Worst-Case Timing Analysis of AeroRing- A Full Duplex Ethernet Ring for Safety-critical Avionics

A. AMARI , A. MIFDAOUI, F. FRANCES, J. LACAN
University of Toulouse-ISAE, France

***Abstract*—Avionics implementation with less cables will clearly improve the efficiency of aircraft while reducing weight and maintenance costs. To fulfill these emerging needs, an innovative avionics communication architecture, based on Gigabit Full Duplex Ethernet ring, is proposed in this paper. To adapt this COTS technology to safety-critical avionics, an adequate tuning process of the communication protocol and the choice of reliability mechanisms to achieve timely and reliable communications are first detailed. Then, efficient timing analyses of such a proposal based on Network Calculus are conducted, accounting the impact of a ring topology and the specified reliability mechanisms. Third, these general analyses are illustrated in the case of a realistic avionic application, to replace the AFDX backup network with AeroRing, to reduce wires, while guaranteeing timely communications.**

***Index Terms*—Real-Time Ethernet, Ring topology, QoS, Performance analysis, Network Calculus, avionics.**

I. Introduction

The inherent complexity and bandwidth requirement of avionics communication architectures are increasing due to the growing number of interconnected end-systems and the expansion of exchanged data. The Avionics Full Duplex Switched Ethernet (AFDX) [3] has been introduced to provide high speed communication (100Mbps) for new generation aircraft. However, this switched network is deployed in a full redundant way, which leads to significant quantities of wires, and thus increases weight and integration costs.

To cope with these emerging issues, an implementation with less cables of avionics communication architecture will clearly improve the efficiency and reliability of aircraft, while reducing integration, fuel consumption and maintenance costs. Furthermore, this communication architecture must fulfill a set of key requirements, which reveal particularly effective for safety-critical avionics. These requirements concern both technical and costs aspects. The technical requirements are mainly the timeliness and the accuracy of delivered data, in addition to the reliability and availability of the communication network. Moreover, the choice of the communication solution shall be efficient to meet the design requirements for the least amount of money. Therefore, the IEEE802.3 compatibility, i.e., AFDX-compliant, a minimized (re)-configuration effort and reduced implementation costs are among the most important issues to guarantee.

The recent research effort towards defining new communication solutions to guarantee high availability level with limited cabling costs and complexity has renewed the interest in ring-based networks, which provide an implicit redundant path by introducing only one additional connection between the two end nodes, compared to line or star topologies [15]. The ring-based networks have been prominently used for industrial applications with the implementation of many Real Time Ethernet (RTE) profiles cited in IEC 61784-2 [4], e.g., EtherCAT [1], SERCOSIII [2] and Profinet-IRT [17], and recently in other application fields like automotive, e.g. RACE [19]. However, most of these existing solutions are based on time-triggered communication schemes, e.g., Master/slave or TDMA, which present some limitations compared to the event-triggered AFDX standard in terms of resource utilization efficiency and configuration flexibility.

Therefore, in [8], a new avionics communication network, called AeroRing[1], based on a Gigabit Full Duplex Ethernet ring and implementing an event-triggered communication scheme with a distributed fault management mechanism, has been proposed to decrease the weight and complexity of wiring, while guaranteeing high real-time performance and availability levels. Furthermore, a qualitative comparative analysis of AeroRing with the most relevant ring-based RTE solutions has been conducted.

In this paper, the relevant aspects of such a proposal and analytical evaluation of offered timing performance are investigated, based on Network Calculus [16]. Many challenges arise from conducting such analysis. First, the implementation of an event-triggered communication scheme on top of a ring topology induces non-feedforward transmissions, i.e., some transmitted flows are interlaced and their paths form cycles, which complicates the timing analysis compared to time-triggered solutions, e.g., Master/slave or TDMA. Second, the AeroRing nodes implement Fixed Priority (FP) policy and the impact of such a policy on delays needs to be integrated. Third, the impact of reliability mechanisms on end-to-end delays have to be taken into account.

Hence, our main contributions in this paper are twofold. First, efficient timing analyses of an avionics ring-based Ethernet network, based on extending the most recent results in Network Calculus theory, i.e. Pay Multiplex Only Once (PMOO) principle [12], are conducted. These analyses integrate the impact of a non-feedforward topology, FP service policy in nodes and the specified reliability mechanisms. Then, these general analyses are illustrated in the case of a realistic avionic application, which consists in replacing the AFDX [3] backup network with AeroRing to reduce cables, while guaranteeing

[1]AeroRing is co-funded by the European Union. Europe is involved in Midi-Pyrenees through the European Funds for Regional Development.

timely and reliable communications.

In the next section, we give an overview of the main features of AeroRing network. Afterwards, we review the most relevant redundancy mechanisms and timing analysis approaches of ring-based networks in Section III. Then, the system modeling and the worst-case timing analyses of such a proposal are detailed in Sections IV and V. Finally, the effectiveness of AeroRing is illustrated through a realistic avionics case study in Section VI.

II. Background: AeroRing Specifications

In this section, we present the fundamental concepts of AeroRing network, and a more detailed description can be found in [8]. The main objective is to guarantee avionics requirements, while decreasing the complexity of wiring and implementation costs.

A. Main features

The AeroRing network implements a daisy-chain wiring scheme on top of a Full Duplex ring topology. It allows any "Ethernet-compliant" equipment to transmit its data via a specific node, named T-AeroRing. Each transmitted packet is forwarded from one T-AeroRing to another until reaching the final destination.

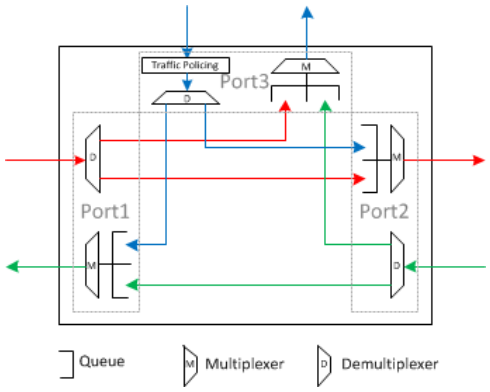

Fig. 1: *T-AeroRing* internal architecture

The T-AeroRing [8] is a specific 3 ports Full Duplex Ethernet switch having the internal architecture, illustrated in Fig. 1, and the following main characteristics:

- ***Cut-Through forwarding technique***: the T-AeroRing starts forwarding the packet just after its identification, i.e. only the header of each packet is decoded to determine its destination port;
- ***Fixed Priority service policy***: packets are queued in each output port of T-AeroRing according to their priorities. Priority is defined according to the IEEE 802.1p standard using the 802.1Q tag. The specified 3-bit priority field is used to manipulate four priority classes;
- ***QoS-aware routing***: unlike COTS Ethernet switches, which relay frames on the basis of the address learning process and the Spanning Tree Algorithm, each T-AeroRing builds its routing table on the basis of the network management messages, exchanged between the interconnected T-AeroRings during the initialization phase, or when a topology modification occurs (i.e. failure or restoration). Each T-AeroRing implements two routing modes to transmit its generated packets depending on their priorities: (i) on both ring ports (Ports 1 and 2 in Fig. 1) for high priority traffic classes, i.e., network management and Hard Real Time (HRT) data, to allow a high reliability level; (ii) on the port corresponding to the shortest path for medium and low priority traffic classes, i.e., Soft Real Time (SRT) and Non Real Time (NRT) data, to offer a high performance level, i.e., short delay;
- ***Traffic policing***: Like an AFDX switch, the T-AeroRing implements traffic policing mechanisms, based on Leaky Bucket method, to control each traffic class compliance with its predefined contract to avoid the network saturation.
- ***Frame Redundancy Management***: Like AFDX end-systems, the T-AeroRing implements a Frame redundancy management mechanism to detect redundant frames generated by the first routing mode, and to determine whether to deliver the packet at the final destination or drop it, since its replica has already been received. In practice, all packets sent on both ring ports are provided with a 2-bytes sequence number field, which will be checked at the destination;
- ***Filtering Function***: To avoid infinite packet looping as a result of broadcast communication or erroneous header information, each T-AeroRing implements a filtering function which consists in: (i) eliminating all its generated packets sent on one port and received on the other port; (ii) eliminating all received packets with erroneous source address. This verification is possible due to the routing table, i.e. an erroneous address does not exist in the routing table.

Based on the description of T-AeroRing ports in Fig. 1, the frames will be processed as follows:

- Any frame received on a network port (1 or 2) is relayed to the other port unless the frame is destined to the connected equipment or it is the source;
- Any frame received on a network port (1 or 2) destined to the connected equipment is delivered to it, according to the redundancy management mechanisms;
- Any frame received from the connected equipment is transmitted on one or both network ports depending on its priority.

B. Fault Detection and Reconfiguration Mechanisms

AeroRing implements a distributed fault detection and reconfiguration mechanisms that allows to avoid the single point of failure. Any T-AeroRing has to consider a connection as down with a neighbor if it does not receive any message from its neighbor during a certain period called *detection period*. In practice, if a T-AeroRing has no data to transmit to a neighbor, then it announces periodically its status to this neighbor by sending control messages, when at least one of the following conditions is satisfied: (i) the *T-AeroRing* does not have any data to send on this port during a period called *announcing*

period, which is less then the *detection period*; (ii) the *T-AeroRing* did not receive any data or control message from this port for a duration equal to the *detection period*. In this case, the T-AeroRing indicates to its neighbor through a control message that the connection is considered as down.

When a connection is considered as down, the T-AeroRing sends a first control message to inform the other T-AeroRings, followed by a second control message to update the routing tables. In this case, the network is transformed into a line and there is only one path to each destination. A down connection is considered operational again (up), if the T-AeroRing starts receiving frames (data or control) from its neighbor. In this case, it sends a control message to update the routing tables of the other nodes.

III. Related Work

In this section, we first present the most relevant redundancy mechanisms for ring-based networks and relate them to our proposal. Then, we discuss the main timing analysis approaches of distributed networked systems with cyclic dependencies.

A. Redundancy Protocols for Ring-Based Networks

Various redundancy mechanisms for ring-based RTE solutions have been proposed and cited in IEC62439-1/7, and the most relevant ones in our case are the Parallel Redundancy Protocol (PRP) [6], High-availability Seamless Redundancy protocol (HSR) [6], Distributed Redundancy Protocol (DRP) [7] and Ring-based Redundancy Protocol (RRP) [5].

Both PRP and HSR offer a zero switchover time when failure, through guaranteeing two redundant paths for each transmitted data. The PRP handles this feature due to a fully redundant network, i.e., two parallel networks, where most of the equipments are attached to both parallel networks, and each data is duplicated at the transmission and filtered at the reception; whereas the HSR protocol achieves the same purpose through a daisy-chain ring topology and sending duplicated data on both directions, then the destination consumes only the first valid one. It is worth noting that PRP implies high implementation costs and weight due to the required fully redundant architecture, and that HSR limits the available utilization capacity to 50% since all data types are duplicated.

The DRP implements a local fault detection mechanisms, where each equipment can check the status of its neighbors by sending a link test frame *"LinkCheck"* to detect failures. However, in addition to these local mechanisms, DRP implements a centralized fault detection mechanism to check the ring status in a cyclic manner, i.e., during each cycle, only one equipment can check the ring status via a ring test frame *"RingCheck"*, gather and broadcast the information to the rest of equipments. Furthermore, an accurate synchronization protocol is required to manage such a cyclic process. On the other hand, the RRP implements a distributed mechanisms to build the routing tables within equipments. However, RRP transforms the ring topology into a line topology to avoid infinite packet looping, through the selection of two adjacent devices, called Ring Network Managers (RNMs), and disabling one of their ports. This choice will clearly deteriorate the reliability level, since sending on both directions becomes forbidden. Moreover, RRP implies high communication overhead to build the routing tables. Indeed, there are as many exchanged messages as equipments to update the routing tables.

Unlike the existing solutions, AeroRing implements a fully distributed redundancy protocol, based only on local fault detection mechanisms and without any need of synchronization protocol. Furthermore, nodes build autonomously their QoS-aware routing tables with a low communication overhead, to send messages on both directions or only on the shortest path, according to their priority level.

B. Timing Analysis of Ring-based Networks

The timing analysis of ring-based networks aims to compute the adequate temporal metric, e.g. minimum cycle duration or end-to-end delays, which will be compared to messages deadlines in order to verify the network predictability.

For the most relevant ring-based RTE profiles [4], adequate analytical approaches have been proposed to compute the minimum cycle time of the network communication, and an interesting overview of the most relevant ones is detailed in [18]. Conducting such approaches has been greatly simplified due to the time triggered communication scheme, e.g. Master/slave or TDMA, implemented by these RTE profiles. However, with an event-triggered communication scheme, the cycle notion becomes no longer applicable and we need to compute worst-case end-to-end delays or at least upper bounds.

The timing analysis conducted to prove the certification requirements of the AFDX standard was based on the Network Calculus theory [16] [14], which is considered as one of the most efficient methodologies for the worst-case performance analysis of switched networks. Hence, we select this adequate method to provide the timing analysis of our proposal. A large body of work based on Network Calculus formalism exists for feedforward networks. The feedforward property is fulfilled when the crossed systems can be labeled with increasing numbers in such a way that data flows goes from i to j with $i < j$. An interesting overview of the most relevant approaches is detailed in [13]. However, AeroRing is a ring-based network and the transmitted flows usually form cycles, which induces a non-feedforward topology. For the particular case of ring-based networks, Cruz [11] defines an interesting approach, called *Time stopping method*, which consists of two steps. First, a finite burstiness bound for transmitted flows is assumed to obtain a set of equations to compute the delay bounds. Then, the feasibility conditions to solve these equations are defined. Afterwards, the authors in [20] demonstrate the ring stability under specific assumptions through the existence of a backlog bound, which has been generalized in [16]. For the general case of non-feedforward networks, Charny and Le Boudec [10] prove that if the maximum utilization rate of any link is less than $\frac{1}{h-1}$ with h the maximum path length, then an end-to-end delay bound exists. However, these main conventional analysis methods limit the network performance in terms of resource efficiency, i.e. the utilization rate decreases dramatically when the network size increases, or system scalability, i.e. the nodes number is hardly constrained to respect temporal deadlines.

To handle these limitations, we propose in this paper an innovative timing analysis method of ring-based networks, based on extending the PMOO principle [12], which consists in paying the bursts of interfering flows only once by taking into account the flow serialization phenomena. To the best of our knowledge, this kind of analytic approach has not been addressed yet for this kind of non-feedforward networks. We will show in the last section that this innovative approach enhances the network scalability, and induces a ring stability condition under full network utilization, i.e., bounded delays.

IV. System Modeling

To conduct the timing analysis of AeroRing Network, we first present an overview of Network Calculus concepts, more details can be found in [16]. Then, we detail the traffic and T-AeroRing models to define the arrival and service curves. The knowledge of these curves enables computation of the end-to-end delay upper bounds.

A. Network Calculus Concepts

The worst-case timing analysis proposed in this paper is based on Network Calculus formalism, providing deterministic upper bounds on delays and backlogs (queue sizes). Delay bounds depend on the traffic arrival described by the so called *arrival curve* α, and on the availability of the traversed node described by the so called minimum *service curve* β. The definitions of these curves are explained as following.

Definition 1. *(Arrival Curve) a function $\alpha(t)$ is an arrival curve for a data flow with an input cumulative function $R(t)$, i.e., the number of bits received until time t, iff:*

$$\forall t, R(t) \leq R \otimes {}^{2}\alpha(t)$$

Definition 2. *(Service curve) The function $\beta(t)$ is the minimum simple service curve for a data flow with an input cumulative function $R(t)$ and output cumulative function $R^*(t)$ iff:*

$$R^*(t) \geq R \otimes \beta(t)$$

The performance bounds are computed according to the following theorem using the arrival and service curves.

Theorem 1 (Performance Bounds)**.** *Consider a flow F constrained by an arrival curve α crossing a system $\mathcal{S}$ that offers a service curve β. The performance bounds obtained at any time t are given by:*
Output arrival curve: $\alpha^*(t) = \alpha \oslash {}^{3}\beta(t)$
Backlog: $\forall\ t:\ q(t) \leq (\alpha \oslash \beta)(0) =: v(\alpha, \beta)$
Delay: $\forall\ t:\ d(t) \leq \inf\{t \geq 0 : (\alpha \oslash \beta)(-t) \leq 0\} =: h(\alpha, \beta)$

The computation of these bounds is greatly simplified in the case of leaky bucket arrival curve $\alpha(t) = b + rt$, with b the maximal burst and r the maximum rate, i.e., the flow is (b, r)-constrained; and the Rate-Latency service curve $\beta_{R,T}(t) = [R \cdot (t - T)]^{+}$ [4] with latency T and rate R. In this case, the delay is bounded by $\frac{b}{R} + T$, the backlog bound is $b + r * T$, and the output arrival curve is $b + r(T + t)$.

Finally, to compute end-to-end delay bounds of individual traffic flows, we need the following residual service curve theorem.

Theorem 2 (Residual service curve - Blind Multiplex)**.** *[9] let f_1 and f_2 be two flows crossing a server that offers a* strict *service curve β such that f_1 is α_1-constrained, then the residual service curve offered to f_2 is:*

$$\beta_2 = (\beta - \alpha_1)_{\uparrow}$$

where $f_{\uparrow}(t) = \max\{0, \sup_{0 \leq s \leq t} f(s)\}$

B. Traffic Model

In our model, to integrate the different characteristics of the traffic classes generated by an avionic equipment connected to a T-AeroRing, five parameters (P, Dl, L, J, PL) are defined for each traffic class:

- The period P: for a periodic message, it is the period and for a sporadic message, it is low bounded as its minimal inter-arrival time;
- The temporal local deadline Dl: (the message life duration) it is the period for a periodic message and the maximal response time for a sporadic message;
- The length L: the maximal payload length of a message;
- The maximum jitter J at the T-AeroRing source, which may be induced by the traffic policing mechanisms;
- The priority level PL: there are four priority levels according to the T-AeroRing specifications. Therefore, PL is in $\{0, 1, 2, 3\}$ where 0 is the highest priority level.

Since the T-AeroRing implements policing mechanisms based on leaky bucket, the arrival curve of traffic class with priority level p sent by an equipment i is $(b_{i,p}, r_{i,p})$-constrained as following:

$$\alpha_{i,p}(t) = L_p + \frac{L_p}{P_p}(t + J_p) = b_{i,p} + r_{i,p}.t \qquad (1)$$

C. T-AeroRing Model

The delay within a T-AeroRing consists of a constant technological latency ϵ depending on the hardware implementation of the T-AeroRing, and a variable queuing delay depending on the service policy FP at its output ports. The FP service policy guarantees for each priority level to be treated before the lower priorities and after the higher priority levels. Furthermore, since the transmission of a packet on the network cannot be preempted, it may be blocked at the worst-case during the transmission time of a maximum packet length with lower priority. Hence, the service curve offered to the traffic class with priority p within a T-AeroRing i is the following Rate-Latency curve:

$$\beta_{R_{i,p},T_{i,p}}(t) = R_{i,p} \cdot [t - T_{i,p}]^{+} \qquad (2)$$

where the offered rate $R_{i,p}$ is the residual capacity after serving the higher priority levels than p, crossing the output port of the T-AeroRing i and generated within any T-AeroRing

[2] $f \otimes g(t) = \inf_{0 \leq s \leq t}\{f(t - s) + g(s)\}$
[3] $f \oslash g(t) = \sup_{s \geq 0}\{f(t + s) - g(s)\}$
[4] $[x]^{+}$ is the maximum between x and 0

m of the ring, denoted $m \ni i$; and the maximum latency $T_{i,p}$ corresponds to the sum of the technological latency ϵ, the transmission time of a maximum packet length with lower priority and the maximum bursts of higher priorities crossing the T-AeroRing. The analytical expressions of these aforementioned parameters are as following:

$$R_{i,p} = R_i - \sum_{pp<p} \sum_{m \ni i} r_{m,pp}$$

$$T_{i,p} = \epsilon + \frac{\sum_{pp<p} \sum_{m \ni i} b^i_{(m,pp)} + \max_{pp>p} L_{pp}}{R_{i,p}}$$

where R_i is the transmission capacity of the T-AeroRing i, and $b^i_{(m,pp)}$ is the burst generated by the T-AeroRing m of the traffic class pp, and arriving at the input of the T-AeroRing i.

V. Worst-Case Timing Analysis

In this section, we first explain the different delivery modes of AeroRing, depending on the physical topology states, i.e., ring or line when fault occurrence. Then, the innovative timing analysis method for a ring-based network, based on the PMOO principle extension, is detailed to compute the maximum end-to-end delay bounds of each traffic class. Finally, the impact of a fault occurrence on the data delivery is presented.

A. Delivery modes

As illustrated in Fig. 2, AeroRing offers two delivery modes, i.e., guaranteed and non-guaranteed, according to the physical topology states, i.e. ring or line.

The data delivery of any traffic class (HRT, SRT and NRT) is guaranteed and maximum end-to-end delay bounds, EED_{max}, can be computed, as it will be detailed in the next subsection, when one of the following conditions is verified. The first concerns the nominal case, i.e., no fault occurrence and the topology still is a ring; whereas the second is fulfilled when all the T-AeroRing routing tables are updated to send SRT and NRT on the right path, after a fault occurrence transforming the physical topology to a line. The time needed from failure to reconfigure all the routing table is denoted $T_{recovery}$. However, the data delivery is non-guaranteed, i.e., the data may be lost, for all SRT and NRT messages transmitted at most EED_{max} before the fault occurrence, and maximum recovery time $T_{recovery}$ after the fault occurrence, as illustrated in Fig. 2. During this non-guaranteed delivery phase, the specified shortest paths in the routing tables for SRT and NRT traffic classes may be no longer correct and have to be updated. Therefore, the data that has to cross the faulty node or link will be lost. It is worth noting that the HRT class has always a guaranteed delivery delay since it is sent on both directions.

Hence, the computation of the maximum end-to-end delay bounds are detailed in the next subsection, based on the extension of PMOO approach to a ring-based topology. Then, the non-guaranteed delivery phase duration will be computed based on this maximum bound and the maximum recovery time.

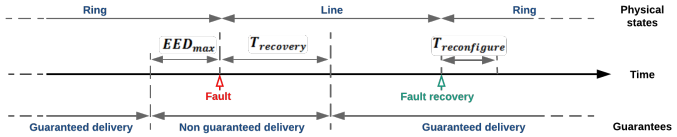

Fig. 2: Guaranteed and non-guaranteed delivery modes

B. End-to-End Delay Bounds during the Guaranteed Delivery Phase

In [12], the authors propose an innovative approach to compute the end-to-end service curve of a flow of interest by integrating the impact of interfering flows on its path only once and taking into account flow serialization phenomena. This recent result allows computing tight upper bounds on end-to-end delays due to proposition 1, as shown in [12]. However, this approach has been applied for feedforward networks with FIFO policy, and could not be directly applied in our case because of FP policy and the ring topology, which is considered as a particular case of non-feedforward networks.

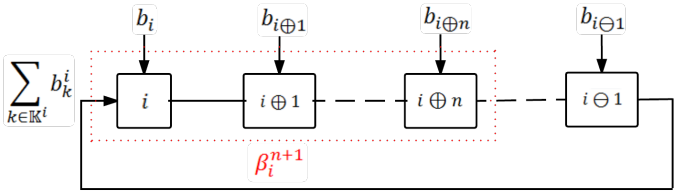

Fig. 3: Direct and Indirect Interferences

As illustrated in Fig. 3, for a ring-based network, the end-to-end service curve offered to a flow of interest i will depend on the direct interfering flows on its path, i.e. delayed by the flows generated by the crossed nodes on its path. Furthermore, it will depend also on the indirect interfering flows arriving upstream the T-AeroRing i, generated by other nodes of the ring. This aggregate flow is unknown a priori due to the cycle issue, i.e., each flow k (part of this aggregate flow) depends on the sum of upstream flows crossing the T-AeroRing k, which is also unknown, and so on until forming a cycle.

Hence, to compute the end-to-end service curve offered to a flow of interest i, we need to compute the arrival curves of flows arriving upstream the T-AeroRing i. Thus, we need to extend the proven end-to-end service curve in Prop.1 of [12] to compute the service curve offered to any flow on any of its sub-paths, starting from its source until reaching any node of the ring. Furthermore, we need to integrate the fixed priority effect by considering the T-AeroRing model, explained in subsection IV-C. The main idea consists in taking into account only flows having the same priority p as the flow of interest i, since the impact of other priority classes in each node k is already taken into account in the expressed service curve $\beta_{R_{i,p},T_{i,p}}$ in Formula (2).

Hence, we propose the following extended formula of the service curve offered to a flow i on its sub-path of length n starting in node i, $\beta^n_{i,p}$ as illustrated in Fig. 3. This curve is a rate-latency curve with a rate $R^n_{i,p}$ and a maximum latency

$T^n_{i,p}$, as following:

$$\begin{aligned}\beta^n_{i,p}(t) &= \left[R^n_{i,p}\right] \cdot \left[t - T^n_{i,p}\right]^+ \\ &= \min_{j \in \mathbb{J}^n_{i,p}} \left[R_{j,p} - \sum_{k \in \mathbb{K}^j_p} r_{k,p} \right] \times \\ &\quad \left[t - \sum_{j \in \mathbb{J}^n_{i,p}} T_{j,p} - \sum_{k \in \mathbb{K}^n_{i,p}} \frac{b^{j_{first}}_{k,p}}{\min_{j \in \mathbb{J}^n_{i \cap k,p}}[R_{j,p}]} \right]\end{aligned} \tag{3}$$

where:

- $\mathbb{J}^n_{i,p}$ is the sub-path of length n of the flow i with priority p;
- $\mathbb{K}^j_p$ is the set of flows crossing the node j and having the same priority p, when excluding the flow i;
- $\mathbb{K}^n_{i,p} = \bigcup_{j \in \mathbb{J}^n_{i,p}} \mathbb{K}^j_p$ is the set of flows, sharing at least one link with the flow i on its subpath $\mathbb{J}^n_{i,p}$ and having the same priority p;
- $\mathbb{J}^n_{i \cap k,p} = \mathbb{J}^n_{i,p} \bigcap \mathbb{J}_k$ with $k \in \mathbb{K}^n_{i,p}$ and $\mathbb{J}_k$ is the path of flow k;
- $b^{j_{first}}_{k,p}$ is the burst of flow k with priority p when crossing the node j_{first}, where $j_{first} = first\{j \in \mathbb{J}^n_{i \cap k,p}\}$ is the first shared link in the considered sub-path by the flows i and k, i.e., the first multiplexing point.

Therefore, when considering the aforementioned direct and indirect interference effects, illustrated in Fig.3, we deduce the following latency expression from (3):

$$\begin{aligned}T^n_{i,p} &= \sum_{j \in \mathbb{J}^n_{i,p}} T_{j,p} + \overbrace{\sum_{k \in \mathbb{J}^n_{i,p}, k \neq i} \frac{b_{k,p}}{\min_{j \in \mathbb{J}^n_{i \cap k,p}}[R_{j,p}]}}^{\text{Direct interference}} \\ &\quad + \underbrace{\sum_{k \in \mathbb{K}^i_p} \frac{b^i_{k,p}}{\min_{j \in \mathbb{J}^n_{i \cap k,p}}[R_{j,p}]}}_{\text{Indirect interference}}\end{aligned} \tag{4}$$

Before any fault occurrence, the network admits a ring topology and the formula (4) can be rewritten as following:

$$\begin{aligned}T^n_{i,p} &= \underbrace{\sum_{j=1}^{n} T_{i \oplus (j-1),p} + \sum_{k=1}^{n-1} \frac{b_{(i \oplus k),p}}{\min_{j \in \mathbb{J}_{i \cap i \oplus k,p}}[R_{j,p}]}}_{\text{Constant}} \\ &\quad + \underbrace{\sum_{k=1}^{M-1} \frac{b^i_{(i \oplus k),p}}{\min_{j \in \mathbb{J}_{i \cap i \oplus k,p}}[R_{j,p}]} \cdot \mathbb{1}_{\{(i \oplus k) \in \mathbb{K}^i_p\}}}_{\text{Indirect interference}} \\ &= cst1^n_{i,p} + \sum_{k=1}^{M-1} \frac{b^i_{(i \oplus k),p}}{\min_{j \in \mathbb{J}^n_{i \cap i \oplus k,p}}[R_{j,p}]} \cdot \mathbb{1}_{\{(i \oplus k) \in \mathbb{K}^i_p\}}\end{aligned} \tag{5}$$

where:

- M is the size of the network and nodes are labeled from 0 to $M-1$;
- $i \oplus k$ is equal to $(i+k) \mod M$ for the $k-eth$ successor of node i, and $i \ominus k$ is equal to $(i-k) \mod M$ for the $k-eth$ predecessor of node i.

On the other hand, the arrival curve of the traffic class p sent by the T-AeroRing j, received at T-AeroRing i is obtained throughout the application of Theorem 1 as follows:

$$\begin{aligned}\alpha^i_{j,p}(t) &= \alpha_{j,p} \oslash \beta^{i \ominus j}_{j,p}(t) \\ \implies b^i_{j,p} &= b_{j,p} + r_{j,p} \times T^{i \ominus j}_{j,p} \\ &= cst2_{j,p} + r_{j,p} \times T^{i \ominus j}_{j,p}\end{aligned} \tag{6}$$

The two equations (5) and (6) show the interdependency (cycle) between the latency and the upstream bursts. To solve this problem, we consider the following matrix system.

Let T_p be the vector that holds all the $T^n_{k,p}$ variables, for $k \in [0, M-1]$ and $n \in [1, M]$; and b_p be the vector that holds all the $b^j_{k,p}$ variables, for $k \in [0, M-1]$ and $j \in [0, M-1]$ with $j \neq k$. The associated matrix system is as follows:

$$\begin{cases} T_p = C_1 + A_1 \times b_p \\ b_p = C_2 + A_2 \times T_p \end{cases} \tag{7}$$

where: A_1 holds all the coefficients of the unknown bursts and C_1 the constants of formula 5; A_2 holds all the coefficients of the unknown latencies and C_2 the constants of formula 6.

Then, by propagating the constraints, we obtain the following relation:

$$T_p = (Id - A_1 \times A_2)^{-1} \times C_3 \tag{8}$$

where: $C_3 = C_1 + A1 \times C_2$

The system admits a solution if the matrix $(Id - A_1 \times A_2)$ is invertible, i.e., its determinant is not null. If this condition is verified, then we can compute the vector T_p. Afterwards, the delay bound of any flow i of priority p, after crossing $n \in [1, M]$ servers, is computed according to the following formula:

$$d^n_{i,p} \leq \frac{b_{i,p}}{R^n_{i,p}} + T^n_{i,p}$$

Consequently, the maximum end-to-end delay bound for each priority p is computed as following:

$$EED_{max,p} \leq \max_{i,n} d^n_{i,p} \tag{9}$$

It is worth noting that to find the residual service for a priority p, all the vectors b_{pp}, for $pp < p$, need to be computed to define the residual service curves offered by the different nodes to the class p, as shown in formula 2, and consequently to compute the vector T_p.

In the simple case of broadcast communication with one traffic class and with an utilization rate per node of x, the determinant of the matrix $(Id - A_1 \times A_2)$ is a polynomial function of x with a degree M as follows:

$$(1 - M) \times (x + 1)^{(M-1)} \times (x - \frac{1}{M-1})$$

This matrix system is stable for $x \leq \frac{1}{M-1}$, which induces the ring stability condition under full network utilization, i.e. bounded delays.

On the other hand, after a fault occurrence, the network topology becomes a line topology. Therefore, the sets $\mathbb{J}^n_{i,p}$,

$\mathbb{K}_p^i$ and $\mathbb{J}_{i\cap k,p}^n$ in Eq. (4) have to be updated, accounting the new paths defined in the routing tables. Furthermore, the indirect interfering flows arriving upstream the T-AeroRing become known and can be directly computed in this case, e.g., matrix system resolution is not needed in this case since no more interdependency between the flows. Hence, the end-to-end delay bounds still are computed based on formula (9).

C. Non-guaranteed Delivery Phase Duration

As illustrated in Fig. 2, the data delivery for traffic class p (SRT or NRT) is not guaranteed for a duration equal to:

$$EED_{max,p} + T_{recovery}$$

The $EDD_{max,p}$ is computed based on Eq. 9, and $T_{recovery}$ is equal to the sum of: (i) detection time $T_{detection}$, which is the maximum time needed to the neighbors of the faulty node or link to be aware of failure; (ii) the delivery times of control messages for fault declaration T_{decl} and routing tables update T_{tab-up}; (iii) the blocking delay due to low priority messages in each crossed T-AeroRing, i.e. in the worst-case, in addition to the technological latency, a maximum packet length of low priority will delay the control messages at each crossed T-AeroRing. Therefore, the recovery time is as follows:

$$T_{recovery} = T_{detection} + T_{decl} + T_{tab-up} + T_{delay} \qquad (10)$$

where:

- $T_{detection} = N_{detection} \times T_{announce}$ is the local fault detection time. It corresponds to a non reception of $N_{detection}$ control messages from the neighbor, which are sent in the absence of traffic each *announcing period* $T_{announce}$.
- $T_{decl} = \frac{8\times 84}{C}$: is the transmission time of one control message of minimum size of 84 bytes (64 bytes for the minimum Ethernet frame size and 20 bytes for the preamble and IFG). C is the network capacity;
- $T_{tab-up} = \frac{L_{adr-list}\times 8}{C}$ where $L_{add-list}$ is the length of the control message containing the list of MAC addresses, used to update the routing table and is equal to $42 + max(42, 2 + 6 \times (M-3))$ bytes, where 42 bytes is the overhead of the ethernet header with the 802.1q tag including 12 bytes for the IFG, 2 bytes to identify the message type, and $(M-3)\cdot 6$ Bytes is the size of an Ethernet MAC address multiplied by the maximum number of crossed nodes, i.e. all the nodes apart the failed one and the two detecting the failure.
- $T_{delay} = (M-3) \times (\frac{\max_{pp>0} L_{pp}\times 8}{C} + \epsilon)$

It is worth noting that the maximum amount of lost data of each trafic class, i.e., SRT or NRT, is proportionnal to the non-guaranteed delivery phase duration and the corresponding data rate.

VI. Validation

In this section, we investigate the offered timing performance of AeroRing through a representative avionics case study. This later consists in replacing the backup AFDX network with the ring-based AeroRing network to reduce wires and weight. First, the considered case study is described. Then, numerical results of maximum end-to-end delays, and recovery times are detailed under different system configurations.

A. Case of study

The considered avionics network consists of 56 nodes and there are three traffic classes generated in each node and served following the FP policy. The characteristics of these traffic classes are described in Table I. Furthermore, we consider the following assumptions: (i) he transmission capacity of AeroRing is $C = 1Gbit/s$; (ii) all equipments generate in broadcast the three types of traffic classes; (iii) technological latency within each *T-AeroRing* is $600ns$; (iv) the *detection period* for fault management is 0.5ms.

It is worth noting that in the broadcast mode, the notion of "shortest path" does not exist for the traffic SRT and NRT. In this case, we consider that all the SRT and NRT messages are sent on the same direction. These assumptions induce the worst-case scenario in terms of performance, i.e., increase contentions.

TABLE I: Traffic Characteristics

TC	P (ms)	Payload (byte)
HRT	4ms	226
SRT	64ms	482
NRT	128ms	1500

To analyse the worst-case timing performance offered under AeroRing, we consider the two following scenarios:

- Scenario 1: to analyze the impact of increasing the network scalability, i.e., network size, on the temporal performance of AeroRing, the upper bounds on end-to-end delays of each traffic class and recovery time are computed under the variation of the node number, from 10 to 100 nodes by a step of 10 nodes.
- Scenario 2: to analyze the network schedulability for HRT traffic, the upper bounds on end-to-end delays of HRT class are computed when the number of nodes is fixed, $M = 56$, and the network load is increasing by a step of 10% until reaching 100%.

B. Numerical results

Figures 4 and 5 illustrate the upper bounds on end-to-end delays of the different traffic classes, and the maximum recovery time, respectively, under scenario 1. Obviously, the upper bounds on end-to-end delays increase with the number of nodes, but still are always less than the associated temporal constraints of HRT and SRT traffic classes. Particularly, for a large network of 100 nodes, the maximum bound on the end-to-end delay of HRT traffic and the maximum recovery time are less than 1.8ms. Hence, the HRT messages are still schedulable, i.e., delay less than period, when the network size increases. Furthermore, the maximum duration of the non-guaranteed delivery phase is equal 32.2ms for SRT traffic, which is less than the associated period (64ms). This fact means that at most one SRT message per node may be lost,

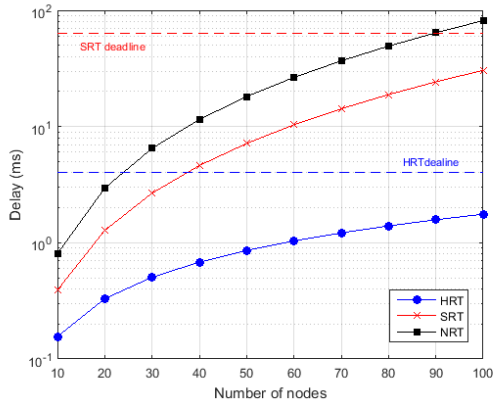

Fig. 4: Upper bounds on the end-to-end latencies vs number of nodes

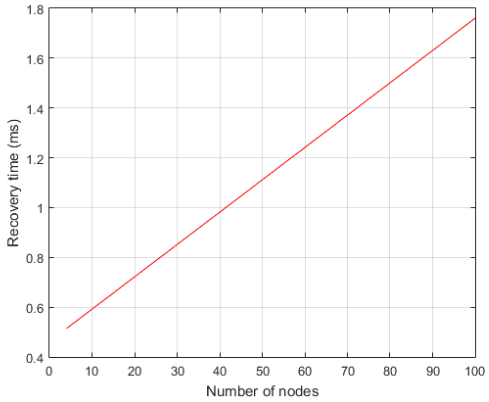

Fig. 5: Maximum recovery time vs number of nodes

when a fault occurs. These results show the high temporal performance of AeroRing for large scale networks.

On the other hand, Figure 6 shows the impact of the network load on the upper bounds of end-to-end delay of HRT class, under scenario 2. As we can notice, the delay bound increases with the network utilization rate, while respecting the temporal constraint of HRT traffic (4ms) under 85.4% of network utilization. This result shows the schedulability performance of AeroRing under high network load.

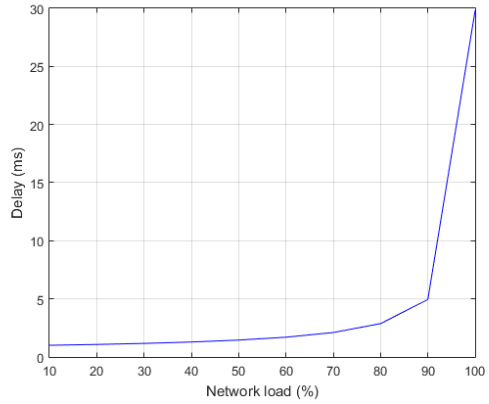

Fig. 6: Upper bounds on end-to-end delays vs network load

VII. Conclusion

The worst-case timing analyses of AeroRing, have been detailed in this paper, to prove its performance in terms of guaranteeing the real-time constraints.

The proposed approach is based on the extension of the most recent results of Network Calculus Theory, PMOO principle, and integrates the impact of the Fixed Priority service policy and the specified reliability mechanisms. The effectiveness of such a proposal has been validated through a realistic avionics case study, where traffic schedulability still is guaranteed for large scale network and high utilization rate. Furthermore, at most one SRT message per node can be lost in case of fault, since the maximum non-guaranteed delivery phase duration is less than the SRT class period.

AeroRing has been specified to fulfill the avionics requirements, but it can be easily extended for other industrial application fields, such as automation and control. This adaptation will be investigated as a next step of our work with a full dependability study.

References

[1] EtherCat - the Ethernet Fieldbus, URL:"www.ethercat.org".

[2] SERCOS - the automation bus, url:"www.sercos.com/technology/sercos3.htm".

[3] Avionics Full-Duplex Switched Ethernet (AFDX) Network, ARINC Specification 664, Part 7. *A. E. E. C*, 2002.

[4] *IEC 61784-2, Digital data communications for measurement and control - Part 2: Additional profiles for ISO/IEC 8802-3 based communication networks in real-time applications*. 2010.

[5] *IEC 62439-7, Industrial communication networks - High availability automation networks - Part 7: RRP*. 2011.

[6] *IEC 62439-3, Industrial communication networks - High availability automation networks - Part 3: PRP and HSR*. 2012.

[7] *IEC 62439-6, Industrial communication networks - High availability automation networks - Part 6: DRP*. 2012.

[8] A. Amari, A. Mifdaoui, F. Frances, J. Lacan, D. Rambaud, and L. Urbain. AeroRing: Avionics Full Duplex Ethernet Ring with High Availability and QoS Management. In *ERTS 2016*.

[9] A. Bouillard, L. Jouhet, and E. Thierry. Service curves in network calculus: dos and don'ts. 2009.

[10] A. Charny and J.-Y. Le Boudec. Delay bounds in a network with aggregate scheduling. In *Quality of Future Internet Services*. Springer, 2000.

[11] R. L. Cruz. A calculus of delay Part II: Network analysis. *IEEE Trans. Inform. Theory*, 1991.

[12] M. Fidler. Extending the network calculus pay bursts only once principle to aggregate scheduling. In *Quality of Service in Multiservice IP Networks*. Springer, 2003.

[13] M. Fidler. Survey of deterministic and stochastic service curve models in the network calculus. *Communications Surveys and Tutorial*, 2010.

[14] J. Grieu. *Analyse et evaluation de techniques de commutation Ethernet pour l'interconnexion de systemes avioniques*. PhD thesis, INP, Toulouse, 2004.

[15] O. Kleinberg and M. Rentschler. Redundancy enhancements for industrial ethernet ring protocols. In *ETFA 2010*.

[16] J.-Y. Le Boudec and P. Thiran. *Network calculus: a theory of deterministic queuing systems for the internet*. Springer Science & Business Media, 2001.

[17] R. Pigan and M. Metter. *Automating with PROFINET*. Publicis Publishing, 2008.

[18] J. Robert, J.-P. Georges, E. Rondeau, and T. Divoux. Minimum cycle time analysis of ethernet-based real-time protocols. *International Journal of Computers, Communications and Control*, 2012.

[19] S. Sommer, A. Camek, K. Becker, C. Buckl, A. Zirkler, L. Fiege, M. Armbruster, G. Spiegelberg, and A. Knoll. RACE: A Centralized Platform Computer Based Architecture for Automotive Applications. In *IEVC*, 2013.

[20] L. Tassiulas and L. Georgiadis. Any work-conserving policy stabilizes the ring with spatial re-use. *IEEE/ACM Trans. Netw.*, 1996.