Deterministic Ethernet as Reliable Communication Infrastructure for Distributed Dependable Systems

DREAM Seminar
UC Berkeley, January 21st, 2014

Wilfried Steiner, Corporate Scientist
wilfried.steiner@tttech.com
MOTIVATION
What They Have in Common …

Reliable Networks

Are a key element of a dependable system
Trend towards Advanced Driver Assistant Systems (ADAS)
Sensors

- Long-Range-Radar (LRR 4)
- Video Camera
- Top view Camera
- Middle-Range-Radar (MRR)
- Ultra Sonic
- Laser Scanner
- Predicitive Map Data Car2x Connectivity
## Actuators

Necessary Actuators for Automated Driving

<table>
<thead>
<tr>
<th>Electronic Stability Control</th>
<th>Powertrain Coordination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold management system</td>
<td>Shift-by-Wire</td>
</tr>
<tr>
<td>Decelleration management</td>
<td>Electric Power Steering</td>
</tr>
</tbody>
</table>

![Diagram of a car showing steering column, accelerator pedal, damper, and shift-by-wire system.](image)
NETWORK BECOMES MORE AND MORE IMPORTANT
Automotive Need of a Reliable Communication Infrastructure

Toolbox of Mechanisms

Comprehensive Toolbox of Mechanisms for Implementing Time and Safety Critical Communication systems

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Traffic</td>
<td>Ultra low latency, Highly deterministic, QoS, Planning &amp; Flexibility issues, Adequate for most challenging applications.</td>
</tr>
<tr>
<td>Flexible Automotive / Industrial Control Traffic Class</td>
<td>Low latency, QoS, Flexible, Goal Adequate for the majority of control applications. Ongoing discussion in 802.1 TSN: BLS? Peristaltic? Urgency based? Per ingress shaping?</td>
</tr>
<tr>
<td>Seamless Redundancy</td>
<td>Safety critical control.</td>
</tr>
<tr>
<td>Ingress Policing</td>
<td>Safety critical, Fault containment, Single point of failure.</td>
</tr>
<tr>
<td>Fault Tolerant Clock Sync</td>
<td>Safety critical, Fault containment.</td>
</tr>
<tr>
<td>Adequate support for reservations</td>
<td>Automotive requirements currently under discussion (=) AAA2C.</td>
</tr>
</tbody>
</table>

Markus Jochim, General Motors Research
IEEE 802.1 Plenary Session
July 14 - 19, 2013 – Geneva, Switzerland

General Industrial Trend towards Converged Networks

Closed World Communication
- Performance guarantees: real-time, dependability, safety
  - Standards:
    - ARINC 664, ARINC 429, TTP, MOST, FlexRay, CAN, LIN, …
  - Applications:
    - Flight control, powertrain, chassis, passive and active safety, ..
  - Validation & verification:
    - Certification, formal analysis, ..

Open World Communication
- No performance guarantees: best efforts
  - Standards:
    - Ethernet, TCP/IP, UDP, FTP, Telnet, SSH, ...
  - Applications:
    - Multi-media, audio, video, phones, PDAs, internet, web, …
  - Validation & verification:
    - No certification, test, simulation, ...

We see a market requirement to use the same physical network for data flows from both worlds.
The Motivation for Ethernet

- Ethernet hardware is low cost.
- Ethernet is a well-established open-world standard and very scaleable.
- The OSI reference model gives a well-structured classification of concepts that can be built on top of Ethernet.
- Existing tools can be leveraged as cost-efficient diagnosis tools.
- Standard protocols like SNMP can be leveraged for maintenance and configuration.
- Engineers learn about Ethernet at school.

Ethernet means to use well-established technology, but needs real-time and dependability improvements.
DETERMINISTIC ETHERNET
Asynchronous Communication

- Transmission Points in Time are not predictable
  - Transmission Latency and Jitter accumulate
  - Number of Hops has a significant impact
- Usually solved by High Wire-Speeds & Low Utilization and/or Priorities
- Problem of "Indeterminism" remains
Towards Determinism: Synchronization of the distributed local clocks

*In an ensemble of clocks, the precision is defined as the maximum distance between any two synchronized non-faulty clocks at any point in real time.*

- Late Clock
- Perfect Clock
- Early Clock
Single-Master Clock Synchronization

Enabler for Synchronous Communication:
- Synchronized Global Time
- Communication Schedule
Synchronized time and a communication schedule allows to realize the time-triggered communication paradigm.
Synchronous Communication (TT)

Exactly one order of messages $M_i$ (in contrast to $\text{PERM}(M_i)$ in async. comm)
Example: 1,000 Frames (Industrial-Sized)

Dataflow Links are enumerated on the x-axis

Time-Triggered Only
Deterministic (TT)Ethernet – Traffic Classes

TTEthernet provides several traffic classes in parallel: time-triggered, rate-constrained, and best-effort.

- **Time-Triggered**: dispatch messages according to a predefined communication schedule.
- **Rate-Constrained**: enforce minimum duration between two frames of the same stream.
- **Best-Effort**: standard Ethernet communication paradigm – no temporal guarantees are given.

Longest Communication Cycle in this Example: $\text{LCM}(30, 40) = 120\text{msec}$
TTEthernet Dataflow: Rate-Constrained Traffic

Rate-Constrained Traffic (RC)

min. duration  min. duration

min. duration
Mixed Traffic on Ethernet – RC Accumulated Jitter

Time Triggered
Rate Constrained
Best Effort

TTEthernet Switch

00:10

00:11
00:11

00:01

00:02

00:01

00:02
00:02

00:02

00:02

00:02

00:02

00:02

00:02

00:02

00:02

00:02
Mixed Traffic on Ethernet – RC Accumulated Jitter

TT is dispatched according synchronized time

TT is forwarded according synchronized time

TT has lowest latency and lowest jitter

RC frame delivery is guaranteed, but potentially has high latency and jitter

RC potentially queue-up in switch memory

TT has lowest latency and lowest jitter

RC potentially queue-up in switch memory

TT is dispatched according synchronized time

TT is forwarded according synchronized time

TT has lowest latency and lowest jitter

RC potentially queue-up in switch memory

TT is dispatched according synchronized time

TT is forwarded according synchronized time

TT has lowest latency and lowest jitter

RC potentially queue-up in switch memory
Mixed Traffic on Ethernet – BE Buffer Overflow

TTEthernet Switch

- Time Triggered
- Rate Constrained
- Best Effort

1
2
3
4

1
2
3

Ensuring Reliable Networks
Mixed Traffic on Ethernet – BE Buffer Overflow

- Time Triggered
- Rate Constrained
- Best Effort

TTEthernet Switch

Rate-constrained frame delivery (standard Ethernet traffic) is guaranteed!

Best-effort frame delivery (standard Ethernet traffic) is NOT guaranteed!
Converged Network Example

Dataflow – Integration
- Time-Triggered (TT)
- Rate-Constrained (RC)
- Standard Ethernet (BE)

TTEthernet Switches are non-preemptive store-and-forward switches using priorities
Example: 1,000 Frames (Industrial-Sized)

Dataflow Links are enumerated on the x-axis.

RC/BE frames are also integrated during TT phases.

Time-Triggered Only

Time-Triggered + Event-Triggered
Example: 1,000 Frames (Industrial-Sized)

Dataflow Links are enumerated on the x-axis

Synthesis of Static Communication Schedules for Mixed-Criticality Systems
Wilfried Steiner
Chip IP Design
TTTech Computertechnik AG

An Evaluation of SMT-based Schedule Synthesis For Time-Triggered Multi-Hop Networks
Wilfried Steiner
Chip IP Design
TTTech Computertechnik AG

Abstract—Networks for real-time systems have stringent end-to-end latency and jitter requirements. One cost-effective way to meet these requirements is the time-triggered communication paradigm which plans the transmission points in time of the frames off-line. This plan prevents collisions of frames on the network and is called a time-triggered schedule (TT-schedule).

In general the TT-scheduling is a bin-packing problem, known to be NP-complete, where the complexity is mostly driven by the freedom in topology of the network, its associated hardware restrictions, and application-imposed constraints. Multi-hop networks, in particular, require the synthesis of path-dependent (TT-schedules) to maintain full determinism of time-triggered communication from sender to receiver.

For the experiments using the YICES SMT solver show that the scheduling problem can be solved by YICES out-of-the-box for a few hundred random frame instances on the network. A customized TT-scheduler using YICES as a back-end solver allows to increase this number of frame instances up to tens of thousands. In terms of scheduling quality, the synthesis produces up to ninety percent maximum utilization on a communication link with schedule synthesis times of about half an hour for the biggest examples we have studied. As a nice side-effect the YICES out-of-the-box approach is immediately applicable for the verification of existing (even large-scale) (TT-schedules) and for

SAFeBus [6, 7] in the Boeing 777 and TTP [8] in the Airbus A380 and the Boeing 787 aircrafts. While these protocols are broadcast-based with the intent to operate on physical bus or hub topologies, Ethernet-like protocols introduce network switches that allow concurrent time-triggered datapaths. TTEthernet [9] which has been selected for upcoming space programs is one of the first time-triggered protocols that inherently supports concurrent time-triggered communication also in multi-hop topologies. Furthermore, as time-synchronization services such as IEEE 1588 found their way into standard Ethernet equipment it seems only a matter of time when time-triggered communication shows up also in a “consumer” flavor. As we are looking at these developments in system size and complexity, scheduling for time-triggered networks becomes even more a challenge.

The scheduling problem for a time-triggered system like many other problems in system design can be formulated as solutions to systems of constraints. The constraints for different types of problems have different characteristics and specialized solvers have been developed for each class of

Analogous to the design of SAE or static bandwidth triggered triggered systems can be described with upper bound. This is also useful in

A tooling infrastructure of time-triggered communication can be composed of

Satellite navigation

IEEE

TTTech

www.tttech.com
Single-Master Clock Synchronization

Enabler for Synchronous Communication:
- Synchronized Global Time
- Communication Schedule
Fault-tolerant synchronization services are needed for establishing a safe global time base.
Need to cover complex failure modes, e.g. Babbling ECU

Faulty ECU starts to send faulty messages.

Without traffic policing functions, the switch forwards all faulty frames.

At some threshold of faulty frames, the switch starts loosing correct frames from other, independent applications.
NATIVE ETHERNET BECOMES MORE DETERMINISTIC
Native Ethernet becomes more deterministic

IEEE 802.1 is standardizing general architectures for local area networks (LANs) and metropolitan area architectures (MANs). Together with IEEE 802.3 they are the main working groups working standards for Ethernet switches.

Efficient utilization of the communication bandwidth and plug-and-play capabilities are topmost requirements in IEEE 802.1.

With AVB, IEEE 802.1 moved into the area of real-time communication. With TSN, IEEE 802.1 moves into the area of dependable communication.

Upcoming mainstream IT equipment aims to provide real-time and dependable communication features (to a significant higher degree than today).
AVB – Audio/Video Bridging

802.1AS Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks: a protocol and technique to synchronize local clocks in the network to each other.

802.1Qat Stream Reservation Protocol (SRP): a protocol that allows applications to dynamically reserve bandwidth in the network.

802.1Qav Forwarding and Queuing Enhancements for Time-Sensitive Streams: an enhancement over strict priority based forwarding and queueing mechanisms that establishes fairness properties for lower priority traffic in the network.

802.1BA: definition of profiles for AVB systems.

→ AVB is incorporated in the IEEE 802.1 standards documents since 2011.
Native Ethernet improves its Reliability

- **Physical Topology**
- **IEEE 802.1Q**
- **Spanning Tree / Virtual LANs**
- **Ring Topology**
- **Redundant “Networks”**
TSN – Time-Sensitive Networks

802.1ASbt Timing and Synchronization: Enhancements and Performance Improvements

802.1Qbv Enhancements for Scheduled Traffic: a basic form of time-triggered communication

802.1Qbu Frame Preemption: a mechanism that allows to preempt a frame in transmit to intersperse another frame.

802.1Qca Path Control and Reservation: protocols and mechanisms to set up and manage the redundant communication paths in the network.

802.1CB Frame Replication and Elimination for Reliability: to eliminate redundant copies of frames transmitted over the redundant paths setup in 802.1Qca.

802.1Qcc – enhancements and improvements for stream reservation
Background:
Industrial Need for FT Clock-Sync

Toolbox of Mechanisms

Comprehensive Toolbox of Mechanisms for Implementing Time and Safety Critical Communication systems

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Traffic</td>
<td>Ultra low latency, Highly deterministic, QoS, Planning &amp; Flexibility issues, Adequate for most challenging applications.</td>
</tr>
<tr>
<td>Flexible Automotive / Industrial Control Traffic Class</td>
<td>Low latency, QoS, Flexible, Goal Adequate for the majority of control applications. Ongoing discussion in 802.1TSN: BLS? Peristaltic? Urgency based? Per ingress shaping?</td>
</tr>
<tr>
<td>Seamless Redundancy</td>
<td>Safety critical control.</td>
</tr>
<tr>
<td>Ingress Policing</td>
<td>Safety critical, Fault containment, Single point of failure.</td>
</tr>
<tr>
<td>Fault Tolerant Clock Sync</td>
<td>Safety critical, Fault containment.</td>
</tr>
<tr>
<td>Adequate support for reservations</td>
<td>Automotive requirements currently under discussion (=&gt; AAA2C)</td>
</tr>
</tbody>
</table>

Markus Jochim, General Motors Research
IEEE 802.1 Plenary Session
July 14 - 19, 2013 – Geneva, Switzerland
802.1ASbt Timing and Synchronization: **Enhancements and Performance Improvements**

802.1Qbv Enhancements for Scheduled Traffic: a basic form of **time-triggered communication**

802.1Qbu Frame Preemption: a mechanism that allows to preempt a frame in transmit to intersperse another frame.

802.1Qca Path Control and Reservation: protocols and mechanisms to set up and **manage the redundant communication paths** in the network.

802.1CB Frame Replication and Elimination for Reliability: to **eliminate redundant copies of frames** transmitted over the redundant paths setup in 802.1Qca.

802.1Qcc – enhancements and improvements for stream reservation
The clock synchronization protocol is a classical master-slave protocol. The master is called the “grandmaster”. When the grandmaster fails, then a new grandmaster is elected. Issues with this mechanism have been reported by industry.
802.1ASbt Clock Synchronization
Proposals for Improvements

Active Case: sends its own Sync (bSync).
Passive Case: detects Primary Sync (pSync) msg and only upon timeout, sends its own bSync. Often shorter hold-over time than Ethernet Stations.

SAE AS6802 –
Fault-Tolerant Clock Synchronization

TTEthernet Executable Formal Specification
• Using symbolic and bounded model checkers sal-smc and sal-bmc
• Focus on Interoperation of Synchronization Services (Startup, Restart, Clique Detection, Clique Resolution, abstract Clock Synchronization)

Verification of Lower-Level Synchronization Functions
• Permanence Function (sal-inf-bmc + k-induction)
• Compression Function (sal-inf-bmc + k-induction)

Formal Verification of Clock Synchronization Algorithm
• First time by means of Model Checking (sal-inf-bmc + k-induction)

Re-use of the Formal Models to prove:
• Layered clock-rate correction algorithm (sal-inf-bmc + k-induction)
• Layered clock-diagnosis algorithm (sal-inf-bmc + k-induction)

Verification and minor corrections of the “Sparse Timebase” Concept
• Distributed computations without explicit coordination (PVS)

Work has mostly been done in the context of the Marie Curie CoMMiCS project
FP7 (FP7/2007-2013) project no. 236701
SAE AS6802 – Fault-Tolerant Clock Synchronization

Ensuring Reliable Networks

Copyright © TTTech Computertechnik AG. All rights reserved.

www.tttech.com

Automated Formal Verification of the TTEthernet Synchronization Quality

SMT-Based Formal Verification of a TTEthernet Synchronization Function

TTEthernet Executable Formal Specification

• Using symbolic and bounded model checkers sal-smc and sal-bmc

• Focus on Interoperation of Synchronization Services (Startup, Restart, Clique Detection, Clique Resolution, abstract Clock Synchronization)

Verification of Lower-Level Synchronization Functions

• Permanence Function (sal-inf-bmc + k-induction)

• Compression Function (sal-inf-bmc + k-induction)

Formal Verification of Clock Synchronization Algorithm

• First time by means of Model Checking (sal-inf-bmc + k-induction)

Re-use of the Formal Models to prove:

• Layered clock-rate correction algorithm (sal-inf-bmc + k-induction)

• Layered clock-diagnosis algorithm (sal-inf-bmc + k-induction)

Verification and minor corrections of the "Sparse Timebase" Concept

• Distributed computations without explicit coordination (PVS)

Work has mostly been done in the context of the Marie Curie CoMMiCS project FP7 (FP7/2007-2013) project no. 236701

Abstract: Clock synchronization is the foundation of distributed real-time architectures such as the Time/Triggered Architecture. Mainly, protocols that have been developed in the synchronous system model. Due to the local clocks, the local clocks synchronize clock synchronization algorithms have to be tested on digital test cases. In this paper, we present an automated proof of the TTEthernet clock synchronization algorithm that is based on the SMT model checker.

Wilfried Steinert and Bruno Dutertre
TTTech Computertechnik AG, Chip IP Design, A-1020 Vienna, Austria
wilfried.steinert@tttech.com
TTEthernet Executable Formal Specification

2014/04/30

Copyright © TTTech Computertechnik AG. All rights reserved.

www.tttech.com
"Architecture Design is Interface Design" [Kopetz]

Red Interface specifies the behavior of the FT Clock Generator 
*as observed by the connecting bridges of the IEEE 802.1 network.*

Internal behavior of the FT Clock Generator may (and most likely will) *be much more complex* than as observed at the interface.

Blue Interface specifies the behavior of the FT Clock Generator *as observed by the FT Clock Consumers.*
The red interface is different from the blue interfaces, because there *is additional behavior introduced by the IEEE 802.1 network* connecting the FT Clock Generator to the FT Clock Consumers.

Both, red and blue, interfaces need to be specified to enable the usage of a fault-tolerant timebase.
SUMMARY AND OUTLOOK
Summary

Our daily life more and more depends on dependable systems. The interconnection and networking of these systems is a main aspect. We see a cross-industry trend towards the use of Ethernet in time-critical, safety-related, and also safety-critical systems, for example in the automotive industry.

Plain Ethernet as of today does not provide all functions to allow building distributed dependable systems.

Hence, Ethernet variants have been developed, for example TTEthernet (standardized as SAE AS6802) that defines a time-triggered paradigm and mixed time-triggered event-triggered paradigm for Ethernet.

Currently, the IEEE is improving native Ethernet with real-time and dependability functions.
Summary

In particular, IEEE 802.3 develops and maintains the Ethernet PHY (e.g., the Reduced Twisted Pair Gigabit Ethernet – RTGBE for automotive use) and MAC standards, IEEE 802.1 develops and maintains bridging (aka switching) standards.

With AVB, the IEEE has moved Ethernet into the real-time applications domain.

With TSN, the IEEE currently moves Ethernet into the hard real-time applications domain and improves Ethernet’s robustness.

With the growing competences in the IEEE standards, products built on these standards increase their market potential.

Well-defined interfaces allow to re-use existing fault-tolerant clock-synchronization protocols.
Outlook: Networks are everywhere

In the European-funded ACROSS project we investigated Network-on-Chip technologies and developed a Time-Triggered Network-on-Chip (TTNoC)

http://www.across-project.eu/
Outlook: Networks are everywhere

In the recently started and European-funded DREAMS project we are taking a holistic view on distributed dependable system as a system-of-systems. Thereby, we research networks on different levels: on-chip, on-board (e.g., on a PCB), within a box, and “local area” network.

In particular we are interested on emerging benefits that come with the realization of the time-triggered paradigm on all these different hierarchical levels.

http://www.dreams-project.eu/
Recent Book on Time-Triggered Technology

Recent Book on Real-Time Systems