IET Intelligent Transport Systems

Review Article

Controller area network reliability: overview of design challenges and safety related perspectives of future transportation systems

ISSN 1751-956X
Received on 25th August 2019
Revised 26th March 2020
Accepted on 8th October 2020
E-First on 6th January 2021
doi: 10.1049/iet-its.2019.0565
www.ietdl.org

Nadhir Mansour Ben Lakhal[1,2] ✉, Othman Nasri[2], Lounis Adouane[3], Jaleleddine Ben Hadj Slama[2]

[1]*Institut Pascal, UCA/SIGMA – UMR CNRS 6602, Clermont Auvergne University, 63178 Aubière cedex, France*

[2]*LATIS Lab, National Engineering School of Sousse (ENISo), University of Sousse, BP 264 Sousse Erriadh 1023, Tunisia*

[3]*Université de Technologie de Compiègne, CNRS, Heudiasyc UMR 7253, 60203 Compiègne cedex, France*

✉ *E-mail: nadhir_mansour.ben_lakhal@etu.uca.fr*

Abstract: The in-vehicular networked control system is among the most critical embedded processes. The controller area network (CAN) has prevailed intra-vehicle communication for decades. Meanwhile, requirements of future transportation systems are expected to emphasise the in-vehicle communication complexity, which endangers the reliability/safety of the intelligent navigation. At first, this study reviews the recent solutions proposed to overcome the CAN expanding complexity. Challenges that tomorrow's intelligent vehicles may raise for CAN reliability are investigated. The comprehensive coverage of current research efforts to remove the impact of these challenges is presented. Further, the in-vehicle system reliability of future automated vehicles is also related to the fault diagnosis performances. Hence, different classes of system-level diagnosis strategies are compared relatively to the requirements of automotive embedded networks. Furthermore, to thoroughly cover CAN reliability engineering issues, focus is given to the automotive validation techniques. The hardware in the loop, real-time analysis and computer-aided-design tools intervene in various phases along the in-vehicular network life cycle. Parameters that stand behind the efficiency and accuracy of these techniques in validating the new generation of vehicles are analysed. The authors finally draw some deductive predictions about the future directions related to the reliability of the intelligent transportation system in-vehicular communication.

1 Introduction

Over time, science has modified the composition of technological processes to take advantage of more powerful functionalities [1]. Migrating from simple architecture to massive modular architecture has led to the emergence of networked control systems (NCSs) [2]. Up to now, with respect to their deep complexity, several aspects in NCSs have remained under study [3]. Latest advances and theoretical issues related to NCSs, as modelling, sampling, detecting failure and optimising computational performances were reviewed in [4, 5]. In particular, in-vehicular NCSs (IVNCSs) are probably the most critical networks. The need for enhancing mobility has kept the automotive preoccupations at the top of industrial and research community interests. For this reason, the upgrade of the vehicular structure from assembled mechanical entities to its contemporary sophisticated disposition has been rapid.

At the present time, modern automotive embedded networks exhibit boundless proofs of complexity. Since more functionalities are incorporated into today's vehicles, the number of electronic control units (ECUs) is continuously and systematically increasing. Another evidence of IVNCS complexity resides in the tight interaction between software (SW) functions and hardware (HW) components [6]. Especially for the intelligent vehicles, the IVNCS outgrowth is accentuated due to the arising attitudes to enhance the vehicle inter-connectivity with its environment [7, 8]. The evasive integration of sensing tools brings additional complications. To acquire the appropriate understanding of the environment, algorithms with demanding computational resources have been utilised [9, 10]. The main purpose from the extra inter-connectivity of the vehicle and its neighbourhood is to raise autonomy [11]. Within this scope, modern cars and intelligent transportation systems are equipped with a large range of critical safety applications. Such applications assist the driver while prohibiting undesired accidents. Adaptive cruise control, advanced drive assistant systems, pedestrian detection and driver distraction detection are samples of these safety-oriented mechanisms [12]. Aside from their complicated nature, these processes impose material constraints and resource availability problems. Communication delays and errors in data transmission are destructive for these applications and the navigation safety [13, 14].

In a way or another, all the stated shapes of complexity have a direct negative impact on the IVNCS operation. Consequently, improving the IVNCS capacities and reliability becomes a priority. To be on the safe side and take measures about its growing complexity, the collaboration between industry and academia has set out precautions for assuring IVNCS reliability. Architectures of HW and SW parts as well as techniques that verify their perfect integration have been introduced [15]. Testing/model checking techniques have been prescribed to monitor automotive operating systems, which are the bottom line of IVNCS control SW [16]. HW/SW certification frameworks have been developed to tackle IVNCS cost-aware design [17]. The establishment of data stream management systems has guaranteed a reliable message exchange inside IVNCSs [18]. Classical diagnosis approaches have been evolved to fit automotive embedded systems [19]. These accomplishments have contributed to define universal standards about: IVNCS design practices, reliability considerations and onboard diagnosis deployment [20].

This work addresses the IVNCS controversial reliability and figures out its complexity reflections on tomorrow's transportation system safety. As a coordinator between abundant interconnected entities, our methodology consists in focalising our research about the controller area network (CAN). This latter has been a de facto standard for the in-vehicular communication over the last decades. The relation between CAN reliability and the future transportation systems requirements and performances is studied. The most part of existing surveys concentrate on separated issues as CAN security, CAN latency behaviour and so on. However, CAN reliability is tightly related to a set of overlapping aspects. We profit from our exclusive interest in the CAN to more closely and comprehensively study and examine IVNCS practical reliability engineering issues. The on-board automotive diagnosis efficiency

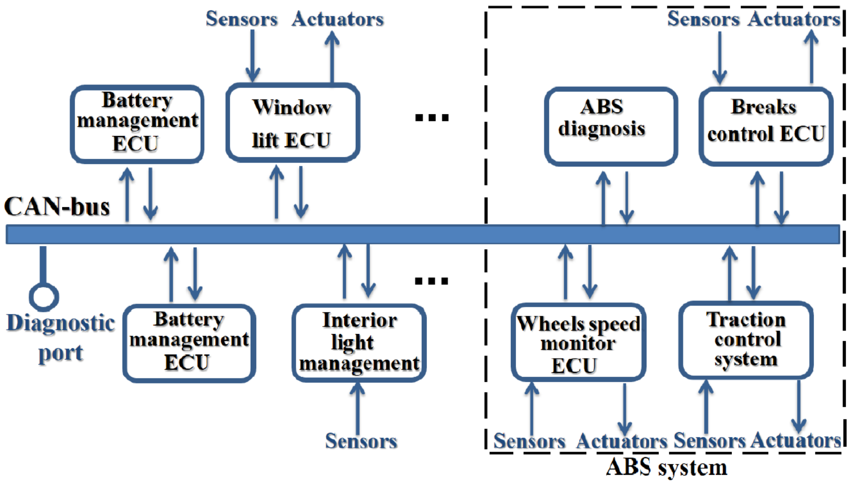

Fig. 1 *Typical IVNCS structure*

and the quality of the IVNCS/CAN validation techniques are also discussed since the safety and reliability of the new generation of intelligent navigation systems depend on these components. The key contributions of this review lie principally in the subsequent aspects:

- Based on expected features of tomorrow's vehicles, challenges that will be raised for CAN reliability are analysed. Solutions offered by the literature to overcome these challenges are also inspected. The link between the ongoing attempts in idealising the CAN and the perspectives related to IVNCS reliability are highlighted.
- A classification of CAN system-level fault diagnosis practices is delivered. Thus, a comparison between these classes is established to assess each category convenience to the IVNCS diagnosis requirements.
- The tight relation between CAN reliability and several means of automotive design validation is investigated. Almost, the hardware in the loop (HIL), real-time analysis (RTA) and computer-aided-design (CAD) tools are the typical practical and theoretical concepts used for this reason. A special interest is given for factors that stand on the accuracy of these means and their contribution to the increase in CAN reliability during all the IVNCS life cycle.

The outline of this paper is as follows. Section 2 introduces the general concepts that may influence the automotive reliability. Section 3 reflects challenges and ambitions presented by CAN researches and its applications for the intelligent navigation. Section 4 underlines the work related to the CAN system-level diagnosis. Section 5 provides a precise idea about the HIL technique and analyses its role in validating CAN-based IVNCSs. Consequently, CAN timing analysis models are studied in Section 6. Section 7 reveals the capabilities of the available commercial tools in verifying CAN reliability over the IVNCS life cycle. Finally, Section 8 depicts discussions and future directions of CAN reliability engineering practices and their reflections on the intelligent navigation safety.

2 Preliminaries

Before proceeding further in detailing the reliability concerns of tomorrow's vehicles, this section highlights the main constituents from the in-vehicular networks. Accordingly, the reliability issues will be analysed not only in accordance with CAN features, but also relatively to all the vehicular composition.

- *Cyber physical systems (CPSs)*: The collaboration between the control sciences, the HW/SW co-design and the electronic communication techniques has introduced the concept of CPSs. CPSs present a set of highly integrated computational units with physical entities. They are drastically advantageous because of their aptitudes of processing data acquired from sensors and their smooth control of entities as actuators [21]. CPSs provide a high autonomy level by overlapping automation, knowledge-based computational algorithms and reliable interaction between components [22]. Regarding its multidisciplinary nature, numerous CPS aspects are constantly improved by a significant number of researchers. For former control systems, the algorithmic design and the implementation phase have been widely independent. In case of CPSs, the optimal HW/SW implementation has been largely studied [17]. The CPS functional correctness, the resource planning, the HW concurrency and the energy efficient/cost-aware design are other main aspects, which have been extensively studied in the literature [23, 24].
- *NCSs*: Due to their modular and distributed hierarchy, the automotive embedded CPSs are roughly studied as NCSs. An NCS is a control process, which includes a high number of CPSs and a communication protocol to ensure a required feedback loop between all these CPSs [25].
- *ECUs*: An ECU is the most elementary computational platform in the vehicular composition. It serves to control the actuators, the mechanical parts and the remaining subsystems. Several functionalities, such as the engine control, the antilock braking system and the electronic stability program, may be distributed on various ECUs.
- *Communication protocol (CAN)*: CAN is an advanced event-triggered communication protocol and a multi-master serial data bus. Over the last decades, it has dominated the automotive industry for being cost-effective, reliable and labelled by resilient arbitration capacities. Full technical details of the CAN features and its frame format are available in [26].

All of the stated elements are important parts from the on-board composition of future intelligent navigation systems. For a clearer idea about the vehicular composition, an example of a CAN-based IVNCS typical structure is illustrated in Fig. 1. Due to its critical use-case in the automotive field, it is fundamental to guarantee the CAN reliability, i.e. the ability to enable the communication between components as expected and without failure. Definitely, the tight relation between the CAN/IVNCS reliability and the vehicle safety is evident. Indeed, the CAN reliability issues may be classified into three different categories. The first one consists in the CAN capacities to adapt to the technical changes witnessed in the automotive embedded systems at the short and long horizon time. Without an entire compatibility with the new vehicular technologies, CAN reliability is controversial. In this sense, this work covers all the requirements of tomorrow's vehicles. Then, the link between those requirements and reliability is established. For the second class, focus is given to the management of probable failures that may menace the IVNCS/CAN in run-time. If these faults are not mastered, the whole automotive system is neither reliable nor safe. Therefore, the IVNCS diagnosis nature (model-driven/data-driven diagnosis etc.), architecture and performances should be suitable for the sophisticated automotive composition. Another important class of CAN reliability issues focuses on the efficiency of the early phase design practices. In particular, accurate validation/verification methodologies are essential to avoid unexpected run-time problems. In this work, the CAN reliability issues are analysed according to the already detailed categories. Otherwise, the reliability issues, which are discussed in this paper are not restricted to CAN. Our study includes all the concerns related to the IVNCS and its sub-systems. Many of the discussed points may be easily extended to IVNCSs that are based on other vehicular communication protocols.

3 Requirements of tomorrow's vehicles and related work about CAN reliability

Since it was introduced by BOSCH, CAN has been subject to a lot of improvements. In spite of the large interest by this in-vehicular bus, prospects of recent CAN advances have been rarely investigated in the literature. In the sequel, the latest attempts in idealising the CAN will be pinpointed and organised given its contribution. The light will be focalised on how current research efforts about CAN reliability will solve problems and complications entailed by tomorrow's intelligent/autonomous vehicles.

3.1 CAN electromagnetic immunity

The automotive industry moves towards the full electrification of transportation means. More and more sensing tools are expected to be mounted on tomorrow's vehicles. Mostly of an electrical/electromagnetic nature, sensing tools generate/receive too much of radiated or conducted electromagnetic disturbances. Thus, the in-vehicle network is prone to enormous electromagnetic interference (EMI) [27]. Shielding and filtering have been proposed for this aim [28]. However, these techniques do not fit all use-cases. Rather, circuit-level EMI mitigation solutions have been suggested. An electro-static discharge risk-aware co-packaged technique for CAN transceivers was discussed in [29]. In [30], the experimental results proved the efficiency of the CAN transmitter design methodology in providing low-electromagnetic emissions. Due to their position as communication bridges, the stated solutions have targeted transceivers to guarantee the communication EMI immunity.

Differently, more global network-level methods have been lately studied. CAN EMI immunity has been guaranteed through applying a specific galvanic isolation technique [31]. Underlined as a major EMI source, the effects of electrical fast transients (EFTs) on the CAN were inspected in [32]. Dominant and recessive immunity analysis of the signal state allowed the characterisation of electrical setups, which had to be strictly avoided. Respectively, the study depicted in [33] revealed an original experimental method in analysing the EFT impacts on the CAN. It showed great accuracy in measuring EMI-induced error-propagation jitters. In [34], RF immunity simulation was performed to predict the CAN behaviour under EMI and facilitate the network immunity analysis.

Obviously, an ongoing effort is carried out to integrate the electromagnetic compatibility (EMC) concerns into the transportation system safety requirements. More attention is paid now to the network-level EMC solutions. Thus, not only the CAN-bus is immunised, but also the overall network.

3.2 CAN payload

For tomorrow's vehicles, the convergence between big data and artificial intelligence (AI) is inevitable for the decision-making automation. Intelligent vehicles manipulate a large range of information to proceed the navigation while guaranteeing safety [35]. Hence, the CAN is not sufficiently reliable without keeping the automotive technologies up-to-date with the ‘big data’ trend.

Huge efforts have been lately done to enlarge the CAN-bus transmission payload. A new concept named CAN-FD (CAN with flexible data rate) has been recently standardised. It offers a larger extent for the data field and a higher baudrate. Marcon Zago and Pignaton de Freitas [36] evaluated the relevance of distinct optimisation presented by CAN-FD compared to other CAN implementations. Aside from CAN-FD, there are too many academical/industrial CAN modified extensions, which provide a larger communication payload. For instance, CAN+, TURBO CAN and CAN XR have proved their good performances in terms of payload and transfer rate [37–39].

On the other hand, extra data may be assigned to the CAN frame owing to some compression techniques. 81.06% of the CAN frame length has been miniaturised via a signal compression algorithm in [40]. Over-sizing the CAN frame brings a lot of advantages for tomorrow's vehicles. Heading towards a more mature in-vehicular communication, Woo *et al.* [41] profited from the CAN-FD payload to introduce a sound security strategy for the network.

3.3 Network-induced imperfections

Modern vehicle IVNCSs include subsystems of different timing features (powertrain system, steering system etc.). All these components exchange information via the CAN-bus. CAN constraints may entail violation of the predefined time-sampling and non-negligible network-induced imperfections. A missed packet or packet disorder may lead to discontinuity in the behaviour of vehicular systems.

To deal with these imperfections, excessive research work has been tackled about CAN scheduling. ECUs/tasks schedulability has a great impact on reducing the blocking time of messages [42, 43]. Under certain constraints on the message streams and with a non-preemptive rate monotonic algorithm, Park and Piao [44] drastically exceeded the normal CAN utilisation bound. In [45], models for the network and the delay-sensitive components were involved in a control synchronisation policy. It takes into account data packet-related problems via Lyapunov stability criterion-based scheduling. Particular methods are currently under study to boost the scheduling of multi-core ECUs [46]. To make scheduling open to some particular cases, the work of Schmidt [47] handled a situation where a message instance is followed by the transmission of additional CAN frames. Alternatively, several information-fusion-based IVNCS delay-compensation approaches have been reviewed in [48]. Unlike the conventional event-triggering CAN communication, the network imperfections have been avoided by a pipeline device with a deterministic data transmission [49]. Delay-dependent proportional–integral control has been developed for the CAN [50]. Another part from the literature has relied on CAN-based coordination control to overcome network-induced imperfections. Dedicated CAN-bus simulation was carried in [51] to validate robustness against CAN-induced delays. A compensation method, proposed in [52], guaranteed the IVNCS asymptotic stability through a closed-loop delayed state-process. The study in [53] used state-feedback control with mixed linear-quadratic and H_∞ regulators.

Clearly, checking timing features of components has become an essential design step due to its direct relation with CAN reliability.

3.4 CAN-frame encoding schema

Technically speaking, the length of CAN frame is variable due to the bit stuffing. In case of the transmission of five homogenous bits, an opposite polarity complementary bit is inserted to prohibit error occurrence [26]. Nonetheless, the bit stuffing increases the exchanged data length. The longer the message content, the higher the network-induced delay. As already discussed, the reliability of CAN-protocol as well as of tomorrow's transportation systems are directly linked to real-time constraints. Accordingly, the ‘zero stuff cyclic redundancy check (CRC) bit’ has been introduced to prevent the stuff bits occurrence in the CRC field [54]. A similar concept to cut-off with the dependency relating the message content and its transmission jitter could be found in [55]. It has suggested a free-jitter payload-encoding schema, namely 8B9B. Later, in-depth analyses of the 8B9B were the start point to introduce the ‘variable-length high-performance code for CAN’ (VHCC) [56]. During experimentation, the VHCC has shown exceptional results in solving the variability in the CAN frame length.

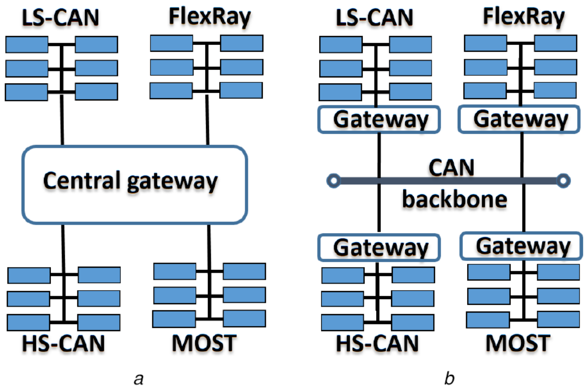

Fig. 2 *IVNCS architecture*
(a) Central gateway-based architecture, ***(b)*** Backbone-based architecture [66]

For a long time, the non-determinism in the CAN frame length was assumed to be a CAN major weakness [26]. Formerly, when synchronisation is extremely required for a given in-vehicular application, protocols as FlexRay were used instead of CAN [57]. With an invariable frame length, CAN might meet strict real-time constraints and maintain its leadership in the automotive field.

3.5 CAN topology

Due to the bus-topology, only a single ECU can allocate the CAN to transmit messages. Since nodes may wait for several periods for the bus allocation, an inter-node dependency and communication delays are invoked. Such an issue is hazardous for future automotive technologies, where real-time constraints are crucial. Hence, innovative reasoning tends to migrate CAN from the bus to a star topology. Gessner *et al.* [58] utilised a pair of coupled hubs to obtain a star structure. Compared to the conventional topology, a quantitative evaluation of profits entailed by the star disposition was conducted by virtue of a stochastic model in [59]. In addition, a CAN star-based fault injector was presented in [60]. As a result, the star-physical disposition accelerated the different diagnosis interventions.

One of the star topology advantages is assuring a wider range of network design choices. An important implication of this concern lies in the security aspect. It is difficult to apply hacking activities when the targeted vehicle has an unpredictable network topology.

3.6 CAN error-handling mechanism

With respect to the safety-critical context, future intelligent vehicles are sensitive to erroneous data exchange. IT can lead the control units to wrong critical decisions. Thus, the CAN reliability is closely related to its error-handling mechanism efficiency.

Accordingly, the feasibility of boosted or an entirely novel CAN error-handling processes has been largely discussed in the literature. For example, through the Poisson law-based model, Shah *et al.* [61] considered the impact faults on data-transmission to introduce a novel CAN error-handling algorithm. Notably, most of the achieved improvements in CAN error-handling system have dealt with the message improper redundant transmission. In case of error occurrence, messages are re-broadcasted until reaching a successful attempt. Definitely, mechanisms managing erroneous transmission-induced delays are highly recommended for the time-critical automotive systems. In [62], the over-transmission was limited by a maximal number of attempts, defined according to the available bandwidth. Similarly, the work presented in [63] approximated the retransmission bandwidth based on the statistical history of the message transmission.

3.7 CAN-based heterogeneous NCS

Future transportation means will include more systems of different specifications. Certainly, the CAN cannot fit all these system requirements. Thus, flexibility in the design of IVNCSs is essential for the automotive reliability. To convene distinct advantages of multiple protocols, e.g. LIN, FlexRay and Ethernet, heterogeneous networks have been lately designed [64]. For instance, the Flex-CAN architecture was regarded in [65] as advantageous to reinforce the CAN with high FlexRay determinism. Gateway components are indispensable to utilise several communication protocols side-by-side with the CAN [66]. Correspondingly, two kinds of possible architecture of futuristic in-vehicle networks have been defined. The central gateway-based architecture uses a unique gateway to coordinate between coexisting IVNCSs. Conversely, in the backbone-based architecture, gateways connect the primary network to a set of subnetworks. Fig. 2 highlights both types of architecture and points out expected networks to cooperate with the CAN in the future. Otherwise, the heterogeneous NCS may configure the in-vehicle network into a desired topology. This important issue is discussed in Section 3.5.

Integrating the CAN into larger networks covers also the off-board level. The wired-wireless networking ensures the vehicle inter-connectivity with its environment. CAN compatibility with Intranet and ISA100.11a, which are cost-effective communication protocols for standard applications, was studied in [67, 68]. Therefore, the obtained co-networks will be handful in assuring simpler and more reliable: infrastructure-to-vehicle (I2V), vehicle-to-infrastructure and vehicle-to-vehicle communication. Currently, this kind of communication is complex and passes through multiple steps. Specific components to act as interface and adapt received/transmitted data to the IVNCS are required [69]. Thanks to the off-board heterogonous communication, the vehicle extern-connectivity would be simpler and more reliable. Additionally, a wireless extension of CAN, called WCAN, has been already proposed to ensure non-automotive applications [70]. Now, problems as the improper data-exchange in case of a high-scalable WCAN network are still under study. Even so, this new WCAN conveys huge perspectives to the automotive area. Due to its harmonious features with the native protocol, WCAN chances in succeeding and predominating the I2V communication are strong. Likewise, the compatibility between heterogeneous IVNCSs with wireless sensor networks is expected to reduce wiring [71].

3.8 CAN security level

Making CAN robust against malicious practices is on the heart of the modern automotive involvements. Especially for future cars, anxiety about CAN system security has been increased recently. Due to advancements in vehicle connectivity, remotely-performed attacks have been applied [72]. Formerly, such attacks are practiced only through vehicle diagnostic and maintenance connectors. Several attacks proof-of-concepts, tested on real vehicles, have demonstrated CAN vulnerability to forbidden physical accesses [73].

Hence, attack scenarios have to be analysed and discussed according to the main security aspects, which are confidentiality, integrity and availability. First, it is crucial to make the vehicular communication at the top of confidentiality. After gaining access to the bus, hackers can reach the driver's private information. These spoofing activities are often provoked by a fake node, which stalls a normal node identifier [74]. Although data must not be modified by unauthorised members, the fake node broadcasts strange messages and threatens the data integrity. More influencing attacks destroy the system availability. When the bus-load attains 100% due to replay attacks, the whole network dysfunction is unavoidable [75].

Encryption, cryptographic and authentication are widely adopted solutions for security [76]. Integrity is also ensured by firewall systems that compare packets content with the exchanged-data history [77]. In fact, the stated algorithmic solutions, as authentication and cryptography, struggle to compromise between the communication load and their practical utility. An increase in the required memory size and the processing time is entailed. To overstep these limitations, hierarchical countermeasures have been developed. The network segmentation limits the ability of fake nodes to attack critical-safety ECUs. However, it complicates the in-vehicular design with more constraints [78].

Several intrusion detection systems (IDSs) are employed to detect attacks at an early stage [79]. Compared to other methods,

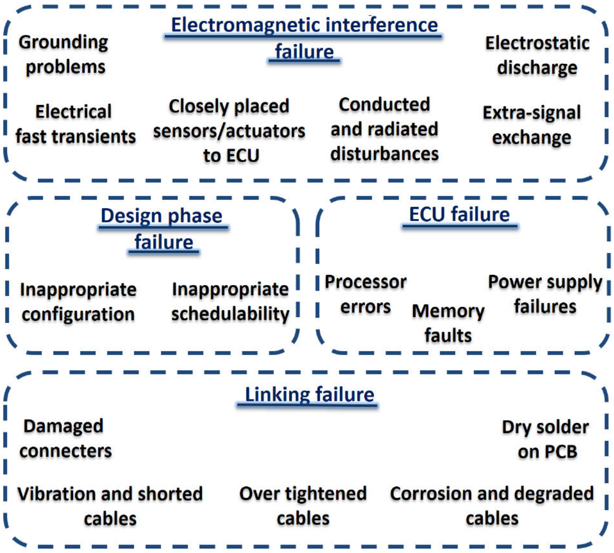

Fig. 3 *Common CAN failure sources*

IDSs are characterised by low computational demands and do not require changes in the standard CAN. A first class of IDSs is based on observing and analysing the exchanged data via the CAN [80]. Various data-driven approaches have been utilised in this context [81]. Nevertheless, accessing CAN packets to provide IDSs is costly and unreliable. As an alternative, physical-based IDSs have been introduced. The electrical behaviour of CAN nodes has been characterised for this aim [82]. Malicious attacks have been recognised through the noticed deviation in the ECUs timing properties and the abnormal increase in the bus load [83].

As a matter of fact, a large part of the mentioned improvements are expected to be standardised. CAN-FD is already appended to the CAN standard ISO 11898. Researches have upraised expectations about a more potent, effective, robust and secure CAN. In a way or another, the CAN is under amelioration to meet future transportation system requirements. It will heavily contribute to turn ambitions about full reliable vehicles into reality.

4 CAN system-level diagnosis

The in-road safety will not be met without the design of fault-aware intelligent vehicles. In the run time, faults may lead to an entire loss of the vehicle control. To ensure safety/reliability, efficient diagnosis functions have to be deployed over the CAN. The current section highlights recent contributions in enhancing the CAN-bus reliability through fault detection methods. Interest is only given to the network-level (system-level) diagnosis, i.e. global techniques targeting the overall CAN-based system (bus, nodes, sensors, actuator etc.). For further details about the node/device level, exhaustive overviews on different diagnosis approaches can be found in [84–86]. Readers have also to attentively distinguish between CAN-bus error handling mechanisms and methods that we are investigating herein. The error handling routines, built in CAN, have the responsibility of detecting erroneous data transmission. However, the system-level diagnosis addresses integrally all the functional and correctness aspects of the CAN-based process. Initially, recognising the origins of CAN failure helps to better understand the system-level diagnosis aims and challenges. The authors in [32, 60, 62, 87] drew attention to several fault sources. In particular, Suwatthikul *et al.* [88] classified these sources into peripheral (wiring and connecters faults) and internal (ECUs faults). Needless to say, admitting only these two bunches of methods ignores other sources. To present a rigorous idea about this point, we admit a more comprehensive classification:

EMIs failures: When external/internal electromagnetic noises propagate through the network, it could affect the components integrated circuits. In several cases, these disturbances can damage or abort the ECUs functioning.

Design phase failures: Failures entailed from wrong decisions taken at the design and the implementation phases.

Linking failures: It consists of intermittent or permanent loss of electrical connection. These failures have distinct impacts on the network operation relatively to its location (at the backbone cable, at the drop cable or at the ECU connecter etc.).

ECUs failures: Formal electronic failures, which threat the computational and functional aptitudes of each node from the network.

Hence, Fig. 3 enumerates common sources of failure assigned to the stated classes. At the best of the authors' knowledge, the CAN system-level diagnosis work has never been comprehensively reviewed by the literature. The remaining of this section oversees and classifies the existent work to discuss each diagnosis category benefits and drawbacks. The feasibility and relevance of the investigated approaches for future transportation systems are examined.

4.1 Physical-based diagnosis

Material-based solutions have been widely proposed to ensure diagnosis for the CAN. These approaches may be applied by supplying CAN with specific HW units dedicated for the diagnosis mission. In this way, diagnosis tasks are implemented on routers, hubs, gateways or simply on ordinary ECUs. The authors in [89, 90] have realised a router-based physical fault detection groundwork for CAN to enhance its safety relevant aspect. With a prior comprehension of the CAN node behaviour, routers have been programmed to isolate faults [90]. In the proposal of Gessner *et al.* [60], a diagnosis tool infrastructure afforded a spatial and time increased resolution for injecting node fault scenarios. A CAN-hub has enabled not only the entire controllability for fault injection, but also a high observability of node reactions against anomalies.

Alternatively, component duplication can also be adopted to guarantee an appropriate network behaviour. Gessner *et al.* [58] equipped all the CAN nodes with a couple of controllers to overcome the Byzantine failures for CAN redundant nodes. A comparator circuit was charged to trigger alerts once a difference was detected in controller outputs. In an attempt to avoid its high cost, Nath *et al.* [87] limited the material redundancy application to critical CAN nodes.

Without any modelling efforts or design struggle, the physical-based diagnosis is appreciated as quite simple and fully reliable. Aside from being expensive, there is little shortcoming to be considered when applying this methodology for an in-vehicular network. Undoubtedly, the additional material, imposed by the physical-diagnosis, emphasises the automotive complexity. Thus, it is crucial to analyse complications coming from adding materials to the network. Nevertheless, this concept remains efficient in providing automotive offline diagnosis boards [60, 91]. Notably, the use of multi-core automotive ECUs rather than single-core ones in the near future may restore the interest in the material diagnosis [92]. Indeed, the implementation of redundant diagnosis functions in different ECU-cores has succeeded CAN fault management [93].

4.2 Model-based diagnosis

Starting from its well-known success in performing device level failure analysis, the model-driven diagnosis has been extensively applied for CAN at the network level. Given its position as a link between nodes and the backbone bus, monitoring CAN transceivers is a pathway for diagnosing the overall system. Prodanov *et al.* [94] elaborated a multi-mode behavioural model associated to these devices. Both of faulty and nominal operating conditions were addressed. The comparison between the online-measured data and outputs of the realised model permitted reporting the network state. Suwatthikul *et al.* [88] developed a fuzzy system to pre-diagnose CAN failure. Faults were detected by analysing the accessible network signals. In this case of study, the diagnosis process was trained with experimental error frames generated from different disturbances.

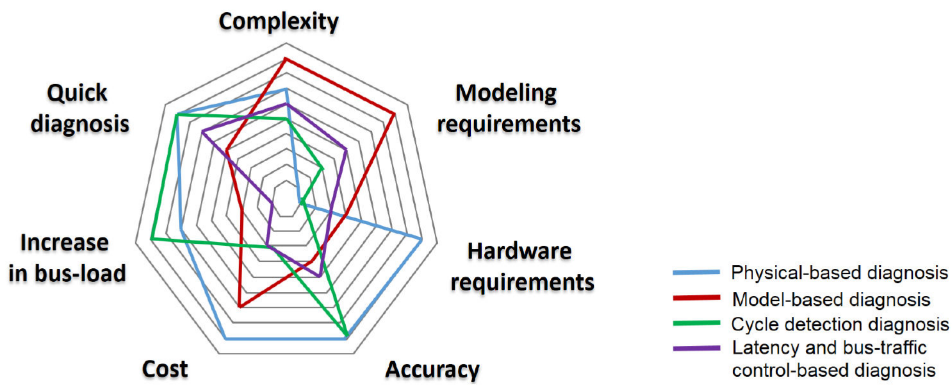

Fig. 4 *Characteristics covered by investigated system-level diagnosis methods*

More recently, an extensive research work has coped with the CAN intermittent connection (IC) failure via stochastic models. IC is a frequent source for CAN failure. Overcoming intermittent faults is not simple for the reason that this failure class is acting between the extremes of transient and permanent faults. Locating the damaged part of a cable is an arduous task, especially in extended networks. A special focus is given to decrease modelling errors and uncertainty in handling this issue. In [95], real error-frames were collected to construct an IC-failure predictive model. Afterwards, the maximal likelihood method was practiced recursively to estimate the model parameters. The recursion improved the IC fault detection quality by putting constraints on the error rate assigned to the estimated parameters. In [96], a stochastic model was utilised to formulate a CAN reliability metric, named MTTB (mean time to bus-off). In similar work, the stochastic properties, extracted from the transmission error contours, were a bridge to assess CAN reliability [97]. The greatest part from the IC detection work exploited the physical-layer data, which were not reliable and sensitive to interference. Zhang *et al.* [98] analysed error records in the link-layer data. Notwithstanding handling the IC problems under global interference, these methods are dedicated to deal with the wiring failure. Obviously, the in-vehicular communication requires a more holistic diagnosis. A recent modelling approach has focused on characterising the message-induced sequences instead of message content since the creation of message series is usually triggered by a particular event [99]. It is worth mentioning that the authors in [95–98] provide interesting comparison between stochastically estimated temporal distribution of error records and experimentally derived results.

Evidently, the model-driven approaches have presented many drawbacks as a network-level diagnosis strategy. Modelling the network multi-functional modes is a bit laborious. Intelligibly, CAN network designers have inevitably to alleviate the modelling imperfections and its misuse cases to reach a trustworthy onboard diagnosis. Even with passively extracting the stochastic features of the network, CAN model-driven diagnosis has costs. The real-time acquisition of error-frames through special devices is expensive and unreliable. Moreover, the probabilistic and/or heuristic nature of the existent models implies huge uncertainty in the diagnosis.

4.3 Cycle detection diagnosis (CDD)

A great part of the research community has shown its interest in developing cycle detection algorithms to settle diagnosis policies for CAN. These techniques rely on the mutual diffusion of periodic messages to detect failures by providing feedbacks about node states. When a feedback is not received in a definite time from a node, it is considered as damaged. Nath *et al.* [87] aimed to reduce the number of detection cycles performed by CDD. Nodes judged as fault-free are exonerated from checking in the next cycle. An approach permitting the reentry of repaired nodes into the network was proposed in [100]. The number of checking rounds was bounded and faulty nodes were rapidly distinguished.

Ideally, the CDD approaches are deterministic and reliable, as they are quick, uncomplicated and trustworthy. However, CAN timing detection approaches may increase the bus load. Hence, the stated algorithms usually eliminate (definitely or temporary) the non-responding nodes from the network. Since a node downfall may engender the shutdown of other nodes and possibly the whole system failure, the CDD approaches do not fit the automotive context, thus partially being applied only for a well-defined set of ECUs.

4.4 Latency and bus-traffic control-based diagnosis

As already stated, the great amount of interchanged data endangers todays' CAN-based automotive system reliability. High transmission rates may slow down or affect the overall system. The authors of [101–103] were pioneer researches dealing with CAN message transmission delays through concrete use-cases. However, due to its criticality, the risk of violating timing constraints when delivering a diagnosis message is much higher. The quick reaction against menaces is an elemental diagnosis requirement [84]. Little diagnosis work has been carried out to handle the CAN huge data-traffic and its induced latency. A first class of research has tried to diminish the CAN traffic to avoid its hazardous impact on failure management. Zhihong *et al.* [104] adopted a constrained communication concept for the CAN, where nodes were prohibited to successively re-broadcast the same values. Under this assumption, the rest of nodes consider that these values are still valid. CAN overloaded-bus side effects have been overcome by the deployment of decentralised on-board diagnosis in [105]. Instead of broadcasting diagnosis messages with normal operating data, all diagnosis reports were received by the ECU supervisor to make a global diagnosis decision. Notably, readers can find valuable and detailed experimental results of the concreate application of the bus-traffic control-based diagnosis in [105]. At this level, an important question arises concerning this tendency in controlling the bus traffic. Can these methods face the pervasive 'big data' trend and the growing complexity of automotive systems?

Indeed, the nature of many diagnosis methods emphasises this issue. For instance, data-driven diagnosis must always deal with massive data [106]. Restricting the data amounts addressed to a node that operates data-driven fault detection will damage the diagnosis quality. A more plausible work compromising between the CAN traffic and the diagnosis reliability was reported in [107]. It rectified latencies by implementing a synchronisation clock on the network.

Most of the examined studies in this section and references cited therein include a very rich comparative analysis based on experimental, analytical and extensive simulation work. Deductions derived from this interesting literature are exploited in this paper to present more comprehensive comparison. Underneath the above undertaken debate and the inspected literature, the comparison results between the reviewed CAN system-level diagnosis approaches are illustrated in Fig. 4. More importantly, aspects considered in the depicted comparison (complexity, accuracy, cost etc.) are the most crucial requirements of the in-vehicular diagnosis for modern vehicles. Obviously, none of the methods seems to be fully infallible. The CCD is more efficient than the remaining methods with respect to most requirements. However, it increases the bus load. The physical-based diagnosis is extremely quick and accurate. Despite its high cost, it may be useful in monitoring CAN segments ensuring communication

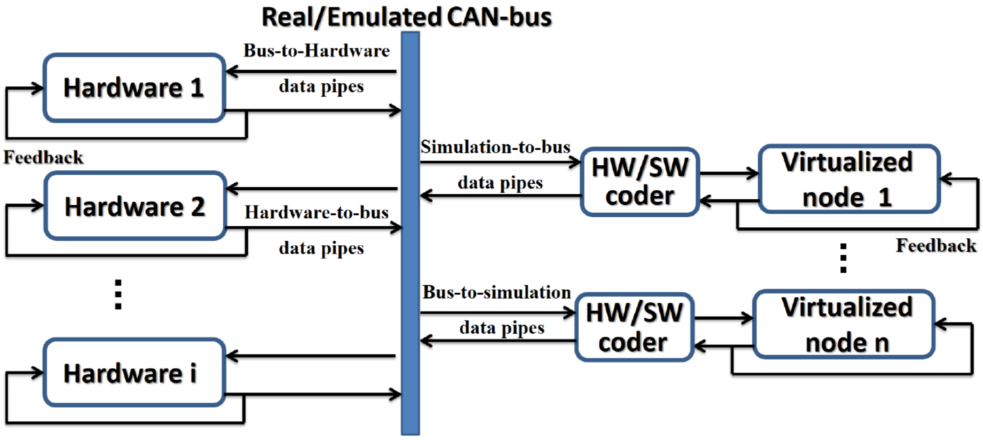

Fig. 5 *CAN-based HIL layout*

between sub-systems of safety-critical nature such as the risk management units, where rapid reactions against faults are crucial. To decrease its complexity, to avoid wasting time in modelling and to guarantee satisfactory performances in terms of accuracy, it is judicious to limit the model-based diagnosis application to CAN-based sub-systems of linear and simple behaviours. Opposite to the physical-based diagnosis, the bus-traffic control-based diagnosis is very slow and inaccurate. It should be only applied when the data traffic load is too much important. Therefore, the CAN system-level diagnosis policy must be well-tailored regarding the particularity of a given process. Especially for automotive embedded systems including several CAN-segments, different system-level diagnosis approaches can be joined simultaneously according to each segment feature.

5 Hardware in the loop

The HIL is a pervasive-applicability design and validation methodology. It provides testing capacities, which fit the new generation of distributed systems [108]. It plays also the role of a substitute for offline model-based simulations. Applying a model-driven approach for testing is difficult and unrealistic, especially when dealing with a multi-mode operational system [109]. Models are powerless in reproducing an over-changing system behaviour. Concerning the automotive sector, the HIL applications are unrestricted for CAN and cover all the in-vehicular networks [110, 111]. However, preoccupying the market-first position has helped to shape a considerable literature for HILs equipped with CAN-bus. The remaining of this section investigates the HIL basis and what it offers to IVNCS designers for intelligent vehicles. Elements defining the CAN-based HIL test quality with respect to its construction costs are analysed. Note that only HILs with CAN-bus backbone are investigated below.

The HIL consists in verifying prototypes at the system level before being interconnected with other nodes. Several executable code specifications must be checked and tuned before its deployment. In this sense, controllers implementation is realised by upgrading codes from the high-level model code (HLMC) initial format to a final prototype. Without any need for entire real-vehicle tests, a careful integration of real ECUs through the simulated functions takes place. The communication occurs either via a real physical CAN-bus and/or an emulated one [112]. Hence, imperative instructions must be followed to build an appropriate interaction between the HIL subsystems in the time as well as the value domain. On the electronic level, modules which adapt the HLMC code to real-time HW/SW execution are badly necessary [113]. Those modules convert the virtual component code to C/C++ which is more adapted to the machine language. With regard to the above mentioned, Fig. 5 presents the general CAN-based HIL middleware layout.

The employment of CAN HIL environments for academic goals is tremendous. Equipping research laboratories by HIL platforms is a key component in solving and demonstrating various under study aspects. Such plants discharge researchers from mastering complicated verification SW. Otherwise, the HIL testbed can act as didactic frameworks, which clarify CAN properties and exhibit automotive reliable practices. In the following, a concise review of work related to CAN is presented to look-over the HIL facilities.

For safety verification aims, the study depicted in [114] used the HIL testing method to assess a monitoring unit response-time. In this proposal, the real CAN-bus implementation was essential to get a realistic estimation of jitters and message latencies. A HIL CAN-board served to balance vigorously between the memory usage, the real-time performances and the accuracy of an energy management control in [115]. A HIL test provided an extreme visibility on several parameters to examine the robustness of a hierarchical transition control between driving modes in [116]. Zhao *et al.* [117] applied a HIL experiment where the manipulation of the time-span guaranteed a broader observability for parameters during the launching process. For accurate prototyping, the HIL established in [113] has assumed a prior knowledge of the error bounds in parameters. Similarly, the HIL performances accuracy was enhanced in [118] via proceeding filtering/signal calibration for noisy data acquisition systems. The HIL has recently become a tool to ensure vehicle automation. Driver-in-the-loop simulation has been realised to proceed the training phase for an intelligent/autonomous navigation approach while investigating safety-related issues [119]. As it can be seen from the literature, the HIL opens vast possibilities as:

- easy development/validation of control and diagnosis functions
- calibrating and exploring results of different configurations
- revealing real-time data analysis and run-time properties
- optimising automotive functions by results issued from various performance-cost tests (in terms of memory, energy consumption etc.).

Another line of work that must be attentively inspected is the use of CAN-based HILs for industrial large-scale purposes. Unfortunately, this latter is scarcely studied by the literature for confidentiality reasons. Indeed, a HIL is a fundamental step in the V-mode process, which regulates the vehicle development life cycle. Plenty of CAN-HIL testbeds have been delivered by automotive manufacturers. For instance, the battery management central unit is a commercial advanced HIL simulator, which is equipped with a configurable CAN [120]. Unlike its utility in verifying the network design, the HIL was applied successfully in monitoring an automotive manufacturing process in [121]. Huge efforts have been made to model real driving environments and outline component test plans. Compared with the academic use-case, an extra effort is spent in developing CAN-HILs for high volume production territories. This struggle arises from the challenge to attain the required fidelity level.

Oppositely to its general use-cases, the HIL reliability and accuracy in validating intelligent transportation systems must be guaranteed. At this point, it is judicious to explore factors ruling the HIL reliability and its development cost through several comparative studies. Comparing between the HIL test and the

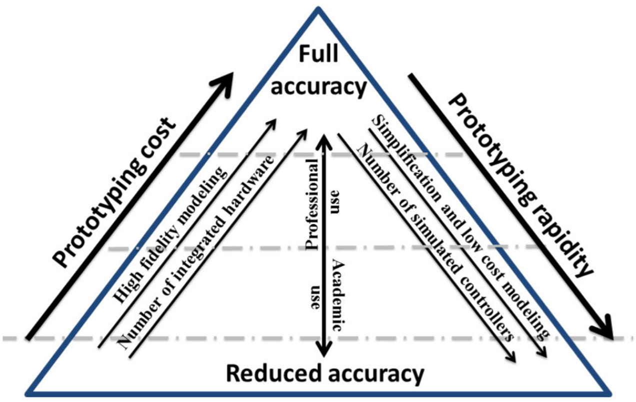

Fig. 6 *HIL test requirements and costs (scheme inspired from [11])*

conventional simulation results was the most significant contribution hailed from [122]. Even though both results were very close, dissimilarities were noticed during fast transients in the vehicle behaviour. In [123], adopting the HIL to compare two oscillation damping methods enabled considering the CAN sampling-time influence on tests. This step led to refined comparison results. A more rigorous benchmarking study was exhibited in [124]. Improved simulation was the main cause to reach a difference of 1% between the HIL and Simulink performances during the design of a vehicular component. By admitting results from a professional simulator as a reference, the impact of adding a brake model into the HIL plant was inspected in [125]. After this component integration, the error range in the estimation of energy consumption performances was drastically decreased from 11.6 to 0.6%. On the basis of the above comparative analysis provided in [122–125], where more rich numerical results are available, the CAN-based HIL accuracy is tightly linked to simulation quality. As illustrated in Fig. 6, involving the overall subsystems and integrating all the intervening parameters into the model-based simulations is the key to a high-fidelity CAN-based HIL. This conclusion is not restricted for the ECU simulations and holds true for all the simulated parts. It must be noted that limited performances of the simulated sensors and actuators can lead to improper results.

In return to the actuator models, the HIL prototypes may be classified into simple and complex testbeds [126]. Simple prototypes incorporate elementary excitation units and models of low dynamics, where only linear control theories are applied. To have a deeper insight of their responses, the complex prototypes utilise more sophisticated non-linear models of the actuation systems [127]. These models consider also the effects of coupling between electrostatic forces, the inertia properties, the friction and so on. [128]. A part from the dynamic properties, the actuator electrical aspects must be well examined to reach a satisfactory testbed performance [129]. In realistic circumstances, the actuation systems are prone to various disturbances, parameter variation and electrical noises. The stability of the simulated actuators must be analysed to avoid undesired system behaviour. Serious electro-vibration issues can originate from the actuators instability [130]. Consequently, real threats of wiring failure may affect the CAN-based HIL testbeds. Beside stability and delay analysis, it is strongly recommended to adopt actuator responses produced by a wide range of potential configurations to improve the HIL experimentations accuracy. Another efficient technique to meet accuracy is comparing the simulated responses with experimental results in both time and frequency domains.

Similarly, the electrical behaviour of the simulated sensors and inter-vehicular communication is tremendously important. Evidently, the accuracy of the CAN-bus HIL systems is closely related to the virtual sensors performances. In reality, several factors as the humidity or temperature variation can influence the sensing devices sensitivity. Correspondingly, the non-linearity, the hysteresis effect, the luminosity or the temperature-dependent behaviour are the most decisive aspects when modelling sensors [131]. Likewise, the use of environmental models (such as road and weather condition models) serves to ensure realistic performances of the HIL simulated sensing devices. Besides, these models permit to test the robustness of the perception subsystems against general problems such as shadowing and occlusion.

Despite its accurate testing capacities, the HIL is a time-demanding and expensive approach. It is also restricted for final design steps. At this stage, the HW layers of the intelligent vehicle embedded system are almost fixed. The most significant barrier for a wider application for the HIL in the automotive industry is the inaccuracy entailed by the network high scalability.

6 CAN real-time analysis

This section is devoted to review CAN real-time analysis. Roughly, RTA models are analytical concepts derived from real-time theories addressing rugged-embedded systems [132]. RTA assesses a given-system ability to react appropriately to events in a pre-defined duration and to meet hard deadlines. The need for real-time analysis has been emphasised by the data proliferation, which is imposed by tomorrow's vehicles. Especially when it targets the in-vehicular communication, end-to-end analysis must encompass all the system timing properties. Correspondingly, RTA examines imperatively data flows, event processing and timing dependencies [133]. The seminal work of Tindell was the first known formalisation of basic CAN analysis [134]. By time, several theories have been suggested to advance RTA for the CAN. The RTA models in their latest shapes are built principally around three central components:

- *CAN frame maximum transmission time*: It is the largest period required to transfer a single CAN frame. Generally, this parameter is recognised directly across the frame payload and the transmission time of one bit.
- *Maximum release jitter*: It is the time lying between the message instance and the beginning of its queuing.
- *Queuing delays*: They are higher and lower priority messages queuing block-time during busy CAN periods.

Otherwise, different statistical studies in computing end-to-end response times have been carried to fill gaps entailed by unavailable information about CAN configurations [135]. To avoid pessimistic results of CAN worst-case response times (WCRT), a constrained probabilistic model-based WCRT estimation was adopted in [136]. Stochastic models integrated the probability of erroneous communication and fault occurrence into ordinary RTA [61, 137]. Similarly, the proposal of Zeng *et al.* [138] bounded CAN response time via probability with the consideration of system-sampling delays.

Since RTA neglects several implementation details, its algorithms are performed only for a theoretical scope for the design of CAN-based intelligent navigation systems. Plenty of design inappropriate assumptions may mislead the timing analysis. It was demonstrated in [139] that messages would miss their conventional RTA-based estimated deadlines if failure probabilities were ignored. 'Data age constraint', i.e. maximal time required to data propagate through multi-rate effect chains, is another example of inadequacy sources in RTA models [140]. Consequently, questions about how to refine RTA models would progressively find answers in the automotive community.

A deeper look at the studied CAN-based system specifications is the key to estimate confidant timing performances. Besides, RTA must tackle all potential transmission scenarios. In this sense, the work of Shuai *et al.* [141] incorporated Taylor series expansion into RTA to accurately approximate the network-induced latencies. Davis *et al.* [142] formulated adequate RTA algorithms, which covered networks including nodes of various priority attributes (FIFO queues, priority queues etc.). The proposal of Mubeen *et al.* [143] addressed CAN timing analysis with different message schedule modes (offset-based schedule and arbitrary jitter messages). The writers in [144] sought for forecasting response-time upper-bounds of mixed periodic and sporadic CAN messages. The authors involved the impact of SW and HW limitations in their models. The response time of gateways was explored in [65] to outline end-to-end delays of heterogeneous networks including the

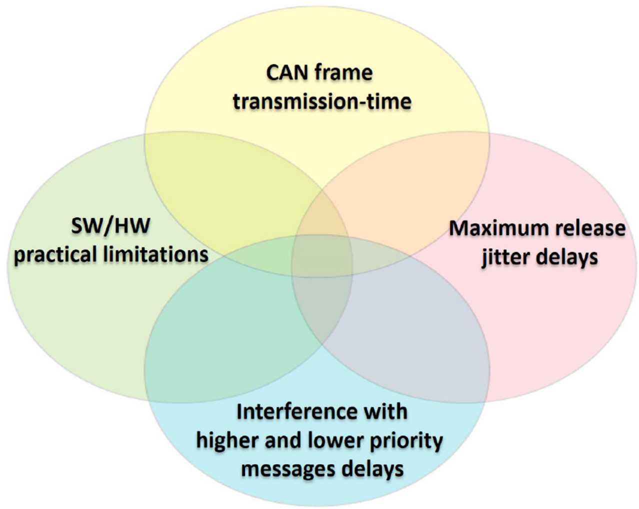

Fig. 7 *CAN real-time analysis main components*

CAN. Moreover, the role of 'component local analysis' in anticipating correct message transmission time was focused on. The WCRT of a message processing in an automotive gateway with multi-core architecture has been recently studied in [145]. From this sight, Fig. 7 illustrates CAN analysis requirements and main components.

Despite struggles in improving RTA models, its exactness is still a vast controversial issue. Many environmental factors as humidity or high temperature arbitrary influence the automotive embedded-system functioning. From this perspective, RTA findings remain a useful information support, which can prevent early wrong steps in the design of intelligent automotive systems. However, it cannot play as a final validation tool. One potential solution to make RTA adequate for automotive intelligent system reliability analysis reposes on confidence intervals. This solution has proven its efficiency in enhancing results of formal verification SW. Seemingly, RTA may benefit from this accuracy concept to consider quantitative and qualitative uncertainties.

7 CAN computer-aided design tools

Current section reveals how commercial tools act to ensure the reliability of CAN-based systems. The number of prototyping frameworks, which assist the design of CAN vehicular networks, is increasing. Companies, as Vector, Arcticus and Symtavision, are leaders in developing in-vehicular engineering solutions. To satisfy customers, these companies work on enlarging their products application scope by supplying new utilities. Each tool can be described with respect to its typical use-case. Network simulation, testing prototypes, data logging and managing the network architecture are the main tasks of the promoted tools. More notably, several tools can actually perform aftermarket performance analysis. Tools providing in-field data acquisition and analysis facilitate CAN maintenance and repair procedures [146]. Another functionality, which is expected to be incorporated soon in these tools, is to deploy CAN security countermeasures.

According to [147], validation platforms examine CAN networks along three dimensions: the network load, the transmission delay and the SW–HW integrity. The average bus-occupancy rate, CAN-bus frame conflict tests and delay diagrams are typical metrics to access the bus features. In view of its high cost, CAN-proven SW solutions have been occasionally reported in the literature. Table 1 exploits the few existent studies in this area to uncover the criteria of several frameworks and their interventions during the CAN life cycle.

Compared to commercial tools, the open-source CAN CAD is quite limited. Most free SW is used to communicate with the CAN in the form of reading and writing. With all its advantages, CAN CAD tools have diverse drawbacks. Such SW requires a considerable experience to master complex development environments. The varied analysis provided by these products is established according to confidential assumptions. In this respect, CAN networks implemented in intelligent transportation systems and which are designed with an unfamiliar electronic hierarchy or a new task schedule cannot be validated properly by such tools with the required confidence.

8 Conclusion and future directions

In this work, we have surveyed several aspects related to CAN reliability in the automotive domain. Currently, transportation systems are evolving towards fulfilling the dream of autonomous vehicles, which are predicted to be a very interleaving and complex process. At the same time, CAN reliability engineering practices must evolve regularly and CAN growing complexity needs to be followed attentively. Indeed, there is an absolute coupling of CAN reliability with future transportation system safety. Several safety-oriented mechanisms are implemented over the CAN in modern cars. These mechanisms perform critical safety functionalities. A proper operating of these functionalities is not guaranteed without ensuring CAN reliability. Enhancements for the CAN, which are related explicitly to vehicle safety, touch different design issues. More potent communication is provided to make the CAN support the huge number of functionalities embedded in its nodes. Another remarkable aspect from CAN improvements consists in addressing the timing performances as a priority concern. This directive reflects the real need to make intelligent automotive systems more reactive in dealing with failure potentialities. In fact, a stronger link between CAN reliability and in-road safety is now under construction. CAN reliability research opens opportunities for larger-scale implementations. AI-based accident prevention systems will be soon implemented over CAN. These systems use data linked to risk-influencing factors (steering wheel angle, brake-pedal pressure etc.) to perform safe navigation [162, 163].

On the other hand, the automotive diagnosis has already overstepped the ECU level to act holistically on the system level. At this level, the high scalability of the automotive network entails two main difficulties. First, diagnosis must consider CAN-imposed material constraints like latencies, messages priority arbitration and so on. Second, since it acts on a wide dimension, multiple uncertainty sources can enormously weaken the diagnosis functioning. The diagnosis accuracy becomes vital for the CAN. Thus, deterministic approaches emerge progressively for this aim.

Changes in CAN verification techniques along the vehicle life cycle to fit the design requirements of modern intelligent vehicles have been also manifested in the literature. Again, encountering uncertainty impacts on reliability engineering practices is the most urgent object sought by the automotive community. Therefore, verification approaches, especially RTA and HIL, are moving from their former theoretical form to enclose more practical issues. CAN CAD SW has been steadily generalised to all CAN development phases. Yet, anxiousness about uncertainty impacts remain existent. The reliability of tomorrow's in-vehicular systems is too critical because it depends on several overlapping issues. A huge number

Table 1 CAN-dedicated design and validation tools

Tool	Company	Use-cases, features and advantages	Nature	Ref.
CANoe	Vector	• support ECU/entire network simulation and multi-functional analysis at early and final phases		
		• assist diagnostic function development		
		• permit customised test scenarios design based on physical setups		
		• achieve test-results under multi-format reports (XML, HTML etc.)	commercial	[148]
		• outperform HIL-based experimentations and offline/online tests		[79]
		• ensure connection with powerful tools (CANalayzer, Matlab etc.) and database systems		[75]
		• perform CAN-based heterogeneous network analysis		
		• main programming language: CAPL		
CANalyzer	Vector	• record and log operational data to realise aftermarket analysis		
		• assure great compatibility with numerous data-acquisition HW platforms		
		• provide automatic interpretation of network data traffic	commercial	[149]
		• assist diagnostic development but not include testing services		[150]
		• main programming language: CAPL		
		• supply network analysis, fault analysis and testing at early development phases		
		• support ECU analogic modelling and multi-domain simulation		
Saber	Synopsys	• evaluate power storage and conversion components performances	commercial	[151]
		• incorporate wiring features in CAN network analysis		[152]
		• main programming language: MAST and VHDL-AMS		
SymTA/S	Symtavision	• support ECU development and optimisation from early to final manufacturing phases		
		• outperform ECU local analysis (nodes utilisation rate based-RTA)	commercial	[153]
		• support various scheduling methods (preemptive/non preemptive methods etc.)		[154]
Volcano Network Architect	Mentor graphics	• assist networked system early development and test validation		
		• assess vehicle functions performances by implying the network architecture into RTA	commercial	[155]
		• support network analysis only for CAN and LIN		
Rubus-ICE	Arcticus	• provide timing analysis and assist component-based simulation		
		• support periodic, sporadic and mixed end-to-end message transmission analysis	commercial	[153]
		• optimise resource utilisation		[156]
		• provide Simulink configurable blocks to develop CAN testing		
RTI CAN		• permit accessing and managing data files from Simulink		
MultiMessage	dspace	• guarantee great compatibility with several commercial HILs	commercial	[157]
Blockset		• perform CAN FD and J1393 analysis		
		• specify gateway block to analyse communication between CAN segments		
		• permit interaction between CAN layers and Linux		
Socket CAN	Volkswagen	• include collection of user-space utilities:	open	[158]
	AG	• enable CAN data queuing and filtering functionalities	source	[159]
		• facilitate sniffing and reverse engineering applications		
Wireshark	IXXAT	• Perform CAN bus interfacing and analyse CAN under Linux		
		• enable data capture from real CAN segments	open	[160]
		• assist reverse engineering and hacking activity to perform attacks proof of concepts	source	[161]
		• furnish statistical graphical plots for logged data		

of realistic testing scenarios and hundreds of millions of miles must be driven to demonstrate the autonomous vehicle reliability [164, 165]. For the CAN-bus HIL system, its accuracy is closely related to the simulated part performances. The HIL-simulated part design must be up-to-date with new aspects imposed by the technological advancements. Issues as the connectivity and scalability of wirelessly interconnected sensors must be investigated while constructing HIL [166, 167]. Likewise, the use of environmental models (such as road and weather condition models) serves to ensure realistic performances of HIL-simulated sensing devices. Clearly, new interdisciplinary research fields are steadily emerging in the transportation systems/IVNCS community (CPSs, IT security, scheduling etc.). Consequently, the automotive design is turning into a constrained multi-aspect-aware design. It is not feasible without considering security, real-time constraints, robustness to faults and so on. There is also a clear intention to unify between all the vehicular validation techniques. It aims to reach full accuracy in evaluating reliability/safety related issues by joining all the advantages of these techniques. Recently, a novel CAN extension, which may perform CAN emulation and real-time execution, has been introduced [158]. This innovation is promising in permitting simultaneous co-testing via HIL and CAN CAD tools.

The evolution in the IVNCS field and CAN reliability engineering practices has a deep impact on the society. The latter has taken advantage of the increase in road safety thanks to the reliable design of CAN-based intelligent navigation systems. The IVNCS concept with the reliability certification techniques has offered the possibility of integrating various driver assistance systems into modern vehicles. However, many hacker attacks and incidents caused by the vulnerability of INVCSs have raised fears and created trust gaps on intelligent vehicles [168]. Hence, the society does not trust yet stand-alone products. As a result, the present focus on reliability issues must be kept-up and enhanced.

To master all reliability and safety problems resulting from vehicle automation, uncertainty and failure probabilities must be included at the decision-making level (to ensure the safe navigation of the vehicle). The future directions are making the vehicle isolated control units aware of IVNCS material constraints. Now, transportation risk management strategies are investigating only in-road hazards. In contrast, vehicular navigation is not safe without solving issues related to IVNCS capacities in reacting appropriately to environmental data. Intra/in-vehicle communication latencies may increase in an unpredicted way given in-road situation criticality. From this scope, risk management strategies will focus on integrating CAN constraints into the hazard identification phase [169–171]. Adaptive and apprehensive control will be the best solution to overcome IVNCS-induced risks and guarantee the safety of next-generation vehicles.

9 Acknowledgment

The present work is supported by the WOW (Wide Open to the World) program of the CAP 20–25 project. It receives also the support of IMobS3 Laboratory of Excellence (ANR-10-LABX-16-01).

10 References

[1] Ivaki, N., Laranjeiro, N., Araujo, F.: 'A survey on reliable distributed communication', *J. Syst. Softw.*, 2018, **137**, pp. 713–732

[2] Tang, W., Daoutidis, P.: 'Distributed control and optimization of process system networks: a review and perspective', *Chin. J. Chem. Eng.*, 2019, **27**, (7), pp. 1461–1473

[3] Mahmoud, M.S., Hamdan, M.M.: 'Fundamental issues in networked control systems', *IEEE/CAA J. Autom. Sinica*, 2018, **5**, (5), pp. 902–922

[4] Zhang, D., Shi, P., Wang, Q.G., *et al.*: 'Analysis and synthesis of networked control systems: A survey of recent advances and challenges', *ISA Trans.*, 2017, **66**, pp. 376–392

[5] Ge, X., Yang, F., Han, Q.L.: 'Distributed networked control systems: a brief overview', *Inf. Sci.*, 2017, **380**, pp. 117–131

[6] Durisic, D., Nilsson, M., Staron, M., *et al.*: 'Measuring the impact of changes to the complexity and coupling properties of automotive software systems', *J. Syst. Softw.*, 2013, **86**, (5), pp. 1275–1293

[7] Martínez-Díaz, M., Soriguera, F., Pérez, I.: 'Autonomous driving: a bird's eye view', *IET Intell. Transp. Syst.*, 2019, **13**, (4), pp. 563–579

[8] Wei, S., Yu, D., Lin Guo, C., *et al.*: 'Survey of connected automated vehicle perception mode: from autonomy to interaction', *IET Intell. Transp. Syst.*, 2019, **13**, (3), pp. 495–505

[9] Song, X., Ling, Y., Cao, H., *et al.*: 'Cooperative vehicle localisation method based on the fusion of gps, inter-vehicle distance, and bearing angle measurements', *IET Intell. Transp. Syst.*, 2019, **13**, (4), pp. 644–653

[10] Elliott, D., Keen, W., Miao, L.: 'Recent advances in connected and automated vehicles', *J. Traffic Transp. Eng.*, 2019, **6**, (2), pp. 109–131

[11] Adouane, L.: '*Autonomous vehicle navigation: from behavioral to hybrid multi-controller architectures*' (Taylor & Francis CRC Press, Boca Raton, FL, USA, 2016), ISBN: 9781498715584

[12] Marina Martinez, C., Heucke, M., Wang, F., *et al.*: 'Driving style recognition for intelligent vehicle control and advanced driver assistance: a survey', *IEEE Trans. Intell. Transp. Syst.*, 2018, **19**, (3), pp. 666–676

[13] Bock, F., Siegl, S., Bazan, P., *et al.*: 'Reliability and test effort analysis of multi-sensor driver assistance systems', *J. Syst. Archit.*, 2018, **85–86**, pp. 1–13

[14] Wang, P., Chen, Y., Wang, C., *et al.*: 'Development and verification of cooperative adaptive cruise control via lte-v', *IET Intell. Transp. Syst.*, 2019, **13**, (6), pp. 991–1000

[15] Kugler, C., Kowalewski, S., Richenhagen, J., *et al.*: 'Metrics-based strategies for quality assurance of automotive embedded software', 17. Int.es Stuttgarter Symp., Springer Fachmedien Wiesbaden, 2017, pp. 711–730, ISBN: 978-3-658-16988-6

[16] Haghighatkhah, A., Banijamali, A., Pakanen, O.P., *et al.*: 'Automotive software engineering: a systematic mapping study', *J. Syst. Softw.*, 2017, **128**, pp. 25–55

[17] Grüttner, K., Görgen, R., Schreiner, S., *et al.*: 'Contrex: design of embedded mixed-criticality control systems under consideration of extra-functional properties', *Microprocess. Microsyst.*, 2017, **51**, pp. 39–55

[18] Rho, J., Azumi, T., Nakagawa, M., *et al.*: 'Scheduling parallel and distributed processing for automotive data stream management system', *J. Parallel Distrib. Comput.*, 2017, **109**, pp. 286–300

[19] Jiang, Y., Yin, S.: 'Recursive total principle component regression based fault detection and its application to vehicular cyber-physical systems', *IEEE Trans. Ind. Inf.*, 2018, **14**, (4), pp. 1415–1423

[20] Maro, S., Steghöfer, J.P., Staron, M.: 'Software traceability in the automotive domain: challenges and solutions', *J. Syst. Softw.*, 2018, **141**, pp. 85–110

[21] García Valls, M., Perez Palacin, D., Mirandola, R.: 'Pragmatic cyber physical systems design based on parametric models', *J. Syst. Softw.*, 2018, **144**, pp. 559–572

[22] Lun, Y.Z., D'Innocenzo, A., Smarra, F., *et al.*: 'State of the art of cyber-physical systems security: an automatic control perspective', *J. Syst. Softw.*, 2019, **149**, pp. 174–216

[23] Chang, W., Goswami, D., Chakraborty, S., *et al.*: 'Memory-aware embedded control systems design', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2017, **36**, (4), pp. 586–599

[24] Álvarez, J.D., Risco Martín, J.L., Colmenar, J.M.: 'Multi-objective optimization of energy consumption and execution time in a single level cache memory for embedded systems', *J. Syst. Softw.*, 2016, **111**, pp. 200–212

[25] Caruntu, C.F., Lazar, C., Vargas, A.N.: 'Chance-constrained model predictive control for vehicle drivetrains in a cyber-physical framework'. In: 2017 Int. Conf. on Engineering, Technology and Innovation (ICE/ITMC), Funchal, Portugal, 2017, pp. 1137–1144

[26] Kim, D.S., Tran Dang, H.: '*Communication using controller area network protocol*' (Springer International Publishing, Cham, 2019), pp. 31–41

[27] Gao, X., Su, D.: 'Suppression of a certain vehicle electrical field and magnetic field radiation resonance point', *IEEE Trans. Veh. Technol.*, 2018, **67**, (1), pp. 226–234

[28] Shirai, R., Shimizu, T.: 'Study of emi caused by buck converter on controller area network'. Int. Power Electronics Conf., Niigata Japan, 2018, pp. 3309–3314

[29] Chuang, C.H., Ker, M.D.: 'System-level esd protection for automotive electronics by co-design of tvs and can transceiver chips', *IEEE Trans. Device Mater. Reliab.*, 2017, **17**, (3), pp. 570–576

[30] Kang, S., Seong, J., Lee, M.: 'Controller area network with flexible data rate transmitter design with low electromagnetic emission', *IEEE Trans. Veh. Technol.*, 2018, **67**, (8), pp. 7290–7298

[31] Bouguet, C., Ginot, N., Batard, C.: 'Communication functions for a gate driver under high voltage and high d*v*/d*t*', *IEEE Trans. Power Electron.*, 2018, **33**, (7), pp. 6137–6146

[32] Fontana, M., Hubing, T.H.: 'Characterization of can network susceptibility to eft transient noise', *IEEE Trans. Electromagn. Compat.*, 2015, **57**, (2), pp. 188–194

[33] Roque, A.S., Pohren, D., Michelin, T.J., *et al.*: 'Eft fault impact analysis on performance of critical tasks in intravehicular networks', *IEEE Trans. Electromagn. Compat.*, 2017, **59**, (5), pp. 1415–1423

[34] Fontana, M., Canavero, F.G., Perraud, R.: 'Integrated circuit modeling for noise susceptibility prediction in communication networks', *IEEE Trans. Electromagn. Compat.*, 2015, **57**, (3), pp. 339–348

[35] Daniel, A., Subburathinam, K., Paul, A., *et al.*: 'Big autonomous vehicular data classifications: towards procuring intelligence in its', *Veh. Commun.*, 2017, **9**, pp. 306–312

[36] Marcon Zago, G., Pignaton de Freitas, E.: 'A quantitative performance study on can and can fd vehicular networks', *IEEE Trans. Ind. Electron.*, 2018, **65**, (5), pp. 4413–4422

[37] Choi, E., Han, S., Lee, J., *et al.*: 'Compatibility analysis of the turbo controller area network (turbo can)', *IEEE Trans. Veh. Technol.*, 2018, **67**, (6), pp. 5146–5157

[38] Cena, G., Bertolotti, I.C., Hu, T., *et al.*: 'Can with extensible in-frame reply: protocol definition and prototype implementation', *IEEE Trans. Ind. Inf.*, 2017, **13**, (5), pp. 2436–2446

[39] Ziermann, T., Wildermann, S., Teich, J.: 'Can + : A new backward-compatible controller area network (can) protocol with up to 16 × higher data rates'. Design, Automation Test in Europe Conf. Exhibition, Nice France, 2009, pp. 1088–1093

[40] Wu, Y.J., Chung, J.G.: 'Efficient controller area network data compression for automobile applications', *Front. Inf. Technol. Electron. Eng.*, 2015, **16**, (1), pp. 70–78

[41] Woo, S., Jo, H.J., Kim, I.S., *et al.*: 'A practical security architecture for invehicle can-fd', *IEEE Trans. Intell. Transp. Syst.*, 2016, **17**, (8), pp. 2248–2261

[42] Davis, R.I., Burns, A., Bril, R.J., *et al.*: 'Controller area network (can) schedulability analysis: refuted, revisited and revised', *Real-Time Syst.*, 2007, **35**, (3), pp. 239–272

[43] Xie, G., Zeng, G., Liu, L., *et al.*: 'High performance real-time scheduling of multiple mixed-criticality functions in heterogeneous distributed embedded systems', *J. Syst. Archit.*, 2016, **70**, pp. 3–14

[44] Park, M., Piao, X.: 'Enhanced utilization bound of rate-monotonic scheduling in controller area networks', *Inf. Process. Lett.*, 2014, **114**, (11), pp. 603–606

[45] Cao, W., Wu, Y., Chang, Y., *et al.*: 'Speed synchronization control for integrated automotive motor-transmission powertrains over can through a co-design methodology', *IEEE Access*, 2018, **6**, pp. 14106–14117

[46] Li, M., Chen, Y.: 'Robust adaptive sliding mode control for switched networked control systems with disturbance and faults', *IEEE Trans. Ind. Inf.*, 2019, **15**, (1), pp. 193–204

[47] Schmidt, K.W.: 'Robust priority assignments for extending existing controller area network applications', *IEEE Trans. Ind. Inf.*, 2014, **10**, (1), pp. 578–585

[48] Ding, J., Sun, S., Ma, J., *et al.*: 'Fusion estimation for multi-sensor networked systems with packet loss compensation', *Inf. Fusion*, 2019, **45**, pp. 138–149

[49] Jiang, B., Chen, M., Chen, F.: 'A network interface device for networked control system with time-driven mode', *Microprocess. Microsyst.*, 2019, **64**, pp. 1–11

[50] Zhang, D., Zhou, Z., Jia, X.: 'Network-based pi control for output tracking of continuous-time systems with time-varying sampling and network-induced delays', *J. Franklin Inst.*, 2018, **355**, (12), pp. 4794–4808

[51] Li, W., Zhu, X., Ju, J.: 'Hierarchical braking torque control of in-wheel-motordriven electric vehicles over can', *IEEE Access*, 2018, **6**, pp. 65189–65198

[52] Zhang, H., Shi, Y., Wang, J., *et al.*: 'A new delay-compensation scheme for networked control systems in controller area networks', *IEEE Trans. Ind. Electron.*, 2018, **65**, (9), pp. 7239–7247

[53] Liu, Y., Zhu, X., Zhang, H., *et al.*: 'Improved robust speed tracking controller design for an integrated motor-transmission powertrain system over controller area network', *IEEE/ASME Trans. Mechatronics*, 2018, **23**, (3), pp. 1404–1414

[54] Cena, G., Bertolotti, I.C., Hu, T., *et al.*: 'A mechanism to prevent stuff bits in can for achieving jitterless communication', *IEEE Trans. Ind. Inf.*, 2015, **11**, (1), pp. 83–93

[55] Cena, G., Bertolotti, I.C., Hu, T., *et al.*: 'Fixed-length payload encoding for low-jitter controller area network communication', *IEEE Trans. Ind. Inf.*, 2013, **9**, (4), pp. 2155–2164

[56] Cena, G., Bertolotti, I.C., Hu, T., *et al.*: 'On a family of run length limited, block decodable codes to prevent payload-induced jitter in controller area networks', *Comput. Stand. Interfaces*, 2013, **35**, (5), pp. 536–548

[57] Sagstetter, F., Lukasiewycz, M., Chakraborty, S.: 'Generalized asynchronous time-triggered scheduling for flexray', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2017, **36**, (2), pp. 214–226

[58] Gessner, D., Barranco, M., Proenza, J.: 'Design and verification of a media redundancy management driver for a can star topology', *IEEE Trans. Ind. Inf.*, 2013, **9**, (1), pp. 237–245

[59] Barranco, M., Proenza, J., Almeida, L.: 'Quantitative comparison of the errorcontainment capabilities of a bus and a star topology in can networks', *IEEE Trans. Ind. Electron.*, 2011, **58**, (3), pp. 802–813

[60] Gessner, D., Barranco, M., Ballesteros, A., *et al.*: 'Sfican: A star-based physical fault-injection infrastructure for can networks', *IEEE Trans. Veh. Technol.*, 2014, **63**, (3), pp. 1335–1349

[61] Shah, M.B.N., Husain, A.R., Aysan, H., *et al.*: 'Error handling algorithm and probabilistic analysis under fault for can-based steer-by-wire system', *IEEE Trans. Ind. Inf.*, 2016, **12**, (3), pp. 1017–1034

[62] Shah, M.B.N., Husain, A.R., Punekkat, S., *et al.*: 'A new error handling algorithm for controller area network in networked control system', *Comput. Ind.*, 2013, **64**, (8), pp. 984–997

[63] Short, M., Sheikh, I., Rizvi, S.A.I.: 'A transmission window technique for can networks', *J. Syst. Archit.*, 2016, **69**, pp. 15–28

[64] Lee, Y.S., Kim, J.H., Jeon, J.W.: 'Flexray and ethernet avb synchronization for high qos automotive gateway', *IEEE Trans. Veh. Technol.*, 2017, **66**, (7), pp. 5737–5751

[65] Lange, R., de Oliveira, R.S., Vasques, F.: 'A reference model for the timing analysis of heterogeneous automotive networks', *Comput. Stand. Interfaces*, 2016, **45**, pp. 13–25

[66] Kim, J.H., Seo, S.H., Hai, N.T., *et al.*: 'Gateway framework for in-vehicle networks based on can, flexray, and ethernet', *IEEE Trans. Veh. Technol.*, 2015, **64**, (10), pp. 4472–4486

[67] Cena, G., Bertolotti, I.C., Hu, T., *et al.*: 'Seamless integration of can in intranets', *Comput. Stand. Interfaces*, 2016, **46**, pp. 1–14

[68] Rezha, F.P., Saputra, O.D., Shin, S.Y.: 'Extending can bus with isa100.11a wireless network', *Comput. Stand. Interfaces*, 2015, **42**, pp. 32–41

[69] Wang, Y., Li, X., Yao, H.: 'Review of trajectory optimisation for connected automated vehicles', *IET Intell. Transp. Syst.*, 2019, **13**, (4), pp. 580–586

[70] Ng, W.L., Ng, C.K., Ali, B.M., *et al.*: 'Performance evaluation of wireless controller area network (wcan) using token frame scheme', *Wirel. Pers. Commun.*, 2013, **72**, (4), pp. 1847–1873

[71] Tavakoli, R., Nabi, M., Basten, T., *et al.*: 'Topology management and tsch scheduling for low-latency convergecast in in-vehicle wsns', *IEEE Trans. Ind. Inf.*, 2019, **15**, (2), pp. 1082–1093

[72] Wang, L., Liu, X.: 'Secure cooperative communication scheme for vehicular heterogeneous networks', *Veh. Commun.*, 2018, **11**, pp. 46–56

[73] Woo, S., Jo, H.J., Lee, D.H.: 'A practical wireless attack on the connected car and security protocol for in-vehicle can', *IEEE Trans. Intell. Transp. Syst.*, 2015, **16**, (2), pp. 993–1006

[74] Iehira, K., Inoue, H., Ishida, K.: 'Spoofing attack using bus-off attacks against a specific ecu of the can bus'. Consumer Communications Networking Conf., Las Vegas US, 2018, pp. 1–4

[75] Murvay, P.S., Groza, B.: 'Security shortcomings and countermeasures for the sae j1939 commercial vehicle bus protocol', *IEEE Trans. Veh. Technol.*, 2018, **67**, (5), pp. 4325–4339

[76] Hoppe, T., Kiltz, S., Dittmann, J.: 'Security threats to automotive can networks—practical examples and selected short-term countermeasures', *Reliab. Eng. Syst. Saf.*, 2011, **96**, (1), pp. 11–25

[77] Pan, L., Zheng, X., Chen, H.X., *et al.*: 'Cyber security attacks to modern vehicular systems', *J. Inf. Secur. Appl.*, 2017, **36**, pp. 90–100

[78] Mortellec, A.L., Clarhaut, J., Sallez, Y., *et al.*: 'Embedded holonic fault diagnosis of complex transportation systems', *Eng. Appl. Artif. Intell.*, 2013, **26**, (1), pp. 227–240

[79] Groza, B., Murvay, P.: 'Efficient intrusion detection with bloom filtering in controller area networks', *IEEE Trans. Inf. Forensics Sec.*, 2019, **14**, (4), pp. 1037–1051

[80] Woo, S., Moon, D., Youn, T., *et al.*: 'Can id shuffling technique (cist): moving target defense strategy for protecting in-vehicle can', *IEEE Access*, 2019, **7**, pp. 15521–15536

[81] Han, M.L., Kwak, B.I., Kim, H.K.: 'Anomaly intrusion detection method for vehicular networks based on survival analysis', *Veh. Commun.*, 2018, **14**, pp. 52–63

[82] Choi, W., Jo, H.J., Woo, S., *et al.*: 'Identifying ecus using inimitable characteristics of signals in controller area networks', *IEEE Trans. Veh. Technol.*, 2018, **67**, (6), pp. 4757–4770

[83] Ji, H., Wang, Y., Qin, H., *et al.*: 'Investigating the effects of attack detection for in-vehicle networks based on clock drift of ecus', *IEEE Access*, 2018, **6**, pp. 49375–49384

[84] Tidriri, K., Chatti, N., Verron, S., *et al.*: 'Bridging data-driven and model-based approaches for process fault diagnosis and health monitoring: a review of researches and future challenges', *Annu. Rev. Control*, 2016, **42**, pp. 63–81

[85] Gao, Z., Cecati, C., Ding, S.X.: 'A survey of fault diagnosis and faulttolerant techniques; part 1: fault diagnosis with model-based and signalbased approaches', *IEEE Trans. Ind. Electron.*, 2015, **62**, (6), pp. 3757–3767

[86] Gao, Z., Cecati, C., Ding, S.X.: 'A survey of fault diagnosis and fault-tolerant techniques; part 2: fault diagnosis with knowledge-based and hybrid/active approaches', *IEEE Trans. Ind. Electron.*, 2015, **62**, (6), pp. 3768–3774

[87] Nath, N.N., Pillay, V.R., Saisuriyaa, G.: 'Node fault detection and tolerance algorithm for controller area networks'. Intelligent Systems Technologies and Applications, Cham, 2016, pp. 247–257, ISBN: 978-3-319-23258-4

[88] Suwatthikul, J., McMurran, R., Jones, R.P.: 'In-vehicle network level fault diagnostics using fuzzy inference systems', *Appl. Soft Comput.*, 2011, **11**, (4), pp. 3709–3719

[89] Kammerer, R., Obermaisser, R., Sharkhawy, M.: 'Mixed-criticality systems based on a can router with support for fault isolation and selective fault-tolerance', *IFAC Proc. Vol.*, 2014, **47**, (3), pp. 12284–12292o. 19th IFAC World Congress, Cape Town, South Africa

[90] Kammerer, R., Obermaisser, R., Frömel, B.: 'A router for the containment of timing and value failures in can', *EURASIP J. Embed. Syst.*, 2012, **2012**, (1), p. 4

[91] Pohren, D.H., Roque, A.D.S., Kranz, T.I., *et al.*: 'An analysis of the impact of transient faults on the performance of the can-fd protocol', *IEEE Trans. Ind. Electron.*, 2020, **67**, pp. 2440–2449

[92] Faragardi, H.R., Lisper, B., Sandström, K., *et al.*: 'A resource efficient framework to run automotive embedded software on multi-core ecus', *J. Syst. Softw.*, 2018, **139**, pp. 64–83

[93] Munir, A., Koushanfar, F.: 'Design and analysis of secure and dependable automotive cps: A steer-by-wire case study', *IEEE Trans. Dependable Secur. Comput.*, 2020, **17**, pp. 813–827

[94] Prodanov, W., Valle, M., Buzas, R.: 'A controller area network bus transceiver behavioral model for network design and simulation', *IEEE Trans. Ind. Electron.*, 2009, **56**, (9), pp. 3762–3771

[95] Lei, Y., Yuan, Y., Zhao, J.: 'Model-based detection and monitoring of the intermittent connections for can networks', *IEEE Trans. Ind. Electron.*, 2014, **61**, (6), pp. 2912–2921

[96] Zhang, L., Yuan, Y., Lei, Y.: 'Data driven can node reliability assessment for manufacturing system', *Chin. J. Mech. Eng.*, 2017, **30**, (1), pp. 190–199

[97] Zhang, L.M., Tang, L.H., Lei, Y.: 'Controller area network node reliability assessment based on observable node information', *Front. Inf. Technol. Electron. Eng.*, 2017, **18**, (5), pp. 615–626

[98] Zhang, L., Lei, Y., Chang, Q.: 'Intermittent connection fault diagnosis for can using data link layer information', *IEEE Trans. Ind. Electron.*, 2017, **64**, (3), pp. 2286–2295

[99] Baek, S.G., Kang, D.H., Lee, S., *et al.*: 'Efficient graph pattern matching framework for network-based in-vehicle fault detection', *J. Syst. Softw.*, 2018, **140**, pp. 17–31

[100] Kelkar, S., Kamal, R.: 'Adaptive fault diagnosis algorithm for controller area network', *IEEE Trans. Ind. Electron.*, 2014, **61**, (10), pp. 5527–5537

[101] Shi, Z., Zhang, F.: 'Model predictive control under timing constraints induced by controller area networks', *Real-Time Syst.*, 2017, **53**, (2), pp. 196–227

[102] Quaglia, D., Muradore, R.: 'Communication-aware bandwidth-optimized predictive control of motor drives in electric vehicles', *IEEE Trans. Ind. Electron.*, 2016, **63**, (9), pp. 5602–5611

[103] Zhu, X., Zhang, H., Wang, J., *et al.*: 'Robust lateral motion control of electric ground vehicles with random network-induced delays', *IEEE Trans. Veh. Technol.*, 2015, **64**, (11), pp. 4985–4995

[104] Zhihong, H., Yuan, Z., Chang, X.: 'A robust fault-tolerant control strategy for networked control systems', *J. Netw. Comput. Appl.*, 2011, **34**, (2), pp. 708–714

[105] Nasri, O., Lakhal, N.M.B., Adouane, L., *et al.*: 'Automotive decentralized diagnosis based on can real-time analysis', *J. Syst. Archit.*, 2019, **98**, pp. 249–258

[106] Chen, H., Jiang, B., Chen, W., *et al.*: 'Data-driven detection and diagnosis of incipient faults in electrical drives of high-speed trains', *IEEE Trans. Ind. Electron.*, 2019, **66**, (6), pp. 4716–4725

[107] Kong, X., Zheng, Y., Ouyang, M., *et al.*: 'Signal synchronization for massive data storage in modular battery management system with controller area network', *Appl. Energy*, 2017, **197**, pp. 52–62

[108] Li, S., Zhao, J., Yang, S., *et al.*: 'Research on a coordinated cornering brake control of three-axle heavy vehicles based on hardware-in-loop test', *IET Intell. Transp. Syst.*, 2019, **13**, (5), pp. 905–914

[109] Şahin Gebizli, C., Kırkıcı, A., Sözer, H.: 'Increasing test efficiency by risk-driven model-based testing', *J. Syst. Softw.*, 2018, **144**, pp. 356–365

[110] Zhang, Z., Eyisi, E., Koutsoukos, X., *et al.*: 'A co-simulation framework for design of time-triggered automotive cyber physical systems', *Simul. Modelling Pract. Theory*, 2014, **43**, pp. 16–33

[111] Petersheim, M.D., Brennan, S.N.: 'Scaling of hybrid-electric vehicle powertrain components for hardware-in-the-loop simulation', *Mechatronics. (Oxf)*, 2009, **19**, (7), pp. 1078–1090

[112] Sakhdari, B., Azad, N.L.: 'Adaptive tube-based nonlinear mpc for economic autonomous cruise control of plug-in hybrid electric vehicles', *IEEE Trans. Veh. Technol.*, 2018, **67**, (12), pp. 11390–11401

[113] Raikwar, S., Wani, L.J., Kumar, S.A., *et al.*: 'Hardware-in-the-loop test automation of embedded systems for agricultural tractors', *Measurement*, 2019, **133**, pp. 271–280

[114] Heffernan, D., MacNamee, C.: 'Runtime observation of functional safety properties in an automotive control network', *J. Syst. Archit.*, 2016, **68**, pp. 38–50

[115] Li, L., Yan, B., Song, J., *et al.*: 'Two-step optimal energy management strategy for single-shaft series-parallel powertrain', *Mechatronics. (Oxf)*, 2016, **36**, pp. 147–158

[116] Yang, C., Jiao, X., Li, L., *et al.*: 'A robust h_∞ control-based hierarchical mode transition control system for plug-in hybrid electric vehicle', *Mech. Syst. Signal Process.*., 2018, **99**, pp. 326–344

[117] Zhao, Z., Li, X., He, L., *et al.*: 'Estimation of torques transmitted by twin-clutch of dry dual-clutch transmission during vehicle's launching process', *IEEE Trans. Veh. Technol.*, 2017, **66**, (6), pp. 4727–4741

[118] Morello, R., Di Rienzo, R., Roncella, R., *et al.*: 'Hardware-in-the-loop platform for assessing battery state estimators in electric vehicles', *IEEE Access*, 2018, **6**, pp. 68210–68220

[119] Zhu, B., Yan, S., Zhao, J., *et al.*: 'Personalized lane-change assistance system with driver behavior identification', *IEEE Trans. Veh. Technol.*, 2018, **67**, (11), pp. 10293–10306

[120] Barreras, J.V., Fleischer, C., Christensen, A.E., *et al.*: 'An advanced hil simulation battery model for battery management system testing', *IEEE Trans. Ind. Appl.*, 2016, **52**, (6), pp. 5086–5099

[121] Ham, W.K., Ko, M., Park, S.C.: 'A framework for simulation-based enginecontrol unit inspection in manufacturing phase', *Control Eng. Pract.*, 2017, **59**, pp. 137–148
[122] Fajri, P., Prabhala, V.A.K., Ferdowsi, M.: 'Emulating on-road operating conditions for electric-drive propulsion systems', *IEEE Trans. Energy Convers.*, 2016, **31**, (1), pp. 1–11
[123] Zhao, S., Lasson, A., Wallmark, O., *et al.*: 'Off-vehicle evaluation of active oscillation damping schemes', *IEEE J. Emerg. Sel. Top. Power Electron.*, 2014, **2**, (2), pp. 264–271
[124] Mura, R., Utkin, V., Onori, S.: 'Energy management design in hybrid electric vehicles: A novel optimality and stability framework', *IEEE Trans. Control Syst. Technol.*, 2015, **23**, (4), pp. 1307–1322
[125] Fajri, P., Lee, S., Prabhala, V.A.K., *et al.*: 'Modeling and integration of electric vehicle regenerative and friction braking for motor/dynamometer test bench emulation', *IEEE Trans. Veh. Technol.*, 2016, **65**, (6), pp. 4264–4273
[126] Olma, S., Kohlstedt, A., Traphöner, P., *et al.*: 'Observer-based nonlinear control strategies for hardware-in-the-loop simulations of multiaxial suspension test rigs', *Mechatronics. (Oxf)*, 2018, **50**, pp. 212–224
[127] Polygerinos, P., Wang, Z., Overvelde, J.T.B., *et al.*: 'Modeling of soft fiber-reinforced bending actuators', *IEEE Trans. Robot.*, 2015, **31**, (3), pp. 778–789
[128] Eun, Y., Park, S.Y., Kim, G.N.: 'Development of a hardware-in-the-loop testbed to demonstrate multiple spacecraft operations in proximity', *Acta Astronaut.*, 2018, **147**, pp. 48–58
[129] Duchaud, J., Hlioui, S., Louf, F., *et al.*: 'Modeling and optimization of a linear actuator for a two-stage valve tappet in an automotive engine', *IEEE Trans. Veh. Technol.*, 2015, **64**, (10), pp. 4441–4448
[130] Fu, Y., Han, X., Sepehri, N., *et al.*: 'Design and performance analysis of position-based impedance control for an electrohydrostatic actuation system', *Chin. J. Aeronaut.*, 2018, **31**, (3), pp. 584–596
[131] Li, Z., Dixon, S.: 'A closed-loop operation to improve gmr sensor accuracy', *IEEE Sens. J.*, 2016, **16**, (15), pp. 6003–6007
[132] Feld, T., Biondi, A., Davis, R.I., *et al.*: 'A survey of schedulability analysis techniques for rate-dependent tasks', *J. Syst. Softw.*, 2018, **138**, pp. 100–107
[133] Mubeen, S., Nolte, T., Sjödin, M., *et al.*: 'Supporting timing analysis of vehicular embedded systems through the refinement of timing constraints', *Softw. Syst. Model.*, 2019, **18**, (1), pp. 39–69
[134] Tindell, K., Burns, A., Wellings, A.J.: 'Calculating controller area network (can) message response times', *Control Eng. Pract.*, 1995, **3**, (8), pp. 1163–1169
[135] Zeng, H., Natale, M.D., Giusto, P., *et al.*: 'Using statistical methods to compute the probability distribution of message response time in controller area network', *IEEE Trans. Ind. Inf.*, 2010, **6**, (4), pp. 678–691
[136] Gong, H., Li, R., Bai, Y., *et al.*: 'Message response time analysis for automotive cyber–physicalsystems with uncertain delay: an m/ph/1 queue approach', *Perform. Eval.*, 2018, **125**, pp. 21–47
[137] Navet, N., Song, Y.Q., Simonot, F.: 'Worst-case deadline failure probability in real-time applications distributed over controller area network', *J. Syst. Archit.*, 2000, **46**, (7), pp. 607–617
[138] Zeng, H., Natale, M.D., Giusto, P., *et al.*: 'Stochastic analysis of can-based real-time automotive systems', *IEEE Trans. Ind. Inf.*, 2009, **5**, (4), pp. 388–401
[139] Xia, J., Zhang, C., Bai, R., *et al.*: 'Real-time and reliability analysis of timetriggered can-bus', *Chin. J. Aeronaut.*, 2013, **26**, (1), pp. 171–178
[140] Becker, M., Dasari, D., Mubeen, S., *et al.*: 'End-to-end timing analysis of cause-effect chains in automotive embedded systems', *J. Syst. Archit.*, 2017, **80**, pp. 104–113
[141] Shuai, Z., Zhang, H., Wang, J., *et al.*: 'Combined afs and dyc control of four-wheel-independent-drive electric vehicles over can network with time-varying delays', *IEEE Trans. Veh. Technol.*, 2014, **63**, (2), pp. 591–602
[142] Davis, R.I., Kollmann, S., Pollex, V., *et al.*: 'Schedulability analysis for controller area network (can) with fifo queues priority queues and gateways', *Real-Time Syst.*, 2013, **49**, (1), pp. 73–116
[143] Mubeen, S., Mäki Turja, J., Sjödin, M.: 'Extending offset-based response-time analysis for mixed messages in controller area network'. In: Emerging Technologies Factory Automation, Cagliari Italy, 2013, pp. 1–10
[144] Mubeen, S., Mäki Turja, J., Sjödin, M.: 'Integrating mixed transmission and practical limitations with the worst-case response-time analysis for controller area network', *J. Syst. Softw.*, 2015, **99**, pp. 66–84
[145] Xie, G., Zeng, G., Kurachi, R., *et al.*: 'Wcrt analysis and evaluation for sporadic message-processing tasks in multicore automotive gateways', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2019, **38**, (2), pp. 281–294
[146] Marx, S.E., Luck, J.D., Pitla, S.K., *et al.*: 'Comparing various hardware/software solutions and conversion methods for controller area network (can) bus data collection', *Comput. Electron. Agric.*, 2016, **128**, pp. 141–148
[147] Wang, J., Li, F., Liu, Y., *et al.*: 'Design of data communication and management system for ground test and verification devices of space laser communication', *Optik – Int. J. Light Electron Opt.*, 2014, **125**, (8), pp. 1937–1941
[148] Sun, X., Cai, Y., Wang, S., *et al.*: 'Optimal control of intelligent vehicle longitudinal dynamics via hybrid model predictive control', *Robot. Auton. Syst.*, 2019, **112**, pp. 190–200
[149] Ettl, J., Bernhardt, H., Pickel, P., *et al.*: 'Transfer of agricultural work operation profiles to a tractor test stand for exhaust emission evaluation', *Biosystems Eng.*, 2018, **176**, pp. 185–197
[150] Gallus, J., Kirchner, U., Vogt, R., *et al.*: 'Impact of driving style and road grade on gaseous exhaust emissions of passenger vehicles measured by a portable emission measurement system (pems)', *Transp. Res. D, Transp. Environ.*, 2017, **52**, (Part A), pp. 215–226
[151] Poudel, B., Munir, A.: 'Design and evaluation of a reconfigurable ecu architecture for secure and dependable automotive cps', *IEEE Trans. Dependable Secur. Comput.*, 2018, pp. 1–18
[152] Mahmud, K., Town, G.E.: 'A review of computer tools for modeling electric vehicle energy requirements and their impact on power distribution networks', *Appl. Energy*, 2016, **172**, pp. 337–359
[153] Ashjaei, M., Khalilzad, N., Mubeen, S.: 'Modeling, designing and analyzing resource reservations in distributed embedded systems', In: Alam, M., Dghais, W., Chen, Y. (Eds.): '*Real-time modelling and processing for communication*' (Springer International Publishing, Cham, 2018), pp. 203–256, ISBN: 978-3-319-72215-3
[154] Salunkhe, H., Lele, A., Moreira, O., *et al.*: 'Buffer allocation for real-time streaming applications running on heterogeneous multi-processors without back-pressure', *J. Syst. Archit.*, 2016, **62**, pp. 24–37
[155] Mubeen, S., Mäki Turja, J., Sjödin, M.: 'Mps-can analyzer: integrated implementation of response-time analyses for controller area network', *J. Syst. Archit.*, 2014, **60**, (10), pp. 828–841
[156] Bello, L.L., Mariani, R., Mubeen, S., *et al.*: 'Recent advances and trends in on-board embedded and networked automotive systems', *IEEE Trans. Ind. Inf.*, 2019, **15**, (2), pp. 1038–1051
[157] Fan, C., Lin, C.Y., Li, K.: 'Hil safety function validation of the multi-power sources electric vehicle'. Power Electronics and Motion Control Conf., Hefei China, 2016, pp. 2770–2774
[158] Cena, G., Bertolotti, I.C., Hu, T., *et al.*: 'On a software-defined can controller for embedded systems', *Comput. Stand. Interfaces*, 2019, **63**, pp. 43–51
[159] Reinhardt, D., Güntner, M., Kucera, M., *et al.*: 'Mapping can-to-ethernet communication channels within virtualized embedded environments'. IEEE Int. Symp. on Industrial Embedded Systems, Siegen Germany, 2015, pp. 1–10
[160] Le Khac, N.A., Jacobs, D., Nijhoff, J., *et al.*: 'Smart vehicle forensics: challenges and case study', *Future Gener. Comput. Syst.*, 2020, **109**, pp. 500–510
[161] Goyal, P., Goyal, A.: 'Comparative study of two most popular packet sniffing tools-tcpdump and wireshark'. Computational Intelligence and Communication Networks, Girne Cyprus, 2017, pp. 77–81
[162] Galarza, M., Paradells, J.: 'Improving road safety and user experience by employing dynamic in-vehicle information systems', *IET Intell. Transp. Syst.*, 2019, **13**, (4), pp. 738–744
[163] Fugiglando, U., Massaro, E., Santi, P., *et al.*: 'Driving behavior analysis through can bus data in an uncontrolled environment', *IEEE Trans. Intell. Transp. Syst.*, 2019, **20**, (2), pp. 737–748
[164] Mullins, G.E., Stankiewicz, P.G., Hawthorne, R.C., *et al.*: 'Adaptive generation of challenging scenarios for testing and evaluation of autonomous vehicles', *J. Syst. Softw.*, 2018, **137**, pp. 197–215
[165] Kalra, N., Paddock, S.M.: 'Driving to safety: how many miles of driving would it take to demonstrate autonomous vehicle reliability?', *Transp. Res. A, Policy Pract.*, 2016, **94**, pp. 182–193
[166] Trang, H.T.H., Dung, L.T., Hwang, S.O.: 'Connectivity analysis of underground sensors in wireless underground sensor networks', *Ad Hoc Netw.*, 2018, **71**, pp. 104–116
[167] Yarinezhad, R., Hashemi, S.N.: 'A routing algorithm for wireless sensor networks based on clustering and an fpt-approximation algorithm', *J. Syst. Softw.*, 2019, **155**, pp. 145–161
[168] De La Torre, G., Rad, P., Choo, K.K.R.: 'Driverless vehicle security: challenges and future research opportunities', *Future Gener. Comput. Syst.*, 2020, **108**, pp. 1092–1111
[169] Lakhal, N.M.B., Adouane, L., Nasri, O., *et al.*: 'Risk management for intelligent vehicles based on interval analysis of ttc', *IFAC-PapersOnLine*, 2019, **52**, (8), pp. 338–343. 10th IFAC Symposium on Intelligent Autonomous Vehicles IAV 2019
[170] Lakhal, N.M.B., Adouane, L., Nasri, O., *et al.*: 'Interval-based/datadriven risk management for intelligent vehicles: application to an adaptive cruise control system'. 2019 IEEE Intelligent Vehicles Symp. (IV), Paris, France, 2019, pp. 239–244
[171] Lakhal, N.M.B., Adouane, L., Nasri, O., *et al.*: 'Interval-based solutions for reliable and safe navigation of intelligent autonomous vehicles'. 2019 12th Int. Workshop on Robot Motion and Control (RoMoCo), Poznań Poland, 2019, pp. 124–130