Università degli Studi di Ferrara

DOTTORATO DI RICERCA IN

SCIENZE DELL'INGEGNERIA

CICLO XXVII

COORDINATORE Prof. Trillo Stefano

Design of a New High Bandwidth Network for Agricultural Machines

Settore Scientifico Disciplinare ING-INF/05

Dottorando
Dott. Giorgio Malaguti

Tutore
Prof. Ruggeri Massimiliano

Anni 2012/2014

1 INDEX

2 Introduction (ISO11783 – ISOBUS and AEF PT10)

This work is the result of the research conducted at the IMAMOTER-CNR, Institute for Agricultural and Earth-Moving Machinery. IMAMOTER is a research centre whose research has focused on different aspects of agricultural machinery, construction equipment and, in general, heavy-duty vehicles. The research staff of the Institute is formed by groups of engineers with diverse specialization and is a national and European excellence for the part of the hydraulic and electronic control of the hydraulic components, namely mechatronics related to electrohydraulic applications.

As a historical note, IMAMOTER was born as an institution dedicated to the mechanics, following the technologies related to agricultural and earth-moving machinery. The electronic technology was introduced in the last fifteen years, and over time has found its space and has gained an increasingly important role in reducing the dependency of applications from single mechanical part and, at the same time, helping to improve the precision of the control systems designed. The advance of the electronics, with the possibility of using higher computing powers, has paved the way to computer technology and automatic controls, namely the possibility of using programmable logic in order to obtain even more advanced controls and valid for different applications. With the advance of the technology and communication, protocols has opened the perspective of being able to integrate systems, originally designed as a stand-alone, in distributed control systems, with multiple electronic control units (ECU), each performing a specific function, increasing the scalability and reusability of each component.

In recent years, the adoption of network protocols in wired and wireless networks with high throughput in the aforementioned scenarios have enabled ECU systems or machines to work in a collaborative or cooperative manner (the so-called clusters) bringing automation and automation of machining on the field at unimaginable levels only a few years ago. Increased automation of processes and the increasing complexity of systems has ultimately led to a careful evaluation of the functional safety components that such systems can offer.

With the publication of SAE J1939, which standardizes communications between ECU in heavy-duty machines, specifically powertrain networks, multi-vendor ECUs could communicate with each other over the same machine. One specialized evolution of this standard, established in 2002, is ISO 11783, which is based on the same architecture of the standard SAE J1939 (up to the ISO OSI's layer 4). The aim of standardizing all agricultural applications, creating a de facto standard for treatments and precision automations (precision farming) and fleet management led to the creation of ISO 11783 (a.k.a. ISOBUS). Unlike J1939, where each ECU occupies a well-defined functionality within the machine, decided by the machine manufacturer (system integrator), a major feature of ISO 11783 is the ability to hotplug, which supports interconnection ECUs on-the-fly, which auto-configure themselves in order to perform the functions in the network. Both SAE J1939 and ISO 11783 use the CAN (Controller Area Network) bus as their fieldbus, which was specified by Bosch Automotive in 1992 with the CAN specification 2.0 A and 2.0 B, then transposed to the ISO standard ISO 11898.

As functionalities of precision farming had increased both in number and maturity, so had the amount of data exchanged for the same operation of the system. However, the introduction of new features, (e.g. the autonomous driving) and the increasing number of ECU within a network of a modern tractor saturated the offered bandwidth on the network, reaching the limit of the CAN bus.

Many automotive vendors saw in Ethernet (and its field busses, as explained later) a complementary bus, side by side to other traditional buses like CAN, LIN and Flexray, which would allow high-speed communication to take place, thus enabling the development of innovative applications which need to exchange high amount of data.. This trend follows the one involving the automotive industry, for which is foreseen an exponential growth.

To fulfill industrial and specific needs of determinism and safety, many products modifying the standard Ethernet were designed, altering its characteristics. Those products can be roughly ranked as follow:

- the access method - whereas standard Ethernet is designed to be random access, many successful fieldbuses provide a time-triggered access method;
- the hierarchy of the network - creating a Master/Slave paradigm, in spite of the usual plain hierarchy (though at application layer various hierarchical models still can be applied, such as Client/Server or Peer-to-Peer).

Examples of the most successful fieldbuses are EtherCAT, Ethernet/IP, Powerlink, Profinet and SERCOS III.

It is beyond the scope of the thesis, to make a comparison between these products, as many of these can be found in literature [1, 2, 3, 4] and respond to a variety of different needs; instead, the research deals with the feasible infrastructures and technologies to be adopted in AG Mobile environments. The focus will be put on cost effectiveness and performances in a standard Ethernet network infrastructure, leveraging well-established and standardized technologies, customizing them for industrial compartments, such as automotive and heavy-duty machines ones, which normally cannot count on such a variety of technological diversity. Industrial automation solutions, referred as fieldbus, also provide interesting approaches that will be evaluated.

Another important advantage is the availability of hardware: even in consumer compartment, a broad support, both commercial and open source, and the easiness of use, which would speed up development and reduce time-to-market of products that can rely on this technology for distributed control. Furthermore, where Ethernet 100base-TX physical layer lacked (e.g. environmental robustness to EMC, cable length, etc.) silicon industries (e.g. Broadcom PHYs) provided with many interesting products that are definitively allowing Ethernet to enter this delicate yet advantageous industry compartment.

The choice of adopting standard Ethernet and TCP/IP stack, for these early tests has been encouraged by the fact that other players in different markets (particularly avionics and) are using the Internet Protocol Suite.

The research focused on the possible ways to prioritize the traffic, in a congested network, in order to achieve a certain level of determinism and prioritize the traffic in order to prevent data losses. The target is to achieve real high dynamics distributed control, such as "x-by-wire". This thesis will try to approach this problem in an architectural and technological way.

The candidate has been nominated expert by CUNA (Technical Committee of Unification in Automotive) to participate at standardization meetings of ISO11783, where he proposed and led a Preliminary Task Force for the investigation of a new "high bandwidth for two years. the work converged in the AEF PT10 "High Speed ISOBUS" working group, to which the candidate attends regularly and actively participates. The Agricultural Industry Electronics Foundation (AEF) assists AEM (Association of Equipment Manufacturers) members as they develop the hardware and electronic communication protocols to allow and confirm reliable communications between several related machines or implements, even though they are made by different manufacturers. The overall objective of AEF is to develop harmonized technology enabling equipment, components and software manufactured anywhere and by anyone to operate seamlessly together.

3 The choice for a new physical layer

Automotive industry is accustomed to CAN bus topology, featuring relatively low cost per meter but high lengths resulting in heavy weight and considerable costs burden for wiring and consumes, without mentioning the low throughput of CAN. On the other hand, Flexray bus enjoys a star topology, which reduces wirings length sensibly, but due to the costs of controllers, wirings and stiffness of the network dynamics, this standard does not seem to be eligible to become the next de facto standard for in-vehicle distributed control. The advantages of having a star topology using Ethernet are multiple:

- Cost effectiveness in terms of wiring costs and weight;
- Easiness in topology changes and transparency for traffic bound outside the vehicle;
- The possibility to use Ethernet as a backbone to interconnect systems rather than single ECUs (cfr Figure 1), which may still communicate, inside their own system with other convenient buses, as feasibility to make gateways to translate traffic between heterogeneous busses has been already proven before [5].

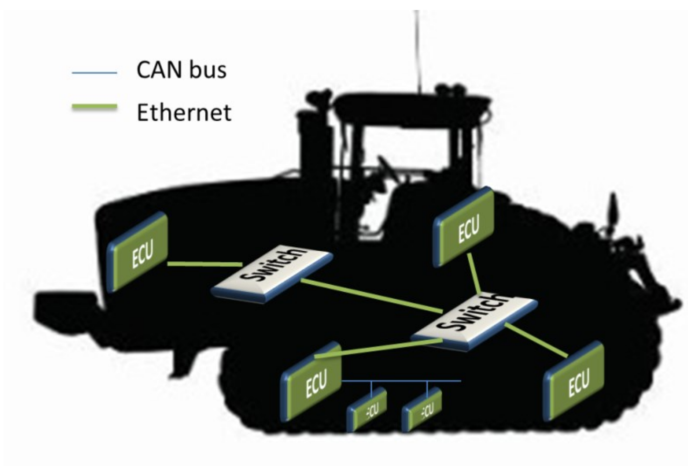

Figure 1: Hypothetical heterogeneous topology for heavy-duty vehicles

With the openings of the AEF PT10 working group, the main objective was to scout with functionalities and relative requirements needed for a new "high-speed" network. Nevertheless, initially it seemed appropriate to rank the currently available busses, to evaluate the feasibility of a certain network in the various application scenarios. The results have been published and resumed in this table. In the table, Wi-Fi also appeared for M2M communication, which is out of the scope for this work, thus will not be discussed, as well as Ethernet AVB and industrial Ethernet fieldbuses, which will be discussed later.

	Openness	Hardware availability/cost	Bandwidth	Hotplug Capability	Topology	Safety	Ag Mobile Compliancy (EMI/EMC, environmental robustness, …)
IEEE 802.3	YES	High availability, both COTS and industrial solutions	100/1000Mbit	YES	Every	NO (possible w/openSAFETY)	PHY dependent
IEEE 802.3AVB	YES	Low availability, expensive network infrastructures	100/1000Mbit	YES	Every	NA	PHY dependent
Eth Fieldbusses	mostly YES	Some have custom PHY and MACs	100/1000Mbit (not every fieldbus is Gigabit ready)	depends on the field bus	Every	Many have IEC-61508 SIL 3 certified layer	PHY dependent
CAN-FD	under ISO standardization	ISO11898-2/6 transceivers	2Mbit for ISOBUS theoretical	YES	Physical bus	NA	NA
Flexray	under ISO standardization	Expensive controllers	up to 10Mbit	NO (attempts were made to enable feature)	Star	NO	YES
IEEE 802.11b/g/n/p	open standard	high availability, COTS solutions	up to 300 Mbit	YES	star or mesh	NO (maybe w/openSAFETY)	NO (p?)

Table 1: comparison between various communication network

3.1 CAN Flexible Data rate

Considered as the successor to the CAN 2.0 [7], namely CAN Flexible Data Rate (CAN-FD) was developed within Bosch and published in 2011. Defined as with standard ISO 11898 and capable of supporting higher throughput using data packets up to 64 bytes contained in the same space of the old 8-byte packets.

The bitrate is dynamic, while the phase of arbitration and acknowledge remains identical to the protocol CAN 2.0, the bitrate of data field can be increased up to 8 times the standard one. Therefore, in the space of 8 bytes + checksum can send packets of 16, 32 or 64 bytes, with a 17 or 21-bit checksum. The main disadvantage is that, despite being defined as compatible, nodes equipped with the device CAN classic do not recognize the data and fail checksum calculation, thus filling the network with Error Frame. Finally, backward compatibility is guaranteed only if certain actions and changes are taken on the legacy, while remaining backward compatible. The bandwidth constraints remain the same, as well as those regarding the length of the Bus. The maximum achievable throughput is still inferior to 8Mbit with baseband network that allows to 1Mbit bus lengths of less than 10 meters.

Using this type of bus on a network in accordance with ISO 11783, would mean to increase the maximum throughput of eight times, so up to 2MBit, insufficient for the new features to be implemented in the medium to long term. This, added to the issues of actual backward compatibility, has made this solution not adoptable.

3.2 Flexray

FlexRay (ISO 17458) allows a throughput of up to 10 Mbps, guaranteeing high levels of reliability. Conversely, it uses very expensive hardware and does not allow features such as plug & play, given the strictly static configuration of the map of the division of beacon time. Flexray suffers from the lack of adaptability of the bus length, mainly due to the need for clock synchronization of devices, managed by complex bus guardian resident in the controller. Although research efforts [8,9] were made to enable the ability to hotplug a node in the network (i.e. the node is energized after an arbitrary amount of time the network setup and is enabled to communicate in it), no industry-ready solutions seemed to grant plug & play facilities.

Its use has been confined in the automotive world for which it was designed, particularly BMW world and for some ECU, typically for safety relevant functionalities. The high cost of devices of this kind are inappropriate to market demands and the maximum throughput available is not sufficient to ensure the scalability required in the medium to long term.

3.3 IEEE 802.3 – Ethernet

Ethernet is, nowadays, the most popular and widespread network of the world. It was born in 1976 thanks to Xerox, which decided to use the CSMA/CD protocol to create a local network working at 2.94 Mbit/s on 100 stations.

Thanks to the use of CSMA/CD a master station is not necessary, because it is a distributed multiple access method. This additional strong point favoured Ethernet adoption.

This algorithm imposes that a station that wants to send a packet, first of all senses the carrier (listening the channel to know if the carrier is present, hence if another station is transmitting). If the channel is free the station can transmit, but because of propagation delays, it is still possible to have a collision. In consequence of that, the transmitting station still hears the channel, comparing the signal on the bus with the transmitted one. If a collision is detected the station stops the transmission and sends a jamming sequence to inform every station of the collision. The receivers, in consequence of the jamming sequence, discard the packet. In the end, the transmitting station retry to send the message after an arbitrary time. It retries maximum for 16 times, then the frame will be discarded. This is the reason for which Ethernet is considered as unreliable.

The collision domain is defined as a single CSMA/CD network in which a collision may occur if two stations transmit at the same time. A practical example of collision domain is shown in Figure 2.

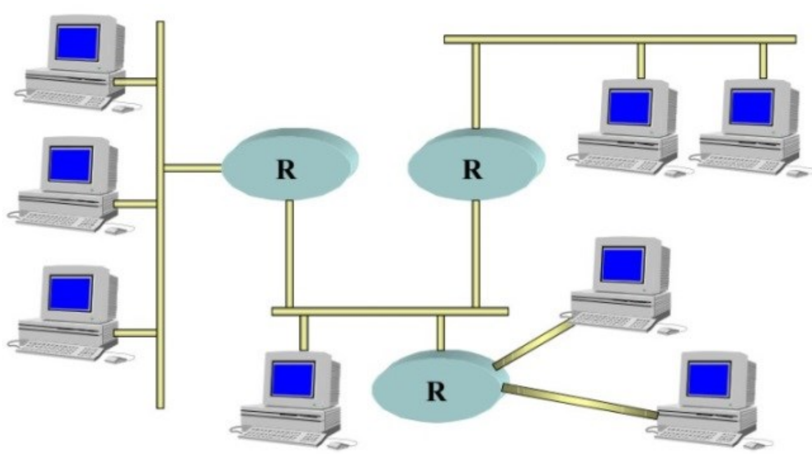

Figure 2: Collision domain

Level 1 devices like repeater, hub and transceivers don't split the network in different collision domains; for this purpose devices that work at higher OSI levels, like bridge, switch and router are necessary.

With the decreasing cost of these devices, Ethernet topology migrated to the star one for the several advantages offered.

In this structure, every station is linked with a point-to-point line with the hub.

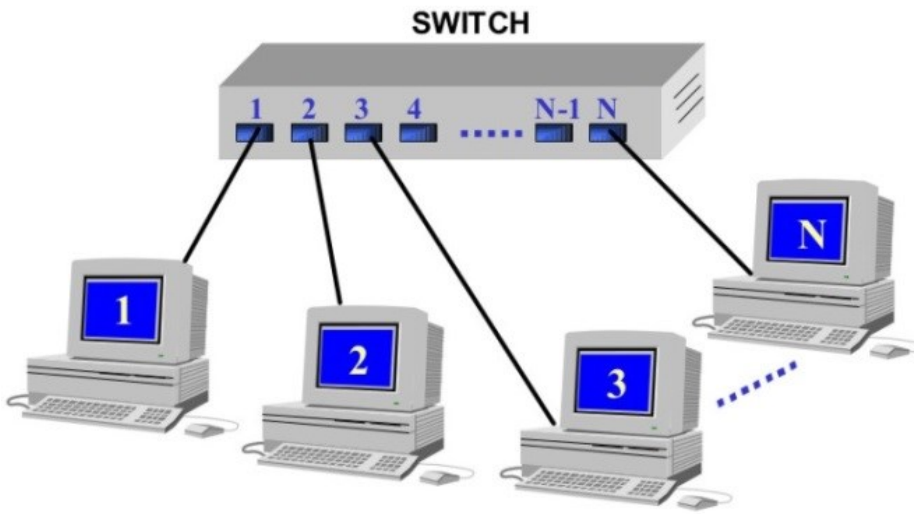

Figure 3: Switched Ethernet

The situation is definitely improved if the star centre is a level 2 device, like a switch, as shown in Figure 3. These devices, in fact, are able to process more frames simultaneously, allowing supplying to every user the maximum speed available on the network.

Thanks to the switch adoption, there is the additional advantage to divide the network in more collision domains, even making every device be in a single collision domain, completely avoiding collisions. This significantly improves network performances because switches can make integrity checks on frames in circulation on the network, discarding bad frames. The disadvantage of this kind of control is the delay introduced by the check operation. Consequently, different switching policies have been studied to reduce the introduced latency.

In the following subchapters, two relevant physical layers (also referred as PHYs) will be discussed; these are the most relevant for feasibility and characteristics in Ag mobile environments.

3.3.1 IEEE 802.3 100-baseTX

100BASE-TX is the predominant form of Fast Ethernet, and runs over two wire-pairs inside a category 5 or above cable (Figure 4). Each network segment can have a maximum cabling distance of 100 meters (328 ft). In its typical configuration, 100BASE-TX uses one pair of twisted wires in each direction, providing

100 Mbit/s of throughput in each direction (full duplex), this is obtained by using a dual simplex communication.

The configuration of 100BASE-TX networks is very similar to 10BASE-T. When used to build a local area network, the devices on the network (computers, printers etc.) typically connects to a hub or switch, creating a star network. Alternatively, it is possible to connect two devices directly using a crossover cable.

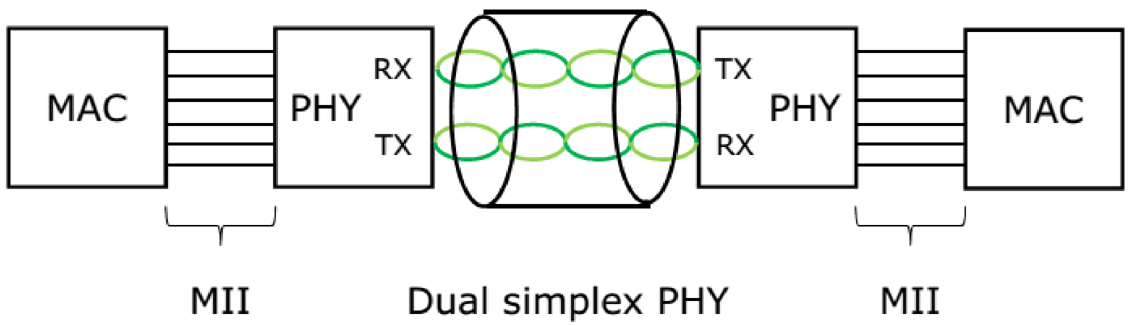

Figure 4: 100base-TX basic network topology

With 100BASE-TX hardware, the raw bits (4 bits wide clocked at 25 MHz at the MII) go through 4B5B binary encoding to generate a series of 0 and 1 symbols clocked at 125 MHz symbol rate. The 4B5B encoding provides DC equalization and spectrum shaping (see the standard for details).

100BASE-TX introduces an additional, medium dependent sublayer, which employs MLT-3 as a final encoding of the data stream before transmission at 125Msps, using 65 to 80 MHz bandwidth.

3.3.2 O.P.E.N. Alliance Broadr-Reach

BroadR-Reach (OABR) [10] is a modified Ethernet physical layer designed by Broadcom for use in automotive connectivity applications.

One of the most important advantages is that it has been designed to use a single twisted pair cable (Figure 5). This characteristic denote OABR vocation for automotive. In fact, Broadcom had a special care in the development of this standard to let it fit to automotive area requirements: low cost and lightweight cabling, low power and cost-efficient components, robust operation under severe noise conditions.

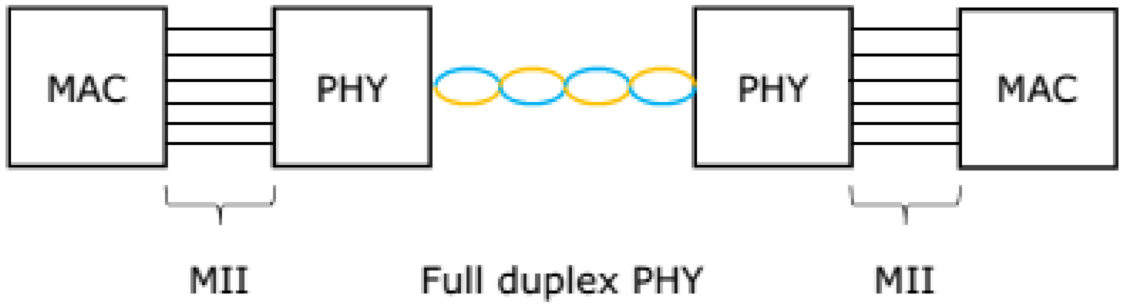

Figure 5: BroadR-reach basic network topology

The objectives that characterized OABR development are:

- To provide a PHY that supports full duplex operation at 100 Mb/s over one pair unshielded twisted pair or better cable for at least 15 m;
- Provide compatibility with the MII and IEEE 802.3 MAC operating at 100 Mb/s;
- Maintain a BER of less than or equal to 1.0E-10 at the MAC interface;
- Support 100 Mb/s operation in automotive and industrial environment.
- Support a start-up procedure which enables the time from power on to valid data to be less than 200 ms;

The PHY needed to have some peculiar characteristics. First of all Broadcom tried to use as more as possible already proven technologies of IEEE standard to support a single pair Automotive Cabling connection, to reach up to 15 meters.

PHYs are also optimized for Automotive EMC requirements. To enhance EMC performance the TX Power Spectral Density has been shaped to fit Automotive Emissions Masks, in particular it has been used a PAM-3 modulation for high noise immunity and DSP-based receiver technologies, using DFE and Echo Cancellation for FDX operation.

A comparison between standard Ethernet and OABR PHYs highlights an improved immunity and lower emission characteristics for the latter.

A system overview can show that the OABR channel uses, as anticipated in the lines above, a PAM3 modulation to reduce Electromagnetics Emissions and has a bandwidth of 33.3 Mhz, which grants a baud rate of 66.6 Mbaud.

The mode of operation is a FDX w/Echo cancellation and the transmission Power Spectral Density respect both lower and upper automotive emissions masks.

The PHY synchronization is realized thanks to a loop timing, the signal mapping is a 3B2T and the equalization is receiver-based. As the transmitter and receiver must be clocked from the same source to grant echo cancellation, the communication has a master that provides with a fixed-frequency clock to one slave.

OABR is under IEEE standardization as a communication standard being part of the IEEE 802.3 family [6] and the first release is expected for the end of 2015.

4 The TCP/IP stack

4.1 IP

Internet Protocol is conceived to be used in interconnected systems of packet switching networks. It transmits data blocks called "datagrams" from a source to a destination, identifying it through fixed length addresses. It provides the possibility to fragment and reassemble datagrams both when a datagram has a big size and when the MTU of the network is smaller than datagram's size.

IP is specifically designed to deliver a datagram from a source to a destination through an interconnected networks system. No mechanisms that increase end-to-end data reliability or that grant flow control, sequentiality or other services are found in other host-to-host protocols.

This protocol is called from host-to-host ones to take internet datagrams to destination.

IP modules uses the addresses reported in IP header to take IP datagrams to destination. The selection of a path for transmission is called routing. IP modules use header's fields to fragment and reassemble internet datagrams when necessary. The operative model requires that there is an internet module per each host interested in communication. These modules will share the rules to parse the address fields and to fragment and assemble datagrams. These modules has also procedures to make decisions about routing.

IP treats each datagram as an independent entity, not correlated to each other. There are no connections or logical circuits.

To supply the service, four key mechanisms are used: Type of Service, Time to Live, Options and Checksum:

- **Type of service (TOS):** it is used to indicate desired service typology. A parameter set characterize the services choice taken in those networks that builds internet. These indications can be used by the routers to:
    - select current transmission parameters;
    - select the network to be used for next hop;
    - select next host when routing an IP datagram;

- **Time to live (TTL):** it is an indication of the upper limit on a datagram lifetime. Its set by the device that sends the datagram and is reduced of a unit at each host that process packet's route. If TTL reaches zero before the datagram has arrived to destination then it is discarded.

- **Options:** this field provides necessary control functions or, however, useful functions for some situations, but not necessary for most common communications. These options include information like the timestamp, information for security and special routing.

- **Checksum:** it provides a verification that the information used in processing the datagram have been correctly transmitted. If errors are revealed then the datagram will be discarded by the entity that discovers it.

IP does not supply a reliable communication: no acknowledge are provided (nor end-to-end or hop-to-hop). There is no error control mechanism on data, but only on header. No retransmission or flow control mechanism is provided.

If any error is found Internet Control Message Protocol (ICMP) notices it back to the source host.

About addressing, it is necessary to make a distinction between name, address and route: the name is what it's searching for, the address is where it can be found and the route is show to reach it. IP mainly works with addresses and the IP routing table. It is going to be an upper level's task to map names into addresses, typically the Domain Name System (DNS) and to construct the routing table, either using a routing protocol such as OSPF (Open Shortest Path First) or RIP (Routing Information Protocol) or a static routing table.

Addresses have a fixed length of 32 bits. They begin with a network number, followed by a local address. There are three classes of internet addressing:

- **Class A:** most significant bit is set to zero, the following seven define the network and the last 24 are the local address;

- **Class B:** the first couple is 10, the following 14 define the network and the last 16 are the local address;

- **Class C:** the first three bits are 110, followed by 21 bits describing the network address, while the last 8 bits are the local address.

It has requested a particular attention in mapping internet addresses to local network's addresses. A single physical host can be able to work like if there are different hosts. Some hosts also have different physical interfaces (multi-homing).

The fragmentation of an internet datagram is necessary when the packet generated in a local network that allows big packages have to cross networks that limits packets to smaller sizes. A datagram can also be marked as non-fragmentable. In this case, if it exceeds network maximum dimensions it is going to be discarded. The fragmentation and reassembly procedure needs to be able to split the datagram in an arbitrary number of pieces that will be reassembled later. The fragment's receiver uses the identification field to ensure that different datagram's pieces are not mixed. The "fragment offset" field indicates in which position the fragment has to be placed to rebuild the packet. The "more fragments" field indicates the last fragment. These fields provide enough information to rebuild the datagram.

Figure 6 shows an IP header's structure. It is going to be analysed the function of different fields:

- **IHL: 4 bits.** It is the IP header's length indicated in 32-bit word's terms. The minimum value for a correct header is 5.
- **Type of service: 8 bits.** Indicates abstract parameters of the specific service typology. These parameters will be used to guide the selection of service's parameters in datagram transmission. In fact, different networks offers different priority for various services. The major choice is a three-way trade-off between low delay, high reliability and high throughput.
- **Total length: 16 bits.** Indicates the length, in byte, of the datagram, including the header and data. A datagram length can reach 65536 bytes, even if this maximum length is not much used in hosts. However, every host has to support at least 576 bytes. This number is chosen to allow a reasonable data block dimension to be transmitted added to header's information.
- **Identification: 16 bits.** Identification number assigned by the sender to help in datagram fragments reassemble.
- **Flags: 3 bits.** Various control flags.
- **Fragment offset 13 bits.** Indicates where it has positioned the received fragment in the complete datagram.

- **Time to live: 8 bits.** Indicates the number of maximum hops that a datagram can have.
- **Protocol: 8 bits.** Indicates the upper level protocol used in the data portion of the datagram.
- **Checksum: 16 bits.** Header's checksum.
- **Source address: 32 bits.**
- **Destination address: 32 bits.**
- **Options: variable.** This field can appear or not in a datagram. However, every IP module must implement the options. Only the transmission in datagrams is optional.
- **Padding: variable.** Used to make the header's length to be multiple of 32 bits.

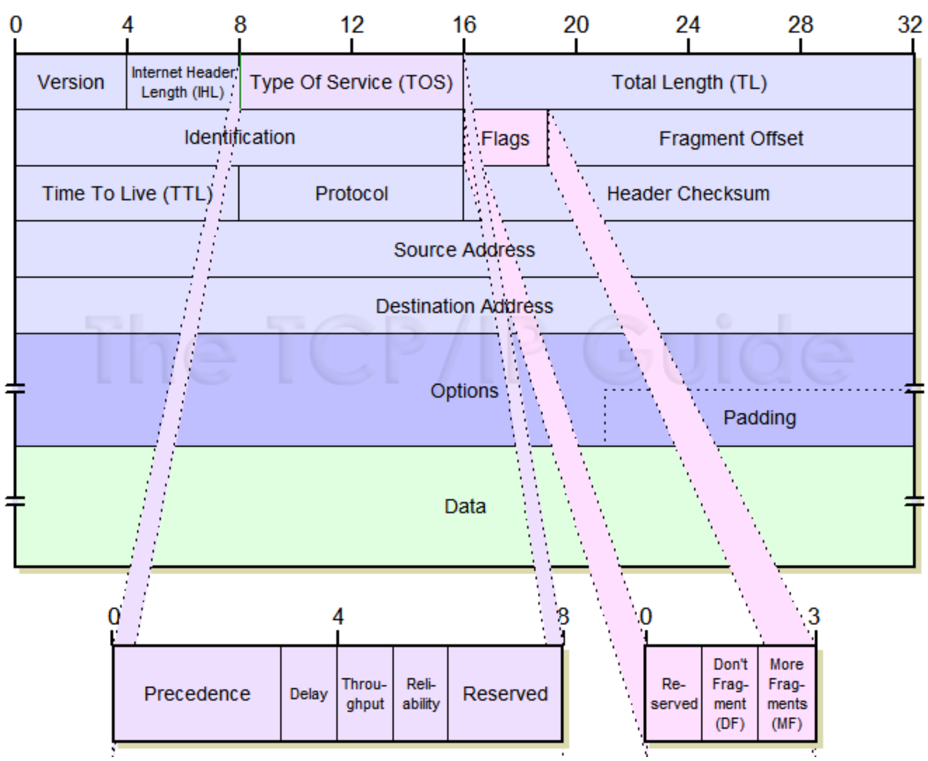

Figure 6: IP header

4.2 ICMP

Internet Control Message Protocol (ICMP) is a protocol for the IP signalling, and as such is an integral part of IP. Every ICMP packet has a structure dependent on the kind of signalling, that is bringing and the constant and qualifying parts are only in the first 32-bits.

They contains:

- ICMP message type (8-bit);
- ICMP code (8-bit) for the particular message type;
- Checksum (16-bit)

Although the signalling messages are varied, it is interesting to consider the most significant, classified according to their function:

- **Error Report**.
  Characteristic ICMP are the following:
  - "*Destination Unreachable*", when a packet is discarded because it was not possible to reach the destination, for any opportunely specified reason.
  - "*Time Exceeded*", when a packet is discarded by a router as its TTL (Time To Live) has reached the maximum depth.
  - "*Parameter Error*", when a packet has a header with some parameter not well interpretable.
- **Reachability test and Performances**.
  ICMP permits, through *"Echo Request"*, *"Echo Reply"* to verify the reachability of a machine or a router and establish the time required to communicate with it, using *"Timestamp Request"* or *"Timestamp Reply"*.
- **Congestion Control.**
  This feature allow, through *"Source Quench"*, to request a reduction of the packet transmission rate.
- **Routing Changing.**
  Through the message *"Redirect"*, a router can inform a machine connected to the local network, to use an alternative router in the same network, to send packets to a specific destination.

- **<u>Network Parameters Request</u>**

Other machines connected to the network, using "Address Mask Request", "Address Mask Reply", could request several parameters, such as the NET_MASK.

Some error messages could be used to set up dynamic configurations. For instance, the determination of the Maximum Transmission Unit (MTU) of a segment.

In fact, generally, is transmitted a MTU, with the indication of not to fragment. In this way, a system error is forced if the MTU was too high, with the transmission of an ICMP with indication about the error cause, but also with an indication of an adequate MTU value.

4.3 IEEE 802.1q (VLAN)

IEEE 802.1q specifies how the MAC Service is supported by Virtual Bridged Local Area Networks, the principles of operation of those networks, and the operation of VLAN-aware Bridges, including management, protocols, and algorithms.

VLANs defines ways to virtually partition a physical network, so that different sub-networks are created. Usually, VLANs are adopted in corporate buildings to divide in branches different compartments of the same firm, to differentiate and isolate traffic, allowing sharing of contents just inside these divisions. Typical issues addressed by VLANs are:

- *Scalability*, over one physical network, sparse hosts can separated from others without placing new cables;
- *Security*, a careful segmentation of the network allows traffic encapsulation so that only hosts belonging to a certain subnet can communicate with each other;
- Improvements in *network management*, in a "divide et impera" fashion, where smaller groups of host can be better manageable.

IEEE802.1Q specifies the modifications to a standard Ethernet frame adding to the end of the standard Ethernet frame header four octets. These are divided as follows:

- *Tag Protocol Identifier*: a 16-bit field set to 0x8100 that identifies the frame as a compliant IEEE802.1Q one;
- *Priority Code Point* (PCP): a 3-bit field that refers to IEEE802.1p. indicates the frame priority level;

- *Drop Eligible* bit: used to indicate if a frame is eligible to be dropped in case of heavy traffic;
- *VLAN Identifier* (VID), a 12-bit field that specifies the VLAN to which the frame belongs.

So, 4094 VLANs are feasible and each can be ranked in 8 different types of priority, whose description can be found in IEEE802.1P. As relevant standards (ISO 11783 for agricultural machines and SAE J1939 for heavy-duty machines) provides with 65535 application streams, hence grouping should be made, but reasonably easy to perform.

5 Industrial Ethernet Fieldbuses and AVB

This chapter deals with relevant fieldbuses and standards, which modifies either IEEE 802.3 or protocols of upper OSI levels.

Paragraph 5.1 lists the selected criteria for evaluate different aspects of the Fieldbuses. In the next paragraphs, these criteria will be examined for each fieldbus selected. Particularly, we will focus on four fieldbuses, AVB (Audio-Video Broadcasting), EtherCAT, POWERLINK and TTEthernet (Time-Triggered Ethernet).

After all, the considerations that emerged will be compared in 5.6.

5.1 Criteria

5.1.1 Technical aspects

- BroadR-Reach Compatibility
- EMC Susceptibility/Transmission Reliability
- Flexible Cabling Topology
  - Tree Topology
  - Star Topology
  - Ring Topology
  - Daisy-Chain Topology
- High Availability
  - Ring Redundancy
  - Master and Cable Redundancy
- Hot Plugging Capability
- Gigabit Readiness
- Products on the Market
- Communication Architecture of the Systems
  - Centralized Control
  - De-centralized Control

5.1.2 Performance

- Direct Cross-Traffic
- Heavy Data Traffic (Prioritization)
- Network Load for Safety Communication
- Capability to support mixed traffic

5.1.3 Implementation Costs

- Master Implementation
- Costs for Potentially Required Network Components
    - External Devices (External Switches or Hubs)
    - Internal Multiport
- Slave Implementation
- Operating Costs
- License Fee
- AUTOSAR support

5.2 AVB

5.2.1 Introduction

Audio Video Bridging (AVB) is a common name for a set of technical standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Audio Video Bridging Task Group of the IEEE 802.1 standards committee. This task group had been renamed to Time-Sensitive Networking Task Group at November 2012 to reflect the expanded scope of work. The charter of this organization is to "provide the specifications that will allow time-synchronized low latency streaming services through IEEE 802 networks".

These consist of:

- IEEE 802.1BA: Audio Video Bridging (AVB) Systems;
- IEEE 802.1AS: Timing and Synchronization for Time-Sensitive Applications (*gPTP* - Generalized Precision Time Protocol);
- IEEE 802.1Qat: Stream Reservation Protocol (SRP);
- IEEE 802.1Qav: Forwarding and Queuing for Time-Sensitive Streams (FQTSS).

IEEE 802.1Qat and 802.1Qav are amendments to the base IEEE 802.1Q document, which specifies the operation of "Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks", which are implemented by network devices typically called Ethernet switches.
Audio and video (AV) equipment connections historically were analog one-way, single-purpose and point-to-point. Even digital AV standards often were point-to-point and one-way such as S/PDIF for audio and the serial digital interface (SDI) for video. This connection model resulted in large confusing masses of cables, especially in professional and high-end consumer applications.

Attempts to get around these problems included new technologies such as IEEE 1394 (known as FireWire), and adaptations of standard computer network technologies such as Audio over Ethernet or Audio over IP.

Specialized professional, home, and automotive protocols did not interoperate. Adapting standard networks could use commodity technology, but tight quality of service control was difficult.

An "Audio Video Bridging" (AVB) network implements a set of protocols being developed by the IEEE 802.1 Audio/Video Bridging Task Group. There are four primary differences between the proposed architecture and existing 802 architectures:

- Precise Synchronization (IEEE 802.1AS),
- Traffic shaping for AV streams (IEEE 802.1Qav),
- Admission Controls (IEEE 802.1Qat),
- Identification of non-participating devices (IEEE 802.1BA).

These are implemented using relatively small extensions to standard layer-2 MACs and bridges. This "minimal change" philosophy allows non-AVB and AVB devices to communicate using standard IEEE 802.3 frames. However, as shown in Figure 7, only AVB devices are able to:

a) reserve a portion of network resources through the use of admission control and traffic shaping
b) send and receive the new timing-based frames.

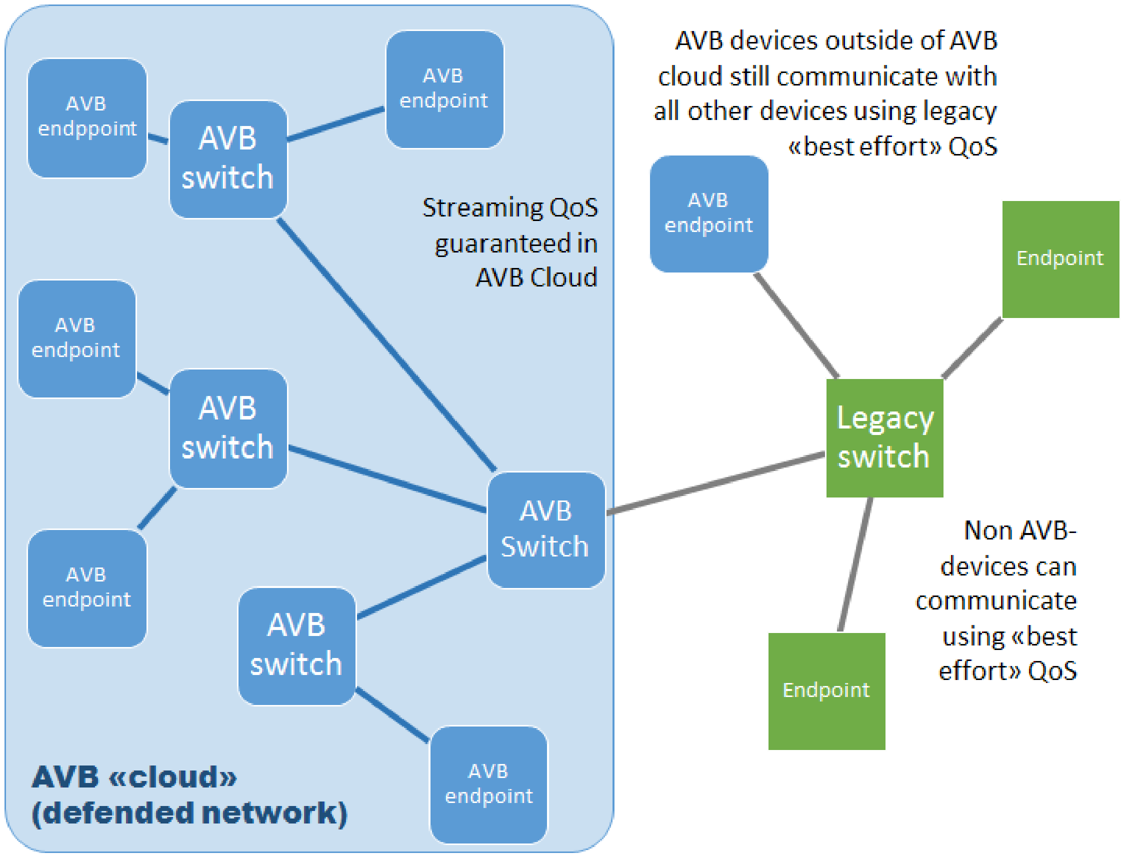

Figure 7: AVB Network Example

Precise Synchronization – 802.1AS gPTP (Generalized Precision Time Protocol)

AVB devices periodically exchange timing information that allows both ends of the link to synchronize their time base reference clock very precisely.

This precise synchronization has two purposes:

- To allow synchronization of multiple streams
- To provide a common time base for sampling/receiving data streams at a source device and presenting those streams at the destination device with the same relative timing.

The protocol used for maintaining timing synchronization is specified in IEEE 802.1AS, which is a very tightly-constrained subset of another IEEE standard, IEEE 1588 PTP (Precision Time Protocol), with extensions to support IEEE 802.11 and also generic "coordinated shared networks" (CSNs).

An 802.1AS network-timing domain is formed when all devices follow the requirements of the 802.1AS standard and communicate with each other using the IEEE 802.1AS protocol. Within the timing domain, there is a single device called the grandmaster that provides a master timing signal. All other devices synchronize their clocks with the *Grand Master* as shown in Figure 8.

The device acting as Grand Master can be either auto selected or specifically assigned. AVB devices typically exchange capability information after physical link establishment. If peer devices on a link are network synchronization capable, they will start to exchange clock synchronization frames. Otherwise, then an AVB timing domain boundary is determined (as shown in Figure 7).

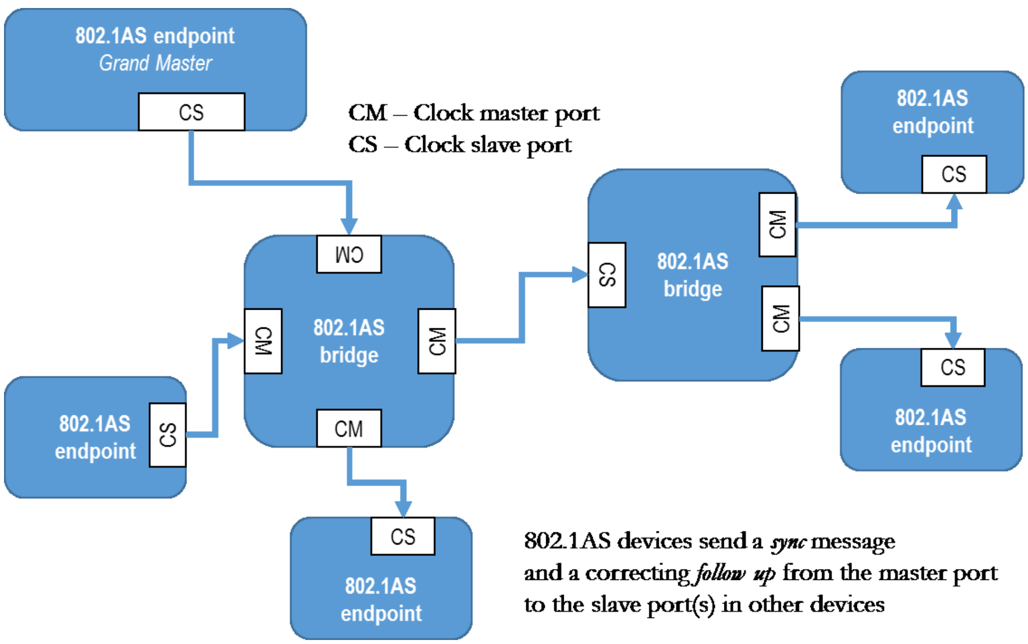

Figure 8: Example of clocking hierarchy

Traffic Shaping for AV Streams – 802.1Qav FQTSS (Forwarding and Queuing of Time-Sensitive Streams)

In order to provide professional AV services, the AVB architecture implements traffic shaping using existing IEEE 802.1Q forwarding and priority mechanisms but also defines a particular relationship between priority tags and frame forwarding behaviour at endpoints and bridges. Traffic shaping is the process of smoothing out the traffic for a stream, distributing its packets evenly in time. If traffic shaping is not done at sources and bridges, then the packets tend to "bunch", i.e. agglomerate, into bursts of traffic that can overwhelm the buffers in subsequent bridges, switches and other infrastructure devices.

AVB streams consist of IEEE 802.3 frames with priority tagging and with normal restrictions on format and length. The default IEEE 802.1Q tagging for a particular market segment should be chosen to avoid potential conflict with existing uses of the IEEE 802.1Q priority tags, within that market segment.

Endpoint devices are required to transmit frames evenly for a particular stream based on the AVB traffic class and on the specific Quality of Service (QoS) parameters that were used when the stream was acknowledged by the network (see Admission Controls below). The specific rules for traffic shaping are described in the IEEE 802.1Qav specification, and are a simple form of what is known as leaky bucket credit-based fair queuing where the bandwidth reserved for a stream controls the time between the packets that make up the stream.

AVB frames are forwarded with precedence over Best Effort traffic (i.e., reserved AVB stream traffic traversing an AVB bridge has forwarding precedence over non-reserved traffic) and will be subjected to traffic shaping rules (they may need to wait for sufficient credits). Just like for stream sources, the traffic shaping rules for bridges require that frames should be distributed evenly in time, but only on an aggregate class basis rather than on a per-stream basis. This means that all the AVB traffic being transmitted out of a particular port is distributed evenly in time measured using the QoS parameters of that class; this is the sum of the bandwidths of all the reservations for a particular AVB class for the particular port, made by the admission control process described below. This is to achieve the effect of smoothing out the delivery times (preventing "bunching" of frames) while a stream propagates through a network. The limited "bunching" provides the very useful benefit of placing a relatively small upper limit on the size of the AVB output buffers needed at all egress ports on a bridge, independent of the number of hops in the path. This bounded buffer size is a key attribute that enables bounded delay and eliminates network congestion for admitted AV streams in AVB networks even when non-admitted traffic does experience congestion.

Admission Control – 802.1Qat SRP (Stream Reservation Protocol)

In the AVB protocols, the term "*talker*" denotes a stream source while "*listener*" denotes a stream destination. In this architecture, it is both the talker's and the listener's responsibility to guarantee the path is available and to reserve the resources. The process to do this is specified by the IEEE 802.1Qat "Stream Reservation Protocol" (SRP), which registers a stream and reserves the resources required through the entire path taken by the stream.

Phase 1. Talkers initiate by sending an SRP "*talker advertise*" message. This message includes a Stream ID composed of the MAC address of the stream source plus a talker-specific 16-bit unique ID and the MAC address of the stream destination. Additionally, the "talker advertise" message includes QoS requirements (e.g., AVB traffic class and data rate information), and accumulated worst-case latency. Even though the talker originates the address and QoS requirements, the worst-case latency is recalculated at every bridge allowing the listener to communicate this information to higher layers for media synchronization purposes.

All AVB intermediate bridges receiving a "talker advertise" message check for bandwidth availability on their output ports. When the bridge has sufficient resources available on that port, the "talker advertise" is propagated to the next station. If those resources are not available, instead of propagating the advertise message, the bridge sends a "*talker failed*" message. Included in this message there is a failure code and bridge identification allowing a higher-layer application to provide error checking or notification. An intermediate bridge receiving a "talker failed" should just pass on the message out towards the listener. When a listener receives a "talker advertise" message, it should know whether the resources are available, and if so, the latency for the path.(Figure 9).

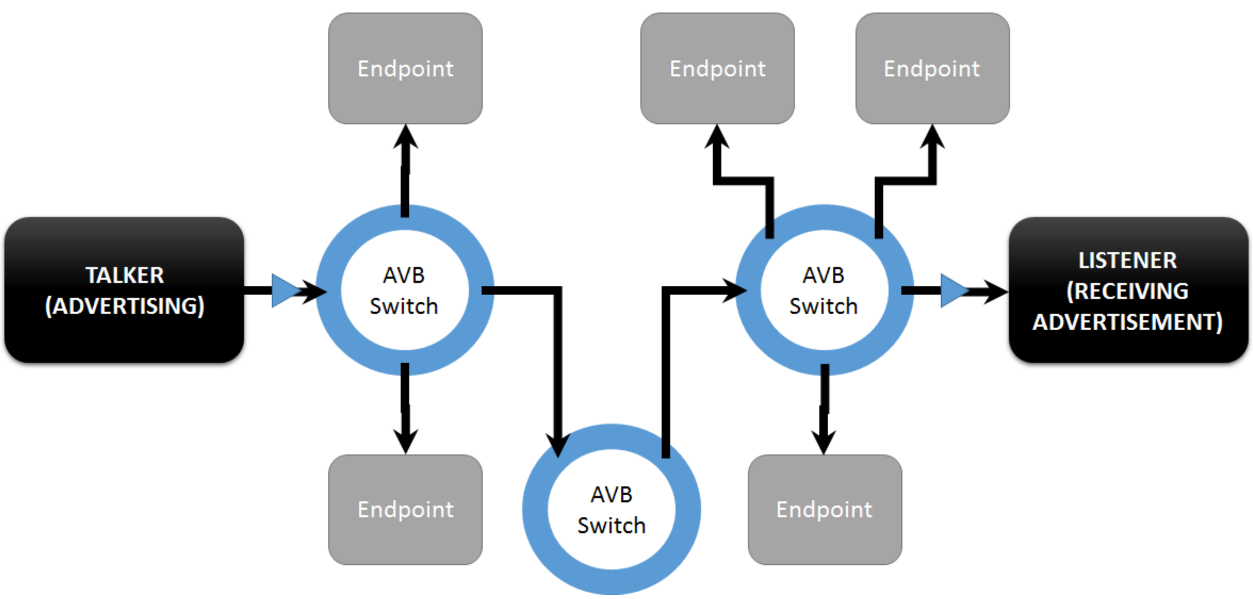

Figure 9: Step 1 for Stream Reservation Protocol

Phase 2. The listener can respond with a "*listener ready*" message that is forwarded back towards the talker. Intermediate bridges use the "ready" message to lock down the resources needed by the stream and to make the appropriate entries in their forwarding database to allow the stream to be sent on the port that received the "ready" message. When the talker receives a "ready" message, it can start transmitting the stream (Figure 10).

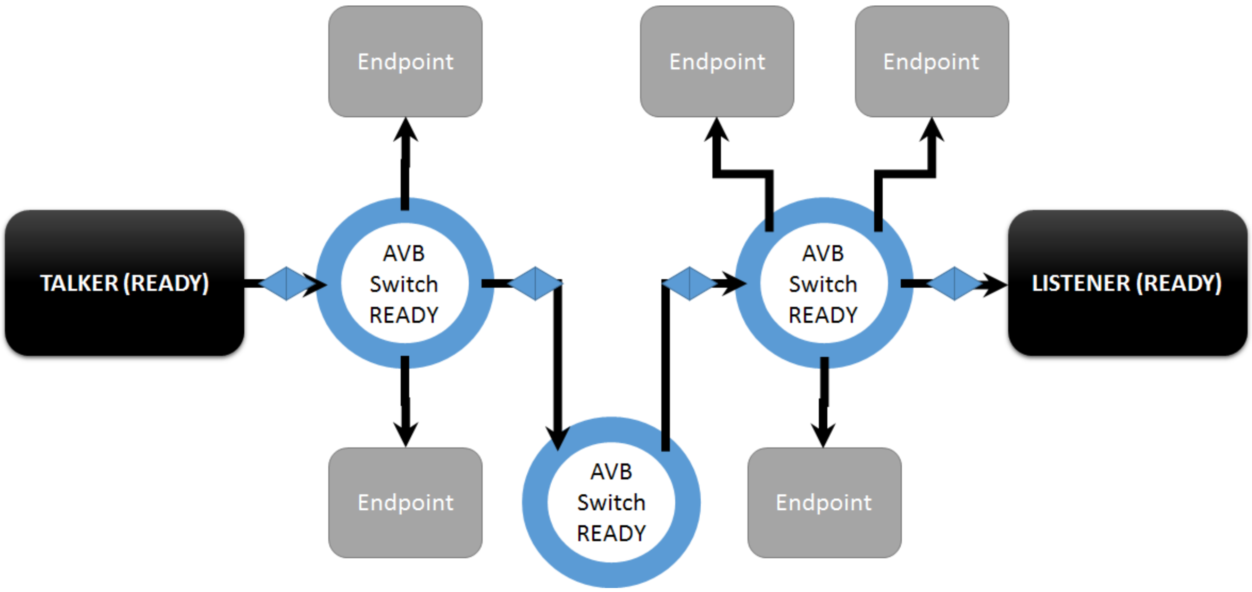

Figure 10: Step 2 for Stream Reservation Protocol

Phase 3. Talker endpoint sends stream and listener endpoint receives it (Figure 11).

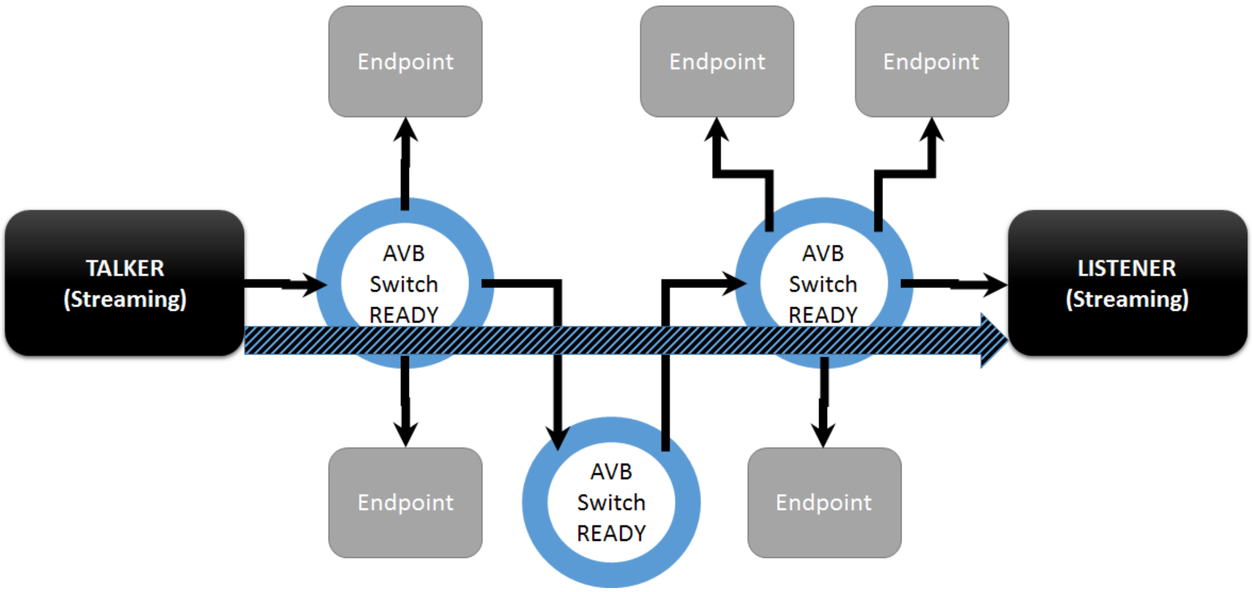

Figure 11: Step 3 for Stream Reservation Protocol

The talker can explicitly tear down a stream by de-registering the "talker advertise", and a listener can disconnect by de-registering the "listener ready". A de-registration message propagates through the network in the same manner as the original registration.

There are also implicit methods used for tearing down a connection and for releasing the allocated resources. For example, the listener must periodically resend registrations and "ready" messages, and talkers must periodically resend "advertise" messages. That way any receiving device (including intermediate bridges) could automatically release assigned resources and notify higher layers if the appropriate registrations and reservations were not received due to a system that, for example, suddenly has lost power.

AVB network are becoming fairly diffuse in automotive environment, especially in high-end cars. [11] provides a comparison with new generation network w.r.t. old ones.

Identification of participating devices – 802.1BA AVB Systems

Since the whole AVB scheme depends on the participation of all devices between the talker and listener, any network element that does not support AVB (including so-called "unmanaged bridges") must be identified and flagged. The developing IEEE 802.1BA "Audio Video Bridging Systems" standard describe this process, which specifies the default configuration for AVB devices in a network. For Ethernet, the method specified by 802.1BA to determine if its peer is AVB capable is a combination of 802.3 link capabilities (determined during Ethernet link establishment) and the link delay measurements done by IEEE 802.1AS. An AVB capable Ethernet port uses AVB if:

1. The link is full duplex with a rate of 100Mbps or 1Gbps;
2. The 802.1AS protocol discovers exactly one peer;
3. The round-trip delay to the responding AVB device is no more than a worst-case wire delay;
4. An SRP reservation request or acknowledge is received on the port

5.2.2 Technical aspects

- **BroadR-Reach Compatibility:**
  Audio Video Bridging is fully-compatible with the BroadR-Reach physical level,

- **EMC Susceptibility/Transmission Reliability:**
  The EMC for AVB is the same of Ethernet standard communication.

- **Flexible Cabling Topology:**

  AVB supports all the possible following depicted network topology. The only limitation is in use of Daisy-Chain topology, where the path delay can grow up and exceed the real time streaming requirements. Generally is implemented a little switch, instead of two separated PHY (ports).

  - Tree Topology (+)
  - Star Topology (+)
  - Ring Topology (+)
  - Daisy-Chain Topology (0)
- **High Availability:**

  AVB presents a high availability, especially for AVB streams, in which constant high-level signalling messages are exchanged between the communication entities.

  - Ring Redundancy (+)
  - Master and Cable Redundancy (+)
- **Hot Plugging Capability:**

  This feature is fully supported by the aid of Stream Reservation Protocol.

- **Gigabit Readiness:**

  AVB can easily supported on Gigabit networks, also thanks to the Stream Reservation Protocol, which can reserve more bandwidth for the communication.

- **Products on the Market:**

  Many products with AVB are present on the market, but principally for Industrial or Consumer applications. Nowadays are popping switches automotive-certified, which supports also BroadR-Reach physical level.

- **Communication Architecture of the Systems**: the network architecture is flat-type, in the sense that there is any "Communication Master". To complete the synchronization, A Grand Master is present, but the control and the communication is de-centralized (i.e. the switches, with SRP). If a Grand Master fails, any other available end-point can be elected as new Grand Master for the synchronization.

  - Centralized Control (-)
  - De-centralized Control (+)

5.2.3 Performance

- **Direct Cross-Traffic:**
  Because AVB constitutes a de-centralized control system, is possible to make direct-cross traffic.

- **Heavy Data Traffic (Prioritization):**
  In AVB, Heavy Data Traffic is well supported, thanks to the Stream Reservation Protocol, which reserves all the necessary resources for the transmission of a stream. This kind of traffic does not take all the network's available resources, because it can take up to the 75% of the available bandwidth. In this way, Best Effort Traffic cannot starve in an AVB switch's buffer. Moreover, thanks to the two different priority classes (AVB class A and AVB class B streams), traffic can be sent from talker to listener station with different priorities, making more simple the stream of real-time information and the appropriate traffic shaping assures both throughput and delivery latency parameters are met for packets of reserved streams.

- **Network Load for Safety Communication:**
  Thanks to Stream Reservation Protocol, all the safety communication can be easily supported and the bandwidth reserved.

- **Capability to support mixed traffic:**
  With AVB, mixed traffic is fully supported, because standard Ethernet communications can be wrapped into a Best Effort messages. However, for support AVB traffic is necessary to use proper switches.

5.2.4 Implementation Costs

- **Master Implementation:** N/A.

- **Costs for Potentially Required Network Components:**
  AVB requires a strong traffic control, over layer 3. This push the use of software stack or hardware solutions (ASICs). In both cases, the cost of the network system grows. Moreover, when the protocol's stack is implemented by software, it is necessary a

powerful microcontroller/microprocessor and this push the developer to oversize the embedded system, selecting a higher-level microcontroller, than the one actually required. However, many devices on the market integrates AVB themselves and therefore, adopting this technology will become cheaper.

- External Devices (External Switches or Hubs):

  An AVB network requires specific switches certified for AVB. The cost for this hardware is higher than other Ethernet solutions.

- Internal Multiports:

  Internal Multiports are cheaper object than external switches.

- **Slave Implementation:** Peer implementation needs the stack layer 1 and 2 to be embedded in the network interfaces. For switches, specific devices are required and have to be designed to support IEEE 1588 and IEEE 802.1AS timing functions.

- **Operating Costs:** There are no operating costs related to AVB use.

- **License Fee:** There is no license fee related to the use of AVB.

- **AUTOSAR support:** AUTOSAR 4.2.1 introduces basic support for AVB and further extensions have been proposed.

5.3 EtherCAT

5.3.1 Introduction

EtherCAT ("Ethernet for Control Automation Technology") was developed by Beckhoff Automation. All users of this technology automatically become members of the EtherCAT Technology Group (ETG).

EtherCAT is based on the summation frame method: the EtherCAT Master transmits an Ethernet frame containing data for all nodes on the network. That frame passes through all nodes in sequence. When it arrives at the last node on a trunk, the frame is turned back again.

The nodes process the information in the frame as it passes through in one direction. Each node reads out data addressed to it on the fly, and inserts response data back into the frame. In order to support the bandwidth of 100 Mbit/s, special hardware based on ASICs or FPGAs is required for fast processing as data passes through. In effect, the topology of an EtherCAT network always constitutes a logical ring.

Even trunks branching out, which can be hooked up to nodes especially designed for such connections, actually only add a two-way junction where the summation frame telegram travels up and back down the branching line.

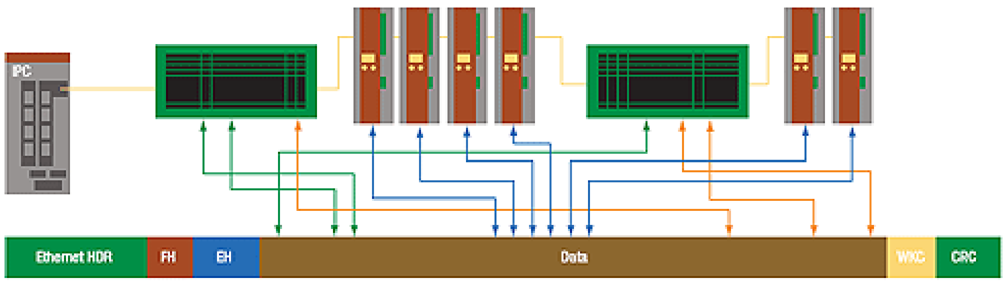

Figure 12: EtherCAT packet example

All EtherCAT telegrams with instructions for individual nodes are contained within the payload data area of a frame, as shown in Figure 12. Each EtherCAT frame consists of one header and several EtherCAT commands. Each of these comprises its own header, instruction data for a slave, and a working counter. Up to 64 Kbytes, configurable address space is available for each slave. Addressing proceeds by auto-increment, i.e. each slave counts up to the 16-bit address field. Slaves can also be addressed via distributed station addresses, which are assigned by the Master in the start-up phase.

Every slave connection provides a real-time clock that is synchronized by the master using a technique similar to IEEE 1588. There are slave devices with and without real-time mechanisms, since these are more demanding on the hardware. Based on the real-time clocks, control signals can be synchronized with high precision. In physical terms, the EtherCAT protocol not only runs on Ethernet, but also on LVDS (Low Voltage Differential Signalling). This standard is used by Beckhoff as an internal bus on the terminals. A PC with a standard Ethernet interface is typically used to implement an EtherCAT master. [12, 13, 14] give some examples of applications in safety-relevant environment

5.3.2 Technical aspects

- **BroadR-Reach Compatibility:** An implementation of EtherCAT Fieldbus over BroadR-Reach is possible only after a complete re-design of the ASIC (or FPGA implementation) due to the different Physical layer.Another possibility is to make a retrofit, with a protocol translation, inserting a BroadR-Reach to Ethernet adaptor on each port of the device.

- **EMC Susceptibility/Transmission Reliability**: Due to summation frame protocol, Ethercat is more susceptible to interference than a single frame protocols. If a frame is destroyed, summation frame protocols always lose an entire cycle.

- **Flexible Cabling Topology:** EtherCAT networks always constitute a logical ring. That ring can be physically closed at the master, or, in the case of a daisy chain, closed internally at the last node in the physical line. EtherCAT does provide for trunks to branch out via special junctions, but the entire frame travels up and back down such lateral network lines, i.e. the network as a whole still represents a logical ring.
  - Tree Topology (-)
  - Star Topology (-)
  - Ring Topology (+)
  - Daisy-Chain Topology (+)

- **High Availability:**
  EtherCAT has a self-redundancy given by the logical ring, where the information passes twice through the same node. No type of Master and cable redundancy is implemented.
  - Ring Redundancy (+)
  - Master and Cable Redundancy (0)

- **Hot Plugging Capability:**
  EtherCAT has some restrictions due to the compulsory ring topology and provides some hot plugging capability. In the EtherCAT Slave Controller, open ports are automatically closed if no link is detected. EtherCAT's distributed clocks, however, requires re-synchronization, which may affect certain applications.

- **Gigabit Readiness:** EtherCAT can be scaled to Gigabit, but requires an ASIC redesign. If it is implemented by an FPGA solution, it can be ported to Gigabit.

- **Products on the Market:** Many EtherCAT products can be found on market.

- **Communication Architecture of the Systems:** Due to the presence of a Master into the communication architecture, is also possible a centralized control.
    - Centralized Control (+)
    - De-centralized Control (-)

5.3.3 Performance

- **Direct Cross-Traffic:** Due to logical ring network topology, direct cross-traffic is not allowed.

- **Heavy Data Traffic (Prioritization):** In applications involving a large volume of process data, the time required for passing through the nodes greatly impacts the overall cycle time.
  For EtherCAT, solutions for this requirement can be implemented as part of a specific application.

- **Network Load for Safety Communication:** Safety over Ethernet is based on a cyclic exchange of protected data between safety nodes (emergency stop switches, drives with Safety controllers). The safeguard procedures in this process involve data duplication and wrapping data in safe "containers". This increases data rates on the network. Solutions using the summation frame method will see the frame count go up, whereas the single frame method will increase the volume of data in each of the frames that are due to be sent anyway. Overall, the theoretically superior performance of the summation frame method is neutralized.

- **Capability to support mixed traffic:**
  In the case of insertion of an Ethernet device, it could be cause a collision into the packet. Supposing the insertion of Ethernet device between Master and the first daisy-chain Slave, if the Ethernet device sends a message to the Master, if it does not collide any other message on the network, it will be probably ignored by level 3 of the Master's ISO/OSI stack.

  If the message is sent to a generic Slave in the daisy chain, if it can reach the destination Slave, it will be ignored.

5.3.4 Implementation Costs

- **Master Implementation:**
  EtherCAT master runs on standard hardware, so any Ethernet MAC are suitable. The software stack for enabling EtherCAT communications are provided by several manufacturers and for different operating systems. Master access is patent-protected and no open source master is suitable, but only sample code that does not warrant applicability.

- **Costs for Potentially Required Network Components:**
  EtherCAT requires specific network components, especially for star or tree topologies. Therefore, specific switches are needed and internal multiport is implemented by the use of specific ASIC developed by Beckhoff.
  - External Devices (External Switches or Hubs) (-)
  - Internal Multiports (-)

- **Slave Implementation:**
  EtherCAT slaves require custom hardware such as ASIC or FPGA controllers. The costs for slave hardware are based on the controller capabilities and device manufacturer. Usually the costs are comparable to any other fieldbus controller.

For EtherCAT, microcontroller-based software solutions are also feasible.

- **Operating Costs:**
  There are no operating costs related to EtherCAT use.

- **License Fee:**
  There is no license fee related to the use of EtherCAT, it is embodied into hardware/software costs.

- **AUTOSAR support:**
  N/A

5.4 Powerlink

5.4.1 Introduction

Initially developed by B&R, POWERLINK was introduced in 2001. The Ethernet POWERLINK Standardization Group (EPSG), an independent user organization with a democratic charter, has taken charge of the further development of the technology since 2003. POWERLINK is a completely patent-free, vendor-independent and purely software-based communication system that delivers hard real-time performance. An open source version has also been made available free of charge in 2008.

POWERLINK fully complies with the IEEE 802.3 Ethernet standard, i.e. the protocol provides all standard Ethernet features including cross-traffic and hot plugging capability, and allows for deploying any network topology of choice. It uses a mixture of timeslot and polling procedures to achieve isochronous data transfer. In order to ensure co-ordination, a PLC or an Industrial PC is designated to be the *Managing Node* (MN). This manager enforces the cycle timing that serves to synchronize all devices and controls cyclical data communication.

All other devices operate as *Controlled Nodes* (CN). During a cycle, the MN sends so-called "*Poll Requests*" (PReq) to one CN after another in a fixed sequence. Every CN replies immediately to this request with a "*Poll Response*" (PRes) on which all other nodes can listen in.

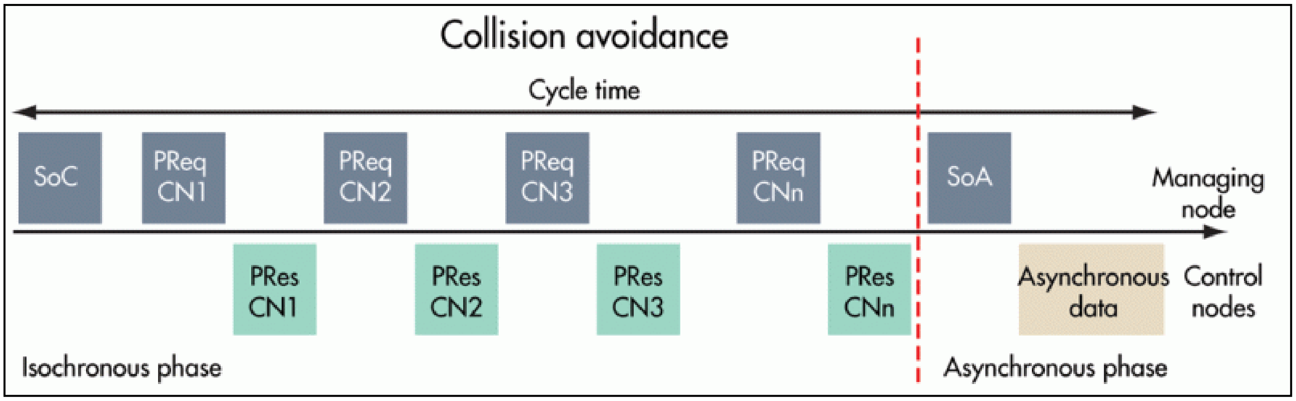

Figure 13: Different phases in a POWERLINK communication cycle

A POWERLINK cycle consists of three periods, as depicted in Figure 13. The first is the "Start Period", where the MN sends a "Start of Cycle" (SoC) frame to all CNs to synchronize the devices. Jitter amounts to about 20 nanoseconds.

Cyclic isochronous data exchange takes place during the second period ("Cyclic Period"). Multiplexing allows for optimized bandwidth use in this phase. The third period marks the start of the asynchronous phase, which enables the transfer of large, non-time-critical data packets. Such data, e.g. user data or TCP/IP frames, is scattered between the asynchronous phases of several cycles. In this last phase, the Managing Node grants the right to one particular node for sending ad-hoc data, by sending out the *Start of Asynchronous* (SoA) frame. Modifications [15] have been proposed to Powerlink in order to increase ASYNC service functionalities.

The addressed node will answer with ASnd frame. Standard IP-based protocols and addressing can be used during this phase.

POWERLINK distinguishes between real-time and non-real-time domains. Since data transfer in the asynchronous period supports standard IP frames, routers separate data safely and transparently from the real-time domains.

The quality of the Real-Time behaviour depends on the precision of the overall basic cycle time. The length of individual phases can vary as long as the total of all phases remain within the basic cycle time boundaries. The MN and the duration of the isochronous monitor adherence to the basic cycle time and the asynchronous phase can be configured.

5.4.2 Technical aspects

- **BroadR-Reach Compatibility:** POWERLINK appears to be fully-compatible with BroadR-Reach networks. An academic proof of concept on POWERLINK over BroadR-Reach is already present in the literature [15].

- **EMC Susceptibility/Transmission Reliability:** POWERLINK uses a series of Broadcast or Unicast messages during the various phases. For do this, a standard Ethernet packetized communication is used. This allow a reliable communication and the EMC Susceptibility is the same of Ethernet.

- **Flexible Cabling Topology:** The POWERLINK network's topology architecture can be the same of Ethernet, with the use of the same PHY.
    - Tree Topology (+)
    - Star Topology (+)
    - Ring Topology (+)
    - Daisy-Chain Topology (+)

- **High Availability:** POWERLINK has master and cable redundancy included in the specifications, and been implemented in actual projects.
    - Ring Redundancy (+)
    - Master and Cable Redundancy (+)

- **Hot Plugging Capability:** Based on standard Ethernet protocol, POWERLINK fully supports hot plugging.

- **Gigabit Readiness:** The original physical layer specified was 100BASE-TX Fast Ethernet. Since the end of 2006, Ethernet POWERLINK with Gigabit Ethernet supported a transmission rate ten times higher (1,000 Mbit/s). As POWERLINK is entirely software-based technologies, this protocol can also be used with Gigabit Hardware.

Repeating hubs instead of switches within the Real-time domain is recommended to minimize delay and jitter.

- **Products on the Market:** POWERLINK is a specific software implementation based on Ethernet. It can be implemented in every market.

- **Communication Architecture of the Systems:** POWERLINK supports both centralized and de-centralized controls.

    - Centralized Control (+)
    - De-centralized Control (+)

5.4.3 Performance

- **Direct Cross-Traffic:** With POWERLINK, direct cross-traffic is a feature even for modules that only have slave functionality.

- **Heavy Data Traffic (Prioritization):** In applications involving a large volume of process data, the time required for passing through the nodes greatly impacts the overall cycle time. Data prioritization, on the other hand, enables lower cycle times. Systems that support prioritization mechanisms allow for reading high-priority data once every cycle and polling for data with a lower priority only every n-th cycle.
For POWERLINK, a variable cycle times has been firmly established in the protocols specifications.

- **Network Load for Safety Communication:** Safety over Ethernet is based on a cyclic exchange of protected data between safety nodes (emergency stop switches, drives with

Safety controllers). The safeguard procedures in this process involve data duplication and wrapping data in safe "containers". This increases data rates on the network. By the use of an Isochronous and Asynchronous Phases every cycle, it is guaranteed the Safety of Communications, especially in the real-time phase.

- **Capability to support mixed traffic:** Due to fully-compatibility with Ethernet Standard communication, POWERLINK supports mixed traffic. The insertion of a non-POWERLINK device into the network should not create collision on the traffic during the communication.

5.4.4 Implementation Costs

- **Master Implementation:** The openPOWERLINK software stack is open-source, so there is no additional costs related to its use. The hardware used for master controller nodes could be COTS device for standard Ethernet.

- **Costs for Potentially Required Network Components:** In order to achieve maximum performances, only switched topology should be used, but hubs are supported. These devices could be standard Ethernet hubs/switches. For internal multiports, standard Ethernet multiport could be used.
  - External Devices (External Switches or Hubs) (+)
  - Internal Multiports (+)

- **Slave Implementation:** As for master implementation no specific one is defined.

- **Operating Costs:** POWERLINK has associated very low costs. Some features supported, such as hot-plugging capability or master-managed synchronization mechanism (that is very precise and very rarely disturbed by faults) permit to achieve very high performance with low design effort.

- **License Fee:** POWERLINK is a completely patent-free, vendor independent and purely software-based communication system, developed by EPSG (Ethernet POWERLINK Standardization Group). Membership fees are required for POWERLINK, but the user organization allow non-members to develop products and put them on the market.

- **AUTOSAR support:** N/A

5.5 TTEthernet

5.5.1 Introduction

TTEthernet (SAE AS6802) is a computer network technology marketed by TTTech Computertechnik AG "for safety-related applications primarily in transportation industries and industrial automation."

TTEthernet expands classical Ethernet with services to meet time-critical, deterministic or safety-relevant conditions [16]. It claims to be compatible with IEEE 802.3 standards and integrate with other Ethernet networks.

Three message types are provided:

- Time-Triggered (TT) messages are sent over the network at predefined times and take precedence over all other message types. The occurrence, temporal delay and precision of time-triggered messages are predefined and guaranteed. The messages have as little delay on the network as possible and their temporal precision is as accurate as necessary. However, "synchronized local clocks are the fundamental prerequisite for time-triggered communication". TT messages are optimally suited for communication in distributed real-time systems. TT messages are typically used for brake-by-wire and steer-by-wire systems that close rapid control loops over the network. TT messages allow designing and testing strictly deterministic distributed systems, where the behaviour of all system components can be specified, analysed and tested with sub-micro second precision.

- Rate-Constrained (RC) messages are used for applications with less stringent determinism and real-time requirements. These messages guarantee that bandwidth is predefined for each application and delays and temporal deviations have defined limits. RC messages are used for safety-critical automotive and aerospace applications that depend on highly reliable communication and have moderate temporal quality requirements. Typically, RC messages are also used for multimedia systems.

- Best-Effort (BE) messages follow the usual Ethernet policy. There is no guarantee whether and when these messages can be transmitted, what delays occur and if messages arrive at the recipient. BE messages use the remaining bandwidth of the network and have lower priority than the other two types.

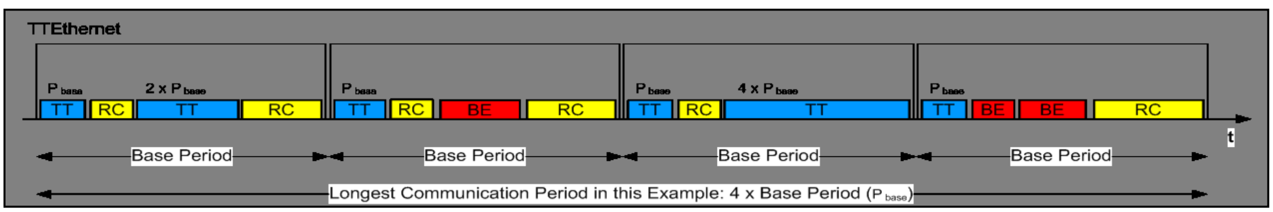

Figure 14: Example of different kind of messages transmission

TTEthernet is a transparent synchronization protocol, i.e., it is able to co-exist with other traffic, potentially legacy traffic, on the same physical communication network (Figure 14). For reasons of fault tolerance, a multitude of devices can be configured to generate synchronization messages. The devices generating the synchronization messages may be distributed with a high number of intermediate devices in between each other.

TTEthernet defines basic building blocks that allow the transparent integration of the time-triggered services on top of message-based communication infrastructures such as standard Ethernet. For this, TTEthernet defines a novel application of the transparent clock mechanism that enables the concept of the permanence point in time, which allows re-establishing the send order of messages in a receiver:

1. Application of transparent clock mechanism: all devices in the distributed computer network that impose a dynamic delay on the transmission, reception, or relay of a synchronization message add this dynamic delay into a dedicated field in the synchronization messages used for the synchronization protocol.

2. Novel precise calculation of the permanence point in time: the application of transparent clock mechanism allows a precise re-establishment of the temporal order of synchronization messages. In a first step, the worst-case delay is calculated off-line. In a second step, each synchronization message is delayed for "worst-case delay minus dynamic delay" upon reception of the synchronization message, where the dynamic delay is the delay added to the synchronization message, as the synchronization message flows through the communication channel. This point after the reception point in time will be called the permanence point in time.

For fault-tolerant algorithms in general, and fault-tolerant synchronization algorithms in particular, the message send order is of highest importance. The re-establishment of the send order of synchronization messages is required for any fault-masking synchronization protocol that ensures synchronization of local clocks in a distributed computer network.

A high level of safety is provided by the time-triggered method of TTEthernet, which detects failures and irregularities in the network and certain systems. Additional measures need to be taken to achieve maximum safety, availability and fault tolerance.

TTEthernet networks can be set up with multiple redundant end systems, switches and segments. Thus, the system will remain in operation even if faults occur. Redundant network paths are always used in fault-tolerant TTEthernet systems so that the failure of a single system or messages can be tolerated without affecting the application. If multiple redundancy is implemented, multiple faults can be tolerated. It is important that the entire system remains in operation without interruptions under the same temporal conditions as defined before.

TTEthernet allows the integration of guardians in switches and end systems. Guardians check if the communication on the network works in compliance with the predefined parameters. If faulty systems block network segments, the guardian disconnects the network segment or port. Multiple redundant guardians can be implemented to meet the highest safety requirements.

5.5.2 Technical aspects

- **BroadR-Reach Compatibility:** TTEthernet appears to be fully compatible with BroadR-Reach networks.

- **EMC Susceptibility/Transmission Reliability:** TTEthernet uses a standard Ethernet packetized communication. This allows a reliable communication and good EMC susceptibility. TTEthernet tolerates arbitrary transient disturbances even in presence of permanent failures: In addition to fault tolerance, TTEthernet also provides self-stabilization properties, i.e., the synchronization will be re-established even after transient upsets in a multitude of devices in the distributed computer system. TTEthernet stabilizes from an arbitrary system state to a synchronized system state.

- **Flexible Cabling Topology:** The scalable network topology offers the opportunity to select star, line or tree as the topology that best fits user requirements.
  - Tree Topology (+)
  - Star Topology (+)
  - Ring Topology (+)
  - Daisy-Chain Topology (+)

- **High Availability:** TTEthernet delivers scalable fault tolerance by allowing single-, dual-, and triple-redundancy for different levels of system integrity and criticality.
  - Ring Redundancy (+)
  - Master and Cable Redundancy (+)

- **Hot Plugging Capability:** N/A

- **Gigabit Readiness:** The TTEthernet product family supports bandwidths of 100 Mbps, 1 Gbps, and higher, which guarantees that one technology is capable to support different speeds.

- **Products on the Market:** A large number of products in the market use TTEthernet fieldbus. TTEthernet is a technology that is rapidly growing and an increasing number of Companies and Vendors are adopting it.

- **Communication Architecture of the Systems:** TTEthernet is designed to scale over a multitude of cross-industry applications. As such, TTEthernet comprises demanding fault-tolerant capabilities.TTEthernet is scalable and it can be configured to operate as a simple master-slave synchronization protocol (i.e. for industrial control) or a multi-master synchronization protocol (i.e. for civil avionics).
    - Centralized Control
    - De-centralized Control

5.5.3 Performance

- **Direct Cross-Traffic:** As TTEthernet is a distributed-control fieldbus, it is capable to support direct-cross traffic.

- **Heavy Data Traffic (Prioritization):** With the distinction of three different class of traffic, allow to ensure different prioritization of the information on the network.

- **Network Load for Safety Communication:** TTEthernet products support inherently deterministic communication and have been designed for safe and highly available real-time applications from the ground up. With the separation between different types of messages, secure critical operations in the network are possible, where less-critical traffic cannot affect highly critical functions.

- **Capability to support mixed traffic:** TTEthernet products enable convergence of hard real-time communication and standard Ethernet traffic in parallel on the same network.

5.5.4 Implementation Costs

- **Master Implementation:**N/A

- **Costs for Potentially Required Network Components:**
  - External Devices (External Switches or Hubs)
  - Internal Multiports
- **Slave Implementation:** N/A

- **Operating Costs:** N/A

- **License Fee:** N/A

- **AUTOSAR support:** TTEthernet is widely supported in AUTOSAR. The modules provided by TTTech are certified and certifiable up to ASIL-D

5.6 Comparison

		AVB	EtherCAT	POWERLINK	TTEthernet
	TECHNICAL ASPECTS				
	BroadR-Reach compatibility	+	-	+	+
	EMC Susceptibility / Transmission Reliability	+	0	+	+
Topology	Tree Topology	+	-	+	+
	Star Topology	+	-	+	+
	Ring Topology	+	+	+	+
	Daisy-Chain Topology	0	+	+	+
High Availability	Ring Redundancy	+	+	+	+
	Master and Cable Redundancy	+	0	+	+
	Hot-Plugging Capability	+	0	+	
	Gigabit Readiness	+	+	-	+
	Products on the Market	+	+	+	0

Comm. Architecture of the System	Centralized Control	-	+	+	
	De-Centralized Control	+	-	+	
	PERFORMANCE:				
	Direct Cross-Traffic	+	-	+	+
	Heavy Data Traffic (Prioritization)	++	0	+	++
	Network Load for Safety Communications	+	0	+	+
	Capability to Support Mixed-Traffic	+	-	+	+
	IMPLEMENTATION COSTS				
	Master Implementation	N/A	0	+	
Cost for Potentially Required Network Components	External Devices (External Switches or Hubs)	0	0	+	
	Internal Multiports	+	+	+	
	Slave Implementation	+	-	+	
	Operating Costs	+	+	+	
	License Fee	+	0	0	
	AUTOSAR Support	+	0	N/A	+ (ASIL-D)

6 Research Methodology

The inputs for this research came from various sources, at different times. Mainly, the seminal work that indicated the way for the adoption of Ethernet in agricultural machinery was [17] and the works made with John Deere Germany, to create a Real Time Ethernet Communication network, over a tractor with implement. In particular, that work focused on develop and demonstrate a high speed real-time communication network for machinery automation, proposing an improved physical communication layer for ISOBUS, adopting an industrial Ethernet fieldbus, particularly EtherCAT.

Another input came from BMW and the creation with Broadcom of a venture to create a PHY compliant with automotive requirements [18]. Whereas 100base-TX was proven not to be compliant with EMC and EMI constraints, as also described in 3.3.2, BroadR-Reach is been designed as a compound of technologies inherited from other PHYs (such as 100base-TX and 1000base-T).

Also in avionic industrial compartment, Ethernet is a reality. Airbus patented a data network, called Avionics Full-Duplex Switched Ethernet (AFDX) as a specific implementation of ARINC 664 pt. 7, for safety-critical applications that utilizes dedicated bandwidth while providing deterministic quality of service using UDP. AFDX supports COTS components and defines how they will be used for future generation aircraft data network.

The last input, in time, came from the AEF PT10 working group, with the large interest put on the Broadr-Reach technology.

These inputs created two different paths eligible to be investigated:

1. A standard IEEE 802.3 network, with standard components that access a switched network with a given priority, whose means had to be investigated and defined;
2. An IEEE 802.3-based network, adopting an industrial fieldbus and its features, optionally modifying some of them, changing the channel access method.

For the first path, the prioritization is intended as the determinism that a specific kind of traffic (to which pertains one specific functionality or application) can be offered. In ISOBUS networks, each Parameter Group Number (PGN) is notified to the network periodically (transmission repetition rate) and has a precise priority. Whereas in CAN bus networks the priority directly influences the access of a CAN message to the network (as the priority field is part of the ID field of the CAN message and CAN is CSMA/BA), the same is not true in Ethernet frames, in terms of both channel access and specific frame field. Therefore, the research focused on trying to create ways to supply this prioritization in standard ways, adopting industry-ready protocols and algorithms.

In addition, the topology of the network seemed to be a hierarchy of switches in order to avoid packet collisions, and take advantage of the features that switches could supply (VLAN tagging, programmability, etc.), in order to administrate the network in detail. However, the increasing complexity of the network infrastructures means higher costs and safety concerns in terms of failure (thus, certification) of active and intelligent components.

The creation of a prioritization system over Ethernet can be achieved in a standard way (i.e. taking advantage of well-proven technologies) either at layer 2 or at layer 3, in the ISO OSI stack. In this setting, a statistical analysis was necessary, to assess the network response, even under heavy traffic burden; however, before evaluating statistical figures of tests, it was necessary to create a test bed upon which have meaningful statistical measurements. Although IEEE1588 and *gPTP* now are supported by Linux, with *ptpd*, at the early beginnings of the tests, the support was not that extended and accurate, particularly with the COTS NICs that were used (Realtek RTL 8139), that did not support IEEE 1588 in hardware.

The chosen way, also in alignment with the ISOBUS requirements and dynamics, was to assess the inter-arrival time and the jitter of the incoming packets, when sending regularly cadenced messages of fixed length. The average of the inter-arrival time is expected to be the same as the cadence of the data stream, unless a considerable amount of packets is lost in the network, while the variance is a figure of the dispersion of the inter-arrival time, so the jitter.

This way of measurement seemed right also for the kind of the network under test, one which any node send messages without any certainty of delivery, unless provided by an upper layer protocol.

For the second path, the prioritization, as later detailed, is no longer necessary. Modifying, similarly as [19], the channel access method from CSMA/CD to TDMA, the time and the way one message enters the network is determined strictly and deterministically by the network itself. The challenge in this path was primarily to find, among the most adopted fieldbuses, the one that could fit in the requirements of agricultural machines environments; some of the main characteristics of the ISOBUS network are:

- *Multi Master* (there is more than one master ECU that could gain the control of the network, at any time);
- *Hotplug* (should a tractor be attached/detached to an implement at any time, the network will recognize the new status and act accordingly, without the need of a key-off procedure)
- *Multi-vendor* (machinery by different manufacturers will be able to communicate with each other).

This task needed a careful evaluation of the most adopted fieldbus, whose outcome is reported in 5. The assessment was done taking into account the feasibility of each fieldbus in the considered scenario, as well as the research' applicability. In this context, Powerlink was chosen.

With the modification of the channel access method, Powerlink itself assures the certainty of delivery (or the notification of loss), hence the research focused on the analysis of the features of that fieldbus, and the modifications needed to assure good applicability.

7 Prioritization

Switches are ISO OSI L2 devices technically implementing an array of interconnected bridges. As these devices have the cognition of packet, they are able to forward Ethernet frames in the correct direction and not just mirroring the content received from one port to the others. The first advantage coming from using switches is that, if only one network node is connected to each port of the switch no collisions can occur, as the switch is in charge of queuing every frame traversing the switch itself. This queuing is done automatically and without any agreement between any nodes of the network, so the importance of these devices grows even more, in terms of dependability and performance.

Thus the resulting topology includes a number of hosts with standard Ethernet MACs (PHYs may be different from standard, in order to counteract environmental needs, without affect in any way the upper layers), interconnected by one or more switches, which, as explained later, influence the traffic by prioritizing some data streams from others.

From the point of view of this work, we shall consider a fairly small network, as small as an in-vehicle one can be, that may bear few but considerable changes in its topology, meaning that some instrumentation has been mounted or towed and also needs digital communications (other than hydraulic and/or mechanical). On this modular vehicle, some Electronic Control Units (ECUs) will implement some functionalities or services, and may need to share or demand data from other ECUs. The criticality of data itself, the temporal constraints of the communication and the safety related to the dynamics associated to it are elements that result in a certain level of priority of the data itself. Thus, prioritizing these streams of data means to provide certain levels of determinism and guarantee throughput without packet losses.

In this chapter we shall introduce two ways of prioritization that take advantage of standard features of Ethernet frame and the Internet protocol Suite [20,21], hereafter referred as TCP/IP stack, then it will compared and different field of application will be pointed out.

7.1.1 Test system setup

The test environment needed several delicate settings to be operative, though topology never varied, as shown on Figure 15. Five Linux hosts (PC-based machines with 3GHz CPU and 512MB RAM, featuring a RT-PREEMPT-patched Linux Kernel) have been connected with CAT5 UTP cables to a switch controller (Vitesse VSC7385), on board of a Freescale MPC8313erdbV2.1 (hereafter referred as Switch), featuring a SoC with a PowerPC e300 core and two Gigabit-capable eTSECs (Freescale's enhanced Triple Speed Ethernet Controller).

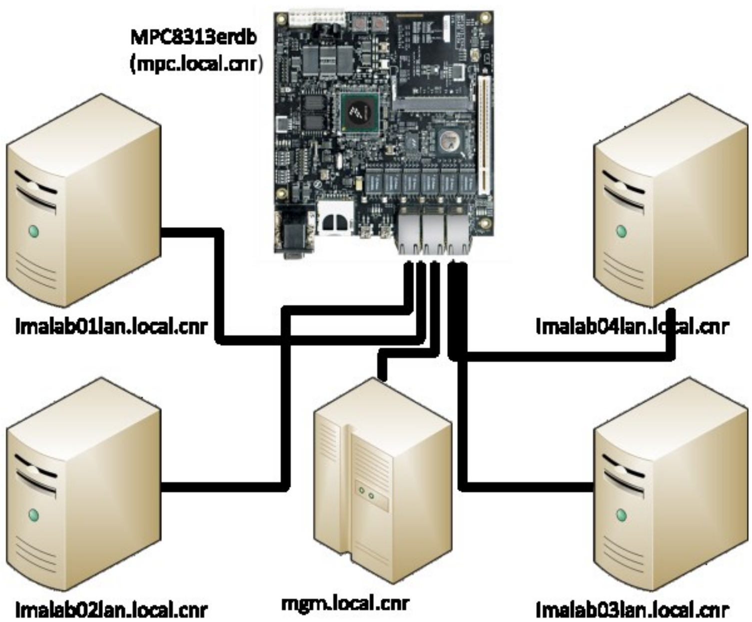

Figure 15: Test topology

One of the five hosts is configured as a server of many services (DHCP, naming, test results collecting, etc.) and the Switch has been equipped with a tailored Linux Kernel (with RT-PREEMPT patch, as well) and flash file system.

Test using both kind of discussed prioritization have been performed. Every test featured a host that functions as a server to coordinate the other hosts, two hosts creating streams of prioritized data and the two hosts used when non-prioritized data was sent, in order to demonstrate the different prioritization. To simulate the non-prioritized traffic an unregimented SCP transfer had been put in place. Every test will feature three prioritized data streams of 10000 packets, sent at various, cadenced intervals; these streams will concurrently access and travel the network; the payload of the data streams will be 50, 500 or 800 bytes.

As the receiver will send no feedback, no "ping-like" calculation will be available, rather than this, both the inter-arrival and inter-sending times will be taken, in order to test the rate, the percentage of successfully received packets and its statistical properties. In order to have a graphical and fast way to test results *octave* and *gnuplot* have been used to have plots of these times. For any graph (Figure 16, Figure 17, Figure 20, Figure 21, Figure 23, Figure 24) the y-axis will display the inter-arrival (inter-departure) time in milliseconds between i^{th} and $i\text{-}1^{th}$ packet, while the x-axis will represent the i^{th} packet.

Before starting with prioritization tests, some ICMP ping tests have been tried in order to have a first glance of the performance degrade: two hosts pinged each other both having Switch as gateway and direct (simply through switch controller without L3 forwarding), statistics are shown in Table 2. No other kind of traffic were present in this test. Results will be coherent with tests made with L2 and L3 prioritization:

1. the round trip time (RTT) is roughly double compared to 100%-arrived minimum time (an ICMP ping message contained 64 bytes, whereas tests contained 50 and 500 bytes);
2. The Time-To-Live (TTL) in L3 tests is the same as L2 tests minus one, as for [21].

As [22] states, ICMP ping is a reasonably good way to measure delay and throughput of a network.

Routing	Packets	Packet loss %	TTL	Average [ms]	Mdev [ms]
2L	10000	0	64	0.104	0.006
3L	10000	0	63	0.515	0.042

Table 2 Reference ping tests with different switch configurations

7.2 L2 prioritization: VLANs and IEEE802.1p

For VLAN to be configured, enabled and made available, switches must be capable of managing and direct VLAN frames accordingly.

PCP	Priority	Traffic Types
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, < 100 ms latency and jitter
5	5	Voice, < 10 ms latency and jitter
6	6	Internetwork Control
7	7 (highest)	Network Control

Table 3: IEEE 802.1p Priority recommendations

Normally, for VLAN configuration, the network administrator will set every single port of the switch in order to declare at which subnet the connected host will be into; for this document, the VLAN concept will adhere mostly on functionalities each host would implement, eventually communicate in more than one VLAN at the same time. Sometimes the physical topology would be unpredictable. Thus, rather than configuring each port of the switch (*static* mode), every switch's port should be configured in *trunk* mode, so it can send and receive tagged frames on all VLANs, but not untagged traffic, for security purposes.

7.2.1 L2 prioritization configuration

In order to set up the test environment for VLAN tests, the Switch has been put in trunk mode, so only "tagged" Ethernet frames could traverse the switches, thus the whole network; so two VLANs have been created:

1. The most prioritized one, with VID = 7 and PCP = 7 (maximum priority);

2. The non-prioritized one, with VID = 2 and PCP = 0 (minimum priority).

To identify the membership of a frame in a VLAN, a L3 VLAN has been used, that is unrelated to layer 3 routing; instead, the network IP subnet is used to classify the VLAN membership. In this way any host willing to communicate in more than one VLAN simply create an IP alias and marks the Ethernet frame accordingly.

In Linux, provided that the Kernel has relative features (embedded in the Kernel or loading the "8021q" module), *vconfig* command is a toolbox to fully configure the host to communicate in various VLANs at various VIDs and PCPs. Priority is handled by this infrastructure both on egress and ingress, providing a finely granulated control even over kernel socket buffers. For the research purposes, *vconfig* configures any socket buffer in order to have IEEE 802.1q tag and relative QoS handling (using the VID settings above).

Reference [23] made a fine comparison between 802.1Q and promising 802.1AVB, which provides a classless, credit-based prioritization.

7.2.2 L2 prioritization tests and results

As Table 4 shows, we achieved outstanding performance, even in busy channel. In order to assure no packet loss a minimum of 80μs-cadenced flows (with a payload of 500B) are used and the results are impressive looking at Figure 18, showing that distribution of packets hardly changes whether there is other traffic or not.

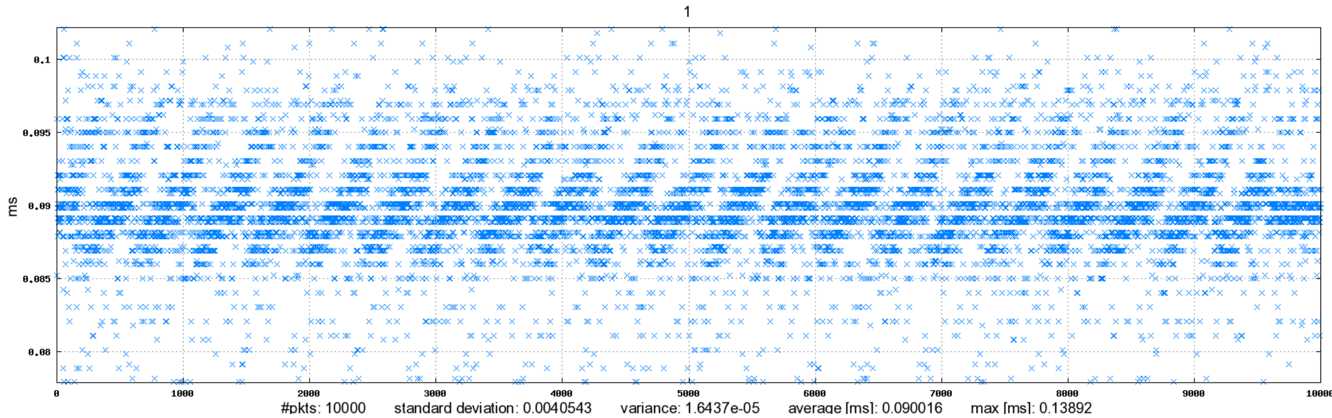

Figure 16: VLAN inter-arrival time plot: 500 bytes @ 90us w/out network load

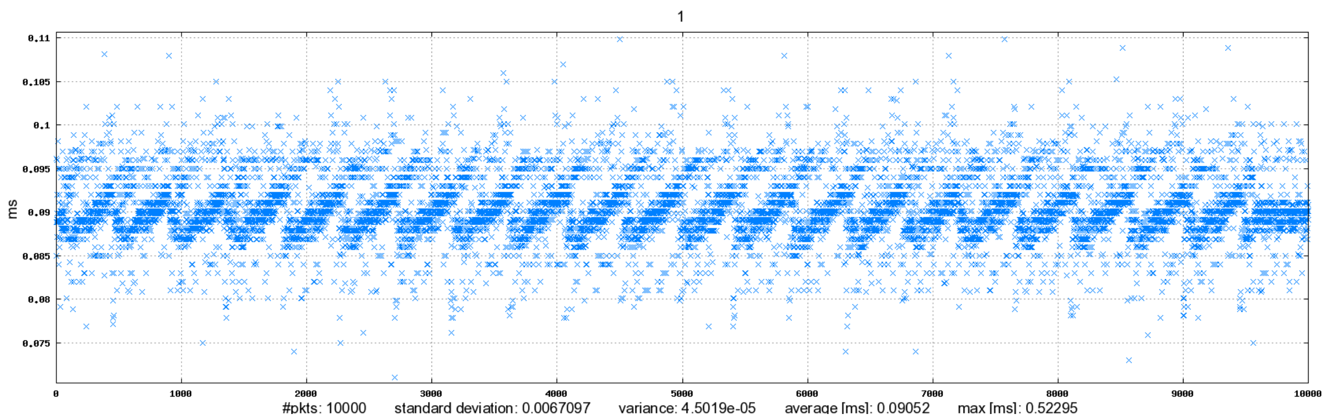

Figure 17: VLAN inter-arrival times plot: 500 bytes @ 90us with network load

Packets Length	Interdeparture times [µs]	SCP enabled	Receiver side		
			Var	Avg [µs]	% arrived
50	70	No	2.56E-4	72.5	98.4
	80	No	4.6E-5	79.98	100
500	80	No	2.7E-5	88.63	100
	90	No	4.5E-5	90.52	100
800	110	No	2.30E-5	116.23	100
	120	No	2.30E-5	119.98	100
50	70	Yes	8.5E-5	73.05	97.66
	80	Yes	1.3E-3	80.00	100
500	80	Yes	3.5E-5	87.11	100
	90	Yes	1.6E-5	90.01	100
800	110	Yes	2.9E-5	113.23	100
	120	Yes	1.7E-5	130.01	100

Table 4: VLAN tests with L2 prioritization

Although the minimum inter-arrival time at which there is no packet loss (hereafter referred as 100%-arrived minimum time), between L2 and L3 prioritization, does not increase with payload, this is not equally true in presence of non-prioritized traffic, probably due to the amount of real bandwidth that the switch can handle. This increase can be explained in the way VLAN prioritize, by arbitrating and scheduling packets, which may collide sometimes with the TCP congestion control, causing temporal lapses where the aggregated actual bandwidth is more than what the switch can handle, thus increasing the 100%-arrived minimum times. Anytime though, statistics are promising, granting high level of determinism to flows. If adding more data streams doubles the minimum inter-arrival time granting 100% receptions, this will be due to hardware constraints of the switch controller, in terms of capacity of the port queues. Figure 17 shows how collateral traffic affect performance in terms of jitter (many packet arrived in the temporal interval between $\mu \pm 2\sigma$ and $\mu \pm 3\sigma$); this imply that VLAN priority implementation causes these problems. In further analysis, the benefit of HTB, in terms of jitter, will emerge, specifically in Figure 25.

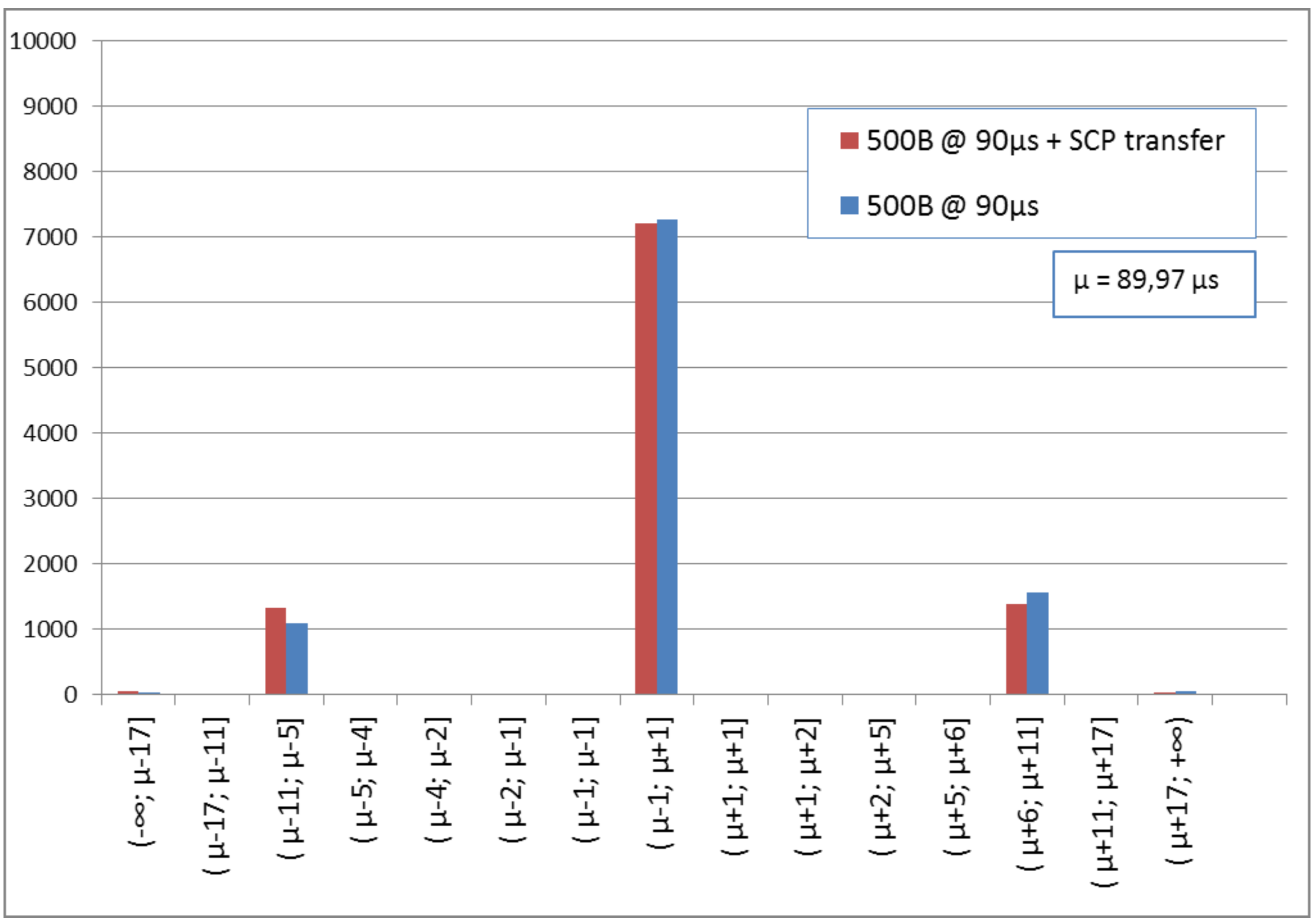

Figure 18: frequency histogram for VLAN tests

7.3 L3

TCP/IP Stack offers many protocols designed for best efficiency on Ethernet. When choosing to migrate from a different bus to Ethernet, TCP/IP stack is at least worth to be considered for supporting the communications.

At Layer 3, the IP protocol Type of Service (before its deprecation) byte defined two fields: precedence (3 bits) and TOS fields (5 bits, four of them settable for as many classes of services, such as low delay, high throughput and high reliability); reference [24] then superseded the Type Of Service concept for *DiffServ*. Anyway, for backward compatibility, the TCP/IP stack API that has been used retains the TOS architecture and tests prove that all inherent packets travelling the network have that bit set, useful for the purpose of the tests, later discussed.

By default, routers that receive a packet with the low delay field enabled, forward that packet towards its destination by putting it in an ad-hoc outbound queue, consumed before any other queue. In addition, GNU-Linux operating system's TCP/IP stack honours that field by creating three queues on egress side.

This prioritization is done at a higher level, so more computational, CPU-bounded load is required. This will indeed affect throughput as well as determinism, because of unpredictability added by the operating system, but still one can fruitfully implement further checks or actions in order to improve or enable services that otherwise (i.e. using IEEE802.1P priority) would not be possible to reach, as traffic would be relegated to the switch controller.

As for the tests, Linux-based PCs (both for normal hosts and for switch) and Linux Traffic Control (LTC) has been used. LTC is a set of queuing disciplines (hereafter *qdiscs*) that handle packets, policing and prioritizing them upon reception (Ingress) or transmission (Egress). Many tests of communications will be performed using in many ways LTC, in the switch.

In order to perform bandwidth partitioning, rather than FIFO prioritizing or dropping packets (adding extra time for transportation, to the extent of packet starvation, or downsizing the actual throughput) Hierarchy Token Bucket (HTB) [25] has been used. HTB reserves a minimum bandwidth for each subclass created (*rate* setting), if a class then requests less than its slack, the remaining bandwidth is distributed to other classes which are requesting to borrow (*ceil* setting), if the burst option is provided, the borrowed bandwidth is enabled only for the amount of bytes provided as an argument.

But, if in [26] many tangled mechanisms had to be implemented in order to obtain inbound priority, here the L3 layer of the switch can reorder the packets bound to any receiver, provided that either one host or a switch is connected to any of the ports of the switch (i.e. no hubs or multiple repeaters are present).

7.3.1 L3 prioritization configuration

For what concerns L3 priority test, the settings involved also concerned ICMP messages and advanced routing. To provide the L3 prioritization on the switch the goal was that for any host physically connected to the Switch, the switch itself should be their next hop for the local network. In networking administration terms this is quite forcing, as any host in a IP network that is one other host in the same L2 network should reach it without appealing to a gateway; in fact, ICMP specifies a control message just for similar events [27], called Route Redirect Message (RRM), for performance purposes.

By design, the RRM is produced by a host A (if we take into account the topology depicted in Figure 19) that received from B an IP datagram bound to host C (through an arbitrary network). A will inform the sender B that further datagrams (D could or could not be actually delivered to C or N) should be diverted to a different host X (X being potentially C itself), in order to deliver the traffic to C. This also applies to traffics that demand specific Type of Service (e.g. if D has High Throughput TOS option enabled and A knows that X has different, less costly paths, then A will tell B to divert further traffic bound to C towards X).

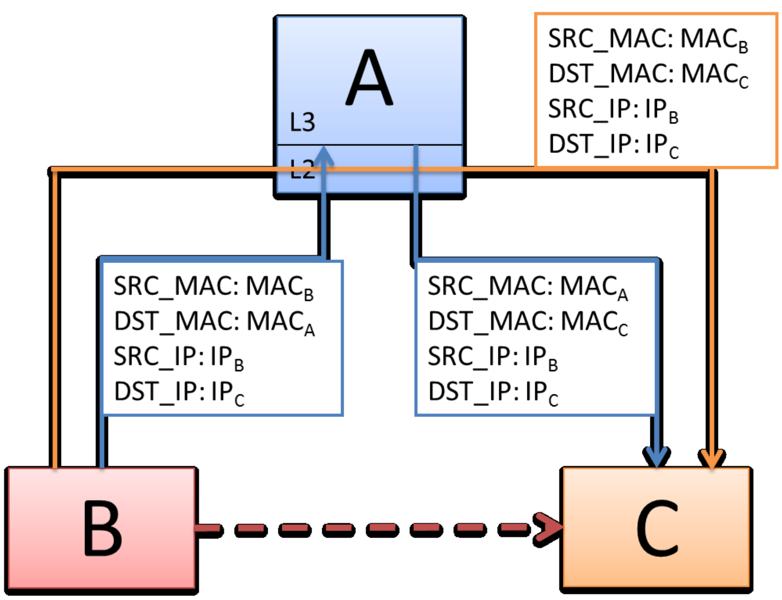

Figure 19 Ethernet and IP packet dynamics, with L3 routing (in blue) and without (orange)

The result wanted is shown on Figure 19. Should the sender B (with MAC address MAC_B and IP address IP_B) want to communicate with C (with MAC address MAC_C and IP address IP_C), drawn in red, it would either send the packet directly (orange line) or through A L3 forwarding.

Using L3 gateway-ing, hence passing through A (a gateway with MAC address MAC_A and IP address IP_A – drawn in blue), B will create a Ethernet frame with MAC destination MAC_A (known with an ARP request for IP_A, obtained from the routing table), MAC source MAC_B, encapsulating an IP datagram with IP source IP_B and IP destination IP_C. When the packet arrives at A, the A's L2 acknowledges the frame to be bound to its MAC address and forward it to the L3. As IP destination address is not IP_A, but IP_C, the stack forwards the IP packet towards C.

This is done by creating a new Ethernet frame, with source MAC_A, destination address MAC_C, IP destination address IP_C, IP source address IP_B. In case the sender B receives the RRM from A, or just uses common settings, a packet bound to C would create a Ethernet frame, drawn in orange, with source address MAC_B, destination address MAC_C, encapsulating a similar IP datagram as before. For topology reasons, still the packet would travel to A, but there, the L2 controller would forward (without passing it to the IP layer) the frame as it is at the correct port (eventually queuing it), thus forwarding it to C; this would prevent the Switch from doing any further action or control on the data.

In the Linux TCP/IP stack implementation, the reception of a datagram bound to a host in the same network of the sender automatically triggers an ICMP RRM. The sender, receiving the RRM message, will change its routing tables accordingly (in this case simply removing the gateway information from the relative line of the table), thus cutting out the Switch from any possible action at layer 3, as previously said. To prevent this, the Switch should just abide from sending the RRM but settable using either the *sysfs* or the *sysctl* infrastructures.

To set the Switch as a gateway for the subnet, *route* or relatively new *ip* command are useful to complete the task, statically. As dynamic network can be needed by network design, taking advantage of DHCP is the best way to achieve same results as above, but dynamically.

Briefly, the approach chosen was to create a DHCP server; in case the topology included just one switch, this should be the only one DHCP server. It will be in charge not just to provide with correct IP, subnet and any other relevant parameter to set up the network, but also to indicate itself as the gateway (not just the default gateway) for its own star, using the standard DHCP option rfc3442-classless-static-routes [12], to be sent to the DHCP clients. In case of multiple L3 switches in the same network, every switch (minus one) will act as a relay DHCP server and will advertise itself as the gateway for the hosts of its star.

Other features useful to avoid, especially in high rated data flows, buffers overflows is to set the transmit queue to a higher value; in Linux, this is simply achieved by using the *ifconfig* command.

Finally, to implement prioritization, similar configurations as [28] has been adopted: due to the high throughput needs for tests that were later descripted, the ratio between the high-priority and the low-priority slacks is much disadvantageous for the latter. Referring [24], we define RATE_LOW and RATE_HIGH the two *rate* options (guaranteed bandwidth) respectively the low priority and the high priority bandwidth slacks, and CEIL_LOW and CEIL_HIGH the *ceil* options (borrowable bandwidth) respectively for the low priority and the high priority slacks. For each class the configurations are:

- RATE_HIGH set to 80Mbit;
- RATE_LOW set to 5Mbit;
- CEIL_HIGH set to 80Mbit;
- CEIL_LOW set to 10Mbit.

These settings are kept less than theoretically achievable ones (i.e. CEIL_HIGH could be set to 100Mbit), in order to prevent any hardware device from exceeding its limits, invalidating the tests.

7.3.2 L3 prioritization test and results

L3 prioritization needed more tests as multiple environments with incremental settings had to be investigated. First tests done deal with an early approach to performance comparison, w.r.t. degrade of latency and determinism due to a host (with relative hardware and software latencies and randomness) being in the middle, compared to inherent ping tests (as shown on Table 2).

The tests reveals lower figures both in RTT and in variance in L2 ping tests, values that will be confirmed, for what concerns variance, also in other tests. Should one infer that the 100%-arrived minimum time is roughly half of the RTT showed, be warned that, as the topology include more than one branch of connections, more than one packet can be traveling the path from the sender to the receiver, or queued in between.

Packet Length	Interdeparture times [µs]	SCP enabled	Receiver side		
			Var	Avg [µs]	% arr.
50	70	No	1.7E-3	78.95	100
	80	No	1.8E-3	80.01	100
500	80	No	1.9E-3	87.11	100
	90	No	2.2E-3	90.32	100
800	110	No	2.0E-3	114.7	100
	120	No	2.4E-3	119.9	100
50	90	Yes	1.7E-3	93.86	96.27
	100	Yes	2.1E-3	100.0	100
500	90	Yes	1.9E-3	91.4	97.25
	100	Yes	1.6E-3	100.0	100
800	100	Yes	1.6E-3	108.4	100
	110	Yes	2.3E-3	110.7	100

Table 5 Tests with L3 routing without custom prioritization (one sender and one receiver)

Packet Length	Interdeparture times [µs]	SCP enabled	Receiver side		
			Var	Avg [µs]	% arrived
50	70	No	6E-4	77.15	92.36
	80	No	1E-3	80.00	100
500	80	No	1.7E-3	83.6	100
	90	No	2.1E-3	90.00	100
800	100	No	2.5E-3	107.48	100
	110	No	2.8E-3	110.81	100
50	80	Yes	7.6E-4	85.86	94.39
	90	Yes	7.1E-4	90.11	100
500	80	Yes	7.1E-4	88.13	97.32
	90	Yes	7E-4	90.0	100
800	100	Yes	2.1E-3	111.08	100
	110	Yes	1.7E-3	110.63	100

Table 6: tests with L3 routing with HTB prioritization (one sender and one receiver)

All results showed in Table 5 and Table 6 seem promising. The time needed by the Switch to forward any packet (performance by the way closely related to the Switch CPU characteristics and optimization of the TCP/IP Stack) is close to nil and, as expected, the slowing-down role of the software layer of the Switch is particularly relevant observing the variance figures. This is sensibly higher than relative ones in VLAN tests, by two orders of magnitude, but still good, granting minimum jitter to packets.

In peculiar cases, though, the L3 switching act as a double buffering, causing less packet to be lost, as Table 5 and Table 6 show. For instance, even though the inter-departure time was set to 80µs, they are instead received with an average of 87µs (Table 5, 500 bytes, no SCP enabled), meaning that the queues in the path had not been filled up yet, but the switching of the data took more time.

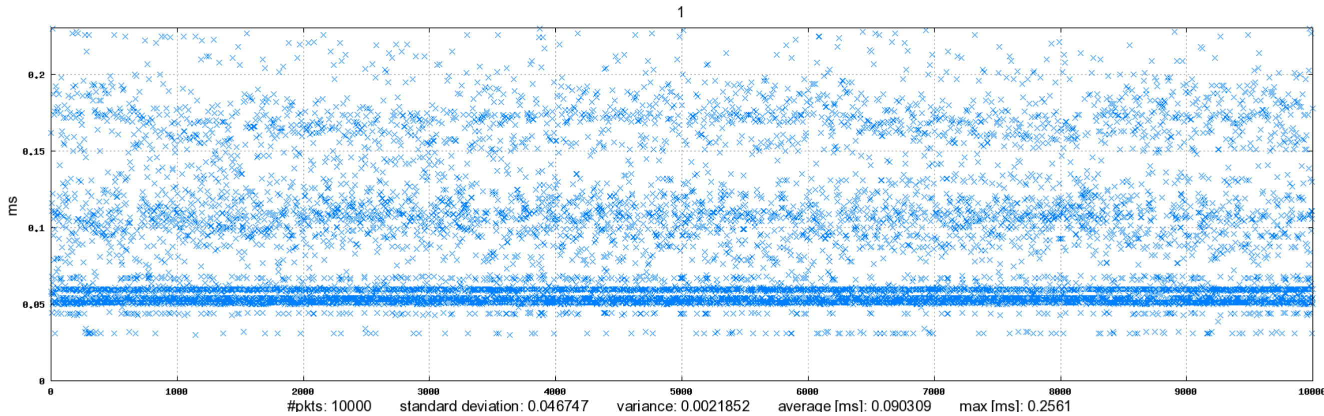

Figure 20: L3 w/out custom priority, interarrival times plot: 500 bytes 90us with network load

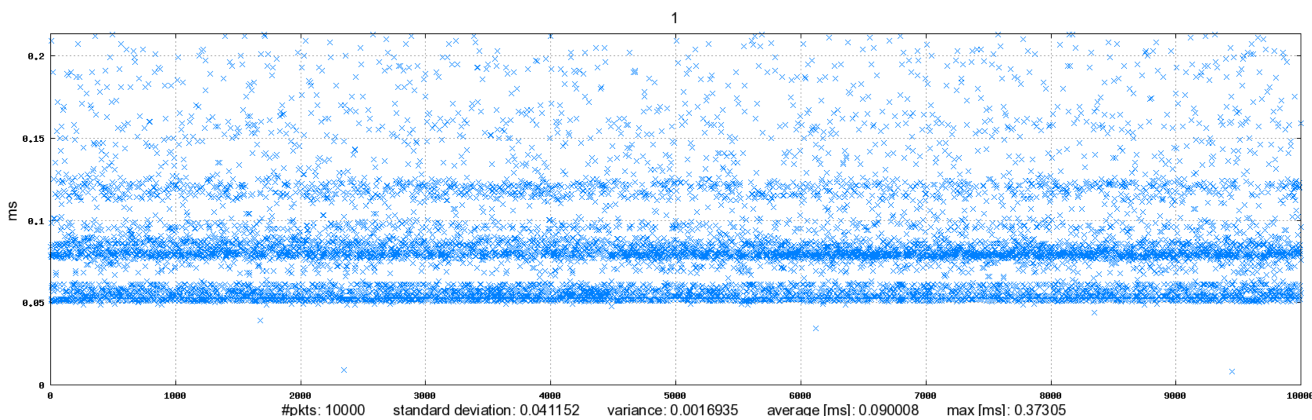

Figure 21: L3 w/out custom priority inter-arrival times plot: 500 bytes 100us with network load

Without priority and in presence of unregimented traffic, results worsen a jot (Figure 20 and Figure 21) and, to achieve 100% arrival of packets in time, the inter-departure times had to be set to fairly more than the ones needed both in VLAN and in HTB-priority tests. This kind of tests worked out as a comparison on how HTB improves performance.

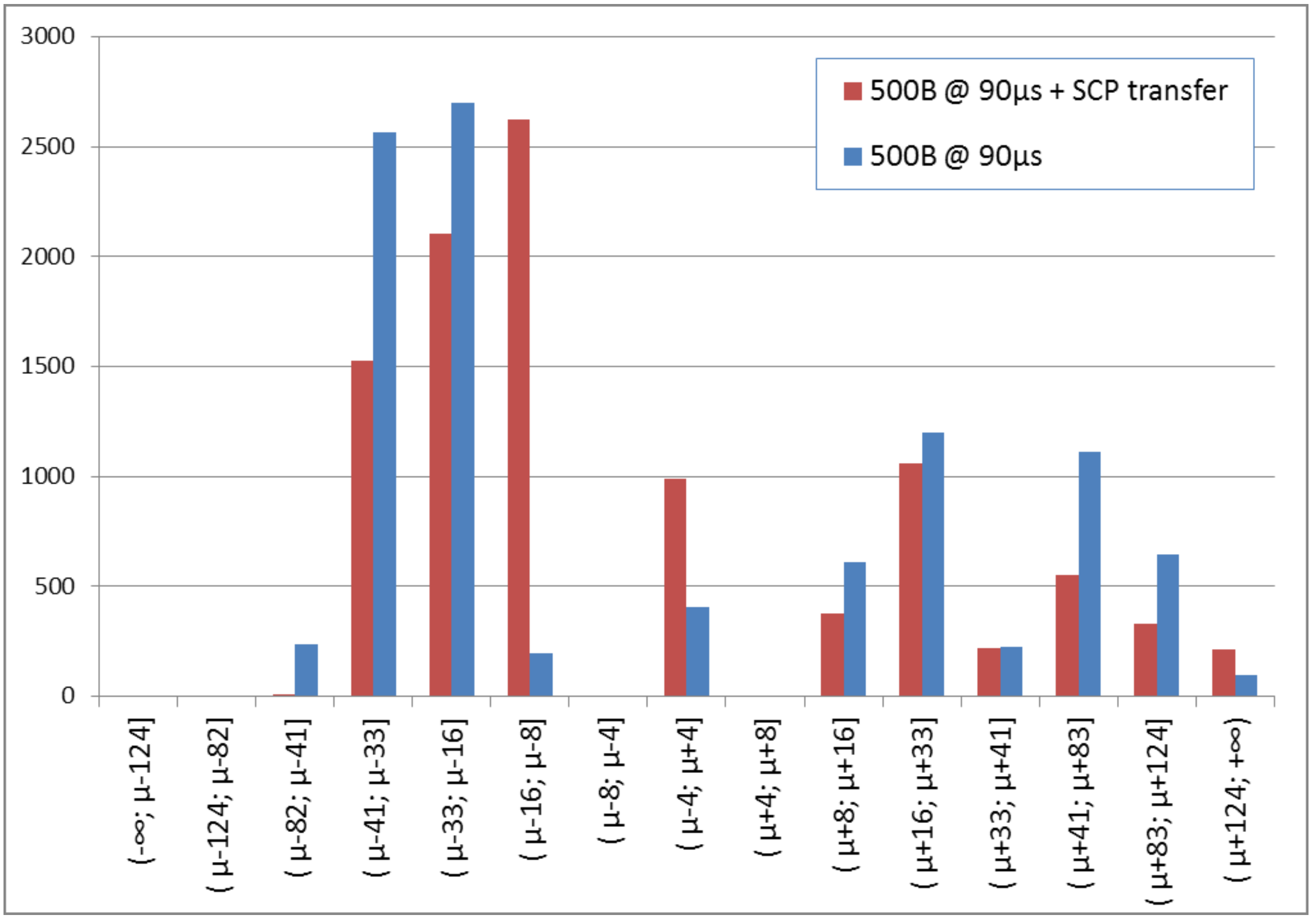

Figure 22: frequency histogram for L3 routing tests without custom priority

Figure 22 clearly shows that two distributions produce the average: the one composed by the packets that are processed immediately (the leftmost peaks, in blue) and those affected by queuing delays (the rightmost, spread ones); when SCP traffic is added, the two distributions somewhat merge. This phenomenon is recurrent in tests with L3 switching.

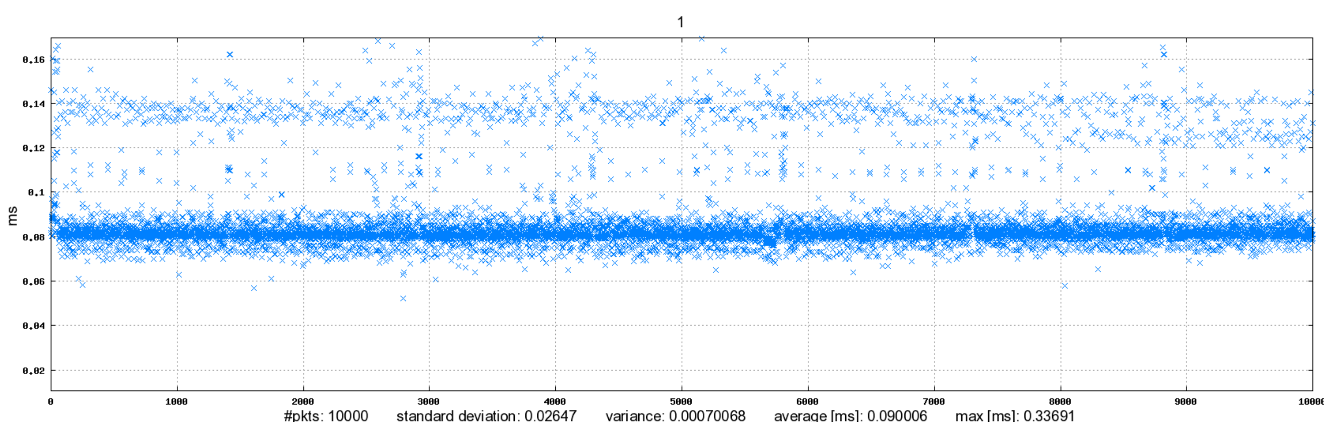

Figure 23: HTB-prioritized L3 inter-arrival plot: 50bytes, 90us w/out network load

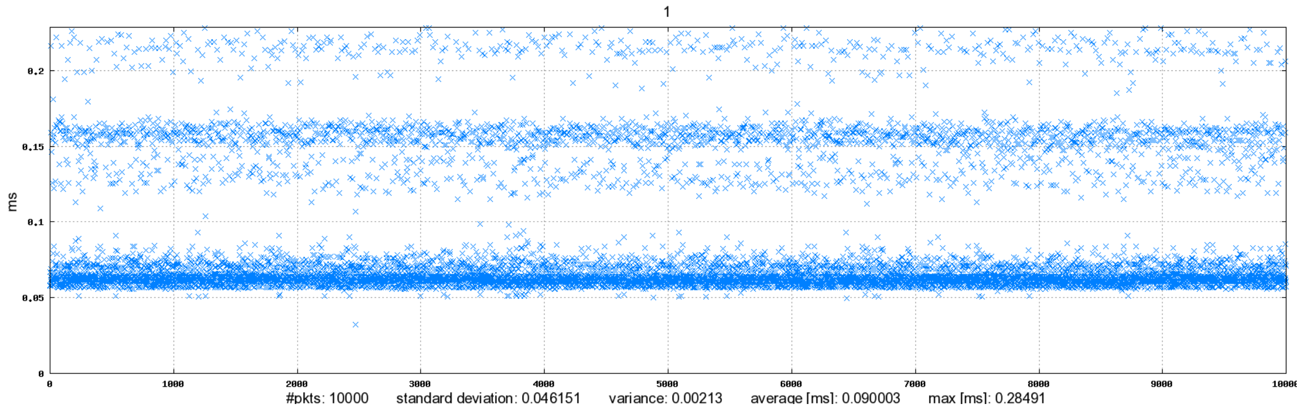

Figure 24: HTB-prioritized L3 inter-arrival plot: 500 bytes, 90us with network load

Enabling HTB (Figure 23 and Figure 24) priority on egress side gives good results both on determinism and on inter-departure time sides. Here we can appreciate roughly the same variance as those tests not involving other source of traffic. Results demonstrate that prioritization concurs in allowing faster and more deterministic data streams.

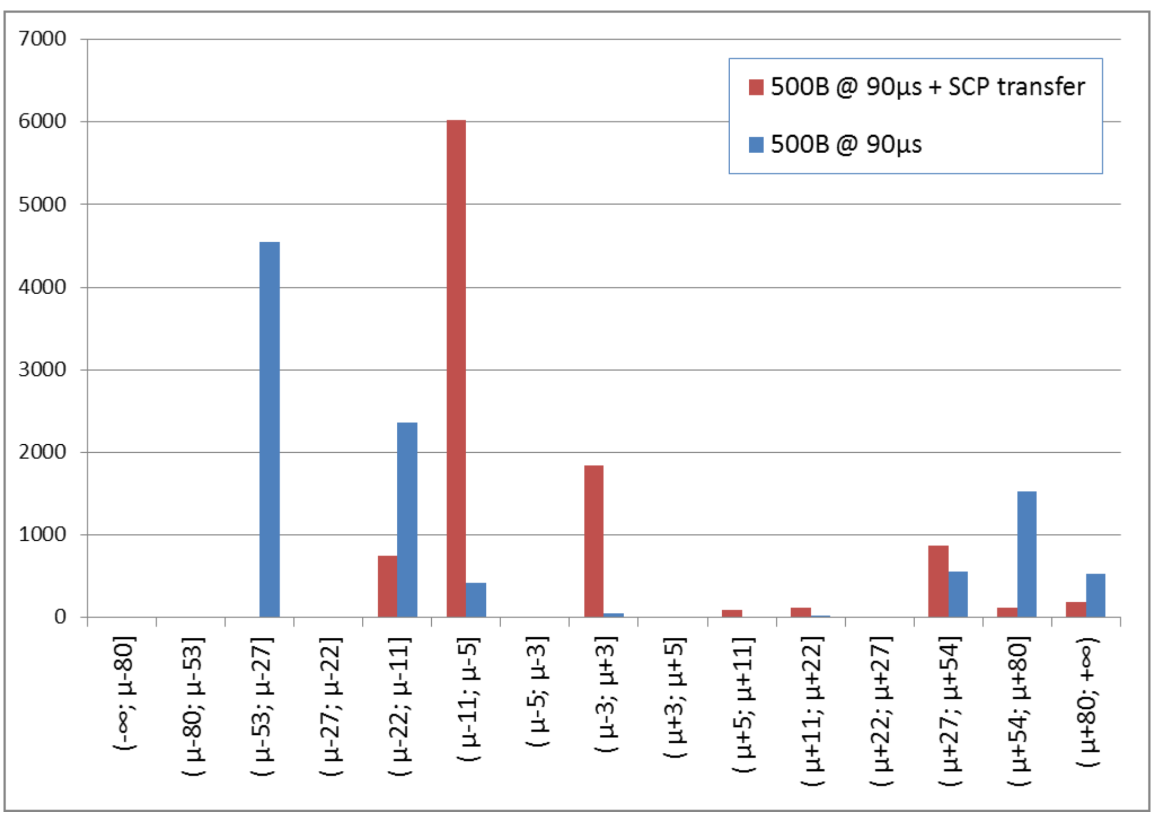

Figure 25: Frequency histogram for L3 routing tests with HTB prioritization

Analysing Figure 24 in respect with Figure 21, the effects of HTB are revealed, in terms of determinism and bandwidth slacking. The comparison with Figure 17 and Figure 24 depicts a different distribution of packet arrivals: it is interesting how VLAN prioritization is able to manage all packets arrival very deterministically. Both histograms that do not depict flows managed by HTB under traffic congestion suffer from a dispersion around the standard deviation quite flat, Figure 25 shows that HTB allows a polarization of the jitter (thus implying determinism) around two temporal lapses and the improvement of performances, becoming comparable with VLAN's.

8 Adopting Powerlink

Powerlink relies on a technical group (EPSG [29]) to standardize, promote and develop the technology[30]. It should be noted that a recent work [31], proved the feasibility (that should not pose issue hypothetically) of Powerlink over BroadR-Reach and also [32] dealt with the applicability of the fieldbus in industrial vehicles.

The bandwidth prioritization led to a feasible architecture, to which well-proven algorithms (HTB and standard VLAN prioritization) assure that the network will put some effort to grant precedence over data. This architecture will not guarantee neither certainty of delivery nor strict delivery deadlines to data. The choice of to divert the investigations to an industrial fieldbus is explained just for the environment that these technologies have been designed for and the features that they provide (i.e. time triggered cycles). Powerlink seemed to win the comparison already described.

This applicability was analysed during the research and some limits were highlighted. Particularly, two major features of the field are taken into account:

1. The architectural view, that creates a hierarchy in which there is one and only Master Node, that is both the network arbiter but also the centre of the exchange of data;
2. The hotpluggability that agricultural machinery need, so that an arbitrary implement can connect to a tractor without restarting the whole system (key-off sequence).

The research associated to this field focused on analyse the possible modifications that can be performed to adapt the Powerlink stack to the AG mobile needs. The next sections will deal the configuration of a Powerlink network and with consequent modifications.

8.1 Topology and effects on cycle time

Before getting into the details of the Powerlink modification to meet the AG mobile requirements, it is good to discuss how the characteristics of a Powerlink physical network.

As for Powerlink technical specifications, both standard switches and hubs can exist in a Powerlink network, though only Class 2 Repeaters are conformant with Powerlink standard. The main reason is the jitter requirement: hubs have a reduced path delay value (equal or below 460 ns) and a small frame jitter (equal or below 70ns). Hubs do not split collision domains, but POWERLINK changes the access method over an Ethernet network and does not cause collisions.

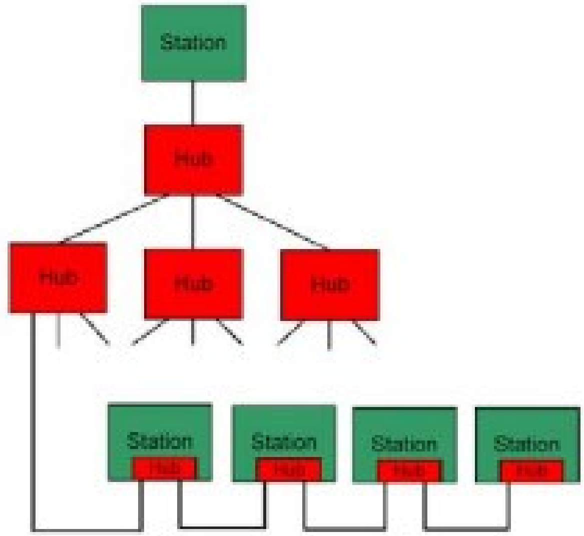

Figure 26: Powerlink network with star and daisy chain topology

The resultant topology can be defined as in Figure 26. In such scenario, the ESPG calculated that the signal requires at most 5ns to travel each meter of cable and up to 1us to traverse a standard Class II hub.

Therefore, it is easy to say that hubs have a direct effect on the POWERLINK cycle time and it should be noted that the runtime for any hub should be counted twice, when evaluating the cycle time. For what concerns the jitter, Powerlink suggests keeping the hub-depth below 10.

The CN response timeout is another parameter to take into account when evaluating the cycle time: it is defined by default to 25us and suits for most agricultural application (in terms of resulting cycle time and performance required).

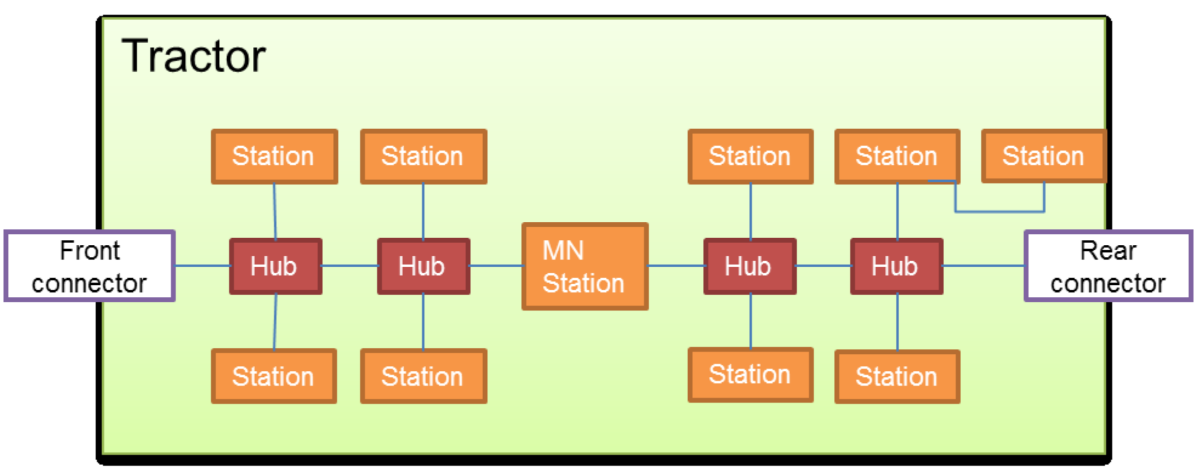

Figure 27: hypothetical network topology on board of a tractor

In terms of actual agricultural application some calculations have been performed, in order to assess a hypothetical, feasible cycle time. At this stage, the hypotheses made are the following:

- The tECU, which is present in any ISOBUS network, is elected as a MN;
- The topology is similar to the one depicted in Figure 27, where two branches start out from the MN, one bound to the front of the tractor, one to the rear (IBBC connectors);
- The MN has at least a 2-port hub (on for each branch);
- Other on-board ECUs connected to the POWERLINK network will be most-likely present, so at least one level of hub is predictable for each network branch.

Some calculations assessessing the magnitude of the cycle time and relative performance are presented in the Table 7, where three scenarios are taken into account. ESPG Powerlink cycle time sheet has been used for the calculations.

8.1.1 Video streaming over 2 "safety" cameras (on the rear left and rear right corner) to a graphical terminal

This scenario features two backup cameras mounted on the rear and a graphical terminal to visualize the streams; the configuration proposed guarantees to deliver the streams using the POWERLINK isochronous service. The term "safety" stems from the need to guarantee the stream to be delivered with certainty, in terms of dependability and performance.

The MN will create a Process Data Object (PDO) communication of the video stream from which the graphical terminal will read in a publisher/subscriber principle. In particular, the MN will send a PollRequest of the PDO sequentially to both the cameras, to which they will respond with PollResponse. The graphical terminal(s) will listen to that PDO as they have previously subscribed.

The needed throughput is calculated to be around 37Mbps based on 2x 640x480 @25fps with MJPEG compression.

8.1.2 Sophisticated visualization on one graphical terminal, from connected to implement ECUs

This scenario features three ECUs of a hypothetical implement attached to the tractor and graphical terminal, from which a user can interact in order to read the state of the treatment and perform some procedures via graphical commands. In this case, either a bi-directional PDO message is necessary or the graphical terminal must be the MN of the network, as later discussed.

The needed throughput is calculated to be 4600Kbps taking account of:

- 100kbps for command/response packets in a RPC fashion, considering a 1920x1080x24bit graphical interfaces, so many objects are visible contemporarily;
- 2000kbps Compressed graphical interface upload;
- 2000kbps Manuals upload;
- 500kbps Instant graphical refresh;

8.1.3 Improved service and diagnosis (flash ECUs, log files, raw data streams)

This scenario features 3 ECUs of a hypothetical implement attached to the tractor and graphical terminal, from which an instructed user connect a USB stick, in order to upgrade existing functionalities in the implement, via secure protocols. Furthermore, the user will be able, through a graphical terminal with diagnosis services to get diagnosis and debug data from the network.

The needed throughput is calculated to be 7000Kbps taking account of:

- 3000kbps Flashing ECUs (50MB image);
- 3000kbps Log files;
- 1000kbps debug data from actuators/sensors/etc;

<table>
<tr><th>Case n.</th><th>Expected throughput [Kbps]</th><th colspan="2">Calculated POWERLINK cycle time [us]</th><th colspan="3">Offered POWRLINK throughput [Kbps]</th></tr>
<tr><td>8.1.1</td><td>36864</td><td colspan="2">256</td><td colspan="3">37430</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Device type</td><td>Amount</td><td>Payload IN</td><td>Payload OUT</td><td>Hub level</td></tr>
<tr><td>Graphical terminal</td><td>1</td><td>64</td><td>125</td><td>2</td></tr>
</table>

		Camera	2	64	550	3
8.1.2	4600	202		12284		
		Device type	**Amount**	**Payload IN**	**Payload OUT**	**Hub level**
		Graphical terminal	1	64	125	2
		ECU	3	64	64	3
3	7000	202		12284		
		Device type	**Amount**	**Payload IN**	**Payload OUT**	**Hub level**
		Graphical terminal	1	64	125	2
		ECU	3	64	64	3

Table 7: cycle time for specified scenario

8.2 Architectural hierarchy, comparison

This chapter discusses the means to create an inter-client communication. As already said, current AG mobile control networks rely on a Multi-Master paradigm, where a restricted number of ECU can, in specific moments, gain control of the network and send commands and requests.

The following subchapters will deal with two ways to recreate that feature in a Powerlink network, without any modifications to the standard:

1. Electing only one node to be a MN, and creating communication that other ECUs can subscribe to, if interested;
2. Having more than one MNs that co-operate to be the MN when the application requires it.

These ways are intended to be mutual exclusive but left to the tractor network designer to be utilized.

8.2.1 One MN, on-demand multicast communications

Only one MN is always in charge of managing the network. This imply that it will always receive command data from all the nodes, even though these data are not strictly important for the MN itself. For this reason, other CNs will declare their interest over other CN's responses. Reference [19] dealt with the feasibility of having a bus master separated to the application master on a Powerlink network

Powerlink provides with means to send continuously real-time data using Process Data Objects (PDO). These follows the PReq and/or PRes isochronous semantic, where PReq are sent unicast while PRes are transmitted as broadcast.

Powerlink defines two types of PDO: transmission and reception PDOs; a MN may support 256RPDO and 256 TPDO channels, while on a CN device one TPDO channel may be available and up to 256 RPDO may be supported. The size of the PDO is application specific (but is constrained in IEEE 802.3 standard lengths, from 64 bytes to 1518 bytes) and communication follows the publisher/subscriber principle: the transmitting node creates a TPDO that contains all actual values of a given set of objects and publishes it frequently to the network. On the receiving side, each node interested in one or several of the values can subscribe to this PDO, thus configuring it as a Receive PDO (RPDO). The process of assembling the TPDOs and RPDOs is called PDO Mapping.

In an AG mobile scenario, the tECU could be the MN, creating mostly PDOs. Each ECUs creates application specific data objects, to which any other CN would subscribe to.

8.2.2 Application-specific MNs

Powerlink supports only one MN at a time. However, the standard has adopted [33] the principle of the High Availability, so that the availability of the system is ensured in the event of a component failure. The nodes and medium redundancy prevent having a single point of failure in the system:

- The Managing Node redundancy ensures the POWERLINK cycle, keeping synchronization and low jitter in case on MN failure.
- The use of two media carrying the same information at the same time ensures to be robust to any network-infrastructure component failure.

Both switchover times (a.k.a. recovery times) of the system are in the range of the POWERLINK cycle time, ensuring a very fast restoring of normal operation without any downtime for the system.

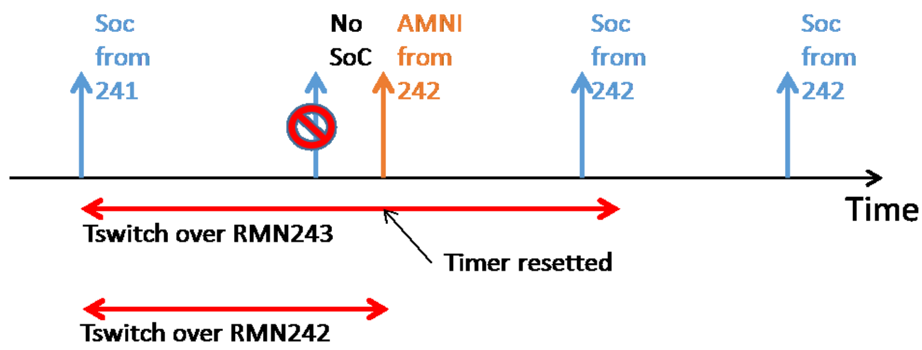

Figure 28: switchover of a MN

Although a typical switchover is shown in Figure 28, caused by the failure of an active-MN (with ID 241) recovered by the standby-MN (with ID 243), there is also an application-defined, voluntarily handover of the network management. In that case, the application on the standby-MN will sent a "go to Standby" state command to the active-MN (*NMTGoToStandby*); afterwards, if the active-MN accepts the request by yielding the control of the cycle, the election process of a new active-MN starts, with mechanisms that include application-specific priority.

In a tractor-and-implement environment, the use of this features that POWERLINK already adopts, can fruitfully enhance efficiency of the network. Referring to the application scenarios mentioned in 8.1.1, 8.1.2 and 8.1.3 the graphical terminal, can request and obtain to be an active-MN through a "go to Standby" state command, and then create an application-specific configuration, supporting other background services, too.

The only scenario that probably still benefit from the PDO structure would be the one mentioned in 8.1.1: other ECUs can use the video streams that are present on the network (i.e. Birdview ECUs), hence a multicast paradigm is perhaps more suitable.

8.3 Hotpluggability and runtime configurations

This chapter presents ways that a Powerlink network has to re-configure itself without restarting the whole system. Usually, the configuration of all the node is done at boot time, and as [19] states, more than one Configuration Manager (CFM) can be present, for the High Availability principle. This is an optional feature of the redundant-MNs; CFM is responsible for the correct configuration of all the devices belonging to a network. Particularly, the configuration include two different stages:

1. Download of the configuration data to a CN;

2. Download of the whole network configuration data from the active-CFM to any standby-CFMs

This procedure, by Powerlink definition, is made at network boot time and could not be repeated, as no re-configuration can be made unless rebooting the whole network. However, as ECUs are much more intelligent devices than simple drives, sensors and actuators, network configurations are most likely to change, rather than ECUs specific ones.

To describe better the dynamics, let us consider, for instance, the attachment of an implement, at the beginning of a normal working session:

1. The POWERLINK network has been put in a reduced cycle (i.e. in this phase the synchronous service is suppressed), before the working session;
2. Every ECUs, during the ASYNC frame, can acknowledge their presence in the network (address claiming), the implement shall have its master ECU that will send all graphical data, along with the requirements of the application (e.g. bytes per PRes needed, cycle time constraints, etc.)
3. The MN will create proper configurations given on-implement and on-tractor features (e.g. baler configuration, rearview configuration, etc) alongside standardized preconfigured mixed configuration (e.g. "standardized seeder plus rear camera" configuration);
4. The active CFM will update the other enabled standby-CFMs;
5. The user will choose the service(s) needed, via graphical input;
6. The MN will start the runtime cycle.

As the access to the ASYNC slot is pre-defined through a specific algorithm, the entering of an arbitrary (though limited) number of ECUs in unpredictable, hence a different approach should be addressed. The research done suggested tweaking the standard IEEE 802.3 CSMA algorithm in order to maximize the probability for n<8 nodes to successfully transmit without collision, but this work will not enter in further details.

Whether the user or an ECU should cause a change in the workflow (e.g. the user changes service from seeder monitoring to an in-tractor service such as GPS guidance while seeding), possibly the network configuration may change. This will not affect radically the functionality each ECU provides, but rather the time cycle and/or the precedence of some ECUs w.r.t. others, the multiplexing of some time slots and other network-related settings. As these are all explicitly determined by the Powerlink messages dynamics a runtime modifications of these settings can be tracked without further changes in the Powerlink standard. In case these changes would affect some dynamics, (specific data can be requested more frequently) the actual implementation of the "go to sleep" message has left 7 bits reserved, that can be used to signal a specific change of configuration.

9 Conclusions

Automotive industry is now approaching the Ethernet world, as a new backbone for infotainment (superseding MOST), end-of-assembly-line ECUs flash and diagnostics; in this context, Broadr-reach is paving this way for Ethernet over vehicles. The AG mobile industry, usually late w.r.t. automotive one, is in this case more reactive, for the dynamicity and the bandwidth that Ethernet provides, mainly for precision farming applications.

If Ethernet (or one of its fieldbuses) will become the next generation bus also for in-vehicle data distribution, many challenges have to be faced: topological and technological above others. Topology will probable decree this success if cost-effective infrastructures will be provided by industry: if star topology sensibly reduces wiring cost and weight (thus consumes), on the other hand switches/hubs become critical from a safety point of view. Strictly connected to the topology lies the cabling and connectors matter: in order to grant EMC compatibility, as well as other environmental conformances, both 100-baseTX and BroadR-Reach shall need support of a multi-source, convenient variety of cables, harnesses and connectors.

If technology would not affect per se costs, as FOSS community enormously collaborates to the diffusion and maintenance of well-established and robust protocols and related technologies, it is also true that lightweight implementations, focused for low performance CPUs will formidably influence requirements on ECUs. Although latest trends seem to testify that CPU power and features put into an ECU are increasing exponentially (Texas Instruments Jacinto 6 architecture is designed just for automotive scenarios and already adopted in Ag mobile).

Two paths have been fruitfully investigated: one heading towards the compatibility with existent technology, without consistent changes in the Layer 2 of the Ethernet Standard and dealing with Prioritization; the other towards the strict achievement of functional requirements of certainty of delivery and control of the network, using an Ethernet fieldbus.

Using standard ways of prioritization, interesting results of topology and technology have been described, comparing the high dependability of VLAN prioritization to achieve good results in throughput (amount of data successfully delivered) and determinism, and the monitoring-oriented customizability of IP prioritization. Various are the scenarios in which these two ways of prioritization may become useful, even in synergy.

VLAN assures the best results, with its semi-hardware prioritization; although a bandwidth division would be safer in order to assure throughput and determinism (variance is always two orders of magnitude smaller than L3 switching tests, as expected). L3 assures the same level of bandwidth but shows worse results in determinism, as the operating system that handle the packets introduces relevant randomness. Thinking of an advanced network, with multiple hosts exchanging data, the VID field can play a fundamental role, where to every functionality managed by the network is assigned a single VID (also for network efficiency and security, where only the hosts allowed to communicate on a certain VLAN will be able to exchange data), prioritized in 7 different levels. On the other hand, the ability granted by L3 prioritization (made advanced by HTB bandwidth slacking) to make monitoring, logging, control activities, among the many is paid with an obvious toll in terms of statistics and speed. These activities, not carried out in the tests, will probably affect scalability and performance.

For what concerns the adoption of an Ethernet fieldbus, the choice of Powerlink seemed fairly good, in terms of adaptability and performance.

The analysis done suggests that this fieldbus can become a good candidate for further on-board testing. Minor changes can adapt this fieldbus with settled characteristics to this kind of networks. The adoption of a fieldbus would prevent the use of other automotive arising de-facto standards, such as DoIP and AVB, practically causing a split between the automotive and the agricultural worlds. However, heavy-duty vehicles are intended for more critical purposes that need level of robustness more similar to industrial solutions.

It has discussed how the topology, defined as two long series of hubs, can affect the performance, deepening the hub level. Three scenarios depict the stress that functionality can impose over the network and, theoretically, the network can support well the burden of more of a video stream in isochronous service.

The hierarchical differences outlined between Powerlink usual structure and the agricultural machinery one seem compatible without great efforts; the research outlined two different approaches.

In this work, performed at IMAMOTER research institute, the goal was to point out insights for both topics. Requirements and functionalities are clearer now: there is an inner need of Ethernet in agricultural machines, hidden to the final user, who will never ask for it, but get used to depend on it, transparently. Therefore, it is the right time to approach these functionalities with technological choices.

10 Abbreviations

AEF Agricultural industry Electronics Foundation

AFDX Avionics Full-Duplex Switched Ethernet

AVB Audio/Video Bridging (a.k.a. IEEE 802.1as)

COTS Commercial off-the-shelf

DoIP Diagnostics over IP

ECU Electronic Control Unit

(g)PTP (generalized) Precise Time Protocol

OABR Open Alliance Broadr-Reach

PHY PHYsical Layer

tECU tractor ECU

VLAN Vritual Local Area Network

11 Ringraziamenti

Desidero ringraziare il tutor di questa tesi, il prof. Massimiliano Ruggeri, per la sua disponibilità, la pazienza e la fiducia accordata nei miei confronti, permettendomi di partecipare attivamente in prima persona all'interno del comitato WG1 e 5 di ISO, dove ho presentato questi lavori, e nel comitato tecnico PT 10 di AEF, di cui ho fatto parte come esperto tecnico. Ringrazio anche i colleghi stranieri con cui là mi sono confrontato, ai quali devo anche una crescita personale, come cittadino del mondo. Questa tesi è stata svolta all'interno dell'istituto IMAMOTER, pertanto vorrei ringraziarne il direttore, l'Ing. Roberto Paoluzzi, per la disponibilità e l'incoraggiamento a proseguire nelle ricerche sulle reti agricole del futuro, e per gli utili consigli; ringrazio anche tutti i colleghi ricercatori e tecnici. Ringrazio di cuore i colleghi e amici, Massimo Dian, Carlo Ferraresi, Luca Dariz, Maurizio Lo Piccolo, Michele Selvatici e i soci di ESTE, che hanno supportato, aiutato, corretto i miei pensieri, i miei lavori e queste parole. I miei genitori, i fratelli, gli amici e i Noisy Neighbours, perché questo mio traguardo non sarebbe potuto arrivare senza di loro. E Laura, i suoi genitori e i suoi gatti, ché per gran parte del dottorato mi hanno amato, sorretto e sopportato, nonostante tutto, anche nel sonno.

12 Bibliography

[1] Manderscheid, M.; Langer, F.; "Network Calculus for the Validation of Automotive Ethernet In-vehicle Network Configurations," *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on* , vol., no., pp.206-211, 10-12 Oct. 2011;

[2] Steinbach, T.; Korf, F.; Schmidt, T.C.; "Comparing time-triggered Ethernet with FlexRay: An evaluation of competing approaches to real-time for in-vehicle networks," *Factory Communication Systems (WFCS), 2010 8th IEEE International Workshop on* , vol., no., pp.199-202, 18-21 May 2010;

[3] Lei Wang; Huijuan Jia; Junyan Qi; Bin Fang; "The construction of soft servo networked motion control system based on EtherCAT," *Environmental Science and Information Application Technology (ESIAT), 2010 International Conference on* , vol.3, no., pp.356-358, 17-18 July 2010;

[4] Arjmandi, F.; Moshiri, B.; "Fieldbus Interoperability on Ethernet," *Industrial Informatics, 2007 5th IEEE International Conference on* , vol.1, no., pp.213-218, 23-27 June 2007;

[5] Ruggeri M.; Malaguti G.; Dian M.; "SAE J 1939 Over Real Time Ethernet: The Future Of Heavy Duty Vehicle Networks," *Proceedings Of The SAE 2012 Commercial Vehicle Engineering Congress. October 2-3, 2012; Rosemont, Illinois, USA. ISSN 0148-7191.*

[6] IEEE 802.3bw, *100BASE-T1 - 100 Mbit/s Ethernet over a single twisted pair for automotive applications*

[7] de Andrade, R.; Lagana, A.A.M.; Guedes, M.A.C.; Justo, J.F.; Hodel, A.A.M.L.N.; Serafim Albaladejo, F., "A didactic platform to study of CAN FD bus," *Global Engineering Education Conference (EDUCON), 2013 IEEE* , vol., no., pp.318,323, 13-15 March 2013 doi: 10.1109/EduCon.2013.6530123

[8] Neukirchner, M.; Negrean, M.; Ernst, R.; Bone, T.T., "Response-time analysis of the flexray dynamic segment under consideration of slot-multiplexing," *Industrial Embedded Systems (SIES), 2012 7th IEEE International Symposium on* , vol., no., pp.21,30, 20-22 June 2012 doi: 10.1109/SIES.2012.6356566

[9] Haibo Zeng; Ghosal, A.; Di Natale, M., "Timing Analysis and Optimization of FlexRay Dynamic Segment," *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on* , vol., no., pp.1932,1939, June 29 2010-July 1 2010 doi: 10.1109/CIT.2010.329

[10] OPEN alliance, “OPEN Alliance BroadR-Reach® (OABR) Physical Layer Transceiver Specification For Automotive Applications” v3.2, 2014

[11] Zinner, Helge; Noebauer, Josef; Seitz, Jochen; Waas, Thomas, "A comparison of time synchronization in AVB and FlexRay in-vehicle networks," Intelligent Solutions in Embedded Systems (WISES), 2011 Proceedings of the Ninth Workshop on , vol., no., pp.67,72, 7-8 July 2011

[12] Il-Kyun Jung; Sun Lim, "An EtherCAT based control system for human-robot cooperation," Methods and Models in Automation and Robotics (MMAR), 2011 16th International Conference on , vol., no., pp.341,344, 22-25 Aug. 2011

[13] Il-Kyun Jung; Sun Lim, "An EtherCAT based real-time centralized soft robot motion controller," *Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on* , vol.1, no., pp.117,120, 25-28 Aug. 2012

[14] Jee Hun Park; Suk Lee; Kyung Chang Lee; Young Jin Lee, "Implementation of IEC61800 based EtherCAT slave module for real-time multi-axis smart driver system," *Control Automation and Systems (ICCAS), 2010 International Conference on* , vol., no., pp.682,685, 27-30 Oct. 2010

[15] Seno, L.; Vitturi, S., "A simulation study of ethernet powerlink networks," *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on* , vol., no., pp.740,743, 25-28 Sept. 2007

[16] Steiner, W., "TTEthernet: Time-triggered services for Ethernet networks," Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th , vol., no., pp.1.B.4-1,1.B.4-1, 23-29 Oct. 2009

[17] P. Pickel et all – «Machine control & guidance aspects on European research roadmaps» - MCG 2010

[18] Rath, Andreas; Waas, Thomas; Degueldre, Dennis; Noebauer, Josef, "A two wire power over Ethernet approach for in-vehicle applications," Intelligent Solutions in Embedded Systems (WISES), 2011 Proceedings of the Ninth Workshop on , vol., no., pp.55,60, 7-8 July 2011

[19] Steiner, W., "TTEthernet: Time-triggered services for Ethernet networks," Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th , vol., no., pp.1.B.4-1,1.B.4-1, 23-29 Oct. 2009

[20] R. Braden, "Requirements for internet hosts communication layers," RFC-1122, IETF Network Working Group, Oct 1989.

[21] R. Braden, “Requirements for internet hosts – application and support” RFC-1123, IETF Network Working Group, Oct 1989.

[22] Mnisi, N.V.; Oyedapo, O.J.; Kurien, A.; , "Active Throughput Estimation Using RTT of Differing ICMP Packet Sizes," Broadband Communications, Information Technology & Biomedical Applications, 2008 Third International Conference on , vol., no., pp.480-485, 23-26 Nov. 2008

[23] Hyung-Taek Lim; Herrscher, D.; Chaari, F.; , "Performance comparison of IEEE 802.1Q and IEEE 802.1 AVB in an Ethernet-based in-vehicle network," *Computing Technology and Information Management (ICCM), 2012 8th International Conference on* , vol.1, no., pp.1-6, 24-26 April 2012;

[24] K. Nicholas, S. Blake, F. Baker, D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers” RFC-2474, *IETF Network Working Group*, Dec. 1998

[25] HTB Home, http://luxik.cdi.cz/~devik/qos/htb/

[26] Dian M.; Malaguti G.; Ruggeri M.; “A Real-Time Wireless Protocol Proposal For Remote Agricultural Machine Control”; *Proceedings Of 7th FPNI PhD Symposium Om Fluid Power; University Of Modena And Reggio Emila* - June 27-30, 2012, Pp. 209-224. ISBN 978-88-7559-069-7.

[27] T. Lemon, S. Cheshire, B. Voltz; “The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4”, RFC-3442, IETF Network Working Group, Dec. 2002;

[28] Ruggeri M., Malaguti, G., Martelli M.; “Improvements Of Determinism In WI-FI Real-Time Protocol For Agricultural Machine Clusters”; Proceedings Of Industrial Electronics (ISIE), 2012 IEEE International Symposium, Pp. 1846-1851 Hangzhou, China. 28-31 May 2012;

[29] EPSG home, http://www.ethernet-powerlink.org/en/organization/about-epsg/

[30] Ethernet POWERLINK Standardization Group “EPSG Draft Standard 301” Version 1.2.0, 2013

[31] Dünnermann, Jens; Fuchs, Stefan; Schmidt, Hans-Peter; Witte, Stefan: Demo: "Real time Ethernet with unshielded twisted single pair cabling". In: IEEE Vehicular Networking Conference (VNC) Dec 2014.

[32] Taxer S., "A better bus service"; IVT Annual 2015

[33] Ethernet POWERLINK Standardisation Group "*EPSG Draft Standard Proposal 302-A - Part A: High Availability*" Version 1.1.0, 2013.

13 Pubblications on Conferences

Ruggeri M., **Malaguti G**., Dian M., Ferraresi C., “Quasi Isochronous Wireless Communication Protocol For Co-Operative Vehicle Clusters”, ISTVS 2012

Dian M., **Malaguti G.**, Ruggeri M., “A Real-Time Wireless Protocol Proposal For Remote Agricultural Machine Control”, FPNI 2012

Ruggeri M., **Malaguti G.**, Martelli M., “Improvements Of Determinism In WI-FI Real-Time Protocol For Agricultural Machine Clusters”, IEEE ISIE 2012

Dian M., **Malaguti G.**, Ruggeri M., “A Safety Compliant Universal Machine Control Unit using Codesys”, Mechatronics 2012

Malaguti G., Dian M., Ruggeri M., “Real Time Distributed Control On Machines Over Quasi Deterministic Ethernet”, FPNI 2012

Ferraresi C., Dian M., **Malaguti G.**, Ruggeri M., “Isobus Over Ethernet: A First Implementation”, FPNI 2012

Ruggeri M., **Malaguti G**., Dian M., “SAE J 1939 Over Real Time Ethernet: The Future Of Heavy Duty Vehicle Networks”, SAE COMVEC 2012

Ruggeri M., **Malaguti G.**, Dian. M., “Real Time Ethernet For Heavy-Duty Vehicle Powertrain Control”, ISTVS 2012

Malaguti G., Dian M., Ruggeri M., “UDP Based Inter/Intra Task Communication For Processes Independence In Safety Critical Embedded Applications”, IEEE ISIE 2013

Malaguti G., Dian M., Ferraresi C., Ruggeri M. “Comparison On Technological Opportunities For In-Vehicle Ethernet Networks“, IEEE INDIN 2013

Malaguti G., Dian M., Ruggeri M.,“Performance Comparison On Traffic Control Methods For In-Vehicle Ethernet Networks”, IEEE ICIT 2013

Dariz L., Ruggeri M., **Malaguti G.**, “A Proposal For Enhancement Towards Bidirectional Quasi-Deterministic Communications Using IEEE 802,15,4“, IEEE TELFOR 2013

Dariz, L. **Malaguti, G.** Ruggeri, M., “Performance analysis of IEEE 802.15.4 real-time enhancement”, IEEE ISIE 2014

Ruggeri, M., Ferraresi, C., Dariz, L., **Malaguti, G.** "A High Functional Safety Performance Level Machine Controller for a Medium Size Agricultural Tractor", SAE COMVEC 2014

Malaguti, G. Ferraresi, C. Dariz, L. and Ruggeri, M. "Augmented Reality Vehicle-Connected Apps for Diagnosis, Fault Recovery and Vehicle Maintenance ", SAE COMVEC 2014

14 Pubblications on Journals

Ruggeri M., **Malaguti G**, Dian M., "The future of heavy-duty networking", SAE OHE 2012

Ruggeri, M., Ferraresi, C., Dariz, L., **Malaguti, G.** "A High Functional Safety Performance Level Machine Controller for a Medium Size Agricultural Tractor", SAE IJCV 2014

15 **Malaguti, G.**, Ferraresi, C., Dariz, L., Ruggeri, M "Augmented Reality Vehicle-Connected Apps for Diagnosis, Fault Recovery and Vehicle Maintenance", SAE IJCV 2014