is to analyze the electrical transient effect on periodic messages, the dynamic segment of the FlexRay protocol was kept at 100% of the busload. The static segment where periodic messages are allocated was tested with three busload variations, 2% (only the control system), 30%, and 80% (with software traffic generation).

In the test procedure, the FlexRay network connection to the VN8910A interface and CANoe software was performed using FlexRay standard cable of 50 cm to the EFT fault injection hardware. Message time slot configurations used in the static segment of FlexRay protocol followed the control loop specification of 5 milliseconds, with the plant states transmission in slot 20 and the control law in slot 40.

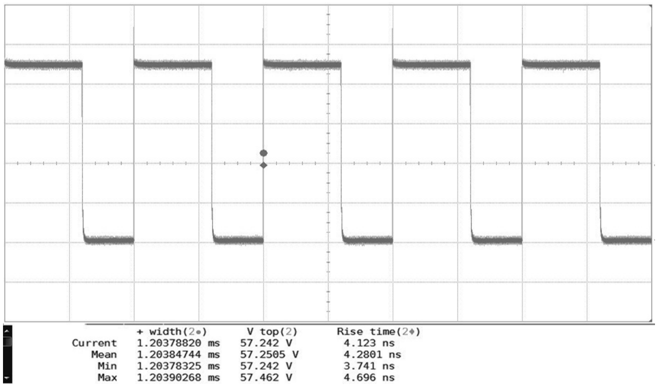
With these definitions, the experiments aim to determine the influences of EFT transients in the FlexRay network, also recording logs and the variation of communication delays. The following steps were adopted: Step 1: Network based on FlexRay protocol; Step 2: EFT injection with the test hardware developed based on IEC 62228 and ISO 26262; Step 3: Traffic generation and communication analysis with Vector CANoe (based on registered logs).

Electrical Fast Transients consist of bursts with variable amplitudes generated in networks by different noise sources (for example Ignition, Headlight, Air conditioner, among other). In order to verify the applicability of the developed test board, a sequence of disturbances was injected into the network, during the control system processing. The pulses were generated using an arbitrary wave generator. Table II presents the sequence of the performed fault injection.

TABLE II: Sequence of EFT Tests

Voltage Peak	Burst Time
47 volts	687 us
57 volts	1,2 ms
63 volts	500 us

For protocol susceptibility analysis and experiment calibration purposes, an initial EFT pulse sequence was injected and measured with the Agilent MSO9104A oscilloscope. This record obtained from the oscilloscope can be viewed in Fig. 4, which shows the injection of an EFT pulse with 57 volts and 1200 microseconds of burst.



```
          + width(2●)         V top(2)      Rise time(2♦)
Current   1.20378820 ms   57.242 V       4.123 ns
   Mean   1.20384744 ms   57.2505 V      4.2801 ns
    Min   1.20378325 ms   57.242 V       3.741 ns
    Max   1.20390268 ms   57.462 V       4.696 ns
```

Fig. 4: First measurement - EFT pulse of 57 vp - 1200 us.

B. Results

After the initial network analysis, a series of EFT injections were conducted with the signals and pulses defined in Table II, to evaluate the impact of electrical fast transients on usual system operation, observing the FlexRay network behaviour. The message control law is the result of the control model computation (ECU controller) after receiving messages from the plant behavior (ECU sensor and ECU actuator), according to the active suspension control system specified in [15].

The average jitter and the difference jitter metrics were used for EFT impact analysis. The difference jitter is obtained by subtracting the best-case transmission time from the worst-case transmission time in the sample set measurement. The average jitter is represented by the standard deviation in the measure of average message transmission time. The performance metric is calculated according to the communication logs, generated by the CANoe software. Before the EFT injection sequences, a communication measurement was performed without interference. Figure 5 shows the FlexRay network measurement, with the control law oscillation within the expected range, around 27 ns.

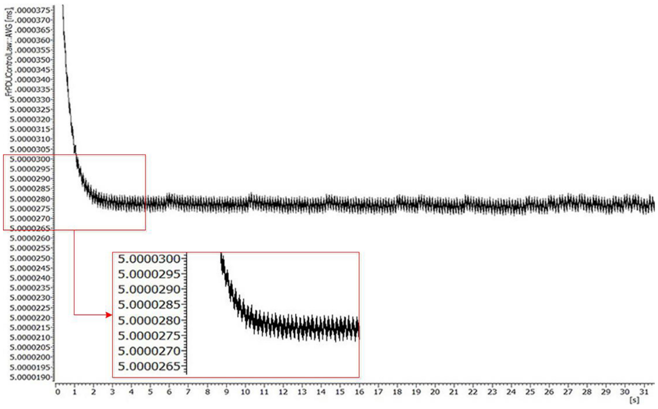


Fig. 5: Control Law without EFT Injection

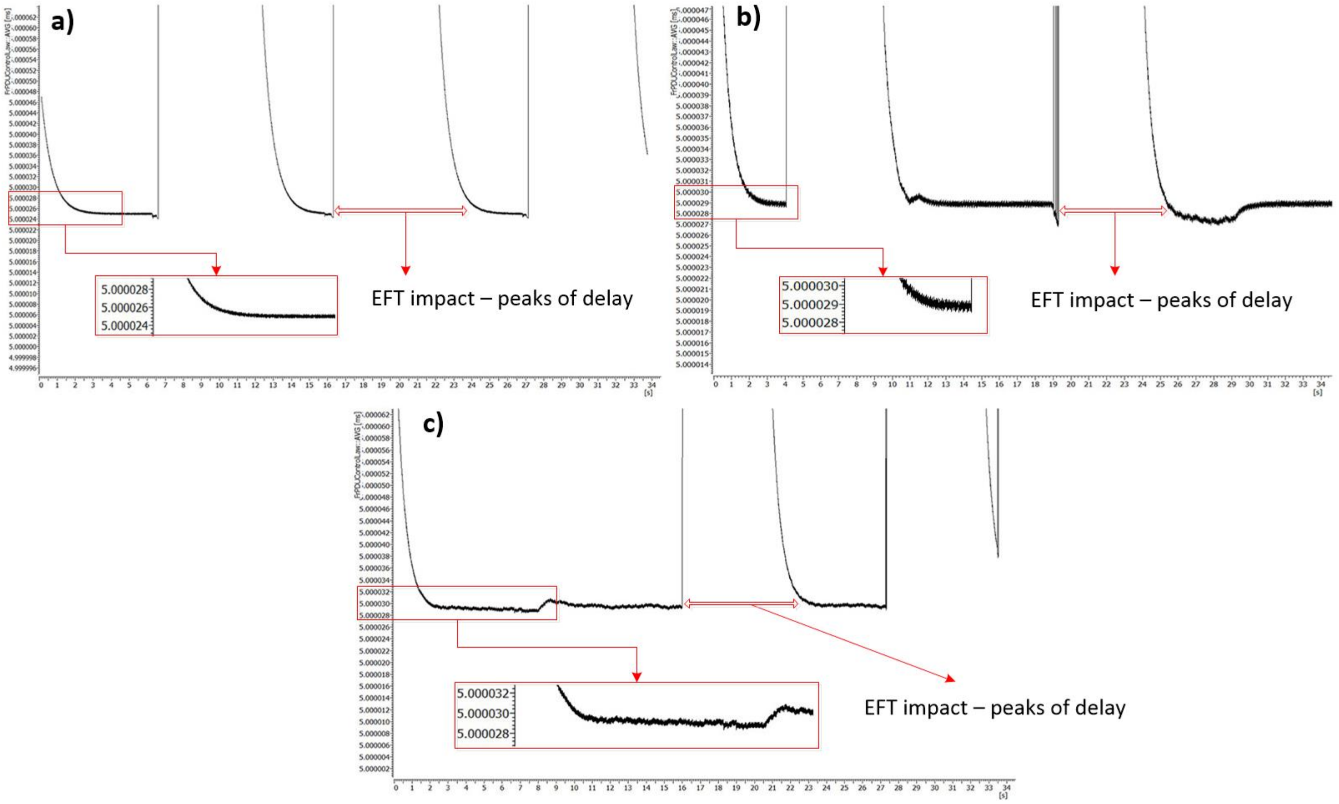


Fig. 6: Measurement graphics of the FlexRay network with EFT injection of 47 volts and 687 us. a) Busload 2% b) Busload 30% and c) Busload 80%.

Then the fault injection procedures were started following the sequence defined in Table II, with three types of busload variation. The graph presented in Figures 6a, 6b and 6c highlight the oscillations in the control law, with EFT injection of 47 volts and 687 microseconds. The oscillation occurs due to the time variation of the received packet in the previous control law and the packet sent in the next control law.

In the EFT tests with 47 volts, it was observed the average oscillation in the control law of 26 ns, with busload of 2% (only the control system). However, with higher busloads (30% and 80%), the oscillation increases (evidenced by the highlighted graph parts), registering delay peaks higher than 80 ns, more frequently and long-lasting. In the second experiment, with EFT injection of 57 volts, the network impact was similar, but the disturbances increase a little the control law average delay, with values between 25 and 30 ns. However, it happened delay peaks in the microseconds scale, with registered peaks of 37 us in a busload of 2%, and 260 us with a busload of 80%, which are much high for this protocol. In the third experiment, with EFT injection of 63 volts, the goal was the transient effect analysis with shorter burst times and a higher frequency of occurrence. In this case, the results emphasize the delay peaks increase with more message traffic, highlighted in the graph with 80% of busload. It is possible to see that the average delay does not return to usual time after 27.5 seconds in the sample analysis period.

Comparing to the first experiment, the results show the most negative impact with EFT of small burst time and higher voltage amplitude. This situation reflects in communication delays in the control law, increasing the number of messages affected by protocol signal disruptions. The error rate, registered by Vector CANOe, increases from 33 to 76 packets per second respectively, in the analysis of 2% and 80% of network busload.

These sequences of EFT injections (47, 57 e 63 volts) allow a deep analysis (under stressful conditions), about the negative impact of transient faults in critical control systems. The analysis emphasizes the greater occurrence of disturbances in the FlexRay protocol signals, due to the fact of the protocol works with shorter bit times, providing higher bandwidth. Thus, the present study emphasizes the importance of susceptibility analysis of communication protocols to electrical fast transients, faults that represent the focus of the present study. Methods and techniques which focus on to mitigate or diagnose these effects, are of paramount importance to add reliability to safety-critical control systems, and in this case, even in a physical environment using a robust communication protocol such as FlexRay.

In order to evidence the performance degradation generated during the EFT fault injections, consistently and following the analysis methodology, the *Difference Jitter* and *Average Jitter* metrics were used to compile the data obtained during the experiments. Fig. 7 and 8, highlight the data obtained after the analysis of the FlexRay communication network.

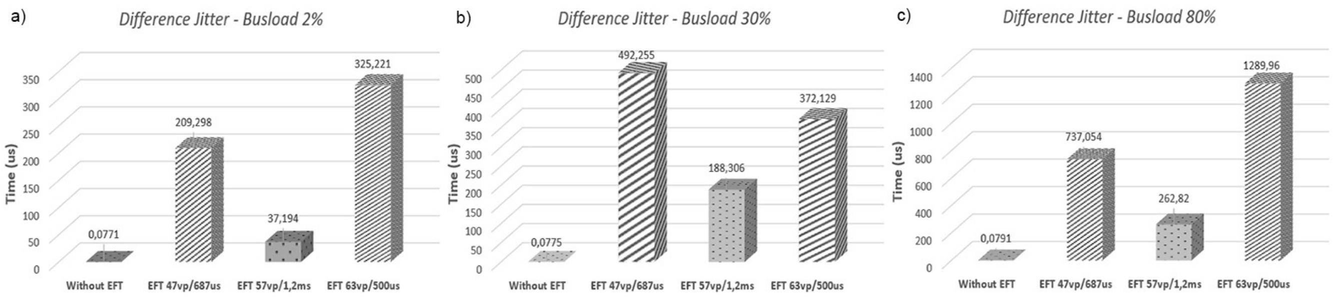


Fig. 7: Difference Jitter in Control Law Messages

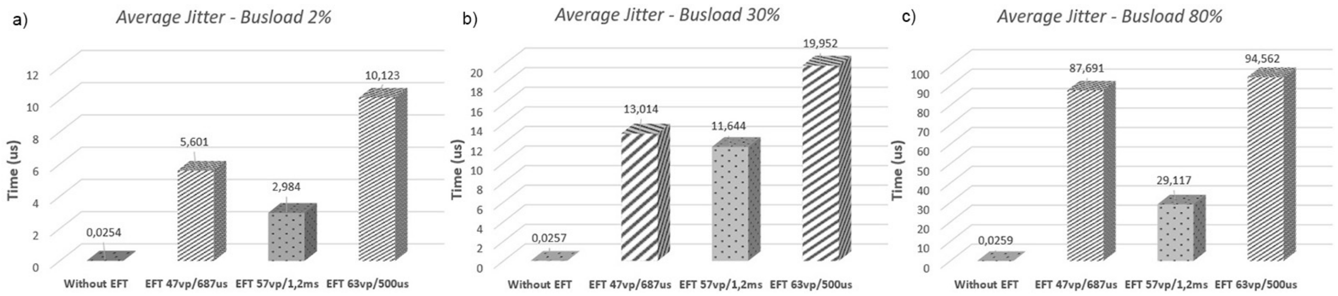


Fig. 8: Average Jitter in Control Law Messages

TABLE III: Degradation summary during the EFT injection tests with the average jitter metric.

	Bus 2%	Bus 30%	Bus 80%
without EFT	0,0254 us	0,0257 us	0,0259 us
EFT 47 volts - 687 us	5,6 us	13 us	87,6 us
EFT 57 volts - 1,2 ms	2,9 us	11,6 us	29,1 us
EFT 63 volts - 500 us	10,1 us	19,9 us	94,5 us

The data resulting from the metrics analysis show the worst performance degradation effects (delay peaks of 1.2 ms and average delay oscillation up to 94.5 us) in the experiments with 63 volts and 500 us. Table III summarizes the degradation effects recorded based on the *average jitter* metric.

Observing the data on Table III, It is highlighted the greater degradation effect on the FlexRay network with EFT transients of shorter burst duration and specifically with higher peak voltages. These values are justified by the fact that the control law cycle used in the case study is 5 ms. In this case, the smaller transient generation interval allows the chance of these pulses affecting the cyclic message with more frequency. On the other hand, with a long burst duration (1.2 ms), during the control law cycle, the amount of transients affecting the data obtained from the system plant is smaller, resulting in lower degradation. It is important to highlight the increase in the control law average delay of 397, 774 and 3648 times, in all busloads of the worst-case test scenario (EFT of 63 volts and 500 us). It is noteworthy that the analyses were performed in a short sampling period, characterizing the EFT transient susceptibility analysis, according to the guidelines of ISO 26262, IEC 61000-4-4 and ISO 7637-3.

The information obtained in this study, confirms the negative effect of faults such as EFT, on critical messages of in-vehicle communication networks. Even though the performed tests were stress (with many injections), the performance degradation recorded show that such effects, even silent, can affect the safety and reliability of a critical real-time control system. Therefore, monitoring and recording these situations is very important, even for further analysis or conformity of the fault tolerance limits in safety-critical control systems.

VI. Conclusions and Future Perspectives

Recent works have been emphasized the impact of electrical fast transients, generating faults on intra-vehicular communication protocols, such as CAN and CAN-FD, leaving gaps about their impact on more robust protocols such as FlexRay. The researches reported in [25] and [26] emphasize that due to the increasing complexity of embedded electronics, many sources of electromagnetic interference and electrical transients have emerged, requiring standardized and reliable testing procedures of possible degradation generated by these faults, providing an overview of the IEC 62228. Besides these important contributions, the observation of the fault impact in specific critical messages is also is necessary.

The present research covers these gaps and corroborates with concerns about them, updating a recently applied test method and also complying with the recent updates to ISO 62228, specifically to verify the impact of electrical transients on communication transceivers. The approach contributes with an alternative way of analysis, checking the fault impact not only in transceivers but also in the network control systems.

An important contribution of this work is related to the development and update of a test board according to IEC 62228 meeting the requirement of the rise and fall times (less than 5 ns) for each EFT injection performed in the experiments.

Experiments were performed based on an active suspension control system, representing an example of a critical control system, with periodical messages and hard timing constraints. The communication was analyzed with logs generated by Vector CANoe software.

The results show that although protocols such as CAN-FD and FlexRay have higher communication bandwidth, part of this communication could be filled by error frames, reducing the effective throughput and also the network reliability. The delays generated on the FlexRay network are significant, especially considering the short communication time (in the order of nanoseconds), which makes the protocol also susceptible to electrical fast transients. The results highlight delays between 2.9 and 94.5 microseconds, which are significant compared to the usual communication time, and could decrease the reliability of the FlexRay protocol.

As observed in the experiments, the EFT leads to signal modulation disruption, having an even more critical effect on FlexRay, because it works with very short bit times. The delays observed in the case study during the message transmission evidenced the performance loss and that the problem is critical. Thus, it is becoming increasingly important to develop methods for testing, diagnosing and recording the occurrence of faults. This research contributes to a systematic and reliable method for in-vehicular network testing, which can reduce component maintenance and improve the design of new safety-critical control systems.

Future works drive to the direction of applying a fault modeling method to provide the fault handling, connecting design e test phases, contributing with more reliable and robust in-vehicle control system design. Another analysis possibility is to apply the method in different critical real-time control systems such as avionic and industrial systems.

References

[1] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 534–545, 2015.

[2] W. Zeng, M. A. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1552–1571, 2016.

[3] ISO-17458, "Road vehicles – flexray communications system," ISO – International Organization for Standardization, Geneva, CH, Standard, 2013.

[4] D.-S. Kim and H. Tran-Dang, "Flexray protocol: Objectives and features," in *Industrial Sensors and Controls in Communication Networks*. Springer, 2019, pp. 17–30.

[5] J. Huang, M. Zhao, Y. Zhou, and C.-C. Xing, "In-vehicle networking: Protocols, challenges, and solutions," *IEEE Network*, vol. 33, no. 1, pp. 92–98, 2018.

[6] Y.-Y. Chen and K.-L. Leu, "An effective two-level redundancy approach for flexray network systems," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*. IEEE, 2016, pp. 168–175.

[7] G. Han, J. Lu, J. Li, S. Hu, and J. Zhang, "Design and optimization of switched flexray networks," in *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*. IEEE, 2017, pp. 769–774.

[8] P. F. do Souto, P. Portugal, and F. Vasques, "Reliability evaluation of broadcast protocols for flexray," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 525–541, 2016.

[9] L. L. Bello, R. Mariani, S. Mubeen, and S. Saponara, "Recent advances and trends in on-board embedded and networked automotive systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 1038–1051, 2019.

[10] M. B. N. Shah, A. R. Husain, H. Aysan, S. Punnekkat, R. Dobrin, and F. A. Bender, "Error handling algorithm and probabilistic analysis under fault for can-based steer-by-wire system," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1017–1034, 2016.

[11] R. Shirai and T. Shimizu, "Study of emi caused by buck converter on controller area network," in *2018 International Power Electronics Conference (IPEC-Niigata 2018-ECCE Asia)*. IEEE, 2018, pp. 3309–3314.

[12] M. Fontana and T. H. Hubing, "Characterization of can network susceptibility to eft transient noise," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 2, pp. 188–194, 2015.

[13] R. Yan, J. Yang, D. Zhu, and K. Huang, "Design verification and validation for reliable safety-critical autonomous control systems," in *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 2018, pp. 170–179.

[14] IEC-62228, "Integrated circuits – emc evaluation of transceivers," IEC – International Electrotechnical Commission, Geneva, CH, Standard, 2018.

[15] J. M. da Silva Jr, C. E. Pereira, and T. J. Michelin, "Performance analysis of distributed control systems using the flexray protocol," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 5252–5257, 2014.

[16] A. S. Roque, D. Pohren, T. J. Michelin, C. E. Pereira, and E. P. Freitas, "Eft fault impact analysis on performance of critical tasks in intravehicular networks," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, no. 5, pp. 1415–1423, 2017.

[17] D. H. Pohren, A. Santos Roque, T. I. Kranz, E. P. P. de Freitas, and C. E. Pereira, "An analysis of the impact of transient faults on the performance of the can-fd protocol," *IEEE Transactions on Industrial Electronics*, 2019.

[18] B. Liu, W. Bai, and G. Zhen, "A prompt retransmission method for in-vehicle network flexray," in *2017 36th Chinese Control Conference (CCC)*. IEEE, 2017, pp. 7841–7846.

[19] T.-Y. Lee, I.-A. Lin, J.-J. Wang, and J.-T. Tsai, "A reliability scheduling algorithm for the static segment of flexray on vehicle networks," *Sensors*, vol. 18, no. 11, p. 3783, 2018.

[20] K.-L. Lu, Y.-Y. Chen, and L.-R. Huang, "Fmeda-based fault injection and data analysis in compliance with iso-26262," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2018, pp. 275–278.

[21] A. Munir and F. Koushanfar, "Design and analysis of secure and dependable automotive cps: A steer-by-wire case study," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[22] B. Poudel and A. Munir, "Design and evaluation of a reconfigurable ecu architecture for secure and dependable automotive cps," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[23] L. Zhang, F. Yang, and Y. Lei, "Tree-based intermittent connection fault diagnosis for controller area network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9151–9161, 2019.

[24] I. NXP Semiconductors, "Flexray transceiver tja1080a," 2019, available in: https://www.nxp.com/docs/en/data-sheet/TJA1080A.pdf, Access in: August, 2019.

[25] S. Matsushima, T. Matsushima, T. Hisakado, and O. Wada, "Trends of emc standards for automotive network devices and communication quality of ethernet in relation to parameters of pulse disturbances," *IEEE Electromagnetic Compatibility Magazine*, vol. 7, no. 1, pp. 46–50, 2018.

[26] F. Klotz, M. Roebl, B. Koerber, and N. Mueller, "New standardized emc evaluation methods for communication transceivers," *IEEE Letters on Electromagnetic Compatibility Practice and Applications*, 2019.