DETERMINISTIC ETHERNET – HIGH-SPEED COMMUNICATION WITH REAL-TIME GUARANTEES

Mirko Jakovljevic, TTTech Computertechnik AG, Vienna, Austria
Markus Plankensteiner, TTTech Computertechnik AG, Vienna, Austria

Abstract

Currently, IEEE802 Ethernet standardization is creating a deterministic networking solution for a broad range of high-volume applications including automotive in-vehicle communication and factory automation. New deterministic Ethernet capabilities are based on time-multiplexed bandwidth sharing and defined in the IEEE802.1 TSN (Time-Sensitive Networking) task group. These capabilities enable the design of different classes of industrial and transportation systems and advanced integrated architectures communicating over a single switched Ethernet infrastructure. Together with other industry–specific open standards implemented in network devices, deterministic Ethernet solutions can be designed to satisfy real-time and reliability communication requirements for industrial applications which were constrained by isolated or proprietary networking solutions in the past.

With increasing requirements on high availability, safety, and fail-operational system performance, the network becomes a core component of an embedded platform and determines, and sometimes limits, platform performance and capabilities. Therefore Deterministic Ethernet can be considered a core technology for the design of advanced integrated systems with both synchronous and asynchronous communication. Deterministic full-duplex switched Ethernet networks with time-driven communication capabilities support hard real-time communication, robust synchronization, time-sensitive traffic shaping and policing, and time-partitioning of the network bandwidth. Integrated systems designed with Deterministic Ethernet can host critical and non-critical, or soft-time functions. This enables the design of open and closed systems with critical and hard-real time distributed functions.

Introduction

Asynchronous packet-switching communication is considered non-deterministic, and it supports a limited number of use cases with real-time communication performance. Therefore special network profiling solutions or adaptations of Ethernet were designed to satisfy industrial real-time communication requirements in the past.

Switched full-duplex Ethernet has been present in industrial applications for more than 15 years, and has experienced progressive growth over the last 7-8 years. There are a number of real-time networking technologies which are similar or somewhat compatible with Ethernet, but in many industrial applications, widely available standard Ethernet components can be used with modified TCP/UDP layers and real-time middleware. For motion drives and other kinds of fast hard real-time controls, more capable (and significantly modified) industrial Ethernet variants are deployed. EtherCAT [1] and SercosIII [2] are defined around Layer 1-compatible Ethernet modifications. Industry-specific Layer 2-modifications are implemented in Profinet IRT [3]. Layer 2 add-ons are provided in ARINC664 [4] and SAE AS6802 [5] for critical infrastructure and embedded applications in the aerospace industry. Profinet RT [6], Ethernet Powerlink [7] and Ethernet/IP [8] add higher layers to differentiate and profile a network for real-time applications.

With increasing adoption of Ethernet as a real-time networking technology and growing awareness that time-sensitive networking has a major part to play in our interconnected world, new Ethernet standards are being defined in IEEE802. IEEE TSN (Time-Sensitive Networking) represents a set of standards which extend Ethernet for use as an industrial-grade real-time communication protocol, with building blocks including synchronization, time-based message handling, seamless redundancy, and frame preemption.

The key players behind the IEEE TSN standardization include IT/networking, telecom, automotive, and industrial OEMs, as well as all major semiconductor companies. Therefore it can be safely assumed that such industry support for this standard will lead to a broad availability of components from different suppliers and affordable pricing for networking solutions. The first announced components in the market with the latest IEEE TSN functionality are NXP SJA1105 chip (announced Dec 2014 [9]) and TTTech's Atlas DE8301 (sampling March 2015, announced June 2015 [10]). The latter also implements SAE AS6802 fault-tolerant clock synchronization and robust partitioning architecture to enable certifiable design of fault-tolerant and highly available systems. The list of deterministic Ethernet standards implemented on Atlas DE8301 is shown in the Figure 1, and includes IEEE 802.3, IEEE 802.1, IEEE TSN, IEEE AVB and SAE AS6802 services.

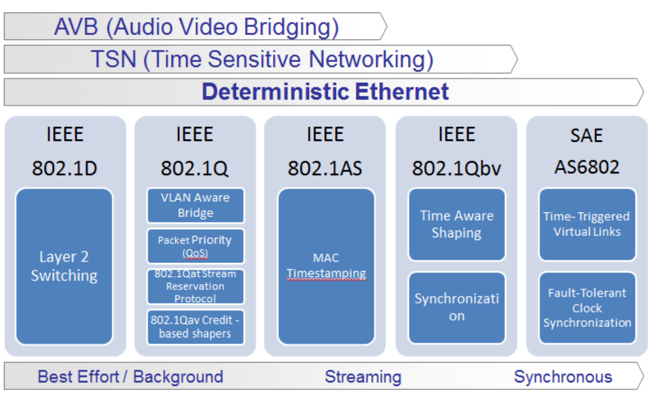

Figure 1. Deterministic Ethernet Protocols implemented on TTTech Atlas DE3801 Switch

Deterministic Ethernet and IEEE TSN

IEEE TSN offers a number of mechanisms [12] , [13] which provide time-aware shaping of unicast and multicast datastream with end station and switch/router synchronization. This standard adds a synchronous communication capability for asynchronous packet-switched Ethernet networks, while keeping full compatibility with VLANs and past asynchronous AVB developments. The core element in IEEE TSN is defined by IEEE 802.1Qbv, whose PAR (project authorization request) references SAE AS6802. IEEE 802.1Qbv describes time-aware shaping, driven by the world clock or system time.

Ongoing standardization efforts in IEEE TSN focus on robust timing and redundancy management support similar to AFDX or PRP standards. IEEE TSN recently included proposals for shaping and policing, with a support for periodic end station frame transfers.

With further development of the IEEE TSN related set of standards, it might be possible to mimic real-time communication performance and some of the safety-related features provided by the combination of both ARINC664 and SAE AS6802, which are applied in critical aerospace applications.

Synchronous/asynchronous communication in packet-switched Ethernet networks

By mixing both asynchronous and synchronous communication, all "variants" of communication determinism are viable. Asynchronous communication supports the relaxation of timing constraints, while synchronous communication allows audio/video and hardreal-time controls to operate in one system together with less critical functions (e.g. map or vehicle health-monitoring data upload). In addition, this approach can support any type of design paradigm and remove technological limitations to system architecture design.

The key benefit of synchronous communication lies in the deterministic resource sharing without interference for a larger set of hosted functions. This allows exact calculation of system performance.

Use Cases for Deterministic Ethernet

IEEE TSN as an off-spring from IEEE AVB extends initial audio/video bridging requirements to any type of real-time and time-sensitive system, and goes beyond the audio and video markets, to focus on high volume automotive and industrial applications. The objective is to accommodate the needs of different models of computation and communication, and enable periodic and transient deterministic communication.

Types of functions hosted on advanced integrated systems

Figure 2 shows a generic set of integrated functions which include functions with various performance and resource requirements (see Figure 2):

- periodic real-time controls (up to several kHz - sample rate)
- data streaming (continuous diagnostics, periodic multimedia streams …)
- transient alarms, safety functions with guaranteed response time in 100s of microseconds to milliseconds
- sporadic soft-time applications (maintenance, updates, inspections, and event driven applications executed in sporadic manner)

Transient and event-driven alarm and protection functions have guaranteed deterministic performance with maximum latency, when triggered by some special critical system event and transients.

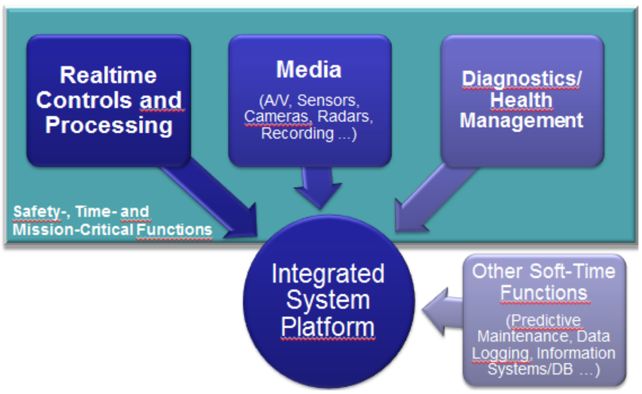

Figure 2. Application types integrated in embedded clouds

Both event-driven and time-driven controls can be integrated without unintended mutual interdependencies in one integrated systems, which simplifies transitions of software functions from automotive domain to new integrated infrastructure. In parallel all other non-critical functions can be hosted and utilize the system resources whenever those embedded resources are not used by critical functions.

Low-latency communication

The objective of low latency communication is to support the design of linear architectures with fast control loop response. In combination with accurate end system synchronization this can lead to improved real-time response and minimized embedded system resource use. Frame preemption can be useful for simpler low-latency applications and critical alarms, and it can optimize network bandwidth use for critical and non-critical traffic. The downside is that this mechanism may significantly increase the complexity and reduce diagnostic capability in those advanced integrated systems which mix different types of network traffic.

The IEEE TSN standard which supports this specific aspect of real-time communication is defined in IEEE 802.1Qbu and IEEE 802.3br (Interspersing Express Traffic).

Another useful service proposal is described in 802.1Qch to support cyclic queuing and forwarding, which can further minimize application-to-application latency in an integrated system. This amendment is in the approval process.

Hard real-time communication with defined temporal boundaries

Time-aware shaping in conjunction with time-synchronization and time-sensitive policing can support defined temporal performance for configured datastreams. 802.1Qbv (time-aware shaping and enhancements for scheduled traffic), 802.1Qbu (frame preemption), and 802.1ASbt (time synchronization improvements) support hard real-time communication with defined temporal boundaries.

As the synchronization represents the cornerstone of time-triggered and time-driven communication, IEEE TSN depends on its quality and robustness. Deterministic Ethernet supports all IEEE1588 transparent clock forwarding and robust SAE AS6802 system time synchronization used in critical aerospace applications.

Integrated systems and vehicle architectures

In order to support simplified design of redundant architectures, IEEE802.1CB is defined. This standard amendment allows the identification and replication of frames for redundant transmission. This capability can be useful for design of redundant, highly available and fault-tolerant systems. There are also industry mechanisms which can be implemented on deterministic Ethernet switches to support similar capabilities for switched and linear architectures. PRP (parallel redundancy protocol) and HSR (high-availability seamless redundancy) defined in IEC62439-2, are used for different industrial applications such as energy production and transmission. In addition to IEEE TSN, industrial networking products for deterministic Ethernet can also support different open standards defined in IEC, IETF, SAE and other standardization bodies to satisfy specific industry niche requirements.

Flexibility and Scalability

IEEE TSN enables the definition of critical datastreams, and stream reservation protocols such as IEEE802.1Qca and IEEE802.1Qcc enable simple reservation of bandwidth, assuming that the requested resources are available. This feature can be interesting for distributed functions, which try to connect and access different resources ad hoc, or subscribe to data publishers, such as audio or video or sensors.

In the majority of integrated systems, critical control traffic is planned in advance, with careful considerations on used resources and data paths, so this data can be also provided or calculated by special centralized services or off-line design tools.

Cross-industry applications for Ethernet-based Integrated Systems

Industrial automation with OPC UA (IEC 62541) can profit from Deterministic Ethernet as it expands its client-server architecture, with a publisher-subscriber model with unicast and multicast communication capability. Deterministic Ethernet with IEEE TSN will provide the quality of service at network layer, which is a prerequisite for deterministic control loop performance and integration of deterministic real-time datafows. This enables the definition of integrated embedded platforms consisting of open technologies, which can support seamless integration of different functions without interference and with hard real-time performance.

Real-Time IoT (Internet-of-Things) can be seen as a future-oriented concept which requires virtualization mechanisms similar to an embedded cloud or integrated modular architectures. The number of end stations in this case can be in thousands or more. Key potential markets are smart factories, smart cities, public transportation control and smart grid – large scale applications with deterministic performance and defined latencies, which can be exposed to resource starvation and denial-of-service attacks. As usual, robust integration of open and closed systems is essential for the operation of such systems, and requires system-wide time-partitioning of embedded computing and networking resources.

The automotive industry with its sheer volumes, new advanced capabilities (active safety, ADAS, autonomous driving), new safety standards ISO 26262 and architecture optimization potential, can become the leader in domain of integrated modular vehicle architectures, assuming the cost of Ethernet-enabled computing and networking devices, and physical layers becomes competitive. Such integrated architectures can lead to a significantly smaller number of ECUs, less wiring and a total reduction of vehicle E/E architecture costs. With close to 100Mio vehicles built yearly, there is a large potential to minimize overall fleet costs for future cars with advanced functions and significantly reduced number of ECUs. Currently, Ethernet plays a side role (diagnosis) for automotive architectures and penetrates into car multimedia and ADAS, but it can significantly change the way how car architectures are built in the future. Vehicle E/E architecture will need to evolve over the next 10-20 years due to new functions and related cost optimizations. Traditionally, the automotive industry uses event-driven and time-driven real-time traffic which optimize resource use. This is essential as unused processing power and network bandwidth mean higher component costs and this is not acceptable in this highly competitive high-volume industry!). Therefore both synchronous and asynchronous communication shall be supported.

Promising studies and evaluation of integrated modular railway controls relying on this concept are targeted by OEMs and EU programs [11]. Based on initial developments in integrated systems for the railway industry, it seems that rolling stock architectures are the most promising use case given the decades of safety experience and digital integration with WTB and MVB standards. Currently the less critical functions are integrated via Ethernet networks for SIL2 and non-critical functions, but there is a clear intention in Europe, USA and Asia to develop fully integrated next generation Ethernet-based systems, which can integrate many safety functions up to SIL4, and thus minimize system lifecycle costs and operational expenses. Integrated architectures with deterministic Ethernet seem to be the only viable approach to overcome complexity challenges in this domain. Physically, such optimized architectures cannot be built by using asynchronous models of computation only, and need to also deploy synchronous communication to accommodate open and closed system functions.

The energy industry is deploying IEC61850, which represents a clear step toward integrated embedded platforms and relies on standard switched Ethernet with VLANs and its adaptations described in GOOSE, and PRP/HSR to establish a solution to integrate critical alarm functions and controls in one system. Typically systems consist of fifty to several hundred end-stations (or IEDs) in substation automation. Such systems have been deployed for the last 10 years and their number is steadily growing. While this industry is not dealing with explicitly safety-critical functions, the loss of function can lead to huge direct damages and societal challenges. There are also niche use cases for energy generation systems, which mandate structural system optimizations, which in turn can require additional safety nets on the embedded platform side. With increasing requirements on safety and availability, distributed grid may require capabilities which are closer to existing aerospace and future automotive or railway vehicle architectures. In the future, existing mechanisms for system integration and architecture design may turn insufficient for system-level optimization. Embedded platforms for embedded cloud computing can remove existing restrictions and simplify design of complex energy and substation systems.

The aerospace industry can fulfill all next-generation integrated architecture (IMA2G) requirements by using a set of technologies proposed in [14], and one of key requirements is to support synchronous models of computation and communication. In addition it is possible to expand the perimeter of IMA systems and integrate other cabin [15] and power distributed power control function [16].

With Deterministic Ethernet embedded clouds can, in terms of scalability and reconfigurability, go beyond the objectives of future IMA 2G avionics systems. Indeed it can more flexibility and better support design of reusable, generic and open architectures. This can be useful for design of integrated cross-industry and open Internet-of-Things (IoT) applications which integrate critical applications.

Cross-industry experiences with deterministic Ethernet in safety-relevant application

From the perspective of embedded computing and design of advanced integrated architectures, it must be noted that aerospace industry can emulate the equivalent capabilities incorporated in IEEE TSN/AVB by using a combination of ARINC664 and/or SAE AS6802 standards. For critical applications it is required to define a “white box” network device design in compliance with DO254, DO178, ARP4574/4761 and DO-297 standards, and guarantee isolation of critical datastreams forwarded within the switch.

Also any timing mechanisms in time-driven systems shall be certifiable and offer a formal proof of correctness. Standard ASSP and ASIC components implementing fault-tolerant synchronization, BIST mechanisms, built-in COM/MON and watchdog mechanisms and white-box design can add value to fault diagnostics/detection and high-integrity design. This ensures high certainty that the system faults will be detected and appropriately handled.

Deterministic data streams with defined QoS

Asynchronous Ethernet communication can support determinism which limits maximum latency for defined data flows, while synchronous Ethernet communication enables defined jitter, message order and fixed latency.

Synchronous communication does not rely on statistical probability of message delivery, but on exactly defined transmission instants relative to common time (Figure 3). The behavior of the system can be defined to follow exact schedules with microsecond jitter and minimize latency. The latency minimization is possible as there is no need for extra margin which is reserved for statistical uncertainties emerging from the lack of synchronization in the system.

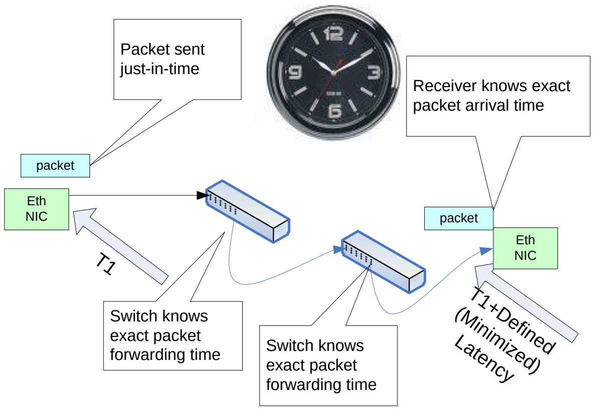

Figure 3. Fixed end-to-endsystem latency and microsecond jitter for synchronous data flows in deterministic systems

In synchronous data flows with accurate periodicity, definition for critical streams will be controlled with a microsecond jitter and all data streams will have exact latency. In synchronous systems, asynchronous streams can be packed on top of synchronous networks such as SONET to provide guaranteed bandwidth for specific functions and applications. In other cases end systems use global timebase and stick to a specific temporal communication schedule.

In standard Ethernet, some level of partitioning is achieved by statistical multiplexing and creating virtual LANs, which limits the bandwidth for broadcast messages and reduces the impact on otherwise unrelated distributed functions. However the traffic relies on probabilistic communication and remains a best effort communication. So there are no guarantees that mixed criticality operation is possible except for a very limited class of applications and systems with significant bandwidth overprovisioning.

Under such conditions any modification or upgrade can impact the overall system performance and make system design and integration more complex. By adapting IEEE802.3 and adding bandwidth partitioning and control mechanisms, mentioned limitations can be avoided. Therefore policing and shaping with scheduling are essential for the design of predictable dataflows.

While closed systems can be designed with both synchronous and asynchronous traffic, only the presence of synchronous traffic in the system enables the integration of critical functions/traffic with other arbitrary Ethernet traffic in open systems. In case the communication bandwidth control and partitioning is based on statistical multiplexing and control of the bandwidth use, the availability of appropriate bandwidth margin and the good understanding of traffic loads within the system is required.

For synchronous Ethernet dataflows, the bandwidth partitioning relies on the robustness of master clocks and their selection. In critical system design, it is essential that the global time base is distributed and tolerant against one or multiple faults. Based on the availability of the global time and predefined schedule for critical functions, the latency, jitter and determinism will always be guaranteed for time-triggered messages. Temporal behavior will be policed by the switch, while the traffic shaping is provided per default by end systems based on global time base.

Robust partitioning at network device level

An Ethernet switch is active component, which can influence the operation of many functions in the system. Therefore it is essential to have a well-understood internal switch structure and architecture with verified communication performance limitations and partitioning mechanisms to guarantee independent processing of all critical data flows in the system. Some sort of design process evidence shall be available to support design of safety-relevant integrated systems and prevent the interference among datastreams passed through the switch. In opposite, the prevention of the interference in network communications is guided by the configuration, robust synchronization, protocol mechanisms and fail-silent device design. Fail-silent network device design can be seen either as a system or device implementation feature, depending on the used device implementation. It prevents malign failure scenarios, and thus simplifies and enables the design of high-integrity and fault-tolerant systems.

Robust fault-tolerant synchronization

In order to establish coordination among application-level functions, the alignment and synchronization is required either at the network, middleware or application layer. In some cases it is combined at different layers at once, and this does not contribute to clean and unambiguous behavior of systems – actually it expands the complexity of interface behavior and system state explosion. If the functional coordination (or "synchronization") is pushed toward higher layers closer to application software, definition of key system interfaces will be influenced by many complex and hard to control interrelations. This is a result of multiple interface properties set at different layers, and incomplete or ambiguous specifications or design data.

In general, asynchronous design may increase the probability of race conditions, deadlocks and other unintended system behavior. As a result, key system interfaces can be more complex to describe. Also, changes and modifications would require more effort to verify, and can create additional integration challenges

Depending of the use case and application domain, different approaches to system synchronization can be selected, as the IEEE802.1ASbt allows different synchronization approaches. IEEE1588 / IEEE 802.1AS-based synchronization or SAE AS6802 fault-tolerant synchronization can be selected for IEEE TSN networks, in network devices with such protocol services and configuration options.

Robust methodology for network design and tool verification

Scheduled traffic requires network engineering and solid methodology and processes. For certifiable integrated architectures and systems, the design methodology is essential for design and verification of different network configurations.

TTTech provides tools for design of complex deterministic networks. They are based on network calculus and trajectory calculus [17], [18] and support worst case calculation for all critical data streams in the system.

Conclusion

Deterministic Ethernet with IEEE TSN can be considered a strictly deterministic networking technology which can handle asynchronous and synchronous traffic. Deterministic Ethernet components incorporating IEEE TSN can solve the majority of system integration challenges for time-, safety- and mission-critical systems. IEEE TSN, as a set of protocol amendments to IEEE802.1Q will expand the perimeter of possible applications and use cases for standard IEEE802 Ethernet components and enable the design of advanced vehicle and factory automation systems.

The application of Ethernet in critical infrastructure and safety-relevant embedded systems will depend on the robustness of network device implementation and the selection of protocol and synchronization mechanisms implemented on the network device. Network engineering methodology is considered essential for the design of complex IEEE TSN-based systems and applications, and verification tools are required to simplify the design of complex networks.

With new time-triggered communication capabilities, real-time communication in Ethernet networks will become a commodity for cross-industry applications, and the differentiators in defining the embedded solution will shift toward embedded platform design, middleware, design/verification/analysis tools and certification methodology.

Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080.

The authors would like to thank to Georg Stoeger and Simon Brooks for their valuable comments and suggestions to improve the quality of the paper.

References

[1] EtherCAT, http://www.ethercat.org/default.htm

[2] SercosIII , http://www.sercos.de/

[3] Profinet IRT, PI Organization http://www.profibus.com/technology/profinet/

[4] ARINC664 , http://www.aviation-ia.com/cf/store/catalog_detail.cfm?item_id=1270

[5] SAE AS6802, http://standards.sae.org/as6802/

[6] Profinet RT, , PI Organization http://www.profibus.com/technology/profinet/

[7] Ethernet Powerlink, http://www.ethernet-powerlink.org/

[8] Ethernet/IP, https://www.odva.org/Home/ODVATECHNOLOGIES/EtherNetIP.aspx

[9] Thomas Suermann, Steffen Müller, "Power Saving in Automotive Ethernet", NXP Semiconductors, AMAA 2014, June 2014 http://www.amaa.de/previous-conferences/amaa-2014/presentations-2014/AMAA201406PowerSavinginAutomotiveEthernetNXPMueller_Steffenv1.2.pdf

[10] TTTech Atlas DE8301 – Deterministic Ethernet, https://www.tttech.com/de/products/industrial-energy-railway/deterministic-ethernet-switches/switch-chips/de-switch-chip-atlas/

[11] European Commicssion (EC), Shift2Rail EU Project, http://ec.europa.eu/research/press/jti/factsheet_s2r-web.pdf

[12] Wilfried Steiner, Norm Finn, "IEEE 802.1 Audio/Video Bridging and Time-Sensitive Networking", Industrial Communication Technology Handbook, Second Edition (Zurawski), CRC press, Aug 26, 2014, ISBN 9781482207323 https://www.crcpress.com/product/isbn/9781482207323

[13] IEEE Time-Sensitive_Networking (TSN) http://en.wikipedia.org/wiki/Time-Sensitive_Networking

[14] M. Jakovljevic, A. Ademaj, C.C. Insaurralde, "Embedded cloud computing for critical systems", Proceedings of 33rd IEEE/AIAA DASC Conference, Oct 2014, Colorado Springs, CO

[15] J. Gatard, M. Jakovljevic, "Embedded Cloud and Critical Systems: Technology Baseline and Architecture Patterns", Proceesings of AST 2015 Conference, Hamburg, Feb 24, 2015

[16] J. Gatard, M. Jakovljevic, "Advanced Embedded Data Platforms for Distributed Power Management", Proceedings on European Conference on More Electric Aircraft, Toulouse, February 3-5, 2015

[17] TTTech, "AeroQ - DO-330 Qualified Tool For Analysis and Formal Verification & Validation of Aerospace Networks", website https://www.tttech.com/products/aerospace/development-test-vv/verification-tools/aeroq/

[18] Craciunas S.S.; Oliver, R.S.: "SMT-based task- and network-level static schedule generation for time-triggered networked systems", to be published in 22nd International Conference on Real-Time Networks and Systems, Versailles, France, October 8-10, 2014