Next-Gen Train Control / Management (TCMS) Architectures: "Drive-By-Data" System Integration Approach

Mirko Jakovljevic, Arjan Geven, Natasa Simanic-John, Derya Mete Saatci

Next-Gen Train Control / Management (TCMS) Architectures: "Drive-By-Data" System Integration Approach

Mirko Jakovljevic, Arjan Geven, Natasa Simanic-John, Derya Mete Saatci,
TTTech Computertechnik AG, Vienna, Austria
Bernd Loehr, Newtec, Mannheim, Germany

Abstract

Based on the European railway industry objectives in the scope of Shift2Rail EU program [1], the work conducted in Safe4Rail (Q4/2016-Q4/2018) [2] proposes a unified embedded platform framework and drive-by-data system integration for the definition of scalable embedded architecture which can integrate critical and non-critical rolling stock / TCMS functions.

The proposed architecture enables integration with other railway transportation systems and similar to aerospace IMA, relies on common computing and Ethernet networking resources. The ultimate objective is to create an integrated infrastructure which can host all hard RT, real-time and soft-time functions, and support different models of computation and communication. Such an integrated architecture will reduce lifecycle costs and system complexity of railway TCMS architectures.

The key challenges in next generation TCMS are: affordability, complexity, modular certification, frequent dynamic reconfiguration, and the capability to host distributed safety-critical functions.

We consider the outcome of this work to be relevant for any future highly integrated and reconfigurable parameter-driven architectures, which requires high levels of software abstraction with support for incremental certification, and rely on new advanced networking approaches related to IEEE TSN, while using the experiences from ARINC 664 and SAE AS6802 standards. The Safe4Rail architecture addresses both safety and security aspects of the embedded platform, and may result in new standards for railway Ethernet networking, including the modifications proposals to IEC61375 [3].

Introduction

Due to specific structural industry constraints (e.g.: national standardization and regulation fragmentation, market and solution fragmentations, and system complexity) and long development of system lifecycles for "service-proven" solutions, railway transportation systems have suffered from a limited adoption of novel technological advancements in electronic hardware and software, communication networks and embedded computing. This still is a hindrance for new business models, innovation and the competitiveness of the European railway industry. The development of new technology and architectural concepts in other transportation industries have led to significant and fast progress in safety, security and in the integration of new functions. While the aerospace industry has introduced new modular avionics architectures [4, 5], the automotive industry continues work on similar developments regarding system integration [6], software platforms [7] and sensor fusion via integrated safety-relevant embedded platforms which accelerated since 2010 with new ADAS (advanced driver assistance systems) platforms and new safety regulations. To achieve similar industry developments in railway systems and take advantage of cross-industry synergies, the Shift2Rail JU multi-annual action plan [8] has given high priority to create a specification that addresses the most common issues hindering the rolling stock efficiency, system optimization and interoperability within the European railway industry.

The system-level high-level requirements for next-generation TCMS are denoted in eight pillars that are related to the different functional and non-functional aspects of an integrated modular platform that hosts safety-critical and non-safety-critical functions. Key objectives are to:

- **simplify integration and hosting** of many functions on common computing and hardware resources to reduce physical system complexity, and to minimize lifecycle costs for design, integration, V&V, testing, maintenance, upgrades, modifications, extension, incremental certification, modernization and reuse.
- enable highly available and highly reliable integrated platform as a "distributed fault-tolerant embedded computer" in order to serve and host the TCMS functionality
- enable integration and hosting of all TCMS and other brake-by-wire, signaling, safety line, and non-critical applications on a platform operating as an embedded cloud of resources, without affecting critical functions
- support the **integration of all critical and non-critical functions** relevant for train operation,

including functional, performance, safety, security, availability and integrity requirements.

- support **independent** design, testing, V&V and certification of hosted functions.
- **establish and guarantee timing and performance of all critical functions**, based on system integration configuration
- support a **(re)configuration management system** that is robust and easy to maintain to allow for (re)deployment of functions and changes in train configuration.
- Enable full **interoperability** with respect to different and frequently changing train configurations at functional and system integration level.

Obviously those key objectives can be considered in any type of "cloud of embedded resources" (or "embedded cloud") used to build generic reconfigurable integrated architectures, consisting of a limited number of generic components for computing, networking, and IO. As such an architecture should host time/safety-critical functions and in fact behave as one system, reconfigurable to operate in different topologies, the notion of a "distributed fault tolerant embedded computer" becomes more apparent.

Furthermore, proposed concepts should serve different use cases (high-speed train, passenger train, metro, …) and different OEMs with different engineering cultures to define their own architecture and integrated modular platform efficiently and at sustainable lifecycle costs. Interoperability of trains and consist for joint operation should be sufficiently supported to satisfy needs of train operators.

Embedded Platforms for Next-Gen TCMS

An embedded platform for integrated TCMS consists of thousands of end devices, and will contain hundreds of Ethernet switches devices, which can be arbitrary permutated depending on the train composition on different routes. Key embedded platforms include the glue logic - system integration (network) part at the consist and train level, and integrate many computers with installed software platform (RTOS, middleware).

The aim is to design an integrated architecture which allows integration of SIL1-4 functions, SIL4 brake-by-wire and doors functions, safety signals and dynamic integration of integrated railway consists and cars. In this project we work around the constraints of existing deterministic time-driven Ethernet communication and define new approaches which enable distributed computing in dynamically modifiable topologies.

In addition, the Safe4Rail architecture enables the integration of non-critical functions and enable safe and secure integration of open world functions with limited trustworthiness. In the scope of WP2 Safe4Rail project, AUTOSAR, ARINC653, OpenTRDP and OPC-UA are considered and a subset of those software platform technologies was analyzed. Both system integration (drive-by-data), network and software platform capabilities determine the capability of the integrated modular platform, and they are tightly interwoven and inseparable. Integrated modular platform also relies on appropriate design, configuration, integration, verification/validation, certification methodology and tooling. Without them a set of software components and networking devices cannot be used productively. Inter-process communication among different partitions and processes on different computers is conducted via deterministic Ethernet network with synchronization and synchronous/asynchronous communication capability. Software components and modules assure robust deterministic communication among partitions and tasks on one computer. Integrated modular platform represents a subsystem which hosts many different applications and incorporates properties listed in Figure 1.

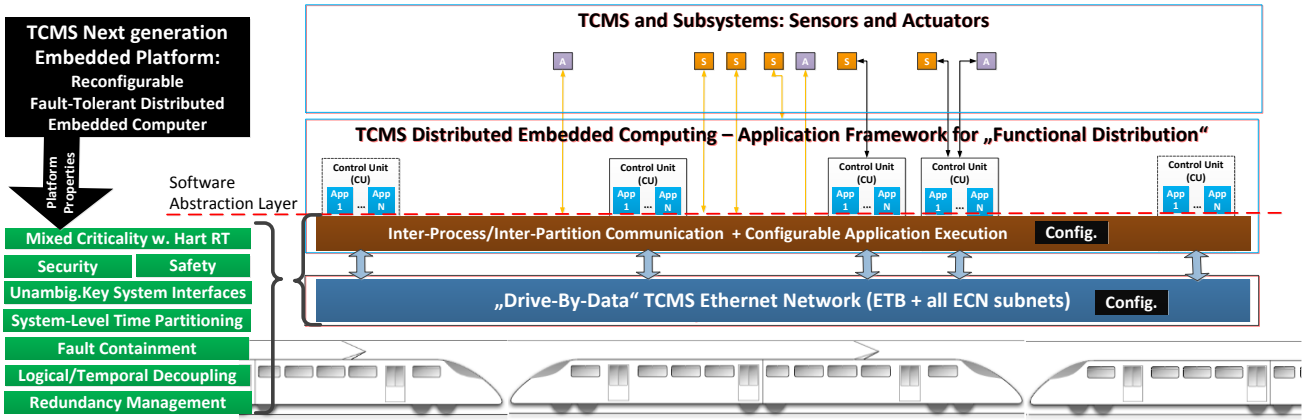

Figure 1 Next-Gen TCMS Architecture

TCMS Integrated Modular Platform as Embedded Cloud for Hosting Critical Functions

A truly generic and configurable embedded computing platform integrated by Ethernet can be compared to an embedded "cloud computer" (see Figure 2). The scalability of deterministic time-driven architectures lies in the fact that the system architecture can be designed out of a set of embedded resources which are statically and/or dynamically virtualized to host many different time-, safety- and mission-critical functions.

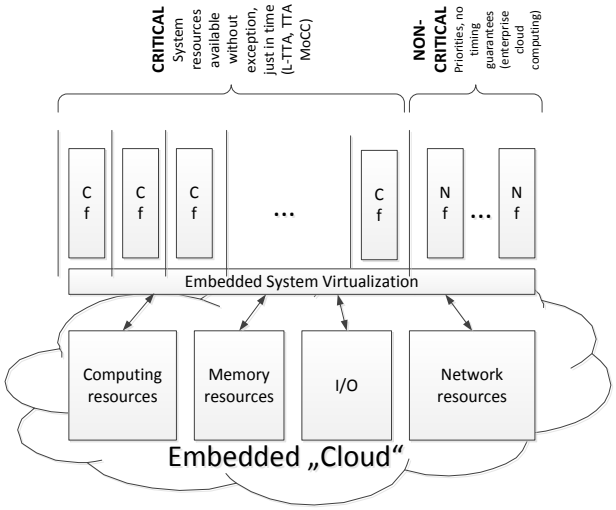

Figure 2. Embedded Cloud Computing and Distributed Embedded Systems Virtualization

Due to time partitioning of network bandwidth, embedded clouds also permit the integration of other non-critical functions without significant restrictions. In comparison to existing closed integrated modular architectures (e.g. IMA or federated systems), embedded clouds can represent a novel tool in system architects' portfolios and support further system optimizations with absolute separation of controlled objects from software functions for arbitrary system topologies. This approach can be applied in the design of open and closed systems with time-critical and hard real-time functions

Deterministic Ethernet capabilities are the key enabler for the design of embedded clouds. New Deterministic Ethernet standards based on time-multiplexed bandwidth sharing are currently worked out in IEEE802.1 and IEEE TSN (Time-Sensitive Networking) working group, in conjunction with time-partitioning of computing resources and other soft-time computing models. This, enables the design of embedded clouds and integrated modular architectures, which can host different time- and event-driven functions without mutual deadlocks and resource starvation. Safe4Rail deploys a subset of mechanisms combining IEEE TSN, but also the experience from ARINC 664 [9] and SAE AS6802 [10] to create a viable and robust integrated architecture with synchronous and asynchronous communications.

Functionally, deterministic Ethernet protocol services offer basic networking capabilities and mechanisms for time-driven/time-aware traffic queueing and message forwarding. Integrated architecture system integration capability is defined as a combination of networking and lower-level COM middleware layers to enable the required levels of abstraction. Design methodology, configuration tools, portioning and layering, and support for different models of computation and communication play important role in design of next-gen integrated systems. Furthermore, Network devices and switches represent a "sink" where all datastreams (dataflows) share common resources, queue memory, and switching engine. Therefore internal component architecture and its robustness against faults, can greatly increase integrated platform availability and prevent interference between different integrated functions.

Advanced System Integration for TCMS

Railway networks today rely on a number of different communication protocols and databuses such as PROFIBUS, CAN, MVB, PROFINET, Ethernet/IP, CIP, IEC61375. This variety creates interoperability, complexity and manageability issues, and increases the costs of design, integration, reuse, certification (homologation) and maintenance.

ETB (Ethernet Train Backbone) and ECN (Ethenret Consist Backbone) Ethernet networks described in IEC61375 are based on Ethernet with VLANs (IEEE 802.1Q). They provide limited support for the design of deterministic and scalable system architectures for applications such as next generation TCMS up to the SIL2. VLANs improve traffic separation, but they cannot provide any real-time guarantees or mixed-criticality network virtualization with robust partitioning among different traffic classes. Some of those shortcomings are handled in different application-specific industrial Ethernet networks: the used mechanisms and protocols are either not fully compatible with Ethernet Layer 2 protocols, or impose severe restrictions on traffic configuration and scalability, or are not applicable for the design of larger mixed criticality integrated modular architectures with SIL4 functions at sustainable lifecycle costs. Neither IEC61375-based TCMS nor the older proprietary IPTCom, PROFINET or CIP based architectures support the integration of SIL4 functions, and cannot handle hard RT functions in large systems. In general all those networks have their strengths in different applications niches, but they are not designed for advanced integrated architecture applications with a large number of functions with different timing and/or criticality properties. Such integrated systems take into account all mechanisms to

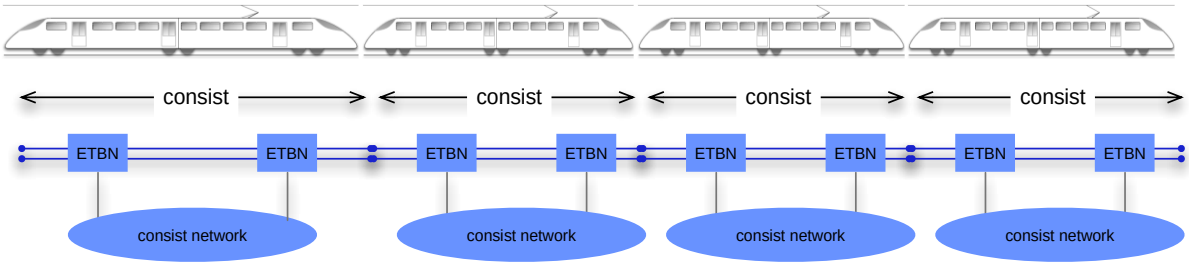

Figure 3: Hierarchical ETB/ECN Networks

prevent interference between less and more critical functions. In most cases this requires well-defined safety cases with internal architecture based on careful consideration of safety, mission and system engineering objectives.Safe4Rail solution targets railway systems with train-wide processing functions which can combine processing for interoperability at up to 100Hz or higher (using Gigabit Networks with up to 64 hops), and can offer advanced hard RT performance for selected functions for higher train-wide control loop functions, using a selection of IEEE TSN and additional network abstraction mechanisms.

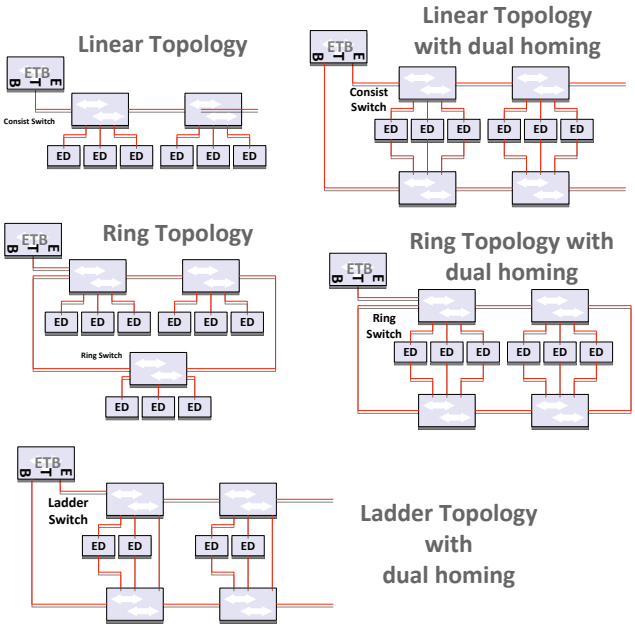

Figure 4. ECN Topology Examples

TCMS Topology

Ethernet is used in TCMS systems for over 10 years. Basic network topology originates from the classic train car/consist physical separation and builds a multi-domain system integrated by an ETB (Ethernet Train Backbone) network in linear topology. In general, each domain represents a separate consist or car, but other variants are deployed depending on the use case. One consist may contain one or several cars, have one or more ECN (Ethernet Consist Network) networks. The physical layer of the ECN is defined in IEC 61375-3-4, while addressing and ETB-related control services (ECSP, ECSC) are laid down in IEC 61375-2-3. As shown in Figure 4, the topology of the ECN (Ethernet Consist Network) can be quite different and depends on the vendor's preferences. While some vendors prefer the ladder topology, where each end device is connected to two lines, others use a ring topology or favor some other hierarchical topology. Figure 4 shows several topology variants, which can have different availability, reliability, integrity, redundancy and fault-tolerant properties.

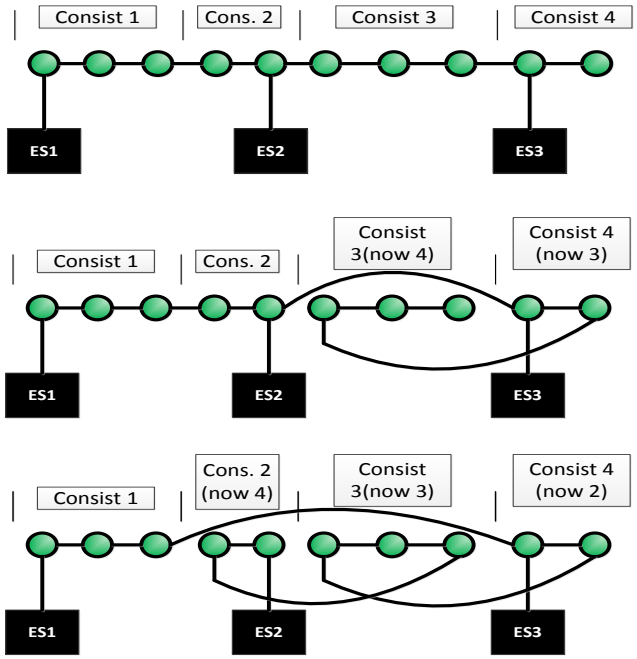

Figure 5: Frequent ETB topology changes

In opposite to the automotive or avionic use cases, the overall network topology is not constant. Cars or consists can be decoupled, train composition may change

daily, consist can be rotated, driver location may change depending on train direction, trains can split (Figure 5). This imposes significant constraints on configuration in integrated modular architectures with deterministic performance and linear topology, due to a large number of possible permutations, with 64 ETB subsystems (n=64! without car rotations).

For safety-critical real-time systems, verification and certification for a large number of configurations can be a challenging (or impossible) task, especially if the timing for the whole design space should be provided.

Network redundancy is not standardized, and every train manufacturer uses redundancy mechanisms which are selected for their own ECN (or ETB) topology. The objective is to create a common set of network and path redundancy mechanisms which can be deployed by all train manufacturers.

Inauguration is a process which utilizes asynchronous broadcasting messages (TLVs) and a modified LLDP protocols [3] to assess the topology of the network. Afterwards the topology can be compared with known ETB configuration tables of the consist. This is used to minimize any errors due to late ETBN switches or startup faults. After inauguration, this service is executed permanently and establishes train topology status every 300-400ms. This mandatory ETB service can be used for ETB health monitoring. Topology modifications are accepted and confirmed by driver, when the train is not moving.

ETB topology may differ for different use cases and mission objectives. Non-redundant ETB line with parallel physical connections, or multiple separate ETB lanes are viable, with different levels of connectivity between lanes for the purpose of communication integrity, availability and reliability are viable. Those variants are currently under discussion based on FTA/FMEA analyses, but also economic constraints relevant for railway industry should be taken into account.

ETB Bypass

The nodes on the train backbone are actually switches (on the ETB-side) and routers between the backbone network and the consist network. To ensure high reliability, there should always be a redundant switch in each consist – also to overcome the maximum Ethernet cable length of 100m. In case of a malfunction (e.g. power supply failure), each ETB Node (ETBN) must provide failsafe relays to allow the passive bypassing of ETB traffic.

In passive bypass setting, the ETB lines will bypass the ETB switch, which then is decoupled from the ETB lines. The Passive Bypass Setting is the default setting in the powerless state and the ETB switch is out of order. This means that in cases when a consist is not powered, the ETB Ethernet network will operate and connect two consist which are separated by non-operational switching devices. This solution was matured and is proven in the railway industry over the last 10 years.

Any ETB solution should ensure that unpowered trains do not interrupt the topology, but also that unpowered train cars, consist or switches may change the physical topology.

Network redundancy is not standardized, and every train manufacturer uses redundancy mechanisms which are selected for their own ECN (or ETB) topology. The objective is to create a common set of network and path redundancy mechanisms which can be deployed by all train manufacturers.

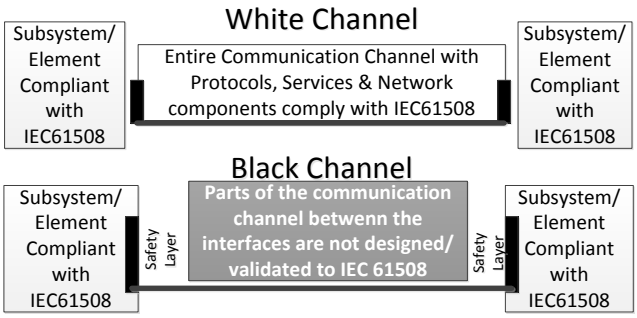

Figure 6. IEC61508 Black channel vs White Channel (ref. IEC61508-2:2010)

Safety Concepts

In systems with fail-safe state which can be turned off on any fault of hazard, it is possible to design critical application by using a black channel approach. In addition, the applications are designed not to rely on network for its operation, and may also include some backup or graceful degradation strategies. With integrated complex Ethernet-based systems which host many functions on different computers, "white channel" designs can provide predictable performance, high integrity, availability and reliability required for safe system operation. To become certified, network components are designed using safety assurance processes which support the system safety objectives and high dependability, or the devices should have sufficient operating history in similar critical applications. "White channel" (Figure 6) will require also protocols services and network components to be designed in line with IEC 61508-2. In aerospace industry, the continuous operation is predominantly the only safe state, so the systems are designed to be fail-operational.

However it can be assumed for railway applications that future distributed controls, autonomous operation and high-availability requirements could impose new constrains on the communication and network reliability, availability, integrity and safety. Integrated platform should ensure non-interference between functions of different safety-criticality, but also it should prevent that

any minor glitch of less critical systems brings the system into a safe state and minimizes its productive operation time, and finally the system lifecycle competitiveness in the market.

System Integration Concept for "Drive-By-Data"

Integrated architecture should support synchronous and asynchronous non-blocking models of computation for mixed-criticality applications, such as L-TTA and TTA, while being completely abstracted from frequent (daily or hourly) topology changes. This aspect is unique for railway industry and has a limited similarity only to integrated modular space systems (modular launchers, space station, habitats, …). Another example are "road train" applications (e.g. SARTRE EU Project) with swarms of vehicles, but with different technology baseline and relaxed real-time constraints.

To simplify (and enable) the system design in frequently changing topologies, it is necessary to:

- abstract application software from network topology, addressing and operation details (as a part of software platform).
- abstract distributed function's temporal behavior from network topology, addressing and operation details (as a part of system integration).

This is required for efficient deterministic network (and computing) resource sharing by many hosted real-time and soft-time functions, and decoupling of software function hosting from controlled objects, so that functions can be hosted anywhere in the system. By doing so we open the door for further system architecture optimization and advanced generic open architecture designs.

For such levels of abstraction, it is required to completely decouple logical and temporal behavior in the system (i.e. TCMS platform with all hosted applications), and introduce strict system-level time partitioning which relies on robust system-wide time in ECN networks, while providing a reasonable alignment and partitioning at ETB level. ETB can be partitioned in time and aligned with all ECNs only in special cases, due to frequent topology changes which impose additional design space constraints, and require complex reconfiguration with potentially thousands of deadlines in a system with several hundreds of switches.

"Drive-by-Data" concept includes statically configured interactions and key system interfaces among critical functions in ETB and ECN networks, defined as statically configured (parameter-defined) policing and time-driven packet forwarding. This allows definition of deterministic dataflows with defined temporal boundaries - defined maximum (or fixed) latency and bounded jitter.

This helps to separate control plane (parametric, predefined) from the data plane, and the approach has some similarities with software-defined networking (SDN) and Layer 2 switching, which is considered the future of flexible and deterministic Ethernet networking.

Network Virtualization

At the same time other network bandwidth is "virtualized" for soft-time traffic, and not used by configured critical functions. Soft-time traffic can be constrained to a defined set of end devices and VLANs.

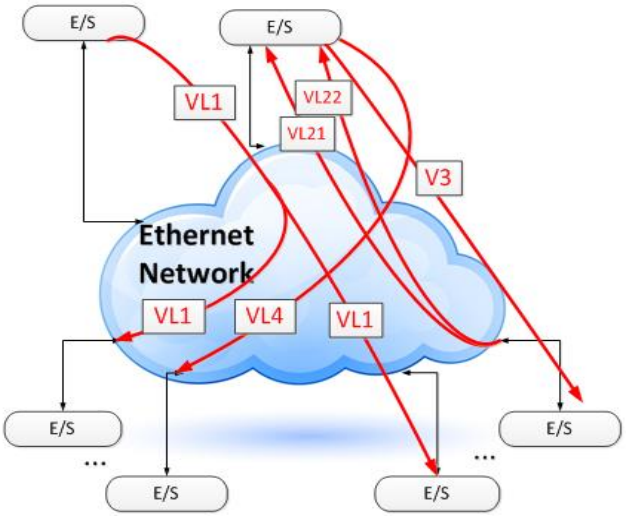

Figure 7. Network Interfaces and Bandwidth Virtualization using deterministic dataflows/streams (i.e. virtual links or VLs in ARINC 664/SAE AS6802)

Network resource virtualization and high levels of abstraction for "Drive-by-data" require different flavors of virtualization at once:

- Bandwidth virtualization - to emulate unidirectional wired connections and host mixed time-criticality dataflows
- Topology virtualization – to emulate different topologies and support both multi-path and dual network redundancy on a common topology
- Configuration (backplane) virtualization – to emulate distributed shared memory capable of hosting all relevant system-wide data, independent of source position and topology (ETB, and when necessary in ECN)

Topology virtualization is conducted by selective policing of dataflows from different applications, so that different applications can only access specific parts of the network or communicate only by using a statically defined logical paths.

Backplane virtualization requires a periodic exchange of system-relevant state variables, among relevant subsystems and computers. With unified configuration for each end device and network switches, this approach can

be adopted to fully abstract dynamic topology changes, and determines the ETB/ECN integration, which can be done for synchronous and asynchronous networks.

Establishing Deterministic "Drive-By-Data" Communication Datapaths over ETB/ECN

TCMS can control the timing of key system interfaces (from application to application) by using predefined parameters at software platform and network level as shown in Figure 1. Software platform should support time-driven operation for critical functions, as well as the alignment with network time.

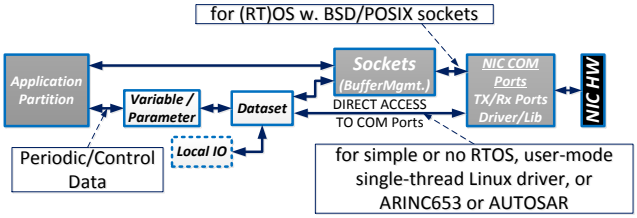

Figure 8. Application to Network Datapath Integration

Applications access system variables, and the platform transfers those variables via network multicasts with defined temporal behavior. Specified set of variables can be transferred using unidirectional ports or sockets associated with such ports. COM ports use principles equivalent to ports proposed and used in ARINC664/ARINC653 and in SAE AS6802-enabled devices.

The specified ports are tied to one deterministic multicast which will transmit data on time to the COM port of another computer, over the multi-hop ETB and/or ECN network using system time for packet forwarding. The level of granularity and control of temporal behavior is determined by OEM system engineering requirements and architecting. However some parts of the configuration may profit from being common for all OEMs to establish basic interoperability at ETB backbone level, and compose trains from different railcars fabricated by different OEMs.

As mentioned in previous chapters, datapaths at network level are defined via time-aware/time-driven multicasts which emulate simple physical wiring ("circuit") on top of the Ethernet network infrastructure (see Figure 7). This allows designer to access all hosted applications independently with apriori defined QoS.

Deterministic Ethernet Services

Different time-triggered standards offer different definition on how time-triggered communication operates. In IEEE TSN (802.1Qbv), time-aware FIFO queues are defined, while in SAE AS6802 standard, the notion of time-triggered buffering is used. The difference seems to be a minor one, but it has an impact on network design approach, latency and buffer use. As timed IEEE802.1Qbv gates control events on the egress (output) ports, and not the order of frames in the queue, the synchronization errors, frame loss, and time-based ingress policing may lead to non-deterministic placement in queues during runtime for IEEE TSN.

	IEEE TSN	ARINC664	SAE AS6802
Bandwidth Partitioning	Yes	Yes	Yes
Asynchronous Packet Switching	Yes	Yes	Yes, using IEEE802 traffic
Synchronous Packet Switching	Yes	No	Yes
Mixed-Criticality Capable	Yes	No or Limited	Yes
Defined max. latency per dataflow	Yes, fixed latency possible for specific (limited) dataflows/datastreams	Yes, defined maximum latency only	Yes, fixed latency for every defined dataflow / stream / VL
Defined max. jitter per dataflow (1GbE)	Yes, depending on the number of streams per queue (typ.<0.1-0.2ms) and gate control period	Jitter < ½ of max. stream latency	Jitter < N x time precison (N ~ 2-3) Jitter-free end-to-end communication viable
Support for Nx 10 determin. Streams/ dataflows per port	Yes, with increasing jitter	Yes	Yes
Synchronization	World-Clock Dissemin. (802.1AS / IEEE1588)	None	Distributed Fault-Tolerant Clock (AS6802)

Figure 9. Comparing Deterministic Ethernet Capabilities in Linear/Circular Topology

Furthermore, there is a difference in maximum allowed network complexity for jitter-less communication. While 802.1Qbv may be less deterministic or more complex to schedule due to design constraints in large networks with mesh/star topology, it offers a significant flexibility provided by FIFO buffering of several datastreams sharing common gate opening slots, which is positioned somewhere between asynchronous (ARINC664) and buffered synchronous (SAE AS6802) communication.

A general list of capabilities of the three standardized technologies is provided in Figure 9.

System and Network Synchronization

System synchronization is the cornerstone for deterministic alignment of functions for hard real-time functions and distributed real-time control loops.

Time-triggered and time-sensitive networking rely on the network device synchronization for network virtualization, system-level time partitioning and deterministic fixed-latency communication. The failure of network synchronization and system time creation may lead to the failure of network bandwidth partitioning, and then to communication interruption.

When comparing computing module time-partitioning which relies on local CPU timers, RTOS time-partitioning functions, the network (system) time would

be an equivalent of local time on a computing module. Computing module and RTOS cannot partition computing resources in time, if local clock malfunctions or such malfunctions cannot be detected. The existing aerospace IMA-1G (integrated modular avionics, first generation) systems rely on time/space partitioning on computing modules, but do not extend the concept to distributed systems and ARINC 664 network, simply because there was no Ethernet technology with robust synchronization capability prior to their introduction in early 2000. With the introduction of SAE AS6802 (2005-2011) and IEEE TSN (2012-2020), synchronous Ethernet networking capabilities have changed significantly.

Fault Type – Manifestation		
Fault Type – Manifestation	**Description**	**Note**
Fail-Silent / Silent Crash	No output on failure, the failure can be detected, and is permanent.	Ideal case – requires careful component design. If the failure is not detected
Undetected Crash	No output, failure is not detected,	can be permanent or transient (with longer interruption of operation).
Message Loss/ Omission	Timing messages are lost, or new master clock search started.	Can be inconsistent (some nodes get data, others don't), or consistent.
Invalid Value	Incorrect timing information	If symmetric can bring timing/control loop disruptions, if asymmetric, the outcome is not predictable and well understood
Invalid Timing	Inaccurate dissemination of packets and time, undefined synchron.startup	Can be a network configuration or device implementation problem. With slightly-of-specification faults it can lead to asymmetric faults.
Fault Type – Observability		
Symmetric	All participants detect the failure, when it occurs	Such errors can be handled by voting and modular redundancy.
Assymmetric / Byzantine	Fault manifests/appears in different way to different nodes.	System alignment and consensus is lost, rare but ugly fault class which can emerge from multiple faults, system design errors or incomplete fault hypothesis. Requires Byzantine agreement to handle and recover.

Figure 10. Simplified network (device) fault classification

For robust synchronization it is essential that different types of faults can be handled and the network can diagnose synchronization faults, synchronously startup within a bounded time, and prevent complex asymmetric fault scenarios. The concept for synchronization in SIL4-capable integrated systems is currently in work, and includes fault hypotheses analysis. The result may contribute to high robustness and system availability.

While SAE AS6802 synchronization is formally verified and designed for fail-operational applications, IEEE TSN relies on the tailoring of IEEE1588, and enhancements to IEEE 802.1AS which distributes world clock to other network devices and end devices in the system. In contrary, SAE AS6802 uses a concept of distributed fault-tolerant clock, which aligns local clock based on the asynchronous message exchange between nodes and Ethernet switches. Such messages do not carry any real-time information, but only indicate the progression of the communication cycle. The synchronization concept described in SAE AS6802 in this case is comparable to proven TTP network synchronization used in commercial aerospace DAL A applications, but it is applied to Ethernet networks.

Synchronization Concepts

The first clock synchronization concept is built based on the mechanisms defined in the time-sensitive networking working group, i.e. IEEE p802.1 AS-rev or gPTP. Figure 11 shows the synchronized S4R communication network with multiple clock domains. The redundant ETB channels are each running on a separate clock, and ECNs attached are also running synchronously, but within their corresponding independent closed clock domain.

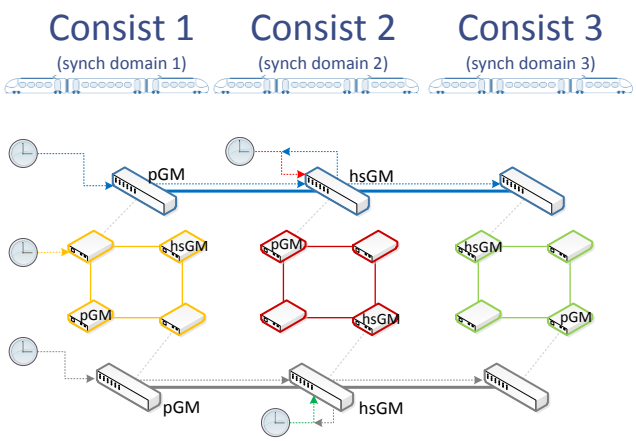

Figure 11. Synchronized S4R Communication Network based on TSN

Each ECN has a local primary grandmaster (pGM), with a Global Navigation Satellite System (GNSS) reference, which enables time-aware communication within a single consist, independent from the ETB or other

consists. The local pGM is not an ETB node. A local hot-standby grandmaster (hsGM) shall synchronize to the local pGM and offer a seamless handover in case of a local pGM's failure.

The ETB-wide clock synchronization concept relies on an election of a global pGM (per redundant line instance), which will be a synchronization reference for all the associated ETBNs. A global hsGM will also exist on this level. This implies external prioritization and manual configuration of the pGM/hsGM, without BMCA or Best Master Clock Algorithm as there is no generic seamless handover with a BMCA execution after pGM's failure.

The second synchronous concept includes the use of rate-constraint-capable devices upgraded with fault tolerant clock-synchronization approach of Time-Triggered Ethernet (SAE AS6802) [10]. It mitigates the issues of the first concept regarding redundancy management (offers a HW-based redundancy handling) and manual scheduling management. Also, the active redundancy from AS6802 supports tolerating a broad spectrum of failures. Opposed to the first concept, this concept provides a communication network synchronous on a single clock domain.

The AS6802 clock synchronization messages are standard Ethernet frames called Protocol Control Frames (PCF). The group of network nodes to be synchronized is called a Synchronization Domain (SD). Time synchronization is a periodic process – a synchronization domain is being re-synchronized at regular intervals, i.e. integration cycles (typically 1-2 millisecond).

Clock synchronization service is provided by two types of nodes:

1. Synchronization Master(s) or SMs, determining the baseline global clock, and

2. Compression Master(s) or CMs, computing the global time and transmitting this time to all clients in the synchronization domain.

Synchronization masters are usually end systems (end device NICs), and compression masters are usually switches. There is no need for any special synchronization masters or wall clocks, as the synchronization simply aligns local clocks.

The AS6802 synchronization is a two-step process:

1. Determining the baseline global time: at the beginning of every integration cycle synchronization master(s) send PCFs to compression master(s), which compare time information from different synchronization masters and use "voting" to establish the global time.

2. Synchronizing the global time with every node in the synchronization domain: The compression master(s) compute the fault-tolerant average from incoming PCFs and derive the global time, which is then sent out as a PCF to all nodes in the synchronization domain. Upon reception of the PCFs, all clients calculate the average global time received from compression master(s) and adjust their local clock.

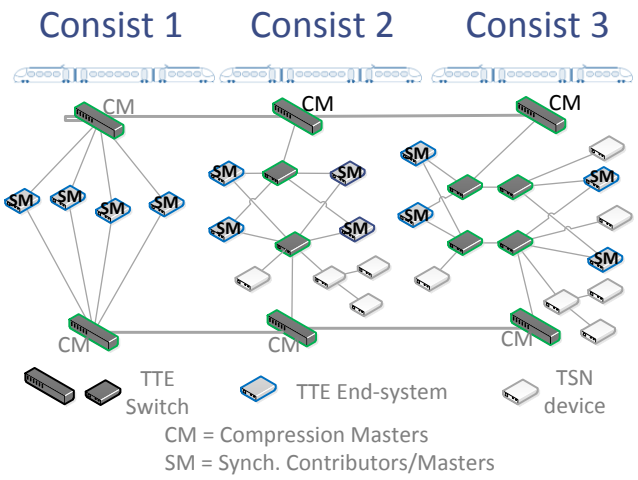

Figure 12. Deterministic Network with IEEE TSN and SAE AS6802 Synchronization

ETB/ECN Integration and Configuration Virtualization

ETB backbone emulates shared system memory behavior in the form of virtual bus, with predictable update rates and predefined data formats, which are periodically multicast between different ECN networks. This concept works with varying number of ECNs (up to 64) in different topologies. All ETB units have a common configuration which determines the worst case traversal times for message and data exchange in any thinkable linear or circular topology. Upon inauguration, every ETB will select and update its configuration based on topology position, and multicast configured system-relevant data over deterministic datastreams (multicasts) characteristic for its identified topology position. Defined multicasts will send data to max. 63 existing and non-existing ETB switches. This approach supports synchronous and asynchronous Ethernet networking.

ETB Backbone Modes

ETB backbone network in Drive-By-Data concept is designed to operate as synchronous and asynchronous network, to minimize performance restrictions or any potential certification limitations. Due to limitations of asynchronous deterministic communication in larger multi-hop networks, this mode is used for degraded TCMS operation for which only key safety and control functions are supported, but without the need for accurate alignment and common time base. Standard mode should ensure

interoperable high-performance operation with synchronization and tight domain alignment.

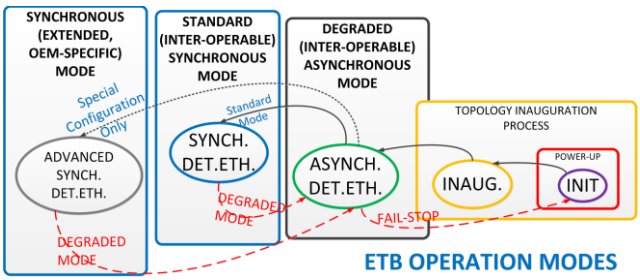

Figure 13. ETB Operation Modes

The third ETB mode – "synchronous/extended" gives all flexibility to OEMs to integrate additional advanced functions and differentiate their TCMS systems. "Drive-by-Data" ensures that there are no significant restrictions on use cases and interoperability. Concerning performance, ETB at 1Gbps can provide completely updated set of system-relevant data to all ECN domains, in less than 10ms, for up to 64 hop ETB network, with jitters below 0.5ms (synchronous) - 2ms (asynchronous) for all modes. In special configurations with 16-24 consists those numbers can be reduced for 2 to 4 times. OEMs have a complete freedom to select the approach for ETB operation and integration which suits the use case. Both synchronous (standard) and asynchronous (degraded) mode can be designed to offer full interoperability for different train makers, while advanced synchronous modes can be designed for special high-performance trains with extended capabilities.

Conclusion

This work describes initial "Drive-By-Data" system integration concept for integration and hosting of functions in the next-generation TCMS architectures, which can integrate all hard RT, real-time and soft-time functions, and support different models of computation and communication for different application requirements.

Such an integrated architecture enables design of innovative more integrated systems using less HW resources, and leading to optimized architectures with very few limitations on system integration. Complexity management is addressed by different forms of abstractions, and the logical complexity mitigation requires robust methodology for design and verification of configurations, as the operation of critical functions is driven by parameters. All other soft-time functions can use remaining networking and computing resources.

With parameter-driven architectures, assuming the separation of logical and temporal behavior, we can better control performance of different functions hosted in the system, and add or modify functions with predictable performance alterations. Applications can reside in different computers, and system architects can define very centralized or very decentralized architectures with high-levels of logical integration for simplified reconfigurability or reuse. Although this work targets integrated railway TCMS systems, this work is relevant for any other mixed criticality integrated modular architecture in cross-industry applications.

Acknowledgments

The research leading to these results has received funding from the Shift2Rail Joint Undertaking under grant agreement No 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation program and Austria, Spain, Germany, Czech Republic, Italy, France.

References

[1] Shift2Rail, https://shift2rail.org/

[2] Safe4Rail, https://safe4rail.eu/partners

[3] IEC 61375-1:2012: Electronic railway equipment - Train communication network (TCN), https://webstore.iec.ch/publication/5397

[4] R. Walter and C.B. Watkins, "An IMA Architecture for Boeing B-787 and Beyond", 3rd Edition, Digital Avionics Handbook, CRC Press 2014.

[5] NASA, "NASA's Orion Spacecarft Comes to Life", [Online]. Available: http://www.nasa.gov/press/2013/october/nasas-orion-spacecraft-comes-to-life/

[6] K. Wittmack (BMW), "Introducing Automotive Ethernet – A Project Manager's Account", Ethernet & IP @ Automotive Technology Day, Yokohama, 2015.

[7] I.N. Camargo (Continental Automotive), "Ethernet and the AUTOSAR Adaptive Platform as basis for future E/E Architecture", Ethernet & IP @ Automotive Technology Day, Yokohama, 2015.

[8] Shift2Rail Joint Undertaking. "Multi-Annual Action Plan". [Online]. Available:

http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/jtis/h2020-maap-shift2rail_en.pdf

[9] ARINC 664, "664P7-1 Aircraft Data Network, Part 7, Avionics Full-Duplex Switched Ethernet Network", http://store.aviation-ia.com/cf/store/catalog_detail.cfm?item_id=1270, accessed Aug 2014

[10] SAE AS6802, Nov 2011, SAE Standards, http://standards.sae.org/as6802/