Journal of Systems Architecture 98 (2019) 249–258

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

Automotive decentralized diagnosis based on CAN real-time analysis

Othman Nasri [a,*], Nadhir Mansour Ben Lakhal [a,b], Lounis Adouane [b], Jaleleddine Ben Hadj Slama [a]

[a] LATIS Lab, National Engineering School of Sousse (ENISo), University of Sousse, BP 264 Sousse Erriadh 1023, Tunisia
[b] Institut Pascal, UCA/SIGMA - UMR CNRS 6602, Clermont Auvergne University, France

ARTICLE INFO

Keywords:
Automotive embedded system
Controller area network
Decentralized fault diagnosis
CAN real-time analysis
Task schedulability

ABSTRACT

Nowadays, modern automotive systems include a great number of Electronic Control Units (ECUs). These ECUs provide many sophisticated systems such as engine control, antilock braking systems, etc. This fact has increased the automotive embedded networks complexity. Another important issue in this field is the necessity to define a suitable diagnosis strategy to prevent faults propagation. The integration of diagnosis functions into the automotive embedded systems contributes to overload the communication protocols. In this context, solutions for checking latencies entailed by extra-data traffic are urgently needed. Throughout this paper, a novel approach for the automotive diagnosis design, which is based on the Controller Area Network (CAN) analysis, is detailed. The principal contribution of this work consists in developing a decentralized fault diagnosis and studying its data traffic effect on messages deadlines. Our novel method, "CAN real-time analysis based on decentralized fault diagnosis", is a step ahead to a reliable early phase automotive design. As a proof of concept, the proposed approach is applied on a model of an advanced anti-crash system. The proposed design methodology presents several advantages. It optimizes the schedulability of tasks and facilitates the design validation. Moreover, a realistic hardware-in-the-loop simulation is carried out to validate our work.

1. Introduction

The growing competition between car manufacturers has led to an exceptional evolution concerning automotive performance over the past decade. The trend is a move towards more and more intelligent vehicles in order to enhance safety and satisfy customers. For those reasons and others, the automotive research and development community is struggling to make drivers feel comfortable, secure and confident at wheels [1]. Notably, several safety-oriented applications, which are detailed in the sequel, have been extensively integrated to modern vehicles. These systems, such as "driver distraction detection" and "lane detection systems", help to avoid accidents and to provide extreme comfort for the driver.

Adaptive Cruise Control (ACC) systems have almost become standard automotive equipment. These systems are developed to enhance regular cruise control and comfort automations [2]. In the perspective of driver comfort and safety, a large scale of Advanced Drive Assistance Systems (ADAS) has been promoted [3,4]. Advancements in computer vision and image processing sciences collaborated to increase automobiles safety [5]. Daytime and nighttime visibility complications during car navigation have been extremely hazardous. Enhanced driver vision and fog detecting systems have been addressed to remove these difficulties [6]. Vision-based technologies have also helped to give rise to "pedestrian detection" systems. Once the background and street scene analysis notice the presence of a road crossing person, the driver is warned [7,8]. In addition, late versions of "pedestrians recognition" systems can anticipate crossing pedestrian behavior to give driver a hand in making decisions [9]. "Road sign recognizing" is another instance of in-vehicle safe navigation systems. In [10], the VIAPIX commercial tool and correlation analysis served to keep the driver aware about signalization especially in high speed cruises. Otherwise, car crashes would be the consequence of distractions preoccupying drivers. As a counter-measure, "driver distraction detection" processes were proposed to check continuously the driver vigilance through eyes and head movements in [11,12]. Similarly, vehicular localization mechanisms had the potential to assist drivers and to present safety interventions. Global Positioning System (GPS) and LIght Detection And Ranging (LIDAR) technologies have been conjoined by detection algorithms to introduce "smart lane level localization" modules. Today's vehicle position estimators are capable of taking into consideration the road slope and managing different road models [13,14]. "Self-parking" and "parking assistance" applications have been practiced for two general intents. First, connected cars with intelligent communication devices can easily guide drivers to vacant parking spots [15,16]. Secondly, a generated feasible path towards a specific spot is automatically followed with a smooth self-reverse parking operation [17,18]. Indeed, the concept of a "co-drivers" agent is promising in vehicular AI applications [19]. Advanced systems that imitate expert human drivers are supposed to achieve human-machine collaborative control of vehicles. For entertainment reasons, modern vehicles offer commonly a set of interactive services thanks to a great aptitude of handling audio-visual media and vocal control modules [20]. Recently,

* Corresponding author.
E-mail address: othman.nasri@eniso.rnu.tn (O. Nasri).

https://doi.org/10.1016/j.sysarc.2019.01.009
Received 20 September 2017; Received in revised form 10 January 2019; Accepted 22 January 2019
Available online 23 January 2019
1383-7621/

[21] has suggested a novel technique to include VHF/UHF television bands In-Vehicular Infotainment (IVI) services.

Despite of its role in enhancing safety, the aforementioned mechanisms have emphasized the vehicular embedded systems complexity [22]. As a consequence, the full reliability of these systems is not guaranteed [23]. It cannot be denied that faults and deficiencies occurring in autonomous or semi-autonomous systems must be managed carefully. Model-based diagnosis approaches have been applied for reliability reasons [24,25]. When models are ineffective in capturing the full system behavior and its distinct operational modes, data-driven diagnosis techniques are adopted [26,27]. Unfortunately, selecting an appropriate diagnosis approach for a specific automotive component is no longer sufficient. Diagnosis has to deal with challenges such as the expanded modular structure of the onboard embedded systems and the great amounts of data exchanged between various Electronic Control Units (ECUs). Networks overloaded with inter-nodes message transfer can suffer from destructive delays. Similarly, conflicts between the system exchanged data and diagnosis messages may slow down the system and give rise to critical situations.

To face the instant automotive challenges, diagnosis schemas have imperatively to overstep the node-level and to act on wider dimension (the network-level). In that respect, we propose a theoretical preliminary network design approach that guarantees the reliability of an in-vehicular system. It consists in a “Real Time Analysis (RTA)-based diagnosis in a decentralized architecture”, which is a design approach compromising between optimizing the network message schedulability and satisfying the node specifications. The data-traffic is enormously reduced thanks to the decentralized architecture of the diagnosis deployment. Meanwhile and since the early design phase, the RTA precludes unacceptable violation of onboard communication deadlines, which can be entailed by diagnosis messages. In particular, we tackle RTA applied on the Controller Area Network (CAN), which is currently the most widespread communication protocol in the automotive field. Conventionally, the automotive network design involves advanced tools, which are based on confidential validation algorithms. These tools are often too inflexible and pose an additional difficulty once a change in a network design is required. In this sense, our proposed approach is an early phase design strategy, which avoids later surprising future modifications in the network layout. It can be relevant before using a professional emulation tool, which is so challenging and a time-wasting task. Therefore, as a proof of concept, we address the fault diagnosis of a smart anti-crash system, namely Smart Distance Keeping (SDK) to prove our proposition efficiency [28]. This system is an example of emergent technologies and in-road safety automations.

The outline of this paper is arranged as follows: Section 2 represents the SDK system and describes its particularities. Section 3 underlines related work to automotive diagnosis and CAN messages schedulability analysis. Section 4 delivers a complete idea about the proposed approach and examines how to settle CAN RTA-based diagnosis in a decentralized manner. Section 5 illustrates the realized experimental work. Finally, Section 6 summarizes the main contributions of this paper and discusses future work.

2. Smart distance keeping system and its main functions

Road incidents daily cause great losses of individual lives, serious human being disabilities and economic impairments. Statistics prove that attention must be assigned to straight road drives. Car-crash risks rise especially around motorways and straight roads due to high speed [29]. According to the French Motorways Companies Organization (ASFA), around 18.43% of mortal accidents that occurred in France in 2011 were in entirely straight ways [30]. As a monotonous environment, drivers lose their alertness along highways. Sleepiness on the wheels, fatigue, alcohols, loss of vigilance and distractions caused by mobile phone conversations lead to fatal highway accidents. Truck drivers are the most

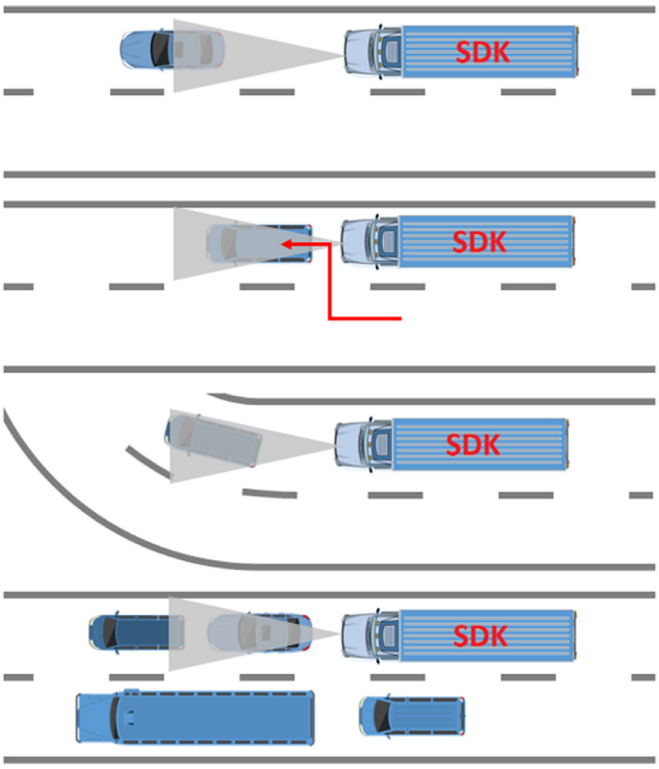

Fig. 1. SDK capabilities.

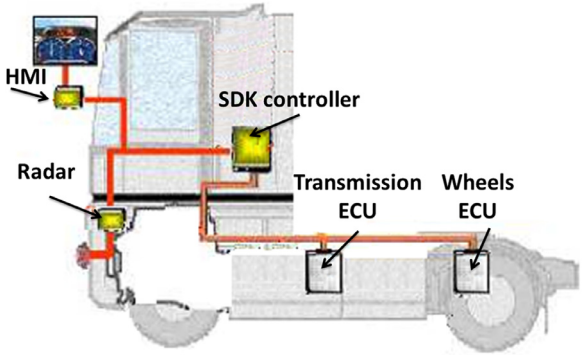

Fig. 2. SDK components.

endangered by highway incidents. Drivers, especially working in transportation services, suffer from exhausting and consecutive travels on their trucks. The longer the cruise, the higher the risk of crash.

In an attempt to improve motorways drivers safety, an SDK system, which is an advanced ACC, is implemented in trucks to play as an anti-crash mechanism [28]. It increases the vehicle autonomy and its reliability by helping the truck drivers to deal with critical situations, such as the unexpected presence of a front object. For instance, a vehicle moving from a side lane to the current lane of the SDK equipped truck is rapidly detected. Thus, the truck speed is adjusted to avoid collision. It also provides significant drive assistance in case of a surprising brake of a relevant object.

Additionally, rough road curvatures are handled through the yaw rate data analysis. To prohibit hazardous eventualities, SDK reduces progressively the truck velocity until the end of the curvature. The SDK equipped truck finds easily its way even in an overcrowded traffic. The smooth speed regulation always helps to maintain a safe distance with a followed in-front vehicle. Fig. 1 recapitulates the in-road SDK system capacities to overcome difficult situations. As a modular process, the SDK

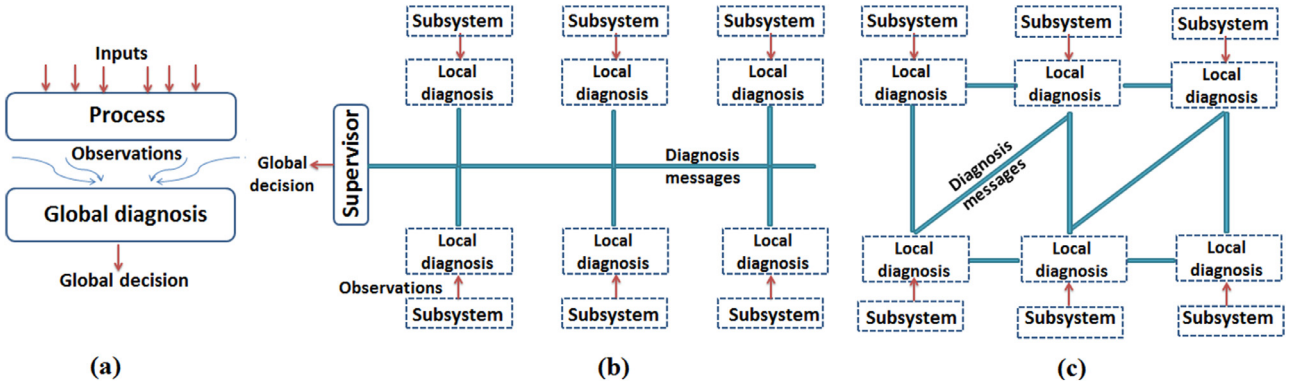

Fig. 3. Diagnosis architectures. (a) Centralized diagnosis architecture. (b) Decentralized diagnosis architecture. (c) Distributed diagnosis architecture.

mechanism is distributed on four fundamental sub-entities: the SDK controller, the radar, wheels ECU and transmission ECU. The SDK controller represents the intelligent part of the whole system. Its challenging mission lies in determining the suitable velocity depending on the vehicle current situation. Regarding its rapid computational capacities, it reacts to command the fuel injector, the braking system, the engine and the gearbox. It is important to note that the SDK controller decisions are based on measurements and data coming from the remaining components.

A radar with a large boundary beam must be mounted on the truck supposed to be supplied with the anti-crash system. The main radar task is to determine the relative velocity and the distance separating the truck from a relevant object. A local diagnosis, which detects infeasible velocities of nearby vehicles, is integrated in the radar component. In other terms, the radar is deficient when it returns unrealistic measurements (vehicles moving at impossible speed).

The SDK equipped trucks are in general six-wheel vehicles. An inappropriate tire pressure is an example of problems that may occur at the wheels level. Such a wheel's erratic behavior corrupts the SDK performances and menaces the vehicle safety. With accordance to this fact, specific sensors are implemented to monitor the wheels angular velocities. The wheels' ECU inspects data collected from the totality of sensors to detect abnormalities. Besides, a particular diagnosis function is embedded in the wheels ECU. In order to exploit the certain redundancy and the existing correlation between the sensor measurements, a data-driven technique, which is the Principle Component Analysis (PCA), is adopted to identify faulty sensors [31].

Finally, the transmission ECU monitors the crankshaft angular velocity to estimate the corresponding longitudinal speed. The SDK includes also a Human Machin Interface (HMI) to interact properly with the driver.

In the following, we intend to exploit the SDK system in order to present a proof of concept of our onboard diagnosis design methodology (see Section 4). Accordingly, we make sure that diagnosis messages will not disturb the SDK normal operation. Technically speaking, a model of the SDK system is employed to establish Hardware In the Loop (HIL) experimentations.

3. Related work

In this section, the state-of-the-art is outlined to investigate different approaches and solutions that researchers have proposed to tackle automotive onboard fault diagnosis based on the CAN network protocol. Motivations for applying the decentralized diagnosis are provided. Hence, techniques permitting real-time analysis for CAN are depicted.

3.1. CAN-based automotive embedded system and diagnosis architecture

The CAN bus is an advanced event-triggered communication protocol and a key component part from several Networked Control Systems (NCS) [32]. Due to the high reliability and low cost, its application fields are numerous (e.g., industrial automation and automotive industry). For our case of study, the CAN bus is the message support and not the target of the diagnosis process. Nevertheless, huge data flows and conflicts in the data transmission within the CAN-based embedded system are destructive. Therefore, a careful selection of the automotive embedded system architecture and the onboard diagnosis hierarchy is necessary. Multiple researches cope with the automotive architecture from Software or/and electrical point of view [33]. In this work, these architectural aspects are supposed to be already managed. Instead of the whole system architecture, the on-board diagnosis architecture (its integration and deployment) is targeted.

Nowadays, the intensive modularity and the great number of ECUs claim intuitively a shallow look at the automotive architecture and its diagnosis specifications. The interest in the automotive embedded architecture is witnessed in military vehicle design. A recent research topic, namely Vetronix, has appeared to put the stress on the automotive architecture and the proper interaction between electronic components, including diagnosis functions [34].

On the other hand, the use of gateways for communicating heterogeneous networks (CAN, LIN, FlexRay and Ethernet) has lately become possible. Indeed, the study presented in [35] predicted that the backbone based architecture would substitute the traditional central gateway-based architecture [36,37]. Additionally, it pointed out the diagnosis functions disposition in both of the aforementioned architectures.

For the sake of safety, diverse universal standards have been imposed on vehicle manufacturers. Over the last years, those standards have mapped several strategies to avoid the vehicle embedded system failures. They have treated also the issue of the diagnosis deployment into the automotive network. Examples of such standards include: ISO 26262, ISO 15031-4, ISO 22901, ISO 15765-4 and Autosar [38,39].

Hence, referring to the well-known terminology "fault-error-failures", a new topology of the diagnosis architecture in relation with the automotive system was highlighted in [40]. The diagnosis deployment takes into consideration the different fault propagation stages (observation level, detection level and fault activation level).

As illustrated in Fig. 3, a recent paradigm has classified the automotive electronic hierarchy into three categories of onboard diagnosis: centralized, decentralized and distributed [41]. The centralized onboard diagnosis counts on one computational unit to ensure the whole diagnosis processing. This diagnosis unit is often called a global or central diagnoser.

Obviously, the centralized diagnosis is not suitable for sophisticated and modular processes. The global diagnoser does not support a huge flow of measurements and observations. This architecture jeopardizes real-time constraints. To withstand such vulnerabilities, the decentralized onboard diagnosis shares diagnosis duty between many sub-entities. Each part from the whole system is equipped with a local

diagnoser. Then a supervisor or a coordinator node is in charge of prohibiting the conflict between local decisions. Generally, making a final decision is done by a fault-tolerant control algorithm. The latter is implemented into the supervisor platform to manage all probable fault scenarios. Evidently, these algorithms vary depending on the concerned system specifications. The two-phase commit protocol, the sensor/actuator switching policies and the fault tolerant fuzzy control have been utilized for either committing or aborting the operation of large distributed systems [42,43].

The main drawback related to the decentralized diagnosis architecture is the use of an extra component, which is the coordinator ECU. The integration of this ECU into the automotive onboard network must be well-studied. Lastly, the distributed diagnosis structure relies on the cooperation between local diagnosers to make a final decision. The call for an auxiliary computational platform to serve as a supervisor is abandoned. A predefined diagnosis data exchange protocol enables the collaboration between all nodes. Notably, the distributed diagnosis gives rise to a communication overload and data extra-exchange.

Henceforth, the decentralized architecture is adopted in this work for its great aptitude to decrease the data-traffic inside vehicle networked systems. However, the CAN-bus topology mandates the transmission of diagnosis messages towards the supervisor through normal communication channels.

3.2. CAN real-time analysis

"Delays induced into NCS" is an alarming issue for present autonomous transportation systems. The large number of components integrated into the onboard vehicular system has emphasized this problem. The huge traffic threatens to slowdown the automotive system and to prohibit critical tasks to meet deadlines. Similarly, designers of automotive embedded systems have to pay attention to the diagnosis deployment. Overloading the network traffic by diagnosis messages would be absolutely destructive.

In this context, Vector, Symtavision and Arcticus are professional engineering software providers, who promote CAN latency analysis solutions [44]. The CAN schedule validation tools like CANoe, CANalyzer, Network Designer CAN, SymTA/S and Rubus-ICE are examples of their products [44]. Despite their widespread usage, the mentioned tools have lots of inconvenience. The majority of these products are non-free commercial tools. Their functionality is based on confidential assumptions and non-disclosed algorithms. Intuitively, the adopted assumptions may mismatch the CAN node's characteristics and the network architecture.

At this stage, RTA applied for CAN helps to overcome the previously mentioned disadvantages of these tools. A preliminary validation of a given automotive network design through RTA certainly provides more reliable results. In fact, RTA is an analytical models derived from response time analysis, which addresses rugged-embedded systems. Guaranteeing the reliability and the safety of tight critical functionalities is the ultimate objective of RTA models. Upper bound estimation of CAN messages response time was presented for the first time in Tindell's seminal work [45]. Statistical and stochastic approaches have been widely developed for CAN latency analysis [46]. exploited distribution models to statistically determine messages response time. The originality of this research belongs to the regression techniques application for having accurate results. A detailed comparison between statistical and stochastic CAN schedulability was delivered. Indeed, [47] united stochastic RTA searches with sampling delays to delineate CAN message latencies. The abundance of variability sources for this kind of RTA remains as its major drawback.

CAN erroneous transmissions may affect the end to end deadlines approximation. In this context [48], consolidated the CAN-RTA with stochastic models based on the Poisson distribution to predict error occurrence [49]. combined conventional CAN schedulability analysis with the usual probabilistic reliability estimation. In the same way, RTA including the study of the fault probability has been applied to verify the meeting of deadlines of steer-by-wire control messages [50,51] included gateway nodes into CAN delay analysis. The gateway node response time estimation for CAN messages was detailed [52]. tried to immune CAN-based onboard systems against network latency effects. Taylor series expansion and time delay models have been employed to counter CAN induced delays seen as non-linear uncertainties.

Finally, the authors in [44,53,54] upgraded CAN response-time bounding to an advanced stage in an effort to address some sophisticated technical concerns. The main contributions of those studies are:

- Enable analysis for CAN different transmission modes, including the mixed message mode with offsets.
- Tackle CAN analysis with simultaneous multiple queuing strategies.
- Boost timing analysis to take into account the software and hardware limitation as the cancelable and non cancelable transmit buffers.
- Involve response-time evaluation for both homogenous and heterogonous networks.
- Deliver a free CAN analysis platform assuring the integration of the above stated properties.

4. Real time analysis for diagnosis in decentralized architecture

A RTA reference model, applied to a FlexRay-CAN automotive onboard system, was presented in [55]. The main innovation provided by this model is performing RTA following a direct graph concept. It maps the set of flows induced by the network messages schedule. A flow comprises the data exchange from a starting point task, up to a destination task. Thus, response time estimation is achieved depending on the resulting flows. In the present work, we intend to adopt this RTA model reference while completely neglecting the FlexRay specifications presented in the seminal work [55]. The RTA model and the decentralized diagnosis hierarchy are combined to introduce a RTA-based decentralized diagnosis approach. The direct graph is expected to stress the extreme reduction in CAN message exchange amounts thanks to the diagnosis hierarchy. Moreover, it permits easily applying RTA for CAN.

The direct graph-based RTA supports analysis for asynchronous network nodes. The capacity of handling asynchronous systems is convenient with the decentralized diagnosis structure, where diagnosis messages are event triggered elements. A diagnosis message is sent towards the supervisor node only in case of a trouble occurrence.

Contrary to the approaches depicted over the literature, the proposed RTA model carries a local component analysis. Not only the ordinary tasks are modeled according to the direct graph, but diagnosis tasks also are considered. Once the message stream modeling phase is accomplished, the response time estimation may be tackled.

4.1. Direct graph-based modeling:

As explained above, the direct graph highlights the propagation of messages. This fact facilitates the data priority setting scheme. In what follows, the necessary steps to establish the direct graph model are detailed.

Considering an automotive network of n components. Every node N_h, with $h = 1, \ldots, n$, executes several tasks denoted by $\Gamma_{h,i}$, where i denotes a given task. To illustrate the node modeling through the direct graph, an example is given in Fig. 4.

We denote by $S_{h,j}$ a message stream that covers the totality of messages created starting from a specific task. Note that a stream message is associated to a particular task and not to a given node. A flow φ_c represents the path that joins message streams and tasks participating in transmitting data from a source to a final destination task. An example of a direct graph model is illustrated in Fig. 5.

To accomplish the RTA reference model, the following assumptions are assumed:

- A task $\Gamma_{h,i}$ is characterized by a maximum execution time $C_{h,i}^{task}$.

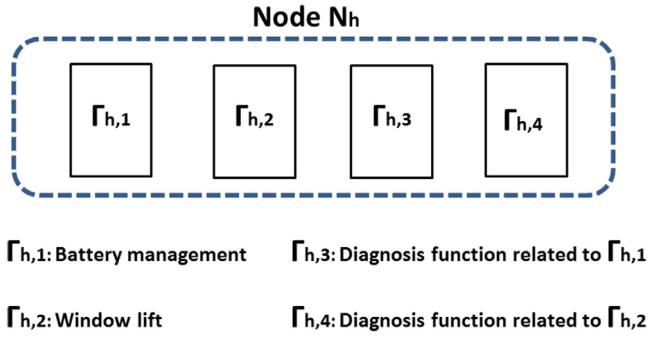

Fig. 4. Node modeling according to direct graph concept.

- A stream message $S_{h,j}$ is characterized by $C_{h,j}^{message}$, which is the maximum amount of time needed to transfer a message. At this stage, the interference from other messages is not considered when defining $C_{h,j}^{message}$.

We denote by $m_{h,j}$ a CAN frame, which is characterized by a unique identifier (*ID*). In this work, we address only the standard CAN frame of 11 bits *ID*. The maximum transmission time for this frame is obtained by Eq. (1) [55]:

$$C_{h,j}^{message} = (55 + 10 \times lm_{h,j}) \times \tau_{bit} \quad (1)$$

Note that $lm_{h,j}$ is the number of data bytes included in a message and τ_{bit} is the required time to transmit one single bit from a given CAN frame. This parameter depends on the network baudrate and its speed. It is worth mentioning that Eq. (1) takes into account the stuffing technique bits added to the CAN frame. Indeed, it relies on overestimating the maximum number of bits that a CAN frame may include. Aside from the data-byte field, the number of bits included in the remaining fields is considered assuming that one stuffing bit per four original bits can take place in the fields where the bit stuffing is used.

4.2. CAN response time analysis

In parallel to the direct graph-based modeling, we define simple steps to apply RTA for CAN. First of all, a Worst Case Response Time (WCRT) must be assigned to each message stream shown in the direct graph. Later, assigning task priority has to be arranged to reduce data transfer blocking periods. In this paper, we change task priority assignment approaches, which are underlined in [55,56], to balance between the network reliability and the schedulability ratio of tasks. Finally, global end-to-end response-time values are obtained.

Suppose that $R_{h,j}$ is WCRT of a given message $m_{h,j}$ induced from a specific stream $S_{h,j}$. With accordance to Tindell's seminal work, $R_{h,j}$ is estimated based on three fundamental elements. Aside from the CAN frame transmission time, two delay sources must be taken into consideration. Eq. (2) permits computing the approximation of $R_{h,j}$:

$$R_{h,j} = J_{h,j} + C_{h,j}^{message} + W_{h,j} \quad (2)$$

where:

- $J_{h,j}$ is the maximum release jitter [56]. Technically, this parameter expresses the time interval between the message instantiation and the instant when the message is queued.
- $W_{h,j}$ denotes the queuing delay. Regarding the non-preemptive CAN schedule, various messages may be simultaneously prepared to be transferred. In that case, two possible latencies can occur. Both higher and lower priority sets of messages may oblige $m_{h,j}$ to wait for the bus availability [55,56]. detailed the queuing blocking time calculation with its two parts (interference delays linked to higher and lower priority messages).

It is important to note that CAN latency analysis is feasible regardless of an explicit priority assignment strategy. However, a reasonable schedulability approach has a great impact on optimizing meeting deadlines [56]. In particular, the link between the system failures and task scheduling has been extensively studied in the literature [57]. Nevertheless, the critical nature of diagnosis tasks has not been considered while fixing priorities.

The Rate Monotonic (RM) scheduler is an example of those scheduling methods applied for CAN. Its principle consists in attributing the highest priority to tasks having minimum execution time. Intuitively, the waiting queue line of tasks is kept short and latencies are heavily diminished. Accordingly, the WCRT of a given fixed priority task may be estimated through Eq. (3):

$$R_{h,i} = I_{h,i} + C_{h,i}^{task} \quad (3)$$

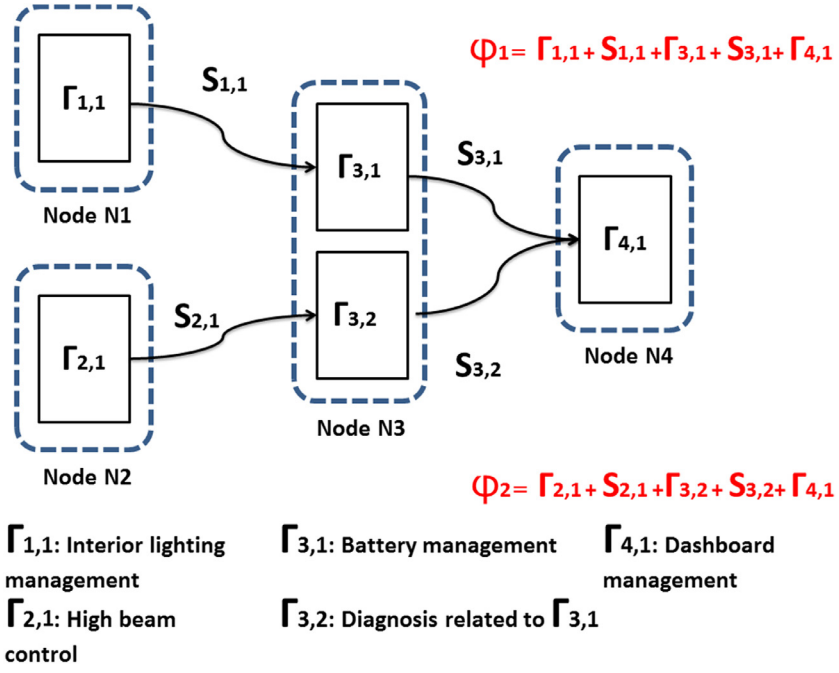

Fig. 5. Direct graph modeling.

where $I_{h,i}$ denotes the interference time induced from the set $hp(h, i)$. This latter represents all tasks of a priority higher than $\Gamma_{h,i}$). For more details, recursive algorithms permitting the calculation of $I_{h,i}$ can be found in [55].

Various approaches, published in the literature, have been used to optimize the network temporal performances. However, including a diagnosis task into the waiting queue is precarious. Within this sense, we introduce the "Emergency Level-Rate Monotonic" (ELRM) schedule. The latter can be seen as an extension of the RM that considers the emergency level of a given task. It aims to balance between the deadline respect and the diagnosis requirements. Algorithm 1 details the proposed schedule. where:

- L and M are two different tasks.
- $T(L)$ and $T(M)$ are the maximum execution time associated respectively to L and M.
- $Em(L)$ and $Em(M)$ are emergency levels associated respectively to L and M.
- $Pr(L)$ and $Pr(L)$ are priorities associated respectively to L and M according to the emergency level-rate monotonic schedule.

Finally, the complete WCRTs assigned to a φ_c is computed by summing all the response time of message streams as well as its source tasks.

Algorithm 1: ELRM schedule.

Input : $Em(L)$, $Em(M)$, $T(L)$, $T(M)$.
Output: $Pr(L)$, $Pr(M)$.

```
if Em(L) = Em(M) then
    if T(L) > T(M) then
        Pr(L) < Pr(M)
    else
        Pr(L) > Pr(M)
    end
else if Em(L) > Em(M) then
    Pr(L) > Pr(M)
else
    Pr(L) < Pr(M)
end
```

4.3. Application to SDK system

In this section, we explain the arrangement of SDK diagnosis functions according to the adopted decentralized architecture. The diagnosis data design as well as its packing are described. In this sense, more details about the supervisor node mission are provided. A final decision making algorithm is implemented in the supervisor to abort the SDK when an enormous loss in capabilities is confirmed. In case of benign faults occurrence, the system carries on until the next maintenance. Tolerating a particular fault depends on the possibility of getting the missing information from redundant data. However, the detection of a radar failure aborts the SDK operation since there is no possible back-up arrangement to calculate the relative velocity with a relevant object. Contrarily, partial wheels ECU failures can be tolerated. The angular velocity of wheels may be obtained from redundant measurements. Overall, the approximation of the truck longitudinal speed from the measured wheels angular velocities can be evaluated by the transmission ECU. In case of conflicts between results from two components, recovery actions are provided to supply the SDK controller with the correct value of the truck longitudinal speed. Fig. 6 gives a detailed schema of actions taken by the supervisor node in different scenarios.

After getting an idea of the SDK decision making concept, more details about the diagnosis messages design are tackled. Each component common source of failures are considered to define the final list of inspected faults.

Radar faults. Faulty radar behaviors are generally entailed by three principle sources. Simply, the radar in-front object detection is based on signal emission and reflection. According to this understanding, the radar deficiency is mostly caused by: faults affecting the reflector or the emitter devices as well as the interference phenomenon.

Wheels ECU faults. This component includes six velocity sensors that monitor wheels. For this reason, only faulty sensor scenarios are considered, while designing the wheels ECU diagnosis messages.

Transmission ECU faults. The transmission block approximates the vehicle longitudinal velocity through the measurements delivered by the crankshaft angular velocity sensors. Similar to the Wheels

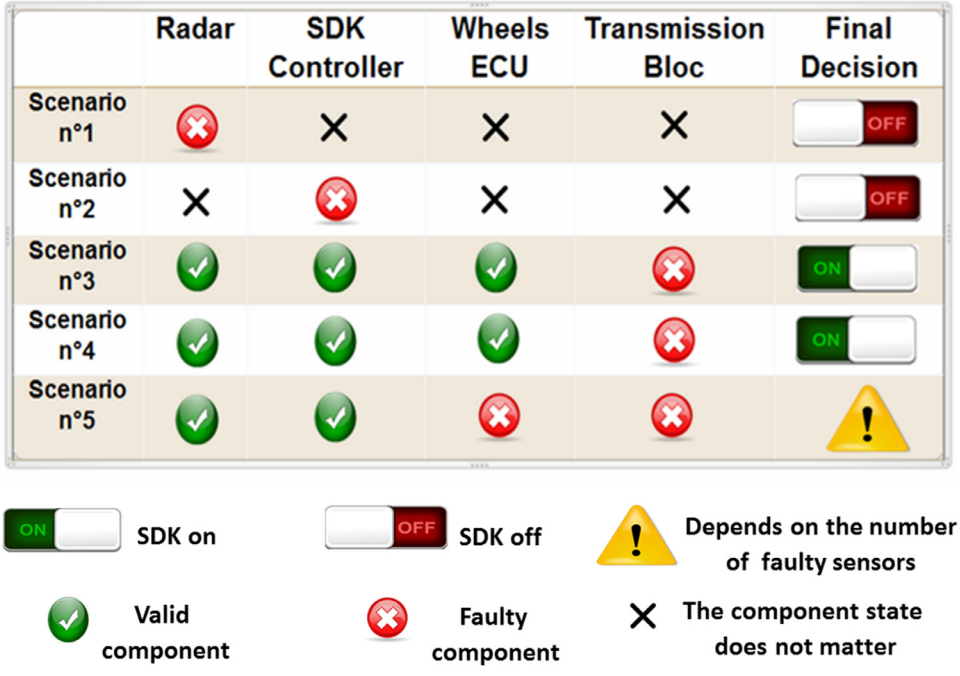

Fig. 6. SDK scenarios.

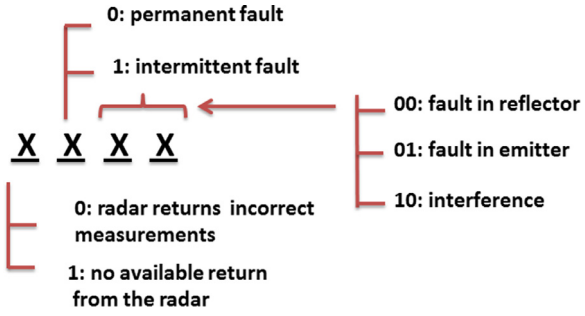

Fig. 7. Radar diagnosis message schema.

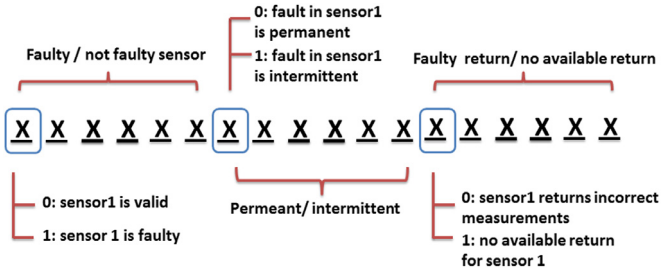

Fig. 8. Wheels ECU diagnosis message schema.

ECU, faulty sensors are the most significant threat endangering this component.

SDK controller faults. As an advanced computing unit, the prediction of fault scenarios related to this component are tightly linked to formal electronic board failures. To alleviate the diagnosis data traffic, no diagnosis functions are associated to the SDK controller and the transmission ECU. The supervisor node detects erroneous behavior of sub-entities by comparing their outcomes with redundant data obtained from the rest of components.

The maximum possible payload of CAN frame is 8 bytes. An optimized frame packing schema, which reduces the frame length is needed to minimize the message WCRT. In our case of study, the outline of the diagnosis message frame is inspired from the diagnosis trouble code. It consists in predefining a specific code value to refer to a particular fault type. By interpreting the trouble code, fault sources are easily identified. The rest of messages are expressing numeric objects (measurements). With a fixed point data representation, 3 bytes are sufficient to reach a respectable precision of measurements. Diagnosis messages are conceived to facilitate the maintenance procedures by a code describing the fault source. Additionally, the message indicates the fault location and whether it is permanent or intermittent (intermittent faults are usually related to wiring problems). Figs. 7 and 8 detail diagnosis messages specifications.

After having a complete idea about the SDK functioning and each diagnosis message length, we introduce its direct graph in Fig. 9.

Without being exhaustive, principle flows implied for the SDK are:

$\varphi_1 = \{\Gamma_{5,2} + S_{5,1} + \Gamma_{1,1}\}$ is responsible for recovery and enabling/disabling SDK.

$\varphi_2 = \{\Gamma_{2,2} + S_{2,1} + \Gamma_{5,1}\}$ is responsible for reporting the radar state.

$\varphi_3 = \{\Gamma_{3,2} + S_{3,1} + \Gamma_{5,1}\}$ is responsible for reporting wheels controller state.

$\varphi_4 = \{\Gamma_{2,1} + S_{2,2} + \Gamma_{5,2}\}$ is responsible for providing the supervisor with the vehicle longitudinal velocity approximated by the radar.

$\varphi_5 = \{\Gamma_{2,1} + S_{2,3} + \Gamma_{1,1}\}$ is responsible for providing the supervisor with the vehicle longitudinal velocity calculated by the radar.

$\varphi_6 = \{\Gamma_{3,1} + S_{3,2} + \Gamma_{5,2}\}$ is responsible for providing the supervisor with the vehicle longitudinal velocity approximated by the wheels controller.

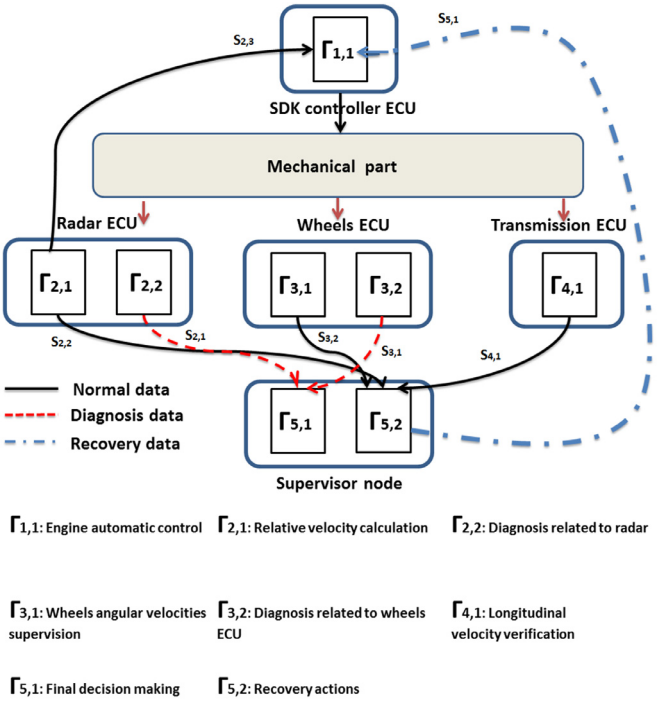

Fig. 9. SDK direct graph.

$\varphi_7 = \{\Gamma_{4,1} + S_{4,1} + \Gamma_{5,2}\}$ is responsible for providing the supervisor with the vehicle longitudinal velocity approximated by the transmission block.

The assignment of priorities according to the emergency level of tasks is assumed in the following order:

- The supervisor task, which ensures the recovery mission. Due to its responsibility in enabling/disabling the SDK system, this task has the highest priority.
- The radar diagnosis task, since losing the radar capacities is a serious hazard.
- The diagnosis tasks related to the wheels controller as well as the transmission controller.
- The rest of tasks have the same level of emergency.

Finally, the results of applying the RTA with the proposed schedulability schema are available in the next section.

5. Test conditions and simulation environment

The current section has as prospects to accommodate a middleware, which outlines the decentralized diagnosis hierarchy in a real environment. Since developing and implementing the whole system is not plausible due to the high cost, the HIL technique is adopted. Actually, the employment of the HIL approach has become lately more mainstream specifically in automotive research applications [58,59]. In this sense, an experimentation platform is implemented to hold simulated and real parts, which are communicating through a CAN bus. The virtual part comprises all the SDK components. It includes a truck mechanical behavior simulator, too. The latter applies physics laws to attain a high fidelity simulation for the truck dynamical parameters.

The real part includes two electronic nodes communicating through a real CAN bus. The first node, namely the bridge node, has the role of broadcasting messages from the SDK model. In accordance with the occurring event, the bridge platform substitutes physically the virtual model and requests the access to the communication bus. The second node represents the supervisor. According to received reports, a global decision is proclaimed. The realized middleware is linked from the supervisor side to in-cabin HMI by an RS232 communication. In this way,

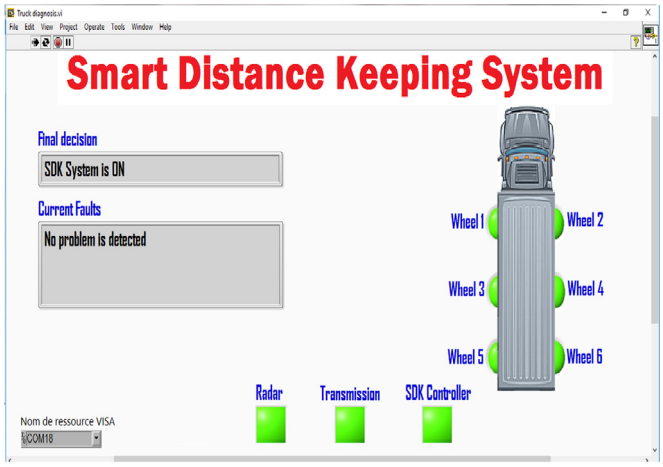

Fig. 10. SDK HMI.

information about the system state is instantly sent to the truck driver. The HMI layout is shown in Fig. 10. The hardware implementation is based on two ARM Cortex-M4 electronic boards. A max3232-based electronic card is used to establish USART communication between computers and real nodes. The USART communication has been used as an interface between the PC and the real electronic boards instead of a CAN bus connection to avoid the use of high-cost CAN-bus emulation software. SN65HVD230 transceivers are employed to enable the communication via the CAN bus. Fig. 11 presents the whole HIL-based experimentation platform.

To validate the efficiency of the proposed diagnosis design approach, it is necessary to compare:

- The WCRT of a given flow, obtained theoretically from the RTA approach.
- The response time of the same flow, which is measured by the experimental HIL platform.

The CAN bus is configured at a bit rate of 500 Kbit/s. Within this configuration, Tables 1–3 detail the approximation of WCRTs related respectively to flows φ_1, φ_2 and φ_3. Indeed, these flows are related to

Table 1
Elements in flow φ_1 and relative local WCRT.

Elements in flow φ_1	Local WCRT (ms)
$\Gamma_{5,2}$	7
$S_{5,1}$	0.36
$\Gamma_{1,1}$	11

Table 2
Elements in flow φ_2 and relative local WCRT.

Elements in flow φ_2	Local WCRT (ms)
$\Gamma_{2,2}$	8
$S_{2,1}$	0.52
$\Gamma_{5,1}$	9

Table 3
Elements in flow φ_3 and relative local WCRT.

Elements in flow φ_3	Local WCRT (ms)
$\Gamma_{3,2}$	4
$S_{3,1}$	0.68
$\Gamma_{5,1}$	11

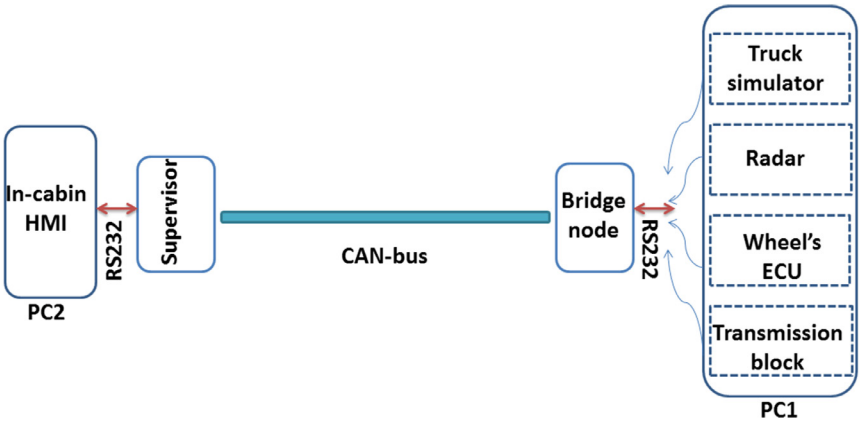

Fig. 11. HIL-based experimentation platform.

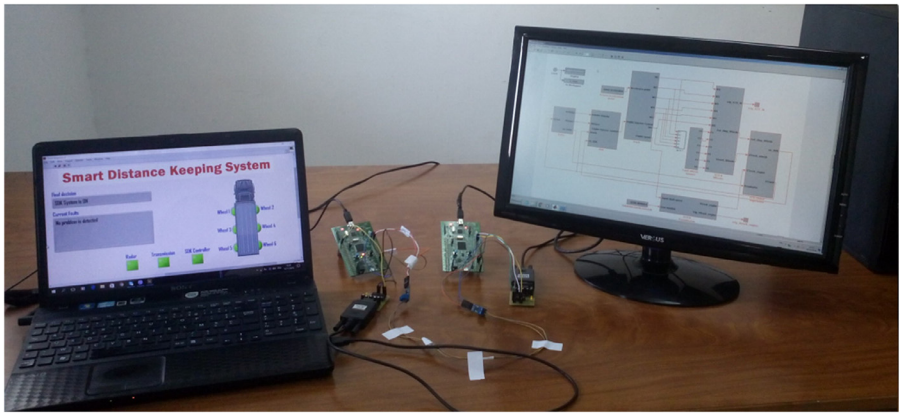

Table 4
Experimental results.

Configuration	MRT of φ_1 (ms)	MRT of φ_2 (ms)	MRT of φ_3 (ms)
Configuration 0	18.272	17.141	15.176
Configuration 1	18.281	17.356	15.258
Configuration 2	18.309	17.427	15.409
Configuration 3	18.407	17.549	15.639
Configuration 4	18.456	17.670	15.760

the most critical message streams. To be concise and rigorous, we only depict the temporal performances of these flows in this section.

Hence, final WCRTs are obtained by summing all the local WCRTs assigned to each element in the considered flow. After that, we consider five different scenarios corresponding to different fault-injection configurations. Particular diagnosis message streams are triggered in each case. During these tests, the number of injected faults is progressively increased and so is the bus-load. As a result, the established set of tests reproduces different situations of interference between tasks. Table 4 summarizes the experimental results of the Mean Response Time (MRT) of each flow (φ_1, φ_2 and φ_3). It shows that in case of a high bus-load (such as configurations 3 and 4), the experimental findings exceed slightly the theoretical results. The experimental results are affected by multiple HIL constraints and the employment of an SDK model instead of real ECUs. Actually, the release jitter period cannot be rigorously set. It is worth mentioning that the depicted experimental results take into account the data transmission time through the USART module. However, delays over RS232 are frequent but very small. Thus, since they are insignificant, these delays have been neglected in the present study. In practice, the CAN bus-load adopted in the established experimentations cannot be reached in realistic circumstances. For this reason, the slight difference noticed between the design phase findings and experimentations does not deny the efficiency of the RTA-CAN-based diagnosis.

6. Conclusion

In this paper, we have presented a novel engineering curriculum in order to reach a reliable and secure design of automotive embedded systems. The originality of the proposed approach lies in joining the decentralized diagnosis architecture with CAN real time analysis. Before looking for exact computation costs and rigorous response time via professional tools, a heuristic automotive design validation has been suggested. Our approach provides several advantages and contributions. Foremost, it effectively decreases the amount of exchanged messages between CAN nodes. Instead of overloading the network with extra-data diffusion, a supervisor node is charged to receive all diagnosis messages to finally report the system state. Otherwise, schedulability analysis is also applied to clearly assess the diagnosis data effect on the system operation. A reference model is adapted to facilitate the accomplishment of this goal. In such a way, the data traffic graphical model enhances the diagnosis architecture legibility and facilitates the establishment of further modifications in the diagnosis design.

Besides, the CAN-RTA tackled in this work oversteps the conventional node-level schedulability and expands our research to study tasks interactions. This point is extremely convenient for the diagnosis hierarchy, which separates the embedded functionalities of CAN nodes into diagnosis and operating tasks. To validate deadlines' meeting and ensure reliability, a novel priority assignment methodology named ELRM has been outlined.

The proposed early design phase has been applied on an anti-crash system. Meeting message deadlines has been approved. The decentralized RTA-based diagnosis design paradigm has contributed to overcome probable risks of network-induced delays. Such a paradigm is certainly efficient for the challenging design of today's automotive systems. Experiments have been carried out through the HIL-based middleware to enable data exchange between real and simulated automotive components.

CAN-RTA-based decentralized diagnosis is sufficiently mature for automotive diagnosis. Our future work should be extended to include uncertainties in deadline approximation. We also intend to provide a software platform in order to easily apply the proposed method. Otherwise, the methodology reported in this paper has to consider more practical limitations.

Acknowledgments

This work is a continuation to the DIAFORE (Diagnosis for Distributed Functions) project. The French National Research Agency (ANR), SYSTEM@TIC PARIS-REGION Cluster, French Environment and Energy Management Agency (ADEME) and French Programme of Research, Experimentation and Innovation in Land transport (PREDIT) are the principle funders and supporters to DIAFORE. Authors thank Renault Trucks/Volvo SAS and SERMA INGENIERIE for their cooperation in achieving the experimentation platform.

References

[1] D. Pan, Y. Zheng, Vehicle following control under a rational initial state, Nonlinear Dyn. 83 (1–2) (2016) 579–590.
[2] N.H. Amer, H. Zamzuri, K. Hudha, Z.A. Kadir, Modelling and control strategies in path tracking control for autonomous ground vehicles: a review of state of the art and challenges, J. Intell. Robot. Syst. 86 (2) (2017) 225–254.
[3] N. Onkarappa, A.D. Sappa, Speed and texture: an empirical study on optical-flow accuracy in adas scenarios, IEEE Trans. Intell. Transp. Syst. 15 (1) (2014) 136–147.
[4] F. Biondi, D.L. Strayer, R. Rossi, M. Gastaldi, C. Mulatti, Advanced driver assistance systems: using multimodal redundant warnings to enhance road safety, Appl. Ergon. 58 (2017) 238–244.
[5] R. Mebarki, V. Lippiello, B. Siciliano, Vision-based and imu-aided scale factor-free linear velocity estimator, Auton. Robot. 41 (4) (2017) 903–917.
[6] R. Gallen, A. Cord, N. Hautière, É. Dumont, D. Aubert, Nighttime visibility analysis and estimation method in the presence of dense fog, IEEE Trans. Intell. Transp. Syst. 16 (1) (2015) 310–320.
[7] S.L. Phung, M.C. Le, A. Bouzerdoum, Pedestrian lane detection in unstructured scenes for assistive navigation, Comput. Vis. Image Underst. 149 (2016) 186–196.
[8] S. Zhang, C. Bauckhage, A.B. Cremers, Efficient pedestrian detection via rectangular features based on a statistical shape model, IEEE Trans. Intell. Transp. Syst. 16 (2) (2015) 763–775.
[9] Y. Hashimoto, Y. Gu, L.-T. Hsu, M. Iryo-Asano, S. Kamijo, A probabilistic model of pedestrian crossing behavior at signalized intersections for connected vehicles, Transp. Res. Part C 71 (2016) 164–181.
[10] Y. Ouerhani, A. Alfalou, M. Desthieux, C. Brosseau, Advanced driver assistance system: road sign identification using viapix system and a correlation technique, Opt. Lasers Eng. 89 (2017) 184–194.
[11] T. Liu, Y. Yang, G.-B. Huang, Y.K. Yeo, Z. Lin, Driver distraction detection using semi-supervised machine learning, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 1108–1120.
[12] C. Purucker, F. Naujoks, A. Prill, A. Neukum, Evaluating distraction of in-vehicle information systems while driving by predicting total eyes-off-road times with keystroke level modeling, Appl. Ergon. 58 (2017) 543–554.
[13] X. Du, K.K. Tan, Comprehensive and practical vision system for self-driving vehicle lane-level localization, IEEE Trans. Image Process. 25 (5) (2016) 2075–2088.
[14] K. Jo, M. Lee, M. Sunwoo, Road slope aided vehicle position estimation system based on sensor fusion of gps and automotive onboard sensors, IEEE Trans. Intell. Transp. Syst. 17 (1) (2016) 250–263.
[15] E. Kokolaki, M. Karaliopoulos, G. Kollias, M. Papadaki, I. Stavrakakis, Vulnerability of opportunistic parking assistance systems to vehicular node selfishness, Comput. Commun. 48 (2014) 159–170.
[16] S.S. Avedisov, G. Orosz, Analysis of connected vehicle networks using network-based perturbation techniques, Nonlinear Dyn. (2017) 1–22.
[17] X. Du, K.K. Tan, Autonomous reverse parking system based on robust path generation and improved sliding mode control, IEEE Trans. Intell. Transp. Syst. 16 (3) (2015) 1225–1237.
[18] B. Li, Z. Shao, A unified motion planning method for parking an autonomous vehicle in the presence of irregularly placed obstacles, Knowl. Based Syst. 86 (2015) 11–20.
[19] M. Da Lio, F. Biral, E. Bertolazzi, M. Galvani, P. Bosetti, D. Windridge, A. Saroldi, F. Tango, Artificial co-drivers as a universal enabling technology for future intelligent vehicles and transportation systems, IEEE Trans. Intell. Transp. Syst. 16 (1) (2015) 244–263.
[20] J. Kim, S. Kim, C. Nam, User resistance to acceptance of in-vehicle infotainment (ivi) systems, Telecommun. Policy 40 (9) (2016) 919–930.
[21] J. Chen, B. Liu, H. Zhou, L. Gui, N. Liu, Y. Wu, Providing vehicular infotainment service using vhf/uhf tv bands via spatial spectrum reuse, IEEE Trans. Broadcast. 61 (2) (2015) 279–289.

[22] M. Becker, D. Dasari, S. Mubeen, M. Behnam, T. Nolte, End-to-end timing analysis of cause-effect chains in automotive embedded systems, J. Syst. Archit. 80 (2017) 104–113.
[23] F. Bock, S. Siegl, P. Bazan, P. Buchholz, R. German, Reliability and test effort analysis of multi-sensor driver assistance systems, J. Syst. Archit. 85–86 (2018) 1–13.
[24] D. Hernández-Alcántara, J.C. Tudón-Martínez, L. Amézquita-Brooks, C.A. Vivas-López, R. Morales-Menéndez, Modeling, diagnosis and estimation of actuator faults in vehicle suspensions, Control Eng. Pract. 49 (2016) 173–186.
[25] S. Huang, C. Zhou, L. Yang, Y. Qin, X. Huang, B. Hu, Transient fault tolerant control for vehicle brake-by-wire systems, Reliab. Eng. Syst. Saf. 149 (2016) 148–163.
[26] A. Haghani, T. Jeinsch, M. Roepke, S.X. Ding, N. Weinhold, Data-driven monitoring and validation of experiments on automotive engine test beds, Control Eng. Pract. 54 (2016) 27–33.
[27] C. Sankavaram, A. Kodali, K.R. Pattipati, S. Singh, Incremental classifiers for data–driven fault diagnosis applied to automotive systems, IEEE Access 3 (2015) 407–419.
[28] O. Nasri, H. Shraim, D. Philipe, O. Heron, M. Cartron, Modeling and deployment of model-based decentralized embedded diagnosis inside vehicles: application to smart distance keeping function, Int. J. Veh. Technol. 2012 (2012) 1–14.
[29] S. Noh, K. An, Decision-making framework for automated driving in highway environments, IEEE Trans. Intell. Transp. Syst. 19 (1) (2018) 58–71.
[30] Autoroutes.fr french motorway companies websited, 2018, Consulted in September, URL: http://www.autoroutes.fr/index.html.
[31] I. Gueddi, O. Nasri, K. Benothman, P. Dague, Fault detection and isolation of spacecraft thrusters using an extended principal component analysis to interval data, Int. J. Control Autom. Syst. 15 (2) (2017) 776–789.
[32] D. Zhang, P. Shi, Q.-G. Wang, L. Yu, Analysis and synthesis of networked control systems: a survey of recent advances and challenges, {ISA} Transactions 66 (2017) 376–392.
[33] P. Pelliccione, E. Knauss, R. Heldal, S.M. Ågren, P. Mallozzi, A. Alminger, D. Borgentun, Automotive architecture framework: the experience of volvo cars, J. Syst. Archit. 77 (2017) 83–100.
[34] D. Abdulmasih, P. Oikonomidis, R. Annis, P. Charchalakis, E. Stipidis, In-vehicle monitoring and management for military vehicles integrated vetronics architectures, J. Syst. Archit. 60 (4) (2014) 405–418.
[35] J.H. Kim, S.-H. Seo, N.-T. Hai, B.M. Cheon, Y.S. Lee, J.W. Jeon, Gateway framework for in-vehicle networks based on can, flexray, and ethernet, IEEE Trans. Veh. Technol. 64 (10) (2015) 4472–4486.
[36] G. Gut, C. Allmann, M. Schurius, K. Schmidt, Reduction of electronic control units in electric vehicles using multicore technology, in: V. Pankratius, M. Philippsen (Eds.), Multicore Software Engineering, Performance, and Tools, Springer, Berlin, Heidelberg, 2012, pp. 90–93.
[37] R. Berger, Consolidation in vehicle electronic architectures, In Think: Act, 2015. URL: https://www.rolandberger.com/en/Publications/pub_consolidation_in_vehicle_electronic_architectures.html.
[38] A. Hazra, P. Dasgupta, P.P. Chakrabarti, Formal assessment of reliability specifications in embedded cyber-physical systems, J. Appl. Logic 18 (2016) 71–104.
[39] D. Heffernan, C. Macnamee, P. Fogarty, Runtime verification monitoring for automotive embedded systems using the ISO 26262 functional safety standard as a guide for the definition of the monitored properties, IET Softw. 8 (5) (2014) 193–203.
[40] R. Pons, A. Subias, L. Travé-Massuyès, Iterative hybrid causal model based diagnosis: application to automotive embedded functions, Eng. Appl. Artif. Intell. 37 (2015) 319–335.
[41] A. Le Mortellec, J. Clarhaut, Y. Sallez, T. Berger, D. Trentesaux, Embedded holonic fault diagnosis of complex transportation systems, Eng. Appl. Artif. Intell. 26 (1) (2013) 227–240.
[42] W. Mu, J. Wang, W. Feng, Fault detection and fault-tolerant control of actuators and sensors in distributed parameter systems, J. Frankl. Inst. 354 (8) (2017) 3341–3363.
[43] Z. Feng, G. Hu, Distributed fault identification and fault-tolerant control for multi-agent systems, in: Proceedings of the 33rd Chinese Control Conference, 2014, pp. 1476–1481.
[44] S. Mubeen, J. Mäki-Turja, M. Sjödin, Mps-can analyzer: integrated implementation of response-time analyses for controller area network, J. Syst. Archit. 60 (10) (2014) 828–841.
[45] K. Tindell, H. Hanssmon, A.J. Wellings, Analysing real-time communications: controller area network (can)., in: RTSS, 1994, pp. 259–263. San Juan, Puerto Rico, USA, USA.
[46] H. Zeng, M. Di Natale, P. Giusto, A. Sangiovanni-Vincentelli, Using statistical methods to compute the probability distribution of message response time in controller area network, IEEE Trans. Ind. Inf. 6 (4) (2010) 678–691.
[47] H. Zeng, M. Di Natale, P. Giusto, A. Sangiovanni-Vincentelli, Stochastic analysis of can-based real-time automotive systems, IEEE Trans. Ind. Inf. 5 (4) (2009) 388–401.
[48] N. Navet, Y.-Q. Song, F. Simonot, Worst-case deadline failure probability in real-time applications distributed over controller area network, J. Syst. Archit. 46 (7) (2000) 607–617.
[49] H.A. Hansson, T. Nolte, C. Norstrom, S. Punnekkat, Integrating reliability and timing analysis of can-based systems, IEEE Trans. Ind. Electron. 49 (6) (2002) 1240–1250.
[50] M.B.N. Shah, A.R. Husain, H. Aysan, S. Punnekkat, R. Dobrin, F.A. Bender, Error handling algorithm and probabilistic analysis under fault for can-based steer-by-wire system, IEEE Trans. Ind. Inf. 12 (3) (2016) 1017–1034.
[51] Y. Xie, G. Zeng, Y. Chen, R. Kurachi, H. Takada, R. Li, Schedulability analysis for messages in gateway-interconnected controller area network, in: 2012 International Conference on Connected Vehicles and Expo (ICCVE), 2012, pp. 83–90. Beijing, China.
[52] Z. Shuai, H. Zhang, J. Wang, J. Li, M. Ouyang, Combined afs and dyc control of four-wheel-independent-drive electric vehicles over can network with time-varying delays, IEEE Trans. Veh. Technol. 63 (2) (2014) 591–602.
[53] S. Mubeen, J. Mäki-Turja, M. Sjödin, Extending worst case response-time analysis for mixed messages in controller area network with priority and fifo queues, IEEE Access 2 (2014) 365–380.
[54] S. Mubeen, J. Mäki-Turja, M. Sjödin, Integrating mixed transmission and practical limitations with the worst-case response-time analysis for controller area network, J. Syst. Softw. 99 (2015) 66–84.
[55] R. Lange, R.S. de Oliveira, F. Vasques, A reference model for the timing analysis of heterogeneous automotive networks, Comput. Stand. Interfaces 45 (2016) 13–25.
[56] R.I. Davis, A. Burns, R.J. Bril, J.J. Lukkien, Controller area network (can) schedulability analysis: refuted, revisited and revised, Real-Time Syst. 35 (3) (2007) 239–272.
[57] J. Liu, M. Wei, W. Hu, X. Xu, A. Ouyang, Task scheduling with fault-tolerance in real-time heterogeneous systems, J. Syst. Archit. 90 (2018) 23–33.
[58] C. Yang, X. Jiao, L. Li, Y. Zhang, Z. Chen, A robust hâ;; control-based hierarchical mode transition control system for plug-in hybrid electric vehicle, Mech. Syst. Signal Process. 99 (2018) 326–344.
[59] P. Fajri, V.A.K. Prabhala, M. Ferdowsi, Emulating on-road operating conditions for electric-drive propulsion systems, IEEE Trans. Energy Convers. 31 (1) (2016) 1–11.

Othman Nasri was born in Kasserine, Tunisia. In July 2004 and December 2007 correspondingly, he received his Post-Graduate Degree in Control Systems and Applied Informatics from Ecole Centrale de Nantes-France and his Ph.D. degree in Signal Processing and Telecommunications from CentraleSupelec of Rennes-France. From 2008 to 2010, he was a research Engineer in Embedded Control Systems in CNRS-University of Paris-Sud 11 / INRIA Saclay Ã;le-De-France. He is now Associate Professor /Director of the Department of Industrial Electronics of National Engineering School of Sousse, university of Sousse - Tunisia. His research interests include fault diagnosis and FTC, process modeling and monitoring, multivariate statistical approaches, safety verification of hybrid systems.

Nadhir Mansour Ben Lakhal is carrying his research works in automatic control on joint Ph.D program between the University of Sousse (Tuinisia) and Clermont Auvergne University (France). He received his engineering degree in Industrial Electronics in 2014 and his Msc. degree in intelligent and communicating systems in 2015 from the National Engineering School of Sousse, Tunisia. He focalizes his researchers on vehicle/robot safe and autonomous navigation and hybrid systems verification.

Lounis Adouane is an Associate Professor since 2006 at the Institut Pascal-Polytech Clermont-Ferrand in France. He received an M.Sc in 2001 from IRCCyN-ECN Nantes, where he worked on the control of legged mobile robotics. In 2005, he obtained a Ph.D. in automatic control from FEMTO-ST laboratory-UFC Besancon. During his Ph.D. studies he deeply investigated the field of multi-robot systems, especially those related to bottom-up and reactive control architectures. After that, he joined in 2005 Ampére laboratory-INSA Lyon and studied hybrid (continuous/discrete) control architectures applied to cooperative mobile robot arms. Dr. Adouane had the opportunity to visit several institutions/laboratories, such as 1 month in 2009 at LIST (Luxembourg) and 6 months in 2014 at Cranfield and Kingston universities (United Kingdom). In 2015, he obtained from Blaise Pascal University a HDR (habilitation to steer research in Robotics). Since 2006, he has authored/coauthored more than 70 international references and 2 books. His main research interests include: Autonomous mobile robots/vehicles, Behavioral/multi-controller architectures, Obstacle avoidance, Lyapunov-based synthesis and stability, Cooperative robotics, Task/trajectory planning and replanning, Artificial intelligence, Multi-robot/agent simulation.

Jaleleddine Ben Hadj Slama (SM'13) was born in Tunisia, on May 30, 1971. He received the engineer and the Ph.D. degrees, both in electrical engineering, from Ecole Centrale de Lyon, Lyon, France, in July 1994 and December 1997 respectively. Since 2015, he is full Professor in Electrical Engineering at the National Engineering School of Sousse, Tunisia, where he is the leader of the Smart Grid and Renewable Energy research group in LATIS laboratory. His main research interests include Renewable Energy and their integration in Smart Grid, power electronics systems and their modeling, Electromagnetic Compatibility (EMC) and reliability of transportation systems and development of remote laboratories for Internet Based Engineering Education.