Partitioned and Composable Communication Systems for Mixed Criticality Architectures

Safe & Secure Systems & Software Symposium
June 3, 2009, Dayton, OH

Reinhard Maier, TTTech Computertechnik AG
Embedded, Real-Time Communication

Smart Distributed System with Sensors, Actuators and Hard Real-Time Control Loops

Time-Triggered Communication Network
Intended Application Domain

Application Domain
- Distributed systems with “hard real-time” requirements
- Fault-tolerant systems
  - Fail-safe
  - Fail-operational
- Highly reliable systems
- Deterministic systems
- Modular systems

TT Buses Facilitate
- Structured design
- Reduced system complexity
- Composability
- Full system simulation
- Fault tolerance
- Testability
- Mixed criticality
- Incremental certification
- Pre-certified components
Challenges addressed by time-triggered data buses:

- Management of complexity
- Design for certification
- Better testability
- Strong partitioning and mixed criticality
- Composability and better integration
- Fault tolerance and fail-operational operation
- Predicable run-time behavior
VxWorks 653 IMA Architecture

XML Configuration Data

ARINC 653 Application Executive

Hardware Board
Time-Triggered Operation

- All protocol operations are initiated at a priori known points in time.
- No external (application) control over the protocol progression.
- All nodes agree a priori on the points in time when send and receive operations are carried out.
- TDMA media access is collision-free and immediate.
Application Messages inside a Frame

- This statically defined pattern is a **complete communication specification**:
  - It specifies timing and order of all transmissions.
  - It is composable, testable and guaranteed.
Composability

- Temporal behavior is independent from the number of nodes
  - Support for independent test
  - Simplified system integration

- Node timing is defined globally (is part of system specification)
  - Simulation and implementation have identical interface behavior
  - Simplified system integration
Key Advantages

Modular Platform

- Separation of platform and application software
- Platform to develop leading edge functions
  - Function distribution
  - Integrated functions
  - Faster turn-around times
    - Simulation
    - Rapid prototyping
    - Code generation
  - Safety and fault tolerance
Key Advantages

Addresses Complexity Growth

- Composable interface technology
  - Interface precisely defined in value and time domain
  - Time-triggered fully deterministic system
  - Integration and testing effort scales with complexity (no exponential explosion)
- Interface controlled by system integrator
- Full tool support

→ Reduced integration and testing effort (cost & time)
TTP - Time Triggered Protocol
Network

Smart Distributed System with Sensors, Actuators and Hard Real-Time Control Loops

App1a
App1b
App2
AppN

CNI
Time-Triggered Controller

Time-Triggered Communication Network (TTP) with Built-In Health Monitoring and Redundancy Services
- The TDMA round is divided into slots: one for each node.
- TTP uses two redundant channels for communication. The sender sends two frames, one on each channel.
- Slots and frames can have different length.
- Different data can be sent on channel 0 and channel 1.
A cluster cycle is a sequence of TDMA rounds.
A TDMA round is a sequence of slots. A slot contains frames.
This statically defined pattern is a **complete communication specification**:
- It specifies timing and order of all transmissions.
- It is composable, testable and guaranteed.

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Hosts</th>
<th>brake_FL_slot</th>
<th>brake_RR_slot</th>
<th>brake_master_1_slot</th>
<th>brake_RL_slot</th>
<th>ABS_control_slot</th>
<th>brake_FR_slot</th>
<th>brake_master_2_slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>brake_FL</td>
<td>brake_RR</td>
<td>brake_master_1</td>
<td>brake_RL</td>
<td>ABS_control</td>
<td>brake_FR</td>
<td>brake_master_2</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>340</td>
<td>2</td>
<td>680</td>
<td>4</td>
<td>1425</td>
<td>5</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>5</td>
<td>1765</td>
<td>6</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>10</td>
<td>6</td>
<td>2100</td>
<td>7</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>10</td>
<td>12</td>
<td>7</td>
<td>2400</td>
<td>8</td>
</tr>
</tbody>
</table>

---

The table above illustrates the timing and order of transmissions for each slot and round.
Features and Resulting Benefits

- Time-triggered operation
- Global clock synchronization
- Membership service
- Babbling idiot avoidance
- Consistency support
- Multiplexing
- Determinism
- Modularity/composability
- Fault tolerance
- Distributed controls
- Partitioning
- Multiple SW levels
- High integrity
- High availability
Certifiable Run-Time Component

- Operating System: TTP-OS
- Download: TTP-Loading Library
- Fault-Tolerant Communication Layer: TTP-Table-Driven COM Layer
- TTP-Driver

Certifiable COTS Components
**TTP Tools**

**TTP Matlink** and **TTP SCADELink**  
SCADE, MATLAB/Simulink Integration

**TTP Plan** – Cluster Design, Scheduling

**TTP Build** – Middleware Configuration

**TTP Verify / TTP TD-COM Verify** Design Verification

**TTP View** – Monitoring, Validation

---

Code Generation:  
RTW Embedded Coder, TargetLink, SCADE KCG
Status: TTP for Aerospace & Defense

1999-2004

TTP-based FADEC (MAC)

2004-2009

TTP in A380, B787

2009-2014

- 2nd Source
- Standardization

www.tttech.com Copyright © 2008, TTTech Computertechnik AG. All rights reserved. Page 18
TTEthernet as COTS Platform Solution:
Technology Overview
TTEthernet Requirements

Scalable and Flexible Topology

Scalable Bandwidth

Scalable Safety and Fault Tolerance

Real-time and Synchronization

Integration with Existing Standards

Lower Cost
Pre-Configured Communication

Statically Configured 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, ...

High cost
Free-Form 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, ...

Low cost
Pre-Configured & Free-Form Communication

Statically Configured 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, ...

High cost

Free-Form 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, ...

Low cost

We see a market requirement to use the same physical network for data flows from both worlds.
TTEthernet in a Nutshell

TTEthernet

- is a *Transparent Fault-Tolerant Clock Synchronization Protocol*,
- on top of and fully compatible with *standard Ethernet* (IEEE 802.3),
- used to establish superior Quality-of-Service (QoS) traffic classes:
  - **Time-Triggered** (TT) Traffic based on synchronized time,
  - **Rate Constrained** (RC) Traffic compliant with ARINC 664, part 7 (AFDX),
  - **Best Effort Ethernet** (BE) Traffic compatible to the Internet.
- It is implemented jointly, by switches at various speeds (10/100/1000 Mbit/s), and end systems, either with software drivers only or with hardware support.

→ a dependable network to host systems of different levels of criticality
TTEthernet specifies an intelligent switch design that integrates data flows with different characteristics and ensures **partitioning** between them.

**Pre-planned Time-Triggered (TT) Data Flows**

Time-triggered data flows are configured in the switch.

Event-triggered data flows are dynamically integrated in between time-triggered data flows.

*Unused bandwidth allocated to time-triggered end systems is automatically reclaimed and available for event-triggered use!***
TTEthernet RC Dataflow

Rate-Constrained Traffic (RC)

Switch/Router

Receiver

Sender

min. duration  min. duration  min. duration
TTEthernet is the first protocol that allows true switched time-triggered data flows.
TTEthernet supports multiple islands of synchronization (synchronization at subsystem level, e.g. chassis, powertrain).
TTEthernet allows arbitrary tree network structures and extensions.
TTTech’s TTEthernet switches provide gateway extensions for legacy protocol support, e.g. TTP and CAN → reuse of legacy boxes.
End systems (ECUs) need only standard Ethernet interfaces, e.g. MPC5567. Time-triggered traffic can be implemented by software.
Sample TTEthernet
Scalable Synchronization Service

- Time-triggered subsystem can be set up locally with at least one time-triggered switch / end system
- Rate-constrained hard real-time operation always possible without synchronization

Switches and Fault Tolerance

- Defined failure hypothesis allows scalable number of tolerated failures, provided adequate resources are available.
- Replicated communication path design guarantees transmission of messages even if one switch becomes faulty.
- Buffered switch technology allows for speed conversion from 10 Mbit/s to 100 Mbit/s to 1 Gbit/s and vice versa.

Certification

- Hardware: DO-254 Level A
- Software: DO-178B Level A
Flexible Integration

- TTEthernet can be applied at the field bus and/or the backbone level

Compatibility

- Legacy backwards capability with other protocols
- Not necessary to use TTEthernet end-system hardware, possible to use existing COTS units (e.g. very low-cost CPUs with on-chip Ethernet controllers)

Scalability

- Subsystems can be as tightly coupled as needed within an application, and may be loosely coupled across subsystem boundaries, if required
- Enables less complex systems, especially once all levels of the system operate under TTEthernet
- Suitable for controls, multimedia, and many other real-time applications
Benefits of Time Triggered Technologies
Fault Tolerance
Trust isn’t enough!

High Integrity
High Availability
- Determinism
- Verifiability & Testability
- Partitioning and Mixing Criticality
- Complexity Reduction & Scalability
- Distributed Controls
- Flexibility
- Composability & Integration
Thank You!

Contact: maier@tttech.com