Quantitative Evaluation of the Safety of X-by-Wire Architecture subject to EMI Perturbations

Françoise Simonot-Lion, François Simonot, Ye-Qiong Song, Cédric Wilwert

Quantitative Evaluation of the Safety of X-by-Wire Architecture subject to EMI Perturbations

Cédric Wilwert
PSA – Peugeot Citroën
La Garenne Colombes
Cedric.wilwert@mpsa.com

Françoise Simonot-Lion[1], YeQiong Song[2], François Simonot[3]
(1) LORIA – INPL, (2) LORIA – UHP,
(3) IECN – ESSTIN
BP 239 – Vandœuvre-lès-Nancy (France)
(simonot,song)@loria.fr
simonot@esstin.uhp-nancy.fr

Abstract

The X-by-Wire systems in cars can only be accepted if they provide at least the same dependability than the traditional ones. In this paper we propose a new approach to evaluate the impact of the EMI perturbations on the dependability of an X-by-Wire architecture. The considered X-by-Wire architecture is distributed around a TDMA-like communication protocol. So a perturbation causes the loss of a communication cycle with a certain probability. The vehicle level failure is then defined as the consecutive loss of a certain number of communication cycles. Its reliability is modeled as that of the well-known consecutive-k-out-of-n:F systems. A case study, together with the EMI perturbations collected on the roads in France, is used to illustrate our approach.

1. Introduction

For the last decade, an increasing number of functions in a car are ensured by electronic systems. This evolution, formerly confined to functions such as engine control, now affects almost all car domains: wipers, lights, air condition, door controls, braking assistance, etc. In the future, even critical functions such as throttle, brake or steering will be fully controlled by electronic systems leading to the *X-by-Wire* concept. As any dysfunction of Steer-by-Wire, Brake-by-Wire or Throttle-by-Wire systems would jeopardize the safety of the occupants and of the environment of a car, it is necessary to prove that such a system respects the safety and more generally dependability requirements. It is a challenging problem to prove such properties because of the lack of experience in the automotive industry with X-by-Wire systems and because of the complexity of these systems.

Several techniques are available for dependability assessment [1]. In particular, on the one hand, fault forecasting based on hardware architectures and on the permanent faults that may affect their hardware components and on the other hand, faults that can occur during the specification, the design and the coding of software components are nowadays well mastered in automotive industry. Nevertheless, these techniques are not sufficient for ensuring dependability properties.

In fact, an X-by-Wire system is a control system that is, for topological reasons, implemented on a distributed architecture and that has to respect stringent time constraints (for example, an end-to-end time constraint between the solicitation of the driver and its effect on the physical equipment, brake or front axle, is about tens milliseconds). This means that an implementation has to respect the required timing properties and their verification must take into account the system behavior specification and the deployment characteristics (processor power, network throughput, local scheduling policies, protocols).

Moreover, any embedded system is sensitive to external physical conditions such as high or low temperatures, EMI (Electromagnetic interferences) perturbations, etc. that are the sources of transient faults. Due to the distributed aspect of the system, any transient fault may lead to additional sensing to actuation delays (for example, on a CAN network, a transmission error leads to the retransmission of the erroneous packet) or loss of data packets (for example, in a time-triggered architecture based on TTP/C or FlexRay). Therefore, the classic dependability analysis of a system by only taking into account the permanent faults and the temporal system behavior verification (e.g. real-time schedulability analysis) disregarding the transient faults that can affect the system are necessary but not sufficient to guarantee the total dependability requirements.

In this paper, we propose a contribution to the quantitative evaluation of the dependability and, more

precisely the safety, for X-by-Wire systems that focuses on transient faults caused by the environment. Section 2 discusses the safety issue in automotive industry by presenting first some possible standards for the X-by-Wire system dependability assessment, then the different faults (and particularly the EMI perturbations) which can lead to system failures. Section 3 presents a steer-by-wire architecture as our case study. Section 4 describes the approach we propose to evaluate the vehicle failure probability when it goes through an EMI perturbed zone and a set of such zones. Section 5 gives numerical results by considering a typical vehicle trajectory. Section 6 concludes our findings and points out future work. Comparing to the approach we proposed earlier in [11], this paper brings new contributions on the EMI perturbation modelling and the mathematic and algorithmic evaluation methods of the vehicle failure probability (or safety).

2. The safety issue in automotive industry

2.1. Which standard for dependability assessment

In several critical domains as nuclear plants, railways, avionics, safety requirements are very rigorous for software-based systems. A certification process has to be followed by the concerned industry in order to prove that the systems obey regulatory policies. At the moment, nothing similar exists in the automotive industry. Nevertheless, as it is a crucial problem for carmakers and suppliers, several proposals either based on the existing certification standards or on some new proposals are presently under study [2]. We can cite, for example: the RTCA/DO-178B [3] that is used in avionics, or the EN 50128 [4], applied in the railway industry; these standards provide stringent guidelines for the development of an embedded system. The constraints imposed by these standards are too stringent for the automotive industry: software partitioning, intensive hardware redundancy, etc. Note that, nevertheless, a similar but looser approach is proposed by the Motor Industry Software Reliability Association (MISRA) [5]. Faced to these proposals, some studies conclude on the need of a quantitative approach (see PALBUS or Brite Euram 111 projects [6]). The same approach is favoured by the automotive actors [7]. So, the generic standard IEC 61508 [8], is, for the moment a good candidate for supporting a certification process in the automotive industry due to its specification of "safety integrity levels" (SIL) defined each by a quantitative safety requirement. The challenge is therefore to verify that a given system respects such a quantitative property. Notice that in this standard, the requirements are expressed in terms of failure probability per hour.

In this paper, we show how to evaluate a failure probability along some reference situation (e.g. a typical vehicle trajectory); future work is on going for an evaluation per hour by considering a statistic situation.

2.2. External transient faults

The main sources for transient faults in an in-vehicle embedded system are the electromagnetic interferences and the temperature variations. Alpha particles, neutrons or electric shocks are some other sources of transient faults. Unfortunately, at the moment, their effect on the electronic component of a micro-controller is not well known and therefore, no realistic model. Nevertheless, as soon as such a model will be available, our approach will be able to integrate them. Furthermore, in this paper, we focus only on the effect of electromagnetic interference (see [9] for more details on the effects of temperature variations).

Electromagnetic interferences are mainly caused by radio communication transmitters, radars, and high voltage lines. Their influence on electronic components depend on the frequency, power and level of the electromagnetic fields. Each carmaker specifies an internal regulatory policy that imposes the robustness of electronic component faced with electromagnetic interference sources under a given voltage level and for a given interval of frequencies. So a test process is applied on each electronic component in order to verify its conformity to the specific carmaker standard. Nevertheless, this conformity is just proved for given frequencies and voltage level. In fact, it is established that the testing condition are not met everywhere; it exists some traffic areas, for example near airports, where a vehicle can go through an area subject to a higher level of voltage and / or other frequencies than the specified ones and therefore, the probability that an in-vehicle embedded system can be corrupted by electromagnetic interferences is not zero. In this paper, we will consider that the upper limit for the robustness assessment of electronic components is 100 V/m. This is to say that when a car goes through an EMI perturbed zone with a force higher than 100 volts per meter, its X-by-Wire systems may exhibit errors.

2.3. Areas under EMI

Some sources of electromagnetic interferences are statically disposed along the road (for example, radars or high voltage lines). CEERF, a French project, funded by Ministry of Transport, proposed a characterization of the electromagnetic pollution for the French road system [10]. This project targeted mainly the automotive industry by proposing a cartography of the EMI sources and electromagnetic field levels in France and a method for its updating. In this paper, we apply our proposed method to a case study (see section 3) and the model of EMI faults is based on the results of this project. These results are obtained thanks to a monitor embedded in a car and whose role is to record the frequency and the level of the ambient electromagnetic field during a

journey along several representative roads. From this recording, we are able to select the length (in km) of each area under EMI perturbation of higher than 100 V/m (see figure 1; on the represented trajectory, two parts of this trajectory, areas Z_1 and Z_2, are subject to perturbations of more than 100V/m).

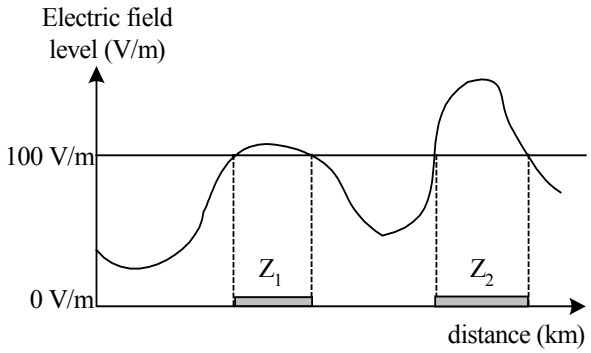

Figure 1. Example of electric field level of a reference road

In our study, since we are dealing with safety-critical systems, worst vehicle situations (e.g. vehicle is taking a bend at its maximum authorized speed when a perturbation occurs) are considered whenever possible.

3. Case study

In order to illustrate the proposed method we apply it on a case study that integrates the main functionalities of a Steer-by-Wire system (note that this case study was formerly presented in [11]).

A Steer-by-Wire system aims to provide two main services: controlling the front axle actuation according to the driver's request and providing a "mechanical-like" force feedback to the hand wheel that is consistent with the current state of the vehicle. We assume in this study that these services are independent and we only focus on the "front axle actuation" service because it implies the most critical safety purpose.

Figure 2 represents the computer-based architecture. Because of its safety criticality, redundancy is omnipresent. Three redundant sensors, S_HW1, S_HW2, S_HW3, measure the driver's request (hand wheel angle and torque), two redundant actuators, FA_m1 and FA_m2, act on the front axle. Two redundant micro-controllers are used for driver's requests filtering, HW_ECU1 and HW_ECU2 while two other redundant micro-controllers, FA_ECU1 and FA_ECU2, are dedicated to the support of the control laws for the front axle movement. Finally, three redundant sensors (S_FA1, S_FA2 and S_FA3) measure the state of the front axle and two redundant actuators, HW_m1 and HW_m2, provide the force feedback on the hand wheel. The four micro-controllers are connected on the redundant channels of a TDMA-like network (could be TTP/C or FlexRay).

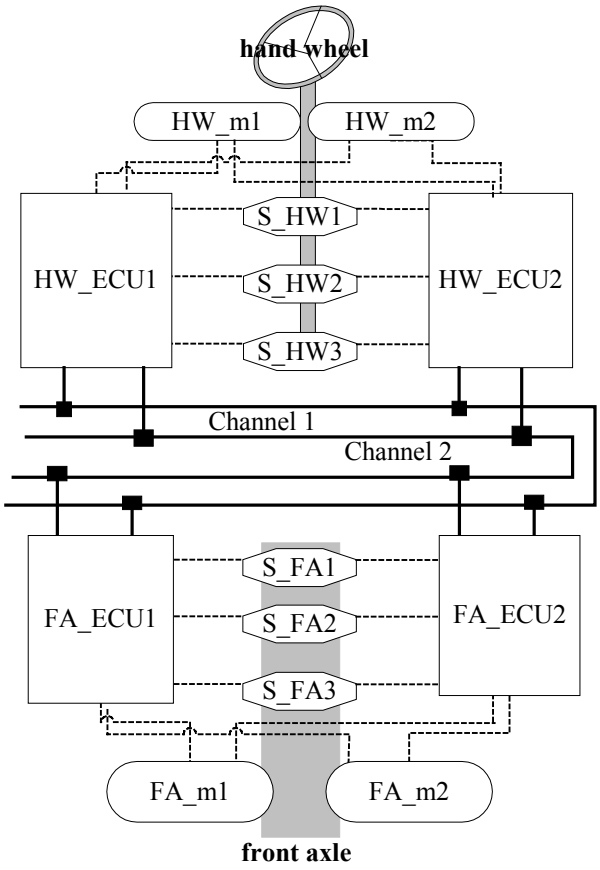

Figure 2. A Steer-by-Wire architecture

The application implementing the two services is deployed on this computer-based architecture. As said formerly, we focus on the service of "front axle actuation according to the driver's request". Two important functions are necessary: the filtering of information measured near the hand wheel (driver's request) and the evaluation of the order to give to the front axle actuators.

The first function, termed *Producer*, gathers the measures of the three sensors and establishes the consolidated information (majority vote, consistency, etc.) that represents the driver's request. This function is replicated onto the redundant micro-controllers, HW_ECU1 and HW_ECU2 and runs periodically. In the case study, the task realizing this function is periodic (period ε_t=2 ms); furthermore, we assume that it takes always the same time, d_t, for the completion of each task instance on HW_ECU1 and HW_ECU2 and that d_t is equal to some microseconds, so we disregard it in the following sections.

The second function, called *Consumer*, aims to compute the order according to the driver's request, the current vehicle situation and the current state of the front axle. It also runs periodically both on FA_ECU1 and FA_ECU2 and its period is based on the TDMA cycle. Note that, at the beginning of each period, this function

requires the driver's request that is transmitted thanks to the replicated channels of the network. Figure 3 presents the TDMA cycle configuration. In both HW_ECU1 and HW_ECU2, the driver's request is packed into a frame (HWFr1 and HWFr2) and these frames are sent (respectively in slot S1 and slot S2) at each cycle and in the same way on both channels. The other slots of the cycle are not considered here.

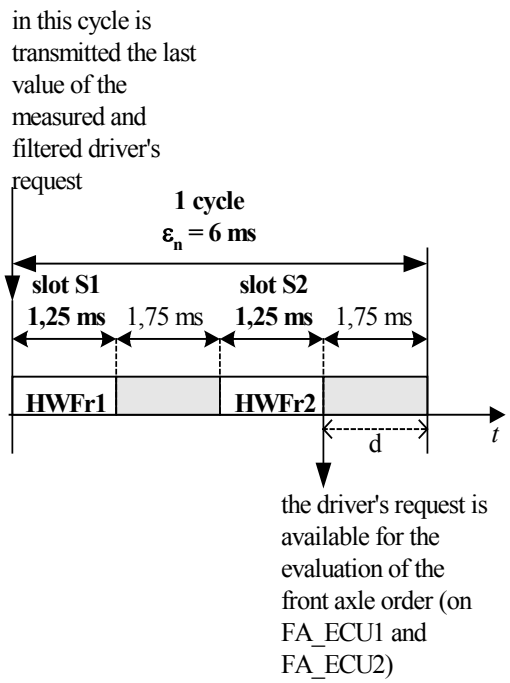

Figure 3. TDMA cycle configuration

The specification of the embedded application is then achieved by verifying that the *Worst Case Pure Delay,* WCPD, that is the greatest age of the information consumed at each start of the *Consumer* is less than the Worst Tolerable Delay, τ_{max}, (defined as the maximum age of the driver's request, measured at its consumption instant, that ensures the safety of the vehicle in an extreme situation; see [11] for more precision on the method of its evaluation); in this case, by applying this method, we obtain $\tau_{\max} = 18\ ms$. The Worst Case Pure Delay, is given by $WCPD = \varepsilon_n - d + \varepsilon_t + d_t = 6{,}25\ ms$. So, this architecture respects the safety property under fault free case. (as said formerly, we disregard d_t). Figure 4 illustrates the evaluation of WCPD.

4. Verification of safety constraints at vehicle level under EMI

4.1. Proposition of metric for the quantitative evaluation of the behavioral reliability of an in-vehicle embedded system

We presented in [11] the concept of *behavioral reliability* as an attribute that characterizes the dependability of an embedded system. More precisely, it is defined as the ability of the embedded system to provide a service with respect to the safety of the vehicle and taking into account the system performances and fault tolerance capacity. The contribution of this paper is a fault forecasting approach thanks to the evaluation of an embedded system with respect to fault occurrences distribution. This evaluation is done on a model of this system and based on a fault injection technique. Finally, the metric proposed is the *probability* that a failure at vehicle level occurs while the vehicle crosses an area subject to EMI above the tolerable value (100 V/m, in this paper).

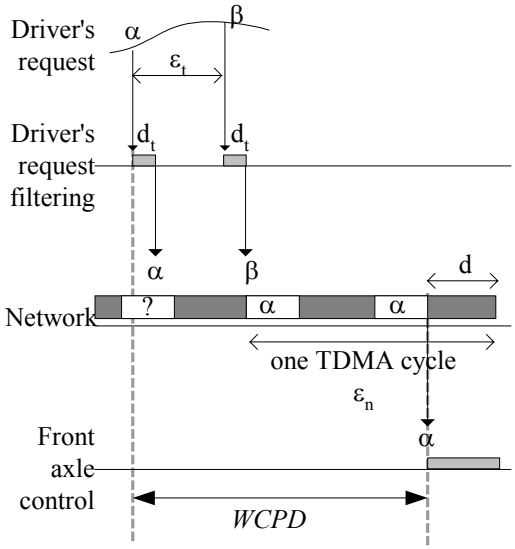

Figure 4. Worst Case Pure Delay evaluation: this occurs when the filtering activity on micro-controller HW_ECU1 or HW_ECU2 sends the value just after the start of the TDMA cycle

For this purpose, we formalize the interaction between transient faults due to EMI and the safety of a vehicle (section 4.2). Then (section 4.3), we present the fault injection technique that provides a quantitative evaluation of this interaction. A system under EMI above 100 V/m is possibly corrupted; so in section 4.4, we furnish a formal expression for the term "possibly" and in section 4.5, we show how to measure the interval during which the system is possibly corrupted. Finally, the probabilistic technique applied for the metric evaluation is given in section 4.6.

4.2. From transient fault to vehicle failure

The verification method lies on the fact that the network used to transmit the driver's request is based on a TDMA protocol. So we aim to define the worst situation that is tolerable by the *Consumer* function in

terms of vehicle safety guarantee. For the identification of this worst case, we make some assumptions.

- First, for focusing on the data production and transmission part, the failure probability of the micro-controllers, FA_ECU1 and FA_ECU2, and of the execution of the Consumer function (actuators) is not considered. In fact, these two parts can be separately studied. The total sensing to actuation failure probability can be obtained using classic reliability evaluation method.
- Second, as commonly admitted, we consider that the two micro-controllers HW_ECU1 and HW_ECU2, are fail-silent (i.e. they produce either correct data or nothing) [12].
- Finally, the mechatronic delay, i.e. the time necessary for the actuator to reach the front axle position, is supposed to be constant.

Under this hypothesis and considering the CRC-based error detection, and the temporal / spatial replications of transmitted data, the probability that an erroneous data would not be detected by the *Consumer* function can be considered as equal to 0. Therefore it is reasonable to consider the impact of the faults in terms of non-presence of driver's request at the *Consumer* side. The two conditions that can cause a loss of data transmission are: a faulty micro-controller (but under the fail silent assumption, no frame is transmitted in this case) or an error during the transmission of a data. An error at the communication level is the loss of a frame while an error at the system level is the loss of all the four replicated frames in one cycle for our case study. The failure of the vehicle occurs when the system error (i.e. absence of driver's request at the *Consumer* side during one cycle) persists beyond a tolerable threshold in terms of the communication (or consumption) cycles.

4.3. Determination of tolerable condition at vehicle level through fault injection technique

Thanks to a fault injection campaign, we evaluate the situations in which the safety of the vehicle is ensured under a pattern of errors at system level, that is a distribution of the loss of cycles. This evaluation is based on Matlab/Simulink; we dispose of a model of the control law realizing the *Consumer* function. This model is, in fact a black box, provided by the supplier of front axle controller. The environment of this control law is modeled through SimulinkCar, a legacy tool developed by PSA Peugeot-Citroën. The available model for the control law allows observing the response of the vehicle in a driving condition: a turn at 90 Km/h. This driving condition is strictly identified and used, among some others, by automatic control specialists for the specification of the control law and is supposed to represent extreme driving conditions.

The result furnished by an execution of these models consists in the evaluation of a couple of parameters, a "turn report" *TR*, and a "trajectory deviation" *TD*, that represent the global quality of the vehicle including the safety aspects. In preliminary studies, the designers of the vehicle define:

- TR_{min}, the minimum value required for *TR*
- and TD_{max}, the maximum value required for *TD*.

We complete this model in order to represent on the one hand, the delay between a driver's request production and its consumption (in fact, we consider always the worst case, i.e. *WCPD*) and, on the other hand, the discrete aspect of the driver's request at the Matlab / Simulink model level. We are therefore able to test the quality of a system in terms of the vehicle stability subject to external faults by fault injection [11]; to do so, as said formerly, we consider that an error at the system level is the loss of a TDMA cycle.

Thanks to the preliminary test activities, we remarked that, for the given case study, the worst condition is the one where several consecutive TDMA cycles are lost. This allows defining a test campaign policy based on two parameters, t_i the initial instant of the loss of TDMA cycles sequence and n_i the number of lost TDMA cycles:

- for each couple (t_i, n_i), the "turn report", TR_i, and the trajectory deviation, TD_i are measured,
- then, we look at the lowest TR_k that is superior or equal to TR_{min} (respectively, the greatest TD_l that is inferior or equal to TD_{max}) and name S_{TR} (respectively S_{TD}) the set of couple (t_i, n_i) leading to the value TR_k (respectively TD_l)
- finally, η_{max}, the largest tolerable number of TDMA cycles between the reception of two driver's requests, is given by:

$$\eta_{\max} = \min_{(t_i,n_i)\in S_{TR}\cup S_{TD}}(n_i)$$

As a conclusion of this fault injection campaign, the safety of a system is guaranteed if the number of TDMA cycles between two correct receptions of driver's requests, η, is less or equal to η_{max}.

For our case study, $\eta_{max} = 7$.

4.4. Error model

As said in section 2.3, a road reference is characterized by a set of areas that are subject to electromagnetic interferences. This means that when a vehicle crosses these areas, the embedded architecture is possibly affected by external faults. We show, in this section, how it is possible to evaluate the probability to have an error in the system, error due to this external transient fault, during a TDMA cycle. This probability of losing a TDMA cycle, denoted by P_{err}, corresponds to losing all replicated data on the redundant channels.

In general P_{err} can be obtained using fault injection techniques. However, in absence of the implemented system on which tests could be realized, we propose the following approach to estimate P_{err}.

As it has been explained in section 4.2, we assumed the total reliability of the command ECUs and actuators; a system error can either be caused by the ECU faulty

producing data or by transmission errors. If we denote by P_{err_ECU} the probability to have an error of all redundant ECUs, P_{err_BUS} the probability to have a transmission error of all redundant channels, and $P_{err\_ECU \cap BUS}$ the probability to have both ECU and transmission error of all redundant ECU and channels, P_{err} can be obtained by:

$$P_{err} = P_{err\_ECU} + P_{err\_BUS} - P_{err\_ECU \cap BUS}$$

To capture the contribution of the redundancy, for each redundant component i (i could be ECU or BUS in our case), we propose a score of the diversification N_i ($0 \leq N_i \leq 1$). Assuming an error probability of a component, λ_i, the error probability of all the n redundant components can be estimated by:

$P_{err\_i} = \lambda_i - N_i(\lambda_i - \lambda_i^n)$

For example, for 2 redundant channels, when the two cables use the same type of medium and follow the same wiring plan, they have great probability to be affected in the same way by an EMI perturbation. In this case the diversification score is near to 0, resulting in P_{err_BUS} near to λ_{BUS}. If the two channels use different mediums (e.g. one with optic fiber and another with metallic wire) and follow different wiring plans, they have smaller probability to be affected in the same way. The diversification score could be near to 1, resulting in P_{err_BUS} near to λ_{BUS}^2.

In our case study, P_{err_ECU} is much smaller than P_{err_BUS}. So we only take into account P_{err_BUS} and have thus $P_{err} = P_{err\_BUS}$. According to [13] and some measurements, λ_{BUS} is approximately about 10^{-2}. With $N_{bus} = 0.5$, we get: $P_{err} \cong 5x10^{-3}$

4.5. Duration of external faults

A system embedded in a vehicle that crosses an area subject to EMI above the tolerable value (100 V/m) is possibly corrupted during a given time. In our approach, we consider that an error at system level is the non reception of a correct driver's request for one TDMA cycle; so, the time interval during which the system can be corrupted has to be expressed in terms of a number of TDMA cycles. Furthermore, we consider a worst case condition for the vehicle; so the evaluation of this number of TDMA cycles is done for a vehicle crossing an critical area at 90 km/h.

The first step consists in translating an area length expressed in meters in a length given in seconds (termed Z in the following). Once this done, we have to evaluate how many cycles are possibly corrupted. Figure 5 illustrates how to evaluate this in the worst case. When $\varepsilon_t \leq \varepsilon_n$ (i.e., the filtering period is less than the TDMA cycle length), the worst case corresponds to the situation where all the replicated frames within the perturbation zone are corrupted and the end of the zone corrupts the beginning of the production of a TDMA cycle, causing thus an additional empty TDMA cycle. For the next valid TDMA cycle, as we assumed that the consumption takes place only after the last replica of a TDMA cycle, if this last replica is near the end of the TDMA cycle, it increases the worst interval between two valid driver's requests by still another additional cycle. So this worst-case interval is by:

$$\eta_{WC} = \left\lceil \frac{Z}{\varepsilon_n} \right\rceil + 2$$

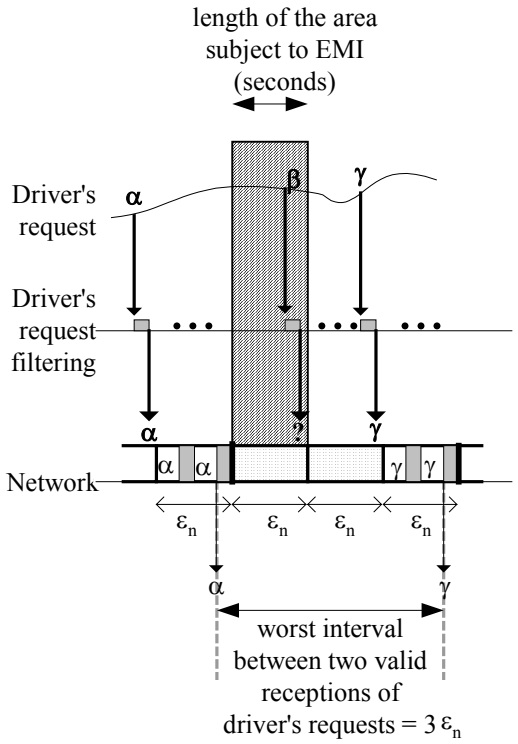

Figure 5. Evaluation of the worst interval between two valid driver's requests

4.6. Behavioral reliability metrics

In the previous sections, we detailed how to measure, η_{WC}, the length of an area in terms of number of TDMA cycles between two valid instances of a driver's request at their consumption instance, the probability, P_{err}, that in a critical area, one TDMA cycle may be corrupted and, $\eta_{\max}$, the maximum tolerable length in terms of number of TDMA cycles between two valid instances of a driver's request at their consumption instance

Therefore, the behavioral reliability in a given critical area, defined by η_{WC}, can be estimated by the probability to have an interval between two valid receptions of a driver's request largest than $\eta_{\max}$ under the assumption of a probability of corruption for one TDMA cycle P_{err}. This problem is to be put together with the evaluation of reliability of a system composed of an ordered sequence of n components and such that the system fails if and only if at least k consecutive components fail. These systems are termed "*consecutive-*

k-out-of-n:F" and denoted by $C(k,n:F)$. For such a system, we note n the number of components, p the probability that a component fails, L_n a number of consecutive failed components and k the largest tolerable number of consecutive failed components; the reliability of the system is evaluated by the probability that $L_n < k$, that is noted by $P(L_n < k) = R(k,n;p)$. This formula was proposed first in [14] and then simplified in [15] and [16] where $q = 1 - p$:

$$R(k,n;p) = \sum_{m=0}^{\lfloor (n+1)/(k+1) \rfloor} (-1)^m p^{mk} q^{m-1} \left(\binom{n-mk}{m-1} + q \binom{n-mk}{m} \right)$$

Thanks to this formula, we can express the probability, P_{fail} that of a failure at the vehicle level by:

$$P_{fail}(Z, P_{err}) = 1 - R(\eta_{\max}, \eta_{WC}; P_{err})$$

The numerical evaluation of the formula presented above is quite complex; so, we developed the following recurrent relation.

Let $u_k(n) = P(L_n < k)$, we can write:

$$u_k(n+1) = u_k(n) - qp^k u_k(n-k) \text{ for } n \geq k$$

This recurrent equation can be calculated with the following initial conditions:

$u_k(n) = 1$ for $0 \leq n \leq k\text{-}1$ and $u_k(k) = 1 - p^k$

We assume that $n \geq 3$ and $P_{err} \in]0,1[$; by noting $U(j) = P(L_n = j)$ and $FR(j) = P(L_n \leq j)$ with $0 \leq j \leq n$, the algorithm is therefore:

```
// initialisation
q=1-p; λ=q
U(1)=q; FR(0)=q^n
For k=2 to n-1 do
    // initial condition
    U(k)=q+pU(k-1)
U(k-1)=1
λ=pλ
    for j=k+1 to n do
        U(j)=U(j-1)-λU(j-k)
    FR(k-1)=U(n)
// Evaluation of FR(n), U(n)
FR(n-1)=1-p^n
FR(n)=1
U(0)=FR(0)
for k=1 to n do
    U(k)=FR(k)-FR(k-1)
```

In order to evaluate the risk of failure occurrences along a given route *T*, we have to apply this algorithm on each of the *nZ* identified critical areas (Z_i) that may be crossed by the vehicle on this route. The probability, $P_{fail,T}$ that a failure occurs on *T* is then given by:

$$P_{fail,T} = 1 - \prod_{i=1}^{i=nZ} \left(R(\eta_{\max}, \eta_{WC}(Z_i); P_{err})^{\eta_{WC}(Z_i)} \right)$$

We applied this method in order to evaluate the behavioral reliability of the system presented in section 3 and obtained the results presented in the next paragraph.

5. Numerical result for a typical trajectory

We studied the behavior of the vehicle along several significant routes. The one that we present here is typical of an urban environment. The values that we used were obtained thanks to the monitoring of the measured EMI in a vehicle driven along a route. Four critical areas were identified whose length in seconds (for a vehicle speed equal to 90 km/h) are respectively 2s, 50s, 20s and 2s. For each of these areas, the probability that a failure occurs at vehicle level was determined.

We recall below the values computed for this case study:

ε_n = 6 ms., the length of a TDMA cycle,

$P_{err} = 5 \times 10^{-3}$, the probability that a TDMA cycle to be corrupted,

η_{max} = 7, the largest interval between two valid receptions of driver's requests.

Thanks to the algorithm presented in section 4.6, we obtain:

$$P_{fail,T} = 1.6409 \times 10^{-10}$$

If we consider the safety level required by SIL4 in [8] or 10^{-9} proposed in [7], or even 5.10^{-10} as suggested by PSA Peugeot-Citroën carmaker, we could conclude that the architecture of the case study meets the safety requirement. This is true even though SIL4 is expressed in terms of failures per hour, as the trajectory we considered is longer than one hour.

The same method can be used in order to optimize the design of an application. In particular, it may be interesting to study how increasing the robustness of a network would improve the safety of the vehicle; this can be done by modifying the value of P_{err} (intuitively, the higher is the robustness of the network, the lower is P_{err}). Another important issue is to analyze the influence of the length, ε_n, of the TDMA cycle. For this purpose, we computed the value of $P_{fail,T}$ for several couples (ε_n, P_{err}). The results are presented in Table 1.

The shaded region represents $P_{fail,T} < 5.10^{-10}$, i.e. the region within which the safety constraint is respected. We can see that for a same P_{err}, a shorter TDMA cycle provides more robustness. This is normal as for a same time period shorter TDMA cycle allows more temporal redundancy. The white region corresponds to $5.10^{-10} < P_{fail,T} < 1.10^{-7}$. This region shows the margin a designer can have in terms of the TDMA cycle duration. The narrowness of this region says that to reduce the failure probability, it is often enough to just reduce a little the TDMA cycle duration. The region marked by "X" corresponds to the case of $P_{fail,T} > 10^{-7}$.

P_{err}	TDMA cycle length (ε_n)									
	1	2	3	4	5	6	7	8	9	10
0,5	X	X	X	X	X	X	X	X	X	X
0,4	X	X	X	X	X	X	X	X	X	X
0,3	X	X	X	X	X	X	X	X	X	X
0,2		X	X	X	X	X	X	X	X	X
0,1			X	X	X	X	X	X	X	X
0,09			X	X	X	X	X	X	X	X
0,08				X	X	X	X	X	X	X
0,07				X	X	X	X	X	X	X
0,06				X	X	X	X	X	X	X
0,05				X	X	X	X	X	X	X
0,04					X	X	X	X	X	X
0,03						X	X	X	X	X
0,02						X	X	X	X	X
0,01							X	X	X	X
0,009							X	X	X	X
0,008									X	X
0,007									X	X
0,006									X	X
0,005									X	X
0,004									X	X
0,003									X	X
0,002										
0,001										

Table 1. Values obtained for the embedded architecture presented in the case study section for several quality of robustness of the network and several length of the TDMA cycle.

6. Conclusion and future work

X-by-Wire (Steer-by-Wire or Brake-by-Wire) systems are safety critical and their deployment is only possible with the proved dependability. In this paper we contributed to the method for evaluating the dependability of X-by-Wire systems taking into account the EMI perturbations. This method is designed for X-by-Wire architectures distributed around TDMA-like communication network. Assuming a TDMA cycle error probability within an EMI perturbed zone, our method allows obtaining the vehicle level failure probability, which is an important quantitative dependability metric for the future certification process.

Our future work includes the extension of the method to finer modeling the EMI perturbed zone by considering a variable P_{err} rather than a constant one, and a statistic study of a large set of typical trajectories for providing the failure probability per functioning hour so that IEC61508-1 can be applied to the automotive industry.

References

[1] A. Avizienis, J-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Trans. on dependability and secure computing*, Vol. 1, NO. 1, Jan.-March 2004.

[2] Y. Papadopoulos, J.A. McDermid, "The Potential for a Generic Approach to Certification of Safety-Critical Systems in the Transportation Sector", *Journal of Reliability Engineering and System Safety*, 1999, vol. 63, pp. 47-66, Elsevier Science.

[3] Radio Technical Commission for Aeronautics "RTCA DO-178B - Software Considerations in Airbone Systems and Equipment Certification", *International Standard*, 1994.

[4] CENELEC, "Railway Applications - Software for Railway Control and Protection Systems, EN50128", *International Standard*, 2001.

[5] P. H. Jesty, K. M. Hobley, R. Evans, I. Kendall},"Safety Analysis of Vehicle-Based Systems", *Proceedings of the 8th Safety-critical Systems Symposium*, 2000.

[6] Brite-EuRam 111 Program, "X-By-Wire - Safety Related Fault Tolerant Systems in Vehicles, Final Report", 1998.

[7] R. Hammett, P. Babcock, "Achieving 10^{-9} dependability with drive-by-wire systems", *in SAE-Society of Automotive Engineers*, Detroit, USA, 2003.

[8] IEC61508-1, "Functional Safety of Electrical/Electronic/ Programmable Safety-related Systems - Part 1: General requirements, IEC/SC65A", *International Standard*, 1998.

[9] E. Bonhoure, C. Wilwert, T. Clément, "Application of the concept of behavioural and static reliability to the evaluation of steer-by-wire system dependability", *Convergence 2004*, Detroit, USA, 2004.

[10] PREDIT-CEERF, "Caractérisation de l'environnement électromagnétique routier en France", *Tecnical report* (in French), 2003.

[11] C. Wilwert, Y.Q. Song, F. Simonot-Lion, T. Clément, "Evaluating Quality of Service and Behavioral Reliability of Steer-by-Wire Systems", *9th IEEE International Conference on Emerging Technologies and Factory Automation 2003 - ETFA'2003*, Lisbonne, Portugal.

[12] J. Rushby, "A comparison of bus architectures for safety-critical embedded systems", Technical report, Computer science laboratory SRI international, 2003.

[13] IST-10748, "Fault injection for TTA-FIT", *deliverable report 3*, TU Wien, Chalmers, Motorola, Volvo, UP Valencia, Carinthia TI, Czech TU, TTTECH, 2001.

[14] E. J. Burr, G. Cane. "End-toEnd Arguments in system design", *Biometrika*, Vol. 48, pp.461-465, 1961.

[15] M. Lambris, S. G. Papastavridis. "Exact reliability formulas for linear and circular consecutive-k-out-of-n:F systems", *IEEE Transactions on Reliability*, Vol. 34, pp. 124-126, 1985.

[16] F.-K. Hwang, "Simplified reliabilities for consecutive-k-out-of-n:F systems". *Algebraic Discrete Methods*, Vol. 7, pp. 258-264, 1986.