Evaluating Quality of Service and Behavioral Reliability of Steer-by-Wire Systems

Cédric Wilwert, Ye-Qiong Song, Françoise Simonot-Lion, Thomas Clément

Evaluating Quality of Service and Behavioral Reliability of Steer-by-Wire Systems

Cédric Wilwert (LORIA-INPL/PSA Peugeot Citröen)
cwilwert@ensem.inpl-nancy.fr
YeQiong Song (LORIA-INRIA)
song@loria.fr
Françoise Simonot-Lion (LORIA-INPL)
simonot@loria.fr

LORIA -TRIO
2, av. de la Forêt de Haye
54516 Vandoeuvre-lès-Nancy CEDEX

Thomas Clément (PSA Peugeot Citroën)
thomas.clement@mpsa.com

PSA Peugeot Citroën
18, rue des fauvelles
PB 16, 92256 la Garenne-Colombes CEDEX

Abstract **– Steer-by-wire systems must meet not only reliability but also real-time requirements. This paper presents an integrated approach for evaluating both the temporal performance and the behavioral reliability of Steer-by-wire systems taking into account the delay variation introduced by network transmission errors. The considered temporal performance is the Quality of Service perceived by the user, i.e. the vehicle stability. Tests in vehicles and simulations have been realized to estimate the maximum tolerable response time of the system, and to evaluate the impact of this delay on the Quality of Service. We quantify then the worst case response time of the system for a generic architecture based on TDMA protocol but independent of the communication network (could actually be TTP/C or FlexRay), and apply these generic results to a case study. We further define the notion of "behavioral reliability" as the probability that "the worst case response time is less than a threshold". In our case study this behavioral reliability is evaluated and linked to the Safety Integrity Levels defined in IEC61508-1 standard. Based on this behavioral reliability concept, the final objective of our work is to propose a new dependability analysis method for X-by-Wire systems by taking into account both dynamic performance, fault-tolerance mechanisms and static redundancy of the system[1].**

1. INTRODUCTION

Car makers are introducing X-By-Wire systems to replace mechanical controls and linkages. Such embedded electronic systems must satisfy both stringent real-time performance and reliability requirements.

An automotive Steer-By-Wire (SBW) system is safety-critical and the first thing a car maker should prove is that the SBW system embedded in a produced car has a very small probability to have a failure. Although regulating organisms have not yet established the automotive-specific requirement on this probability but the 10^{-9} failures/hour from the regulators of the commercial aircraft industry seems to be adopted [Ham03], [Wil03].

According to [Lap92], a system is dependable if a user interacting with the system has good reasons to trust the service the system delivers. The safety is the probability that the system will not cause severe damage to humans or substantial economic loss. The reliability, probability that a system will fulfil the service a user expects, is computed with the Mean Time To Failure (MTTF) $1/\lambda$ (λ is called failure rate) according to the failure distribution: $R(t) = P(1/\lambda>t)$. So, depending on the mission phase of the vehicle, the safety can sometimes be considered as the reliability of the system. For given MTTF of the components (Sensors, Computers, Network links, actuators) and their redundancy, static reliability analysis can give the total reliability of the SBW system. However a static reliability of less than 10^{-9} is a necessary condition but as we show below it is not a sufficient one. For example, transient faults aren't treated in these kinds of evaluation as well as the time consideration. [Zwi99] added that the transitions between a nominal mode and a failure mode can be progressive, sudden or random, however the reliability doesn't know the notion of partial or progressive failure.

In fact, a SBW system is also time-critical and its timely reactivity directly impacts on the safety of the car. For instance the delay introduced by a SBW system between a driver's request and the activation of the wheels can be

[1] This work is supported by the grant ANRT N°582/2001 LORIA - PSA Peugeot-Citroën

considered as a performance measure until a certain threshold value but must be considered as a dependability measure when the delay is beyond this threshold value since in this case the driver could totally loss the control of his car ! So only the reliability of 10^{-9} is not sufficient and the real-time performance should also be evaluated.

Note that X-by-Wire systems usually integrate a lot of fault tolerant mechanisms; not only static redundancy, but also dynamic reconfiguration, acknowledgement of transmitted messages, software diversifications, etc. All these services contribute to achieve the dependability. But their impact on the dependability is difficult to evaluate. Some work [Ham03] considers these services with a Fault-Tolerance Coverage Rate. But the main problem is that with X-by-Wire systems, we haven't any experience feedback, so it seems complicated to give a coverage rate to a fault-tolerant service, even if it is possible for some of them.

So, if it is today established that the reliability is a static measure which is independent of the dynamic behaviour of the system, we can consider a new kind of reliability which is dependant on the past and present events. This new measure, which can vary during the time, will be named “Behavioural Reliability”.

Classic performance evaluation and reliability analysis are two separate studies on the same system. However as we have explained above, the total dependability is a function of these two aspects. Moreover, transient faults such as transmission errors may lead to degrading the performance of the system or even transgressing the dependability. Therefore some integrated dependability measures are necessary. The difficulty is how to combine these two aspects into an integrated approach.

Some methods go in this direction. HRT-HOOD [Bur95] proposes to integrate the schedulability analysis into the dependability study but without taking into account the dynamic performance and transient failures. GUARDS (Generic Upgradable Architecture for Real-Time Dependable Systems) (ESPRIT project 20716) [Pow99] has objective to develop a generic design architecture for real-time dependable systems by integrating performance evaluation into classic dependability analysis. However the methods are only put together and there lack links between different results produced by the different methods. HIDE (High-Level Integrated Design Environment for Dependability) (ESPRIT Project 227493) [HID98] does more on the integration of the methods by using a common UML-based model description allowing thus the automatic generation of analysable sub-models on Petri net and Kripke structures. However because of the complexity of the tool, the sub-models generated are not easily analysable. PALBUS project [PAL01] tried to give a framework to X-by-Wire system design. The main advantage of PALBUS project is that it gives an overview of the recent work addressing the X-by-Wire dependability problematic, at every level of the design process (architecture, software, testing…).

Our main idea for integrating these two aspects is based on the data validity and its timely delivering perceived by the data consumer (actuator). Redundancy of network links and producers of a same datum (sensors) could thus be seen as increased data validity probability and transient faults such as loss of a data packet by network as an increased data delivery delay.

The main objective of this study is to propose an integrated method for evaluating both the real-time performance and the “Behavioural Reliability” of the system. The criteria evaluated is the Quality of Service (QoS) as perceived by the user according to the response time of the system, considering that this response time can also impact the availability and in the worst case, the safety. In fact, if the response time of the system is too important, the safety of the user can be impacted. Then, we also quantify the probability of impacting the user’s safety by means of Behavioural Reliability.

The rest of the paper is organised as follows. In section 2, for generic SBW architectures with TDMA-based communication protocol (could actually be FlexRay, TTP/C…), we present the method to quantify the Worst Case Pure Delay and its relation with the Quality of Service and the Behavioural Reliability. In section 3 we propose a realistic study case with an example of SBW architecture and its temporal characteristics. According to the corresponding hypothesis, we apply the method and present the obtained results. Section 4 concludes this study and points out the future work by replacing our study within a more general context.

2. PRESENTATION OF THE METHOD

The main objective of this study is to propose a method to evaluate the Behavioural Reliability of the system. The criteria evaluated is the QoS depending on the response time of the system, considering that this response time can also impact the availability and in the worst case, the safety.

We first define the pure delay introduced by a SBW system between the hand wheel request to the reception of the driver’s request by the front axles actuators (Fig.1).

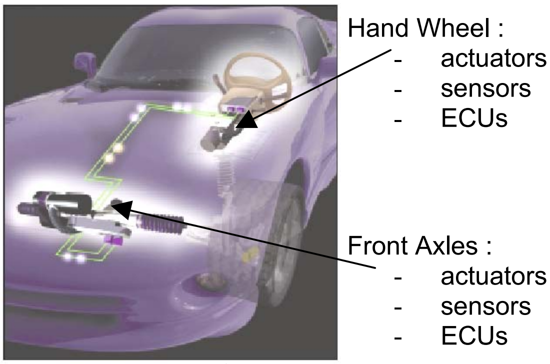

Figure 1[2]: Steer-by-Wire system

The total response time of the system hand wheel request and front axle response is divided into the pure delay and the mechatronic delay (figure 2).

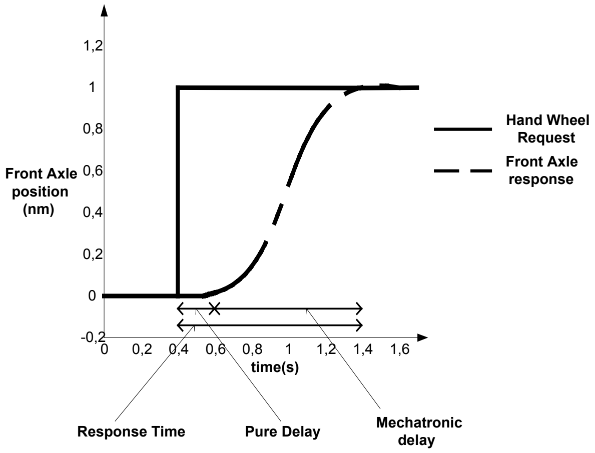

Figure 2: Steer-by-Wire system response time

The mechatronic delay is the time necessary for the actuator to reach the front axle position and the pure delay is directly related to the “by-wire” operation (processing time in the ECUs (Electronic Control Unit), network delay, …) (figure 2). As we consider that the mechatronic delay is constant, we will only analyze the impact of the pure delay on the Quality of Service.

A. Impact of the pure delay on the QoS

PSA Peugeot Citroën has realised a series of tests in vehicle to evaluate the impact of the pure delay on the QoS with an embedded SBW system. The QoS relative to the prestation of the system like variable demultiplication of the force applied to the wheel, or feedback force are beyond the scope of this paper. Simulations have also been realised on Matlab Simulink with injection of parameters perceived by the user during the tests. An estimated model Δ[3] has been deduced, that gives a relationship between the QoS "as perceived by the user" and the pure delay of the SBW system. Such a model is used to dimension actuators, sensors and processing delay in mechatronic systems like electrical assisted steering.

The parameters injected in this model are the time necessary to reach the desired position and the vehicle stability according the 3D axis represented in figure 3. The QoS is then estimated as a score denoted by N according to the time dedicated to reach the desired position and stability. Until a certain limit the QOS is “acceptable” (the delay is not impacting the user sensitivity). After this limit, the safety of the user is not guaranteed. In fact, the *availability* of the function “turning the wheels according to the user’s will” can impact the *safety* of the user after a certain delay.

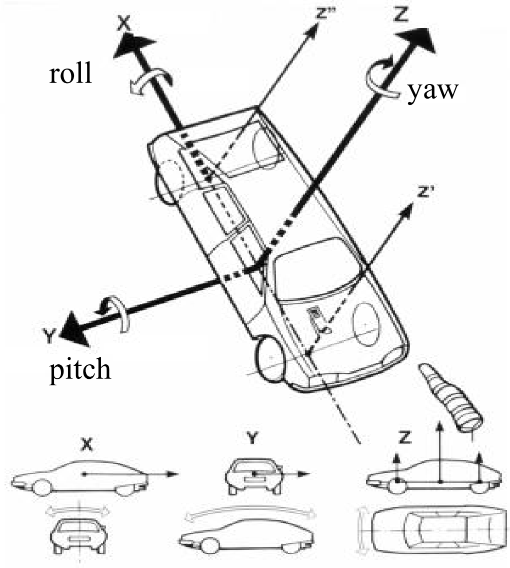

Figure 3: stabilisation of the vehicle according to the 3 axis

According to theses considerations, the table 1 has been obtained for a specific vehicle type:

[2] Picture taken from: www.delphi.com

[3] Details are not given for the confidentiality reason.

Configuration of the Steering System	Pure Delay (ms)	Score N
Mechanical steering system	0	11.23
Steer-by-Wire	5	11.21
Steer-by-Wire	10	11.19
Steer-by-Wire	15	11.15
Steer-by-Wire	20	11.13
Steer-by-Wire	25	11.10
Steer-by-Wire	30	11.05
Steer-by-Wire	**35**	**11**
Steer-by-Wire	50	10.90
Steer-by-Wire	100	10.45

Table 1: QoS score vs. Pure Delay

Table 1 shows the relation between the score N given to the system and the pure delay recorded, but it also shows the critical limit for the pure delay: after this limit, the safety of the driver can be impacted. This critical limit has been detected at 35 ms for pure delay. We notice that this limit of 35 ms is specific a vehicle type so readers should not consider it as available for theirs. All these results will be the criteria for the proposed method.

B. Hypothesis

We will only consider here the functionality of "turning the wheels according to the user's will". For this control chain we identified four functions:

- F1: Hand wheel position acquisition
- F2: Front axle activation
- F3 : Hand wheel measure treatment
- F4: Front axle order computation

As well as the information flow between these functions (Fig. 4). The behaviour of each function is specified according to the control law and the coordination between them follows time-triggered approach.

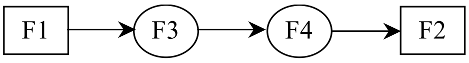

Figure 4: Functional Architecture (FA)

The implementation of this FA respects the following hypothesis:

- Distribution of functions on separate equipments (F1 on sensor, F2 on actuator, F3 and F4 on Electronic Control Units)
- Replication of each function (so replication of equipments)
- Flow exchange ensured by a TDMA-like communication protocol
- Algorithms on each equipment are periodically activated and if replicated inputs exist the activation is assumed at the end of the last input of the period

The information is transmitted from the Hand Wheel Sensor to the Front Axle Actuator through different nodes via network. Sensors and actuators are assumed directly linked to an ECU via point to point links. For the considered control chain, the first node is always the Hand Wheel ECU - or the replicated Hand Wheel ECUs – and the last the Front Axle ECU (figure 1). Between these ones, central ECUs can exist.

The access of each ECU to the network is organized in a cyclic way with a macro cycle which is composed of several micro cycles, each micro cycle being divided into slots:

- T_{MA} is the duration of a macro cycle
- T_{MI} is the duration of a micro cycle
- A macro cycle of communication is composed of n micro cycles: $T_{MA} = nT_{MI}$.
- A node is allowed to access the communication medium one time per micro cycle, in a predefined and static temporal window (a slot).
- For a given node, an information is delivered one time per macro cycle (but the same information can be delivered several times per macro cycle if replicated nodes deliver replicated information).

The actuator begins to reach the desired position on the Front Axle when it has received all the replicated information (it waits for the last replicated information).

C. "Worst Case Pure Delay" without transmission errors

We generally use the notion of the worst case response time when the objective is to dimension real-time systems. However, in this study, what really impacts the QoS is the variation of the pure delay. We will study the "worst case pure delay" denoted by T_{WCPD}, first in nominal mode (without faults).

As the macro cycles are predefined and cyclic, the pure delay is not the same whether the hand wheel stimulus arrives at the beginning of the cycle or at the end, that's why a "worst case pure delay" exists. As we consider the function "turning the wheels according to the user's will", we can assert that the "worst case pure delay" appears when the stimulus is given at the beginning of the first temporal window reserved for a Hand Wheel ECU in the macro cycle. In fact, it is the worst case because the treated information is the last received from the sensor just before this temporal window. So, the stimulus given at the beginning of the first temporal window reserved for a Hand Wheel ECU in the macro cycle has to wait for the treatment of the last information plus a macro cycle (see example 3.B). The treatment of the last information will last from the beginning of the first temporal window reserved for a Hand Wheel ECU in the macro cycle until the end of the last temporal window that contains the information in its final form for being treated by the actuator (see example 3.B), we call it T_{NET} added to the treatment time of the Front Axle ECU T_T.

So we can assert that:

$$T_{WCPD} = T_{NET} + T_T + T_{MA}$$

$$T_{WCPD} = T_{NET} + T_T + nT_{MI} \quad (1)$$

This result should be used for the system dimensioning during the design step in order that T_{WCPD} is smaller than the deadline (e.g. 35 ms for the example of Table 1).

D. "Worst Case Pure Delay" with transmission errors

Our study considers an error the fact that the information is delayed because of diverse faults as EMI perturbation, or physical faults on the ECUs or sensors. If the information is delayed, it will be translated by an empty or erroneous (we treat it as an identical case) slot (temporal window). But, as the information is replicated in different slots, for the actuator, the information is considered as lost only if all the replicated slots are empty or erroneous. So, with our hypothesis, an error will be translated by the lost of a macro cycle. From a temporal point of view, for every error, T_{MA} will be added to the precedent pure delay.

As an error burst can impact consecutive macro-cycles, the more the error burst is longer, the more the pure delay is augmented. So we study the response of the system to the sequences with valid and erroneous macro cycles.

The erroneous macro cycles are assumed independent events and the probability of losing one macro cycle can be calculated given the frame error rate (or equivalent to the slot error rate).

If E_R is the frame error rate, and if the information is replicated r times per macro cycle, it can be shown that the probability of losing a macro cycle is $(E_R)^r$. It is worth noting that this result remains valid for whatever distribution of the r slots (or frames) within a macro cycle.

For time varying frame error rate (e.g. burst error arrival pattern in [Nav00]), more complicated mathematical analysis should be used to deduce the probability of losing a macro cycle. This is beyond the scope of our paper.

So we only focus on the study of the response of the system to a sequence of valid and erroneous macro-cycles by using the following approach similar to that in [Jum03], which defines a explicit formal relation between a failure of the control system and a failure of the regulated system in the simple case of a tankwater Let us consider a sequence $(\varepsilon_i, \varepsilon_{i+1}, \ldots, \varepsilon_{i+n})$, such as $\varepsilon_i \in [0\ ;1]$. For example, the sequence (0,0,1,1,0,0,0,0) corresponds to 2 valid macro cycles, and 2 erroneous macro cycles, and finally 4 valid macro cycles.

If $\varepsilon_i = 1$, we have lost one macro cycle, so T_{MA} will be added to the precedent pure delay. Consequently, the response T_{ERR} to such a sequence is:

$$T_{ERR}(i) = (1- \varepsilon_i)T_{WCPD} + \varepsilon_i.T_{ERR}(i-1)+\varepsilon_i.T_{MA}$$

According to equation (1) we have

$$T_{ERR}(i) = (1-\varepsilon_i)(T_{NET}+T_T+nT_{MI})+\varepsilon_i.T_{ERR}(i-1)+\varepsilon_i.nT_{MI} \quad (2)$$

(if $\varepsilon_i = 1$, then we add the elapsed time corresponding to the number of erroneous macro cycles

if $\varepsilon_i = 0$, the pure delay is T_{WCPD} *(see relation (1)*)

E. Behavioural reliability evaluation

As $T_{ERR}(i)$ is random and time varying, it is not always possible to dimension the system for meeting the requirement of $T_{ERR}(i)$ < Deadline for $\forall i \in \mathbb{N}$. So we propose to evaluate the probability of meeting this requirement.

According to Table 1, if $T_{ERR}(i)$ > 35 ms, the safety is impacted. In terms of the dependability, we can then study the probability of having the event $T_{ERR}(i)$ > 35 ms. [Wil03] indicates that the probability of having such an event (event that can impact the safety of the user) must be inferior to 10^{-9} per hour. So, in addition to the QoS evaluation, our method can also be used to analyse if the studied system verifies the reliability requirements. This measure is called behavioural reliability as the event of $T_{ERR}(i)$ > 35 ms is only because of the dynamically occurred transmission errors but not because of the system design.

We define:

- D= maximum tolerable pure delay
- P_{BR}= behavioural reliability
- SIL= Safety Integrity Level of the system

So the Behavioural Reliability is calculated by:

$$P_{BR} = P[T_{ERR}(i) > D] \quad (3)$$

This probability can be directly used to determine the SIL as shown in Table 2.

Safety Integrity Level (SIL)	Probability of dangerous failure per hour (P_{FAIL})
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 2: Safety Integrity Levels [IEC]

The CEI61508 [IEC] determines the Safety Integrity Levels (SIL) for safety related systems in term of probability of dangerous failure per hour. The requirements for X-by-Wire systems are discussed in [Wil03] and different SILs can be given for every high-level functions.

So, for the studied function and the corresponding SILi, we must have:

$$P_{BR} < P_{FAIL}[SILi] \qquad (4)$$

3. CASE STUDY

To illustrate our proposition, this following case study is considered showing how to apply our method to a SBW architecture (figure 3) .

A. Presentation of the architecture

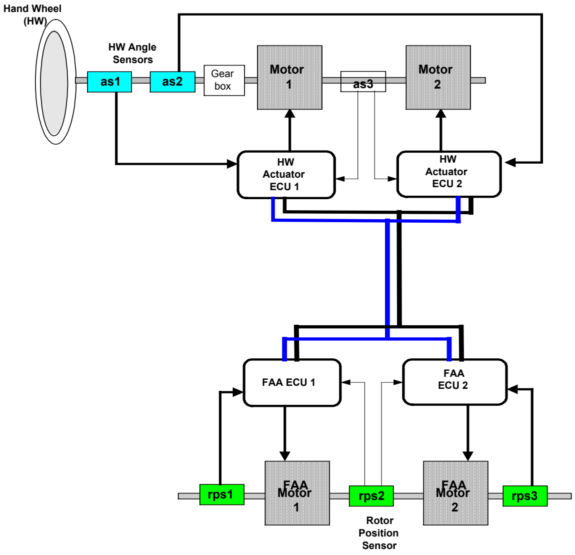

Figure 5: Steer-by-Wire architecture

Legend :

▬ TDMA network

→ Point to point link

as: hand wheel angle and speed sensors

HW actuator : Hand Wheel actuators for Force Feedback

ECU : nodes

FAA : front axle actuators

rps : front axle position sensors

The chosen architecture seems a realistic one for commercial vehicles. In fact, a lot of SBW architectures are presented with central ECU between the Hand Wheel and the Front Axle [ESP98], but in terms of cost it seems not to be very realistic for mass production. That's why we have chosen an architecture with only four ECUs (Fig. 5). This architecture is constructed with three Hand Wheel Sensors connected to two Hand Wheel ECUs, a Time-Triggered communication network, two Front Axle ECUs connected to three sensors. Hand Wheels ECUs are also connected to 2 actuators for the Force Feedback, and Front Axles ECUs are connected to actuators to turn the wheels.

Treatments in redundant ECUs are made in parallel. For example, ECU HWA1 and ECU HWA2 (Fig. 5) receive the data from the sensors synchronously, so they treat it at the same time. The figure 6 shows that during temporal window HWA1, ECU HWA1 and ECU HWA2 are treating data in parallel.

B. Temporal characteristics

Hypothesis:

- duration of a micro cycle : T_{MI} = 4ms
- duration of a macro cycle : T_{MA} = 8ms
- number of micro cycles per macro cycle: n = 2
- every slot has the same duration: 1ms
- T_{NET} *(form the beginning of the first temporal window reserved for a Hand Wheel ECU in the macro cycle until the end of the last temporal window that contains the information in its final form for being treated by the actuator)*= 2 ms
- T_T = 0.5 ms

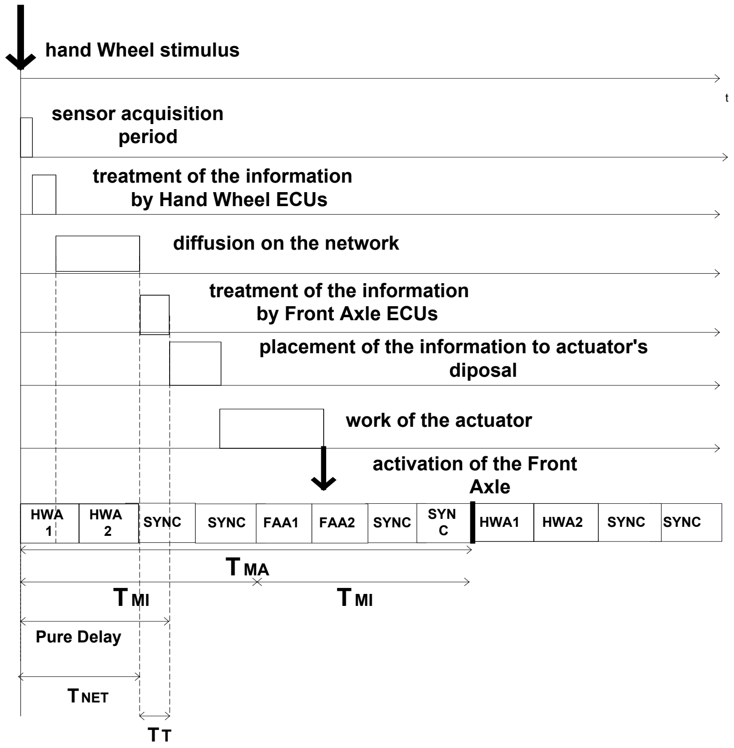
hand Wheel stimulus
t
sensor acquisition period
treatment of the information by Hand Wheel ECUs
diffusion on the network
treatment of the information by Front Axle ECUs
placement of the information to actuator's diposal
work of the actuator
activation of the Front Axle
HWA 1
HWA 2
SYNC
SYNC
FAA1
FAA2
SYNC
SYN C
HWA1
HWA2
SYNC
SYNC
T MA
T MI
T MI
Pure Delay
T NET
T T

Figure 6: Temporal characteristics of the function “turning the wheels according to the user’s will”

We now have enough information to apply the method of evaluation of the QoS presented in section 2.

C. “Worst Case Pure Delay” without transmission errors
We recall the hypothesis:

- $T_{MI} = 8ms$
- $n = 2$
- $T_{NET} = 4ms$
- $T_T = 1ms$

So, according to the relation (1), the “Worst Case Pure Delay” T_{WCPD} of the proposed system is:

$$T_{WCPD} = T_{NET} + T_T + nT_{MI} = \mathbf{21\ ms}$$

This means that the studied SBW system provides in the worst case (without transmission errors) a QoS of about 11 according to Table 1.

D. “Worst Case Pure Delay” with transmission errors
It is quite difficult to fix a frame error rate today, mainly because the experience feedback for steer-by-wire systems is quite reduced, with new fault tolerant mechanisms such as the redundancy of the transmission channels. Moreover, this will be one of the next step of our work. So we developed a software to simulate the response of the system to a sequence of different macro cycles with increasing error rate according to the hypothesis of the precedent paragraph. To every pure delay corresponds the score of the QoS according to Table 1. So, by averaging the obtained scores, we can deduce and score that is representative of the QoS score of the studied system..

Qos Score of the system	**Probability of losing a macro cycle**				
	10^{-3}	10^{-4}	10^{-5}	10^{-7}	**Probability of reaching the QoS score**
11,13	*10^{-3}*	*10^{-4}*	*10^{-5}*	*10^{-7}*	
11,05	*10^{6}*	*10^{-8}*	*10^{-10}*	*10^{-14}*	
<11	*10^{-9}*	*10^{-12}*	*10^{-15}*	*10^{-21}*	

Table 3: QoS score of the system in function different error rates

Table 3 shows the different probability of reaching a QoS score at an instant t during the exploitation of the system, in function the macro cycle error rate. We restrict the study with a macro cycle error bounded by 10^{-3} because it seems to be the most realistic values.

E. Behavioral Reliability Evaluation
As explained above, the frame error rate is for the moment difficult to quantify, that’s why we evaluated the probability of having the event $T_{ERR}(i) > 35$ ms in function of different macro cycle error rates (Figure7).

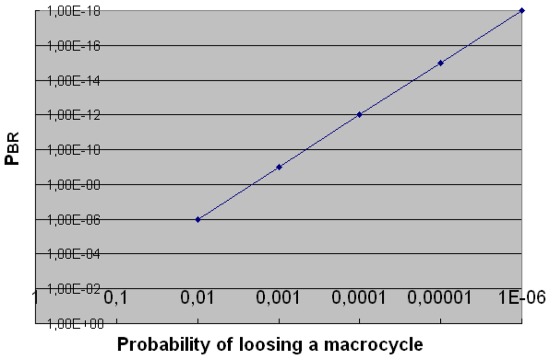

Figure 7: Probability P_{BR} of having the event $T_{ERR}(i) > 35ms$ in function of different error rates

The analysis of the curve shows that for a macro cycle error rate of less than 10^{-3}, the studied system meet the requirements of SIL 4 (Table 2).

4. CONCLUSIONS AND FUTURE WORK

The method presented in this paper is the first step towards to a more global work aiming to define a method for the dependability and Quality of Service evaluation of X-by-Wire systems taking into account both dynamic performance, fault-tolerance mechanisms and static redundancy of the system. The present paper shows that it is possible to integrate dynamic performance behavior such as response time variation into the dependability evaluation. Moreover, the presented method evaluates the QoS of the system, then, if two architectures verify both the dependability requirements, it is possible to compare them according to their QoS. This paper also introduce the notion of "behavioural reliability": even if the event "not performing the specified functionality within a specific time frame" is a failure - so the probability that this failure appears can be simply quantified by evaluating the MTTF -, as the specific time frame can vary according to the mission phase of the vehicle, the scheduling, and other dynamic parameters, this notion is different from the static reliability usually quantified.

However, static aspects such as the redundancy and the reliability of the components (ECUs, Communication medium, etc.) are indispensable for dependability evaluation. So, the next step of our work will be to inject these considerations into our method.

Fault Tolerant mechanisms, either proposed by the communication protocol or implemented in the ECUs [Ham03], change dynamically the performance of the system. They will also have to be included in the method. This is another consequent part of the future work. A lot of studies [Rus01] are provided today in this topic, mainly focused on the comparison of the protocols for X-by-Wire systems: TTP/C and FlexRay. Evaluating the impact of the fault tolerant mechanisms of both the communication protocol and ECUs on the global dependability is a very ambitious challenge.

REFERENCES

[Bur95] A. Burns and A. Wellings, "HRT-HOOD: A Structured Design Method for Hard Real-Time Ada Systems," *Real-Time Safety Critical Systems*, Elsevier, Vol. 3, 1995.

[ESP98]http://www.vmars.tuwien.ac.at/projects/xbywire/projects/tuwien.html (conclusions of ESPRIT project)

[Ham03] R, Hammett, P Babcock, "Achieving 10U-U9 Dependability With Drive-By-Wire Systems", *SAE 2003 World Congress & Exhibition*, Detroit (USA), March 2003

[Ham85] R, Hammett, P Babcock, "IEC Reliability, Maintainability and Quality of Service", *Chap . 191, International Electrotechnical Vocabulary, Document 1-IEV-191-Central Office-1243 and 56-IEV-191-Central Office-119*, Genève (Switzerland), IEC, 1985.

[HID98] HIDE, "Esprit LTR 27439 HIDE," Public home page: https://asterix.mit.bme.hu:998/ 1998.

[IEC] IEC61508-1, "Functional Safety of electrical electronic programmable electronic safety-related systems - Part 1 : General requirements", IEC/SC65A, October 1998.

[Jum03] F. Jumel, N Navet, F. Simonot-Lion, "Influence des performances d'une architecture informatique sur la fiabilité des systèmes échantillonnés", *RTS03*, Paris (France), april 2003.

[Lap92] Laprie, J. C., (ed.) "Dependability: Basic Concepts and Terminology", Springer-Verlag, Wien, 1992.

[Nav00] N. Navet, Y.Q. Song, F. Simonot, "Worst-case deadline failure probability in real-time applications distributed over CAN (controller area network)", Journal of systems architecture - the EUROMICRO Journal, 46 (2000) pp607-617.

[PAL01] PALBUS Project http://www.sp.se/electronics/RnD/palbus/

[Pow99] D. Powell, J. Arlat, L. Beus-Dukic, A. Bondavalli, P. Coppola, A. Fantechi, E. Jenn, C. Rabéjac and A.Wellings, "GUARDS: A Generic Upgradable Architecture for Real-time Dependable Systems," I*EEE Trans. on Parallel and Distributed Systems*, 1999.

[Rus01] J. Rushby, "A Comparison of Bus Architectures for Safety-Critical Embedded Systems", *Technical report, Computer Science Laboratory, SRI International*, 2001.

[Sta88] J. Stankovic, "Misconceptions About Real-Time Computing: a serious problem for Next Generation Systems", *IEEE Computer*, pp. 10-19, Oct 1988

[TTP] TTP/C Specifications, http://www.tttech.com

[Wil03] C. Wilwert, A. Charlois et F. Gailliègue, "Les services réseaux pour les systèmes X-by-Wire", *RTS03*, Paris (France), april 2003.

[Zwi99] G. Zwingelstein, « Sûreté de fonctionnement des systèmes industriels complexes », *Techniques de L'Ingénieur*, article S8250, volume S, septembre 1999.