Journal of KOSSE. (2017. 6) Vol. 13, No. 2 pp. 9-17
DOI: https://doi.org/10.14248/JKOSSE.2016.13.2.009
www.kosse.or.kr

ISSN (print) : 1738-480X
ISSN (online) : 2288-3592

A Systems Engineering Approach to Real-Time Data Communication Network for the APR1400

Ahmad Salah Ibrahim, Jae-cheon Jung*

Department of NPP Engineering, KEPCO International Nuclear Graduate School

Abstract : Concept development of a real-time Field Programmable Gate Array (FPGA)-based switched Ethernet data communication network for the Man-Machine Interface System (MMIS) is presented in this paper. The proposed design discussed in this research is based on the systems engineering (SE) approach. The design methodology is effectively developed by defining the concept development stage of the life-cycle model consisting of three successive phases, which are developed and discussed: needs analysis; concept exploration; and concept definition. This life-cycle model is used to develop an FPGA-based time-triggered Ethernet (TTE) switched data communication network for the non-safety division of MMIS system to provide real-time data transfer from the safety control systems to the non-safety division of MMIS and between the non-safety systems including control, monitoring, and information display systems. The original IEEE standard 802.3 Ethernet networks were not typically designed or implemented for providing real-time data transmission, however implementing a network that provides both real-time and on-demand data transmission is achievable using the real-time Ethernet technology. To develop the design effectively, context diagrams are implied. Conformance to the stakeholders needs, system requirements, and relevant codes and standards together with utilizing the TTE technology are used to analyze, synthesize, and develop the MMIS non-safety data communication network of the APR1400 nuclear power plant.

Key Words : APR1400; MMIS; DCN-I; FPGA; TTE; Systems Engineering; Life-cycle

Received: November 18, 2016 / **Revised**: June 13, 2017 / **Accepted**: December 18, 2017

* 교신저자 : Jae-cheon Jung, jcjung@kings.ac.kr

1. Introduction

In nuclear industry domain. Ethernet switched networks are used to transfer data between digital control systems, software servers, engineering workstations, and information display systems at the main control room (MCR). The data communication network for information (DCN-I) is to interconnect the non-safety control and monitoring systems as well as transfer data from safety control and protection systems to the monitoring and information display systems. [1, 2]

For reliable monitoring of the plant functions and processes, DCN-I provides both periodic (real-time) and on-demand data transmission between the control and monitoring systems, and information display systems. TCP/IP is used as the communication protocol.

Original IEEE standard 802.3 Ethernet was not typically designed or developed for real-time data transmission, so that Ethernet protocols like TCP/IP, does not meet the requirements for establishing a real-time communication.

Regarding the most demanding need to ensure real-time data transmission of control systems, TTE is a communication architecture that deals with both event-triggered (ET) and time-triggered (TT) data traffic in the same communication system. The ET transmission is typically based on the existing standards of IEEE Ethernet networks, while the TT transmission is handled in temporal guaranteed communication where predictable real-time communication occurs utilizing the time scheduling features of TTE to transmit data frames. TTE data network utilizes the time-triggered protocol (TTP) to provide deterministic, real-time, and fault-tolerant data transmission. [5]

Most of data network architectures depend on Ethernet switched topologies that are comprised of bulky cabling and networking devices. FPGA is a digital semiconductor technology provides reconfigurable interconnections and on-chip communication capabilities introducing notable enhancements over conventional interconnections. Implementation of digital systems, using FPGAs, improves the flexibility, scalability and power efficiency of systems-on-chip (SoCs) compared to other designs.

The MMIS implements modern digital technology to monitor, control, protect, and display all equipment, functions, and processes associated with all modes of plant normal and abnormal operation conditions. The monitoring systems, including the Information Processing System (IPS) and the Qualified Indication & Alarm System-Non safety (QIAS-N), make information available to the plant operation staff both on periodic (real-time) and historical (non-real-time) bases. [1, 2]

Systems engineering approach is used to describe the life-cycle model of the design process. A. Kossiakoff et al, [4] describe the life-cycle as three successive stages, the first two stages, concept development and engineering development, about the developmental part of the life-cycle, while the third is about the post-development. In this paper, the concept development stage including three successive phases are discussed: needs analysis; concept exploration; and concept definition.

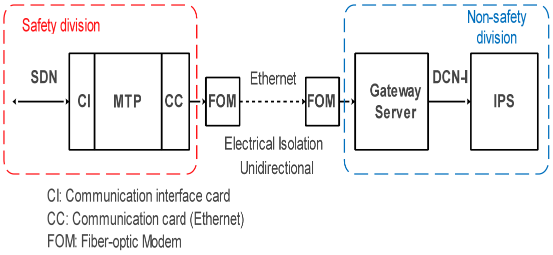
In this paper, the proposed TTE network is not a replacement for the existing Ethernet TCP/IP switched network, having its real-time characteristics, that is used for current MCR designs. The proposed design is to bring a proven technology that implemented in real-time applications (e.g., aerospace, railway, and automotive domains) to be implemented in the nuclear industry introducing a promising solution with high levels of determinism, scalability and flexibility for the future of real-time Ethernet networks.

This paper is organized as follows: Section 2 gives an overview of the current data communication networks used in the APR1400, specifically DCN-I network for the non-safety division of the MMIS system. The systems engineering approach in Section 3 introduces a life-cycle model for the concept development stage. The design methodology is given in Section 4, and paper is concluded in section 5.

2. APR1400 Data Communication Systems

This section describes how the data transmitted between the non-safety control and monitoring systems of MMIS. The DCN-I network is an Ethernet switched network, internetworking non-safety control systems, Engineering workstations (EWS), software servers, information displays, and peripherals. The DCN-I interfaces the Maintenance and Test Panel (MTP) of safety data network (SDN) via distributed control system (DCS) gateway server guaranteeing unidirectional data transmission from safety to non-safety systems using simplex fiber-optic cable. Figure 1 shows the data transmission from SDN to DCN-I. DCN-I interfaces the QIAS-N MTP via multi-channel DCS gateway server. [1, 2]

As mentioned above, the DCN-I integrates the data transmission from safety and non-safety control systems. TCP/IP is the communication protocol of DCN-I, providing an IEEE Standard 802.3 Ethernet and fast Ethernet (10/100 Mbps) networking communication via copper or fiber-optic cabling with the capability of interconnecting to the network peripheral devices (e.g., printers). [3]



[Figure 1] Data Communication from SDN to DCN-I

The IPS is to process, update and transfer the dynamic plant operating parameters information on the operator workstation (OWS) information flat panel displays (IFPD) and the Large Panel Display System (LPDS) at the MCR, based on operator demand.

DCN-I is redundant, but not physically separated and electrically isolated, so each control and safety system interface with the DCN-I via redundant communication paths, each internetworked system has two Ethernet network interfaces, such that a single failure in the communication path will not cause a total loss of data transmission capability between these systems and the DCN-I.

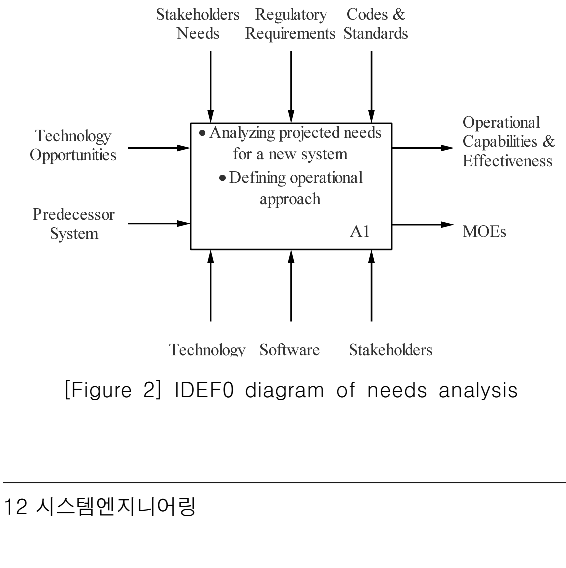
3. Systems Engineering Approach

System life-cycle [4] is defined as the stepwise evolution of a new system from concept through development and on to production, operation, and final disposal (e.g., decommission). In this paper, the systems engineering approach for the concept development stage of the life-cycle is discussed.

3.1 Need Analysis

The needs analysis phase defines the need for a new system to upgrade a predecessor system or exploit a technological opportunity. In this paper, needs analysis phase addresses the need to bring a new technology to the nuclear industry for establishing deterministic (i.e., predictable and repeatable) real-time data transmission between the non-safety systems of the MMIS. The current data network is based on the existing IEEE standard 802.3 Ethernet switched network using TCP/IP as the communication protocol. Response time, capacity latency, and transmission delays must be considered to meet the operational and performance requirements of internetworked systems; however, use of TCP/IP Ethernet networks may constrain the levels of performance that may be achieved because its response time does not meet that of real-time communication.

One of the most important measures of effectiveness (MOEs) is the interconnectivity; it is defined as the ability of data network to effectively transmit data to interconnected systems meeting their operational and performance requirements. Figure 2 shows the context diagram (IDEF0) for the needs analysis phase.



[Figure 2] IDEF0 diagram of needs analysis

3.2 Concept Exploration

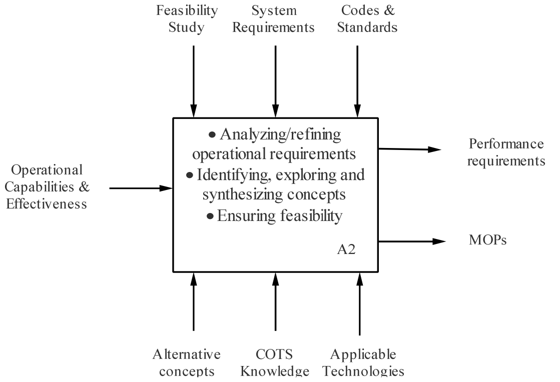
This phase is to explore ideas and technologies, examine potential alternative concepts that should formulate the performance requirements for the new design to meet the perceived need. Feasible approaches are explored to achieve such performance at an affordable cost, as Kossiakoff stated [4]. The objectives of this phase is to convert the operational requirements of the system into performance requirements to develop the system architecture.

In this phase, alternative networking architectures are studied and analyzed. Real-time Ethernet technology may be applied to DCN-I that provides both periodic (real-time) and on-demand (non-real-time) data transmission. Using TTP as the communication protocol, TTE technology combines the real-time and non-real-time traffic into one single network architecture with temporal guarantees for the TT messages. TTE distinguishes between two types of traffic; the standard ET traffic that is handled by the existing IEEE standards of Ethernet, and the TT traffic that is temporally guaranteed. The periodic data transmission through DCN-I is state-based (TT) not event-based (ET). State messages are transmitted with constant load, which increases utilization of the physical bandwidth but eliminates process related data overloads, while the event messages are transmitted only when necessary (on-demand), which has more efficient utilization of bandwidth but has probability for congestion and overload. Table 1 illustrates the characteristics of state and event messages. [5]

A TTE switch is used in the TTE communication system to handle the time-predictably TTE messages while continuing the support of standard Ethernet "commercial off-the-shelf"

<Table 1> State and event messages

Characteristic	State Message	Event Message
Temporal type	Periodic	Sporadic
Transmission	At least once	Exactly once
Sender access	Overwrite memory	Add to queue
Receiver access	Read from memory	Take from queue
Error detection	At receiver	At sender
Jitter	Minimal	Significant



[Figure 3] IDEF0 diagram of concept exploration

(COTS) without any modifications, but the Ethernet controllers for COTS Ethernet switches do not differentiate between TT and ET messages. To achieve the predictable temporal properties of TTE communication, TTE switch is implemented on an FPGA board introducing a TTE layer 2 switch has specific data frame format is different than that of standard Ethernet data frames. [6]

The measures of performance (MOPs) for this design are including but not limited to, real-time communication, deterministic response time, latency delays, fault-tolerance, flexibility, scalability, and data rates (bandwidth). Explanation of these MOPs is discussed in the next phase.

By applying the previous phase output to the input of this phase, the concept exploration phase can be identified using the IDEF0 context diagram shown in Figure 3.

A set of candidate concepts is available for the evaluation and decision-making processes to meet the stakeholders' needs and system operational requirements. Tables 2 and 3 show SWOT (strength, weakness, opportunity, and threat) analyses for these alternative concepts.

3.3 Concept Definition

This phase selects the preferred concept for architecting the new design. The concept to be selected among alternative concepts is to meet the perceived needs, and operational and per-

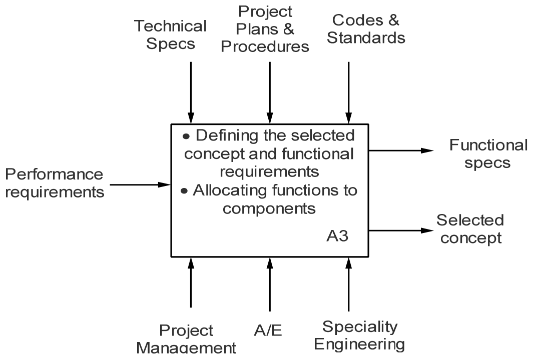
<Table 2> Ethernet network protocol SWOT analysis

Network Protocols	Strength	Weakness	Opportunity	Threat
TCP/IP	Experienced for data networking	Longer response time	COTS marketing	Decrease network reliability

TTP	Determinism;
	Fault-tolerance;
	Scalability
		Inexperienced for nuclear domain	Proven; Simple implementation	Difficulty of V & V

<Table 3> Ethernet switch platform SWOT analysis

Ethernet Platform	Strength	Weakness	Opportunity	Threat
Standard COTS	Compatible to existing IEEE standards	Increase of long-run cost	Upgradeable	Vulnerability to Cyber-attack
FPGA-based	Reconfigurability, Listenability, Invulnerability	Inexperienced for nuclear domain	Cost effectiveness; High reliability; Long lifespans	Radiation effect on volatile SRAM FPGA



[Figure 4] IDEF0 diagram of concept definition

formance requirements. Also the preferred concept is to achieve such a feasible performance at an affordable cost (i.e., cost-performance ratio). Developing an FPGA-based TTE switch is to meet the need for real-time deterministic data transmission and achieve the balance between performance and cost. The output from this phase is two perspectives on the same system; a set of functional specifications that describe the exact functions of the new system design, and the selected concept. Figure 4 shows the context diagram for this phase.

Regarding the selected concept in this study, TTE combines the fault-tolerance (multiple redundancy) and real-time characteristics of TT data transmission providing deterministic communication, with the high flexibility characteristics of legacy Ethernet communication, this combination allows conventional PCs, office devices, multimedia systems, and real-time systems to be interconnected to the same network, providing a TTE network that is compatible to standards like IEEE Ethernet 802.3. [7]

Scalability of TTE technology allows development of fail-safe applications (i.e., high-safety systems that must reach a safe state in case of failure), or fail-operational applications (i.e., high-availability systems that must remain fully functional even if a failure occurs).

TTE operates on the Open System Interface (OSI) model layer 2, *Datalink Layer*, and can support any physical layer that provides constant communication latencies for the data transmission. Wireless does not support TTE because signal strength affects the data rates). Also it is expected to provide data rates (bandwidth) meeting the system performance requirements.

TTE exchanges the traffic by guaranteeing the temporal behavior (i.e., predictable time delays) of the TT messages. The duration of message transmission, over the TTE network, depends on the category of data transmission (i.e., TT or ET). Standard Ethernet (ET) messages are transmitted in those time intervals where the communication for real-time (TT) messages is not required. In order to avoid Ethernet traffic interferes the temporal properties, TT messages always preempt all ET messages.

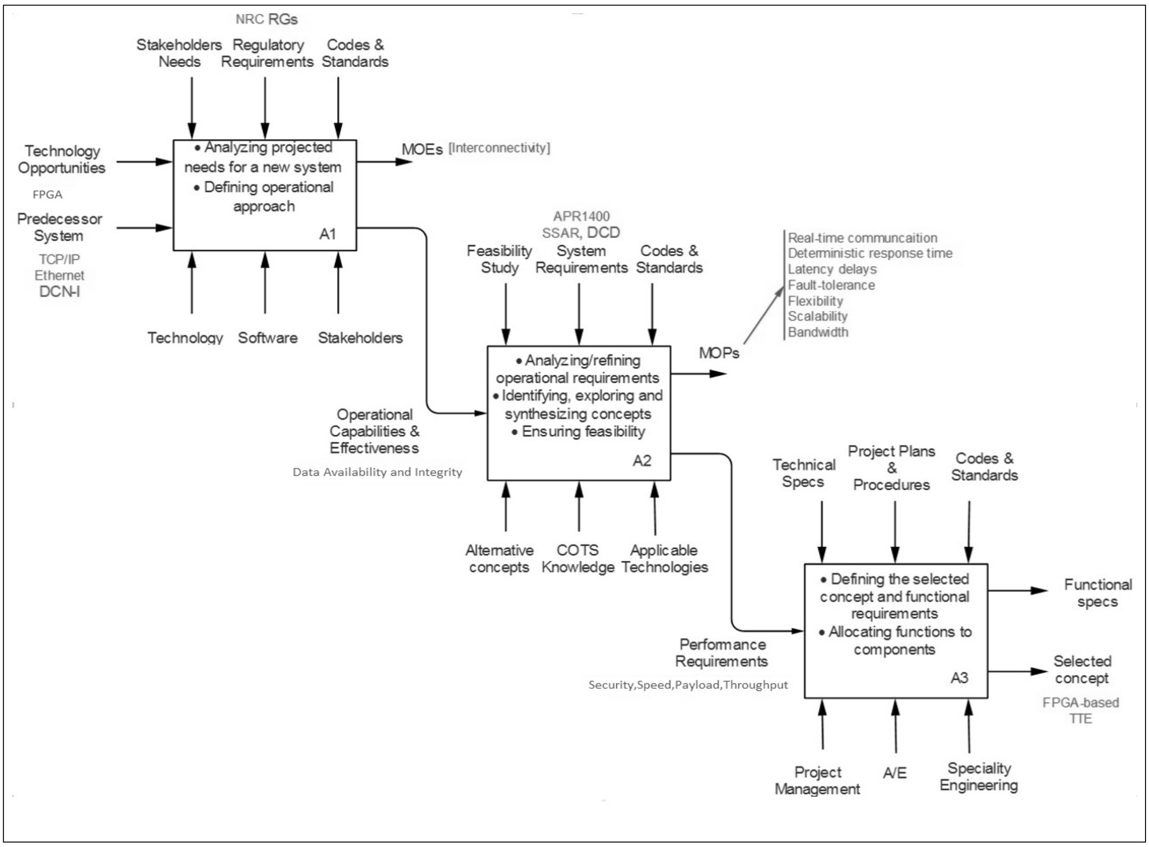
FPGA is used to implement TTE controllers, Obermaisser [8] and Zurawski [9] stated that the diversity of FPGA-based TTE solutions mainly depends on the transmission speed (data rates) they support.

TTE switch provides full duplex (bidirectional) point-to-point links to the internetworked devices.

As a conclusion for the systems engineering approach, Figure 5 shows the context diagram for the concept development stage.

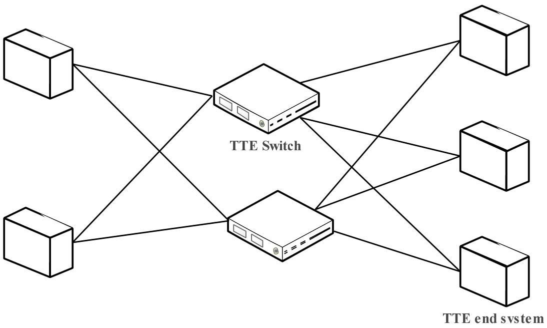
4. Proposed Network Architecture

As mentioned above, TTE supports full duplex communication. Star topology configuration with one, two, or three channels is possible. Com-



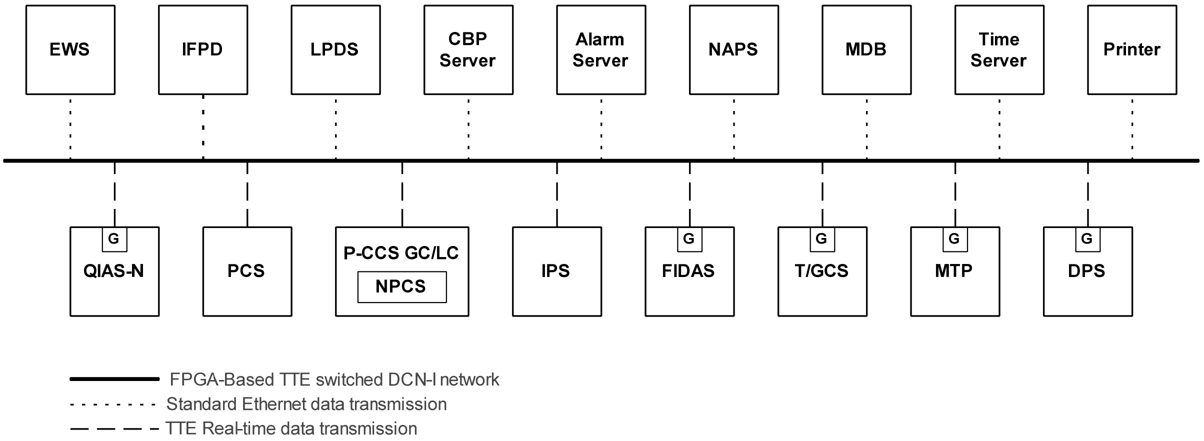
[Figure 5] IDEF0 Level 1 context diagram of concept development

munication channel in TTE star topology identifies the physical connection between any two TTE end systems with the TTE switch. Each device connected to the DCN-I has two NICs (network interface cards), so that implementing a TTE star topology configuration with dual channel is to ensure the network redundancy. In this case, the sending TTE end system transmit identical copies of the TT traffic over the two redundant channel, and the receiver will pass over only one copy of the redundant data frames. Figure 6 shows the TTE star topology with dual channel.



[Figure 6] TTE star topology with dual channel

TTE provides deterministic real-time data transmission to the non-safety control and monitoring systems connected to the DCN-I network. Various workstations, software servers, soft control commands, data acquisition from remote networks, and other network peripheral devices may internetworked via IEEE standard 802.3 Ethernet TCP/IP protocol where the non-real-time data transmission is not required (i.e., on demand transmission). Figure 7 illustrates the proposed FPGA-based TTE switched DCN-I network.


EWS
IFPD
LPDS
CBP Server
Alarm Server
NAPS
MDB
Time Server
Printer
G
QIAS-N
PCS
P-CCS GC/LC
NPCS
IPS
FIDAS
T/GCS
MTP
DPS
FPGA-Based TTE switched DCN-I network
Standard Ethernet data transmission
TTE Real-time data transmission

[Figure 7] Illustration of FPGA–based TTE switched DCN–I network

5. Conclusions and future work

The FPGA–based TTE switched DCN–I network is developed in this work using the systems engineering approach. In this work, the design methodology is conducted through the concept development stage of the life–cycle model, this simplified the analysis and synthesis of stakeholders needs, and performance requirements, and development of the new design. Selecting the MOEs and MOPs for the proposed design is to formulate the operational and performance requirements that meet the stakeholders needs.

TTE technology is to provide real–time data transmission for maintaining reliable monitoring and control processes of plant operation. Time–Triggered Ethernet provides two types of traffic, the TT traffic for real–time communication, and the ET traffic which is compatible with the existing standards of IEEE Ethernet.

Developing a TTE data network, based on FPGA–based switches, introduces a scalable, deterministic solution with fixed latencies. The proposed design introduces a future solution to utilize FPGA on–chip communication technologies for real–time systems where the transmission time scheduling is needed.

The future work will focus on the testing process for the proposed design by simulating the network architecture and verifying the design measures according of the functional and performance requirements such as throughput, payload, and cybersecurity robustness comparing with the current design performance, specifically those measures related to execution time and network complexity.

Acknowledgements

This work was supported by the 2016 Research fund of the KEPCO International Nuclear Graduate School (KINGS), Republic of Korea.

References

1. Korea Hydro & Nuclear Power Co, Ltd, Standard Safety Analysis Report for APR1400, Chapter 7, Instruments and Controls, 2002.

2. KEPCO/KHNP, APR1400-K-X-FS-14002-NP, Apr1400 Design Control Document Tier 2, Chapter 7 Instrumentation and Controls, December 2014.
3. Jae-cheon Jung, Information Processing System for APR1400, lecture notes, KEPCO International Nuclear Graduate School.
4. A. Kossiakoff et al, Systems Engineering Principles and Practice, Second edition, John Wiley & Sons, 2011.
5. H. Kopetz et al, The time-triggered Ethernet (TTE) design, Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2005.
6. K. Steinhammer et al, A Time-Triggered Ethernet (TTE) Switch, Proceedings of the Design Automation & Test in Europe Conference (Volume:1), 2006.
7. A. Ademaj, Time-Triggered Ethernet - A Powerful Network Solution for Multiple Purpose, TTTech whitepaper, https://www.tttech.com/
8. R. Obermaisser, Time-Triggered Communication First edition, CRC Press, 2011.
9. R. Zurawski, Industrial Communication Technology Handbook, Second edition, CRC Press, 2014.