Ensuring Reliable Networks TTTech

Deterministic Ethernet

From Oriented Basic Research to a Powerful Technology Portfolio

Wilfried Steiner

at.linkedin.com/in/wilfriedsteiner

www.tttech.com

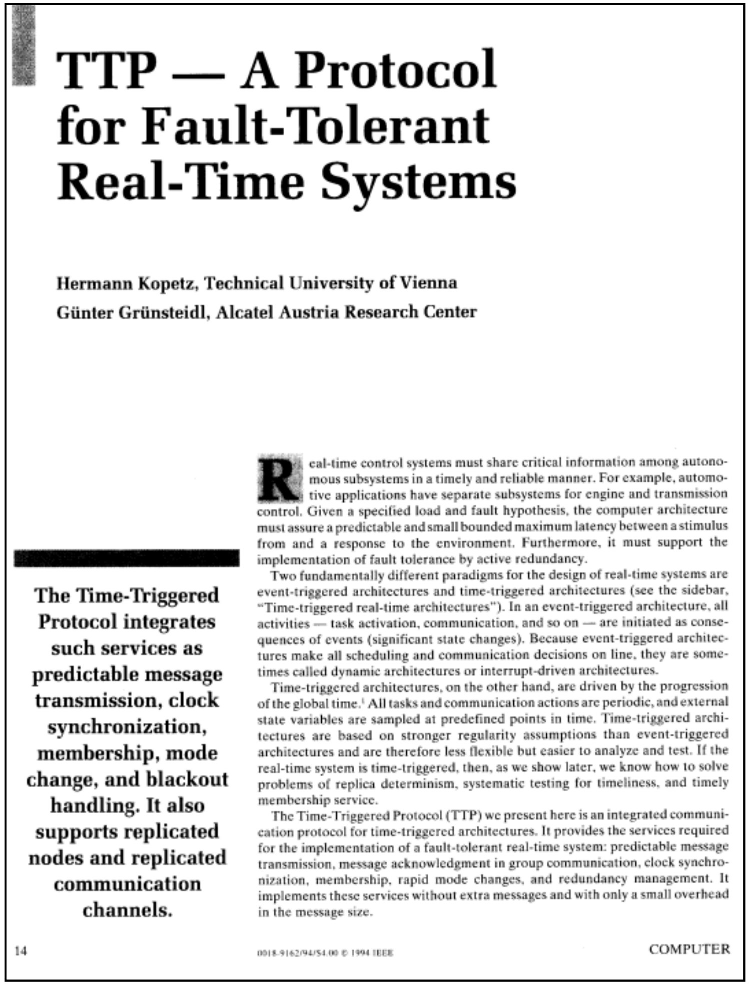
Oriented Basic Research

Oriented Basic Research

“Oriented basic research is research carried out with the expectation that it will <u>produce a broad base of knowledge</u> likely to form the <u>background to the solution</u> of recognised or expected current or future problems or possibilities.”

OECD Frascati Manual, Fifth edition, 1993, para. 227, page 50.

Deterministic Ethernet: Origins



TTP — A Protocol for Fault-Tolerant Real-Time Systems

Hermann Kopetz, Technical University of Vienna
Günter Grünsteidl, Alcatel Austria Research Center

Real-time control systems must share critical information among autonomous subsystems in a timely and reliable manner. For example, automotive applications have separate subsystems for engine and transmission control. Given a specified load and fault hypothesis, the computer architecture must assure a predictable and small bounded maximum latency between a stimulus from and a response to the environment. Furthermore, it must support the implementation of fault tolerance by active redundancy.

Two fundamentally different paradigms for the design of real-time systems are event-triggered architectures and time-triggered architectures (see the sidebar, "Time-triggered real-time architectures"). In an event-triggered architecture, all activities — task activation, communication, and so on — are initiated as consequences of events (significant state changes). Because event-triggered architectures make all scheduling and communication decisions on line, they are sometimes called dynamic architectures or interrupt-driven architectures.

Time-triggered architectures, on the other hand, are driven by the progression of the global time.[1] All tasks and communication actions are periodic, and external state variables are sampled at predefined points in time. Time-triggered architectures are based on stronger regularity assumptions than event-triggered architectures and are therefore less flexible but easier to analyze and test. If the real-time system is time-triggered, then, as we show later, we know how to solve problems of replica determinism, systematic testing for timeliness, and timely membership service.

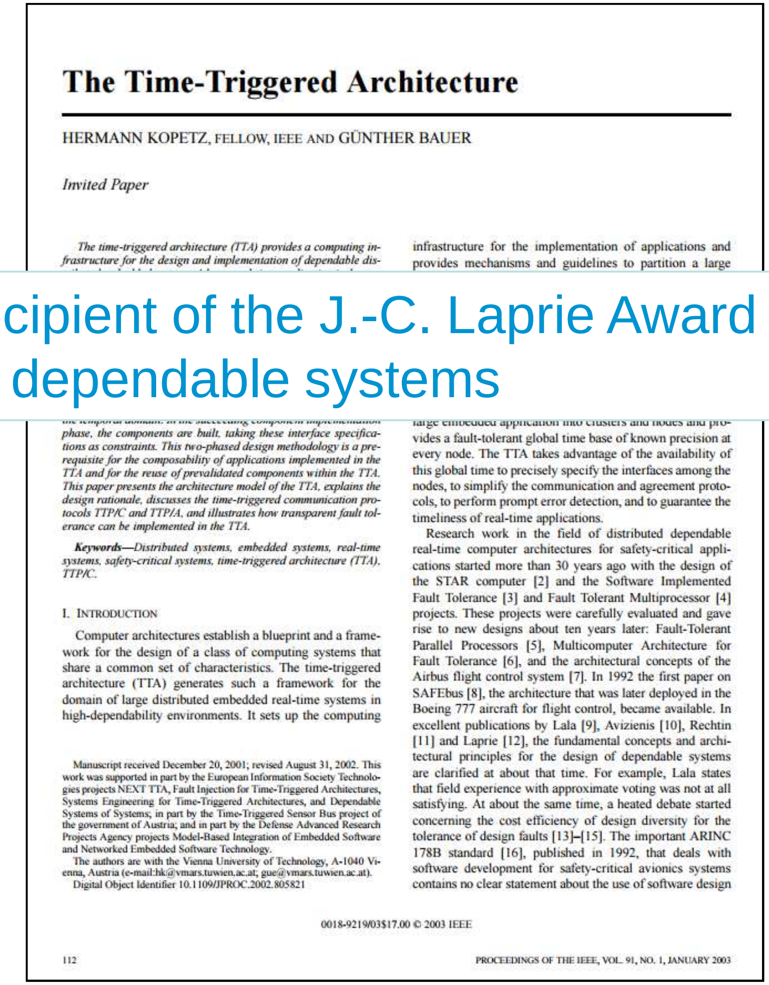
The Time-Triggered Protocol (TTP) we present here is an integrated communication protocol for time-triggered architectures. It provides the services required for the implementation of a fault-tolerant real-time system: predictable message transmission, message acknowledgment in group communication, clock synchronization, membership, rapid mode changes, and redundancy management. It implements these services without extra messages and with only a small overhead in the message size.

The Time-Triggered Protocol integrates such services as predictable message transmission, clock synchronization, membership, mode change, and blackout handling. It also supports replicated nodes and replicated communication channels.

0018-9162/94/$4.00 © 1994 IEEE

Kopetz, Hermann, and Günter Grünsteidl. "TTP-a protocol for fault-tolerant real-time systems." Computer 27, no. 1 (1994): 14-23.

Kopetz, Hermann, and Günther Bauer. "The time-triggered architecture." Proceedings of the IEEE 91, no. 1 (2003): 112-126.



The Time-Triggered Architecture

HERMANN KOPETZ, FELLOW, IEEE AND GÜNTHER BAUER

Invited Paper

The time-triggered architecture (TTA) provides a computing infrastructure for the design and implementation of dependable dis-

the temporal domain. In the succeeding component implementation phase, the components are built, taking these interface specifications as constraints. This two-phased design methodology is a prerequisite for the composability of applications implemented in the TTA and for the reuse of prevalidated components within the TTA. This paper presents the architecture model of the TTA, explains the design rationale, discusses the time-triggered communication protocols TTP/C and TTP/A, and illustrates how transparent fault tolerance can be implemented in the TTA.

Keywords—*Distributed systems, embedded systems, real-time systems, safety-critical systems, time-triggered architecture (TTA), TTP/C.*

I. Introduction

Computer architectures establish a blueprint and a framework for the design of a class of computing systems that share a common set of characteristics. The time-triggered architecture (TTA) generates such a framework for the domain of large distributed embedded real-time systems in high-dependability environments. It sets up the computing infrastructure for the implementation of applications and provides mechanisms and guidelines to partition a large

large embedded application into clusters and nodes and provides a fault-tolerant global time base of known precision at every node. The TTA takes advantage of the availability of this global time to precisely specify the interfaces among the nodes, to simplify the communication and agreement protocols, to perform prompt error detection, and to guarantee the timeliness of real-time applications.

Research work in the field of distributed dependable real-time computer architectures for safety-critical applications started more than 30 years ago with the design of the STAR computer [2] and the Software Implemented Fault Tolerance [3] and Fault Tolerant Multiprocessor [4] projects. These projects were carefully evaluated and gave rise to new designs about ten years later: Fault-Tolerant Parallel Processors [5], Multicomputer Architecture for Fault Tolerance [6], and the architectural concepts of the Airbus flight control system [7]. In 1992 the first paper on SAFEbus [8], the architecture that was later deployed in the Boeing 777 aircraft for flight control, became available. In excellent publications by Lala [9], Avizienis [10], Rechtin [11] and Laprie [12], the fundamental concepts and architectural principles for the design of dependable systems are clarified at about that time. For example, Lala states that field experience with approximate voting was not at all satisfying. At about the same time, a heated debate started concerning the cost efficiency of design diversity for the tolerance of design faults [13]–[15]. The important ARINC 178B standard [16], published in 1992, that deals with software development for safety-critical avionics systems contains no clear statement about the use of software design

Manuscript received December 20, 2001; revised August 31, 2002. This work was supported in part by the European Information Society Technologies projects NEXT TTA, Fault Injection for Time-Triggered Architectures, Systems Engineering for Time-Triggered Architectures, and Dependable Systems of Systems; in part by the Time-Triggered Sensor Bus project of the government of Austria; and in part by the Defense Advanced Research Projects Agency projects Model-Based Integration of Embedded Software and Networked Embedded Software Technology.

The authors are with the Vienna University of Technology, A-1040 Vienna, Austria (e-mail:hk@vmars.tuwien.ac.at; gue@vmars.tuwien.ac.at).

Digital Object Identifier 10.1109/JPROC.2002.805821

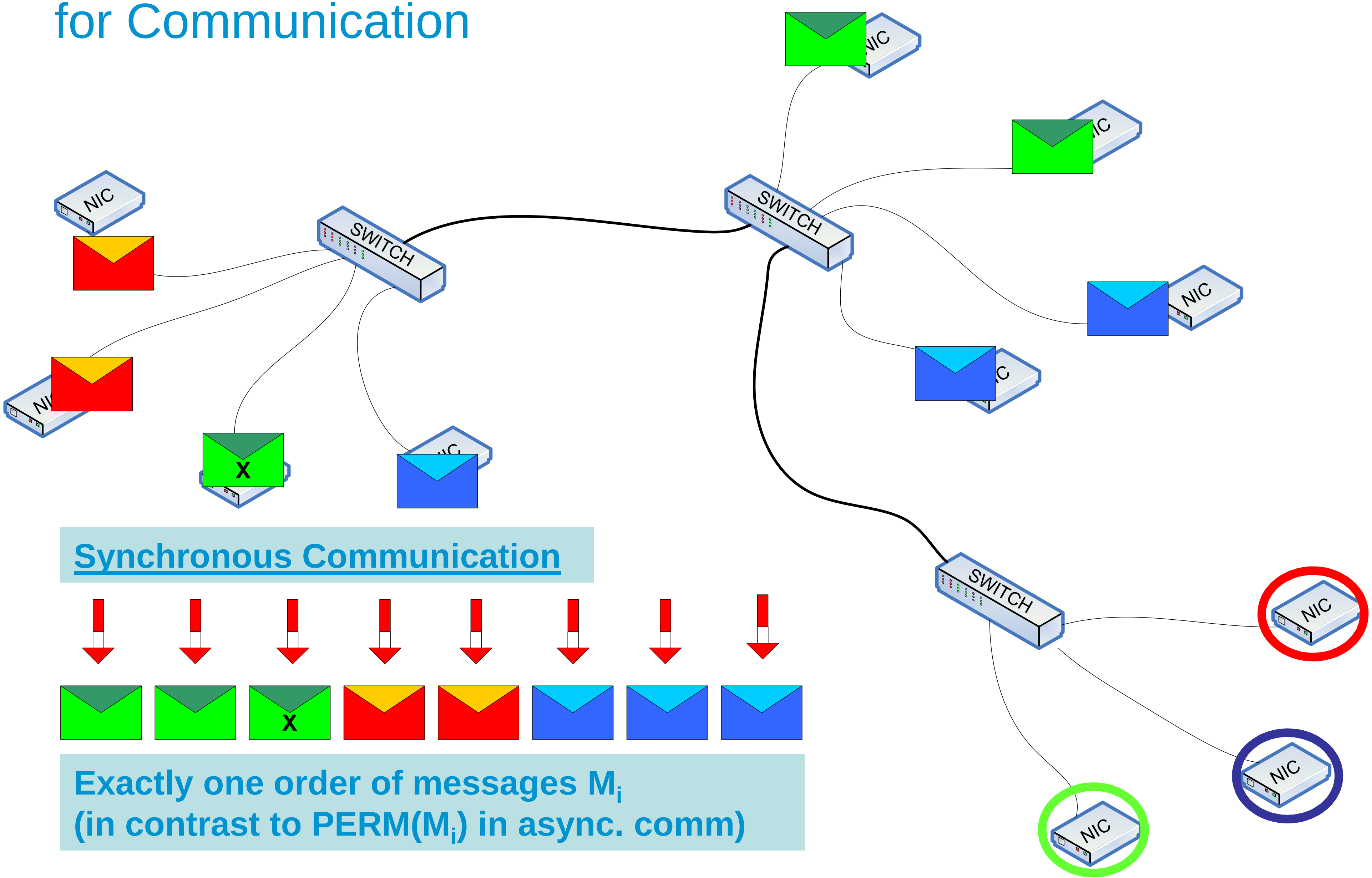
0018-9219/03$17.00 © 2003 IEEE

Recipient of the J.-C. Laprie Award for dependable systems

The Time-Triggered Paradigm

- Nodes (processes, switches, end systems, etc.) synchronize local timers to each other.
- Events are off-line scheduled with respect to the synchronized time to avoid resource conflicts.
- For example,
  - time-triggered communication may cause a node A to send a message M1 to a node B at time t1.
  - Likewise, the schedule may instruct another node C to send a message M2 to node B at another point in time t2.
  - Thus, the transmissions of M1 and M2 are separated in time.

Example: Time-Triggered Paradigm for Communication



Synchronous Communication

**Exactly one order of messages M_i
(in contrast to PERM(M_i) in async. comm)**

Broad Base of Knowledge

- Fault-Tolerant Clock Synchronization
  - Kopetz, Hermann, and Wilhelm Ochsenreiter. "Clock synchronization in distributed real-time systems." Computers, IEEE Transactions on 100, no. 8 (1987): 933-940.
- Communication Scheduling
  - how to find points in time t1, t2, etc.; how to execute a schedule
- Membership Service
  - identify which systems are synchronized and which are not
- Local and Central Guardian
  - fault-masking mechanisms, e.g., to mask the “babbling idiot” failure
- Architecture Design

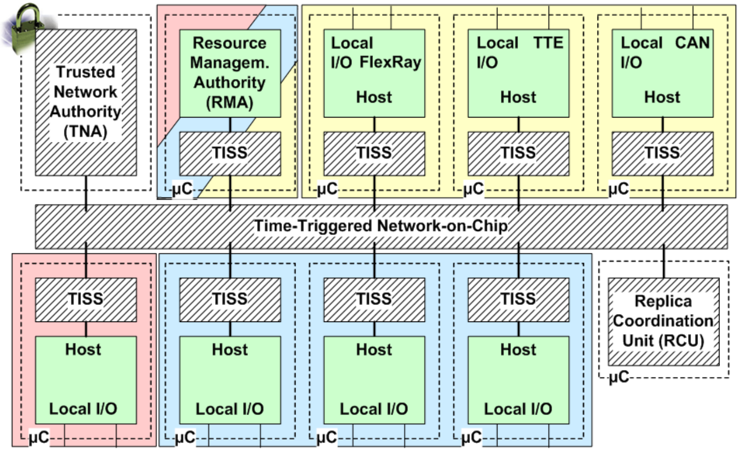
Background of Solutions

- TTP

- FlexRay

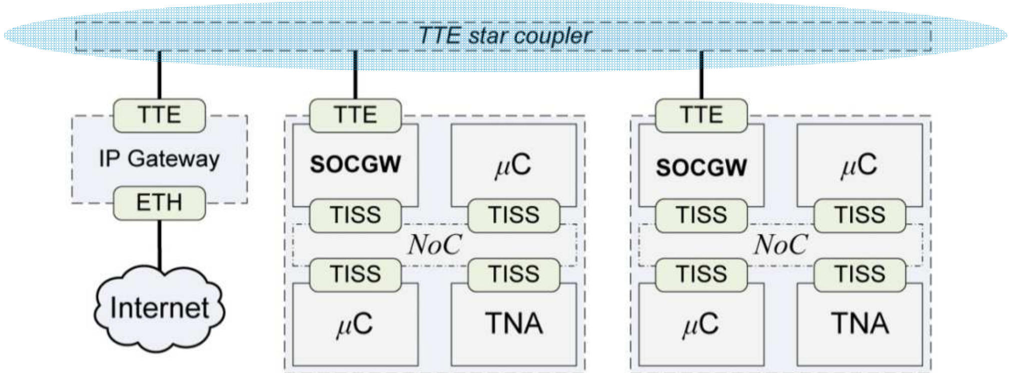
Mixed-criticality platforms evolve

- Cross-industry growth in embedded systems applications
  - e.g., top-of-the-line cars comprise already beyond 100 ECUs
- Growth of silicon capabilities
  - especially many-core, multi-core



→Integrated architectures that allow hosting applications with <u>mixed criticality become cost-efficient</u>.

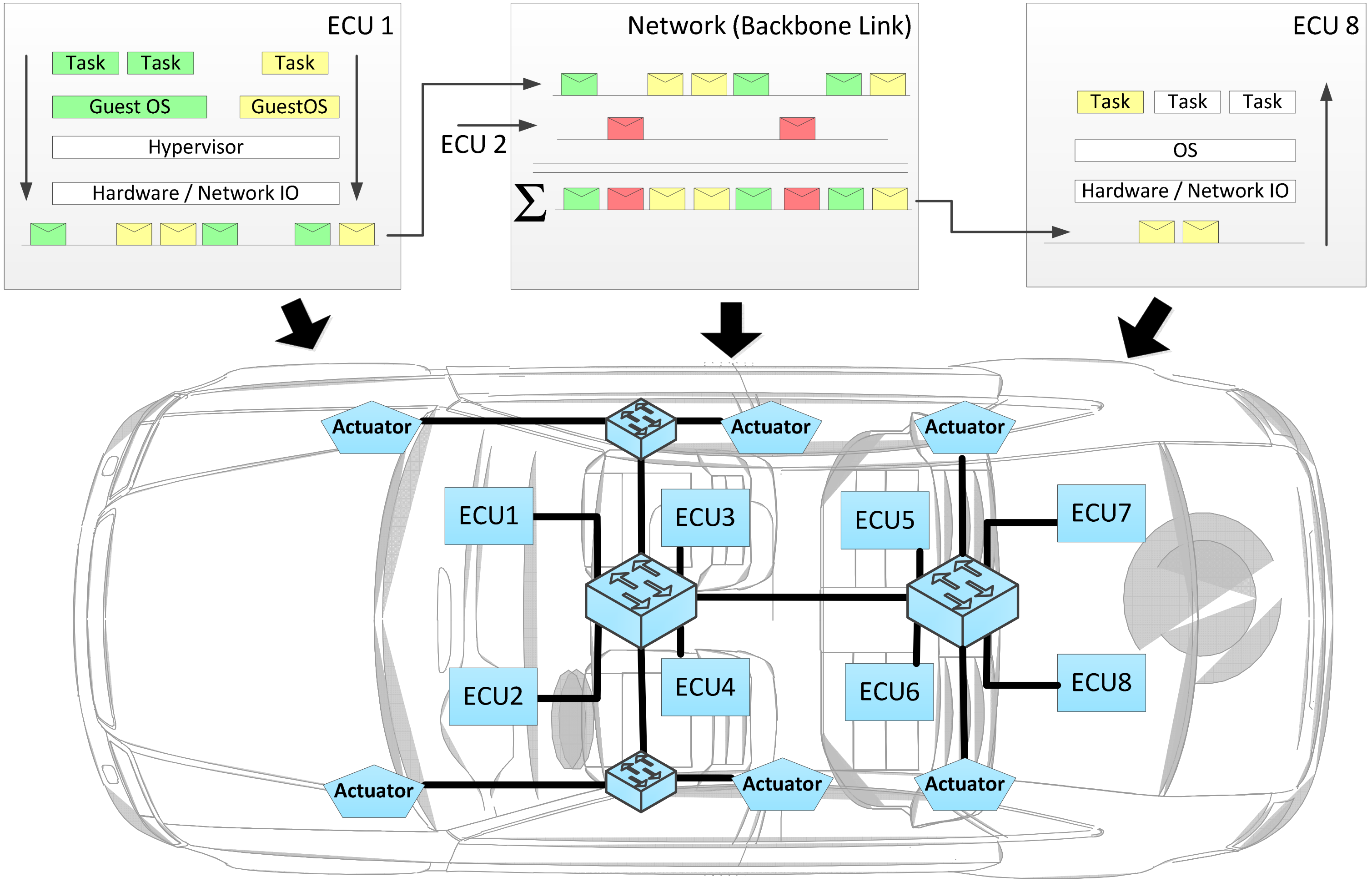
→Mixed-criticality on a node level is supported by <u>mixed-criticality on a network level</u>.



www.tttech.com

Mixed-criticality network support

TTTech



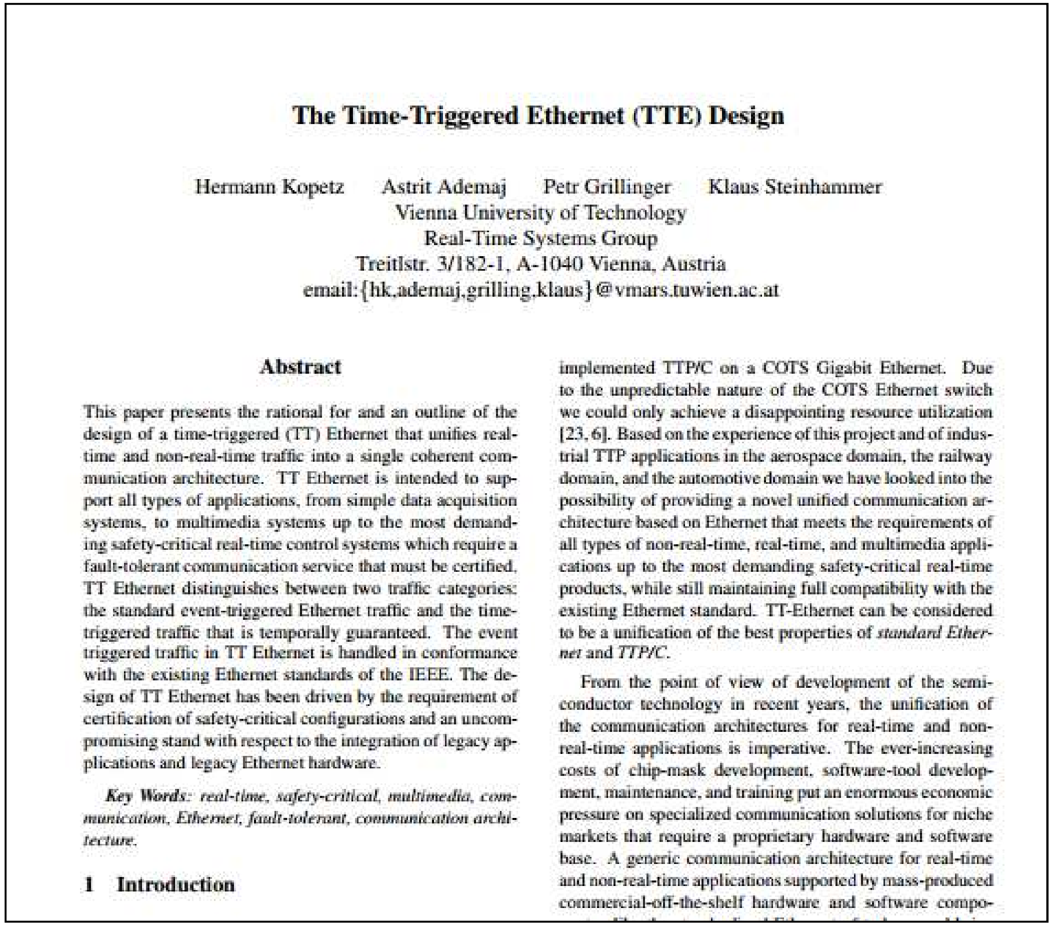
www.tttech.com

Real-Time design goals: - minimize interferences on the network

- allow real-time and non real-time traffic

A network for mixed-criticality systems: Time-Triggered Ethernet

TTTech



The Time-Triggered Ethernet (TTE) Design

Hermann Kopetz Astrit Ademaj Petr Grillinger Klaus Steinhammer
Vienna University of Technology
Real-Time Systems Group
Treitlstr. 3/182-1, A-1040 Vienna, Austria
email:{hk,ademaj,grilling,klaus}@vmars.tuwien.ac.at

Abstract

This paper presents the rational for and an outline of the design of a time-triggered (TT) Ethernet that unifies real-time and non-real-time traffic into a single coherent communication architecture. TT Ethernet is intended to support all types of applications, from simple data acquisition systems, to multimedia systems up to the most demanding safety-critical real-time control systems which require a fault-tolerant communication service that must be certified. TT Ethernet distinguishes between two traffic categories: the standard event-triggered Ethernet traffic and the time-triggered traffic that is temporally guaranteed. The event triggered traffic in TT Ethernet is handled in conformance with the existing Ethernet standards of the IEEE. The design of TT Ethernet has been driven by the requirement of certification of safety-critical configurations and an uncompromising stand with respect to the integration of legacy applications and legacy Ethernet hardware.

Key Words: real-time, safety-critical, multimedia, communication, Ethernet, fault-tolerant, communication architecture.

1 Introduction

implemented TTP/C on a COTS Gigabit Ethernet. Due to the unpredictable nature of the COTS Ethernet switch we could only achieve a disappointing resource utilization [23, 6]. Based on the experience of this project and of industrial TTP applications in the aerospace domain, the railway domain, and the automotive domain we have looked into the possibility of providing a novel unified communication architecture based on Ethernet that meets the requirements of all types of non-real-time, real-time, and multimedia applications up to the most demanding safety-critical real-time products, while still maintaining full compatibility with the existing Ethernet standard. TT-Ethernet can be considered to be a unification of the best properties of *standard Ethernet* and *TTP/C*.

From the point of view of development of the semiconductor technology in recent years, the unification of the communication architectures for real-time and non-real-time applications is imperative. The ever-increasing costs of chip-mask development, software-tool development, maintenance, and training put an enormous economic pressure on specialized communication solutions for niche markets that require a proprietary hardware and software base. A generic communication architecture for real-time and non-real-time applications supported by mass-produced commercial-off-the-shelf hardware and software compo-

„This paper presents the rationale for and an outline of the design of a time-triggered (TT) Ethernet that unifies real-time and non-real-time traffic into a single coherent communication architecture.“

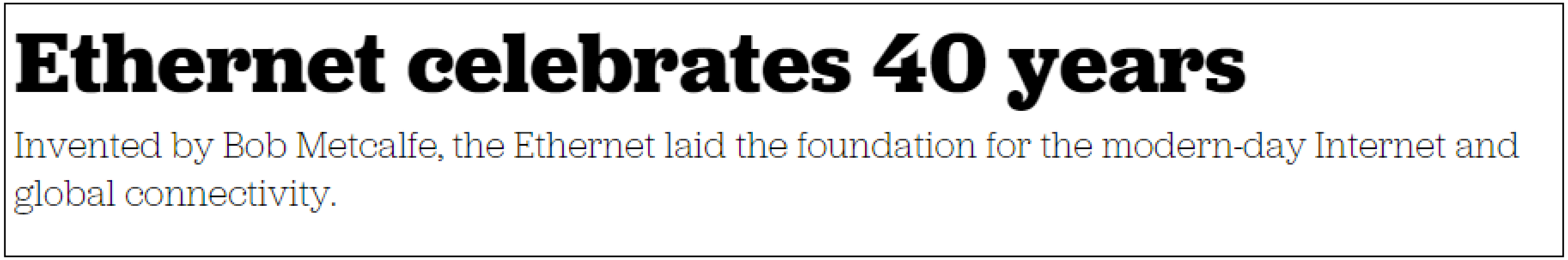
Kopetz, Hermann, Astrit Ademaj, Petr Grillinger, and Klaus Steinhammer. "The time-triggered ethernet (TTE) design." In Object-Oriented Real-Time Distributed Computing, 2005. ISORC 2005. Eighth IEEE International Symposium on, pp. 22-33. IEEE, 2005.

Some specifics of the early TTEthernet prototypes

- Compatible with standard Ethernet IEEE 802.3 (100Mbit/sec)
- Supports mixed-criticality on a node-level by providing mixed-criticality on the network-level
  - Distinguishes two traffic classes, time-triggered and best-effort (i.e., standard Ethernet)
  - Critical applications may use time-triggered communication
  - Less critical applications may use best-effort communication
- Design Detail: switches were designed to be simple.

  Thus, when in progress of transmitting a best-effort frame, they would preempt the frame transmission for time-triggered frames.

Ethernet – a success story on its own



Ethernet celebrates 40 years

Invented by Bob Metcalfe, the Ethernet laid the foundation for the modern-day Internet and global connectivity.

http://www.cnet.com/news/ethernet-celebrates-40-years/ May, 2013

Industrial Ethernet variants, e.g., ProfiNet, EtherCAT, Ethernet Powerlink, etc.

ARINC 664-p7, Avionics-Switched Full-Duplex Ethernet (AFDX®) http://www.afdx.com/pdf/ATM_AFDXTest_June05.pdf

TTTech

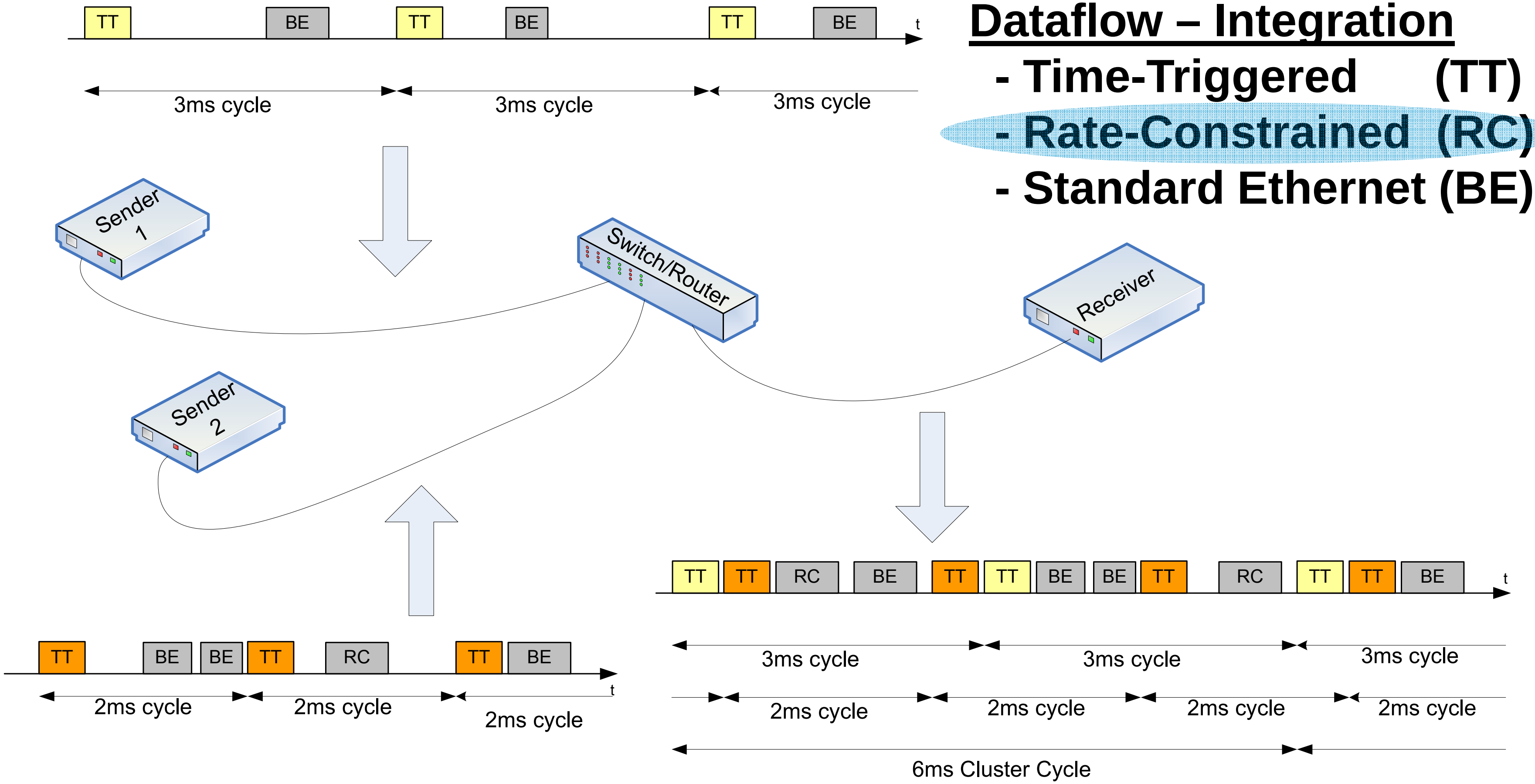
Transformation of the Technology into a Product

Initial Target Market: Avionics

- In general TTEthernet has been designed as communication platform for any system with mixed-criticality applications.
- Avionics has been the first target market.
- We used the avionics specific Ethernet variant (AFDX) as baseline protocol for TTEthernet, but at 1Gbit/sec
- Co-development of TU Vienna, TTTech, and Honeywell.

Integrating AFDX with TTEthernet Technology

TTTech



Dataflow – Integration

- **Time-Triggered (TT)**
- **Rate-Constrained (RC)**
- **Standard Ethernet (BE)**

TTEthernet Switches are non-preemptive store-and-forward switches using priorities

Enhanced Protocols for Fault-Tolerant Clock Synchronization

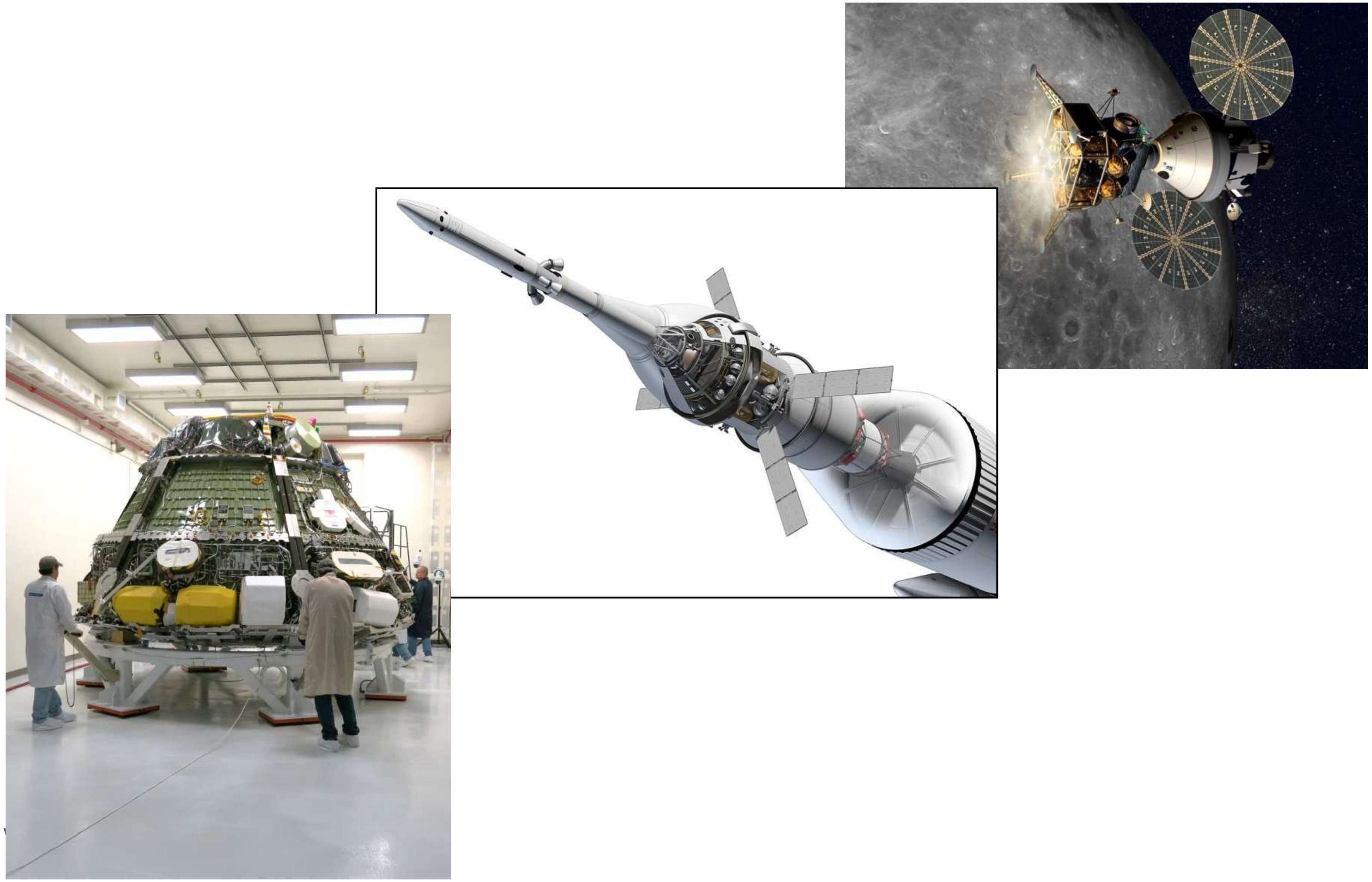
TTTech

- Target synchronization guarantee in the range of single digit microseconds (in distinguished settings even below one microsecond)
- Tolerates multiple concurrent failures
- Recovers from system-wide disturbances
- Design Detail: protocols take benefit of distributed algorithms as well as the high-integrity design of selected components.

No Frame Preemption

- Other than in the initial prototypes of TTEthernet, the product does not support preemption (at the time)
  - Switches become much more sophisticated, because the support AFDX. Thus, they can also store a schedule.
  - Move from 100Mbit/sec (prototype) to 1Gbit/sec (product) marginalized the latency benefit of preemption (in the initial target market)
  - Truncation of valid Ethernet frames complicates diagnosis
  - Truncation may “accidently” generate a valid frame

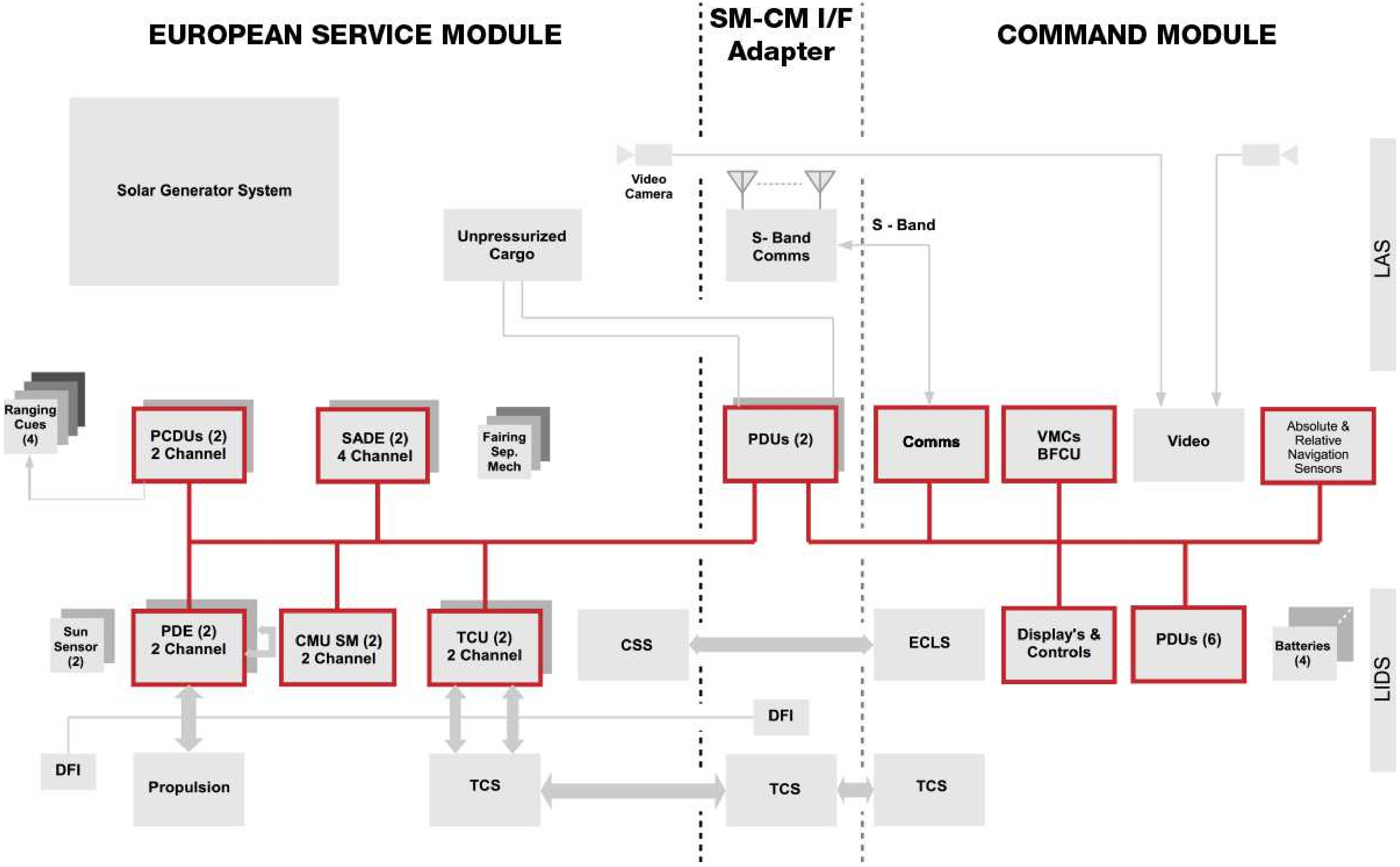
Example use case:
Orion Crew Module



Time Triggered Gigabit Ethernet

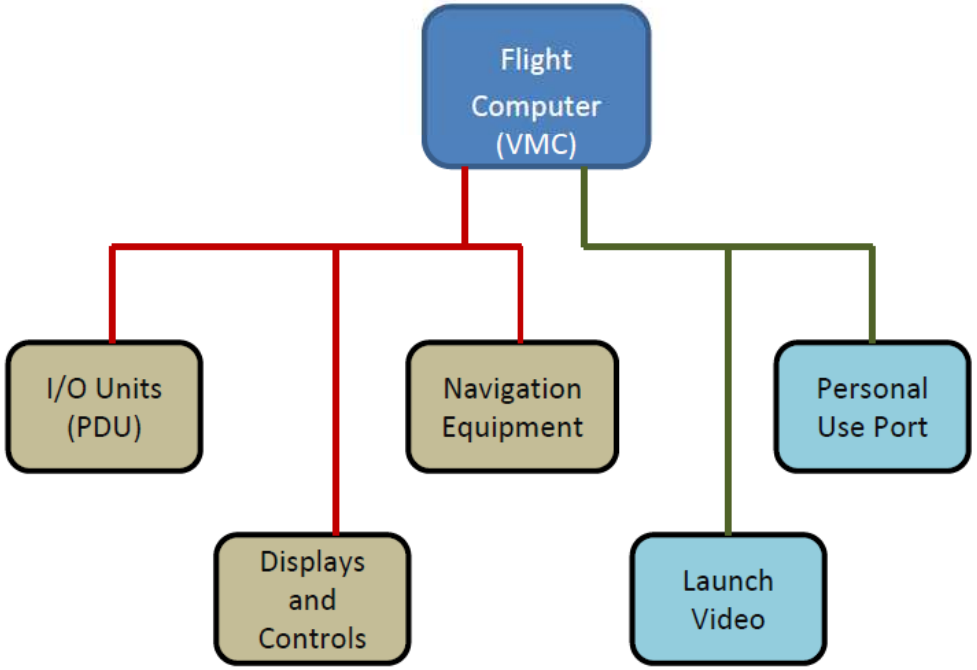
The Backbone of Orion's State of the Art, High Reliability Avionics System

48 Network end points 3 planes of connectivity for every device



Orion Network Unification

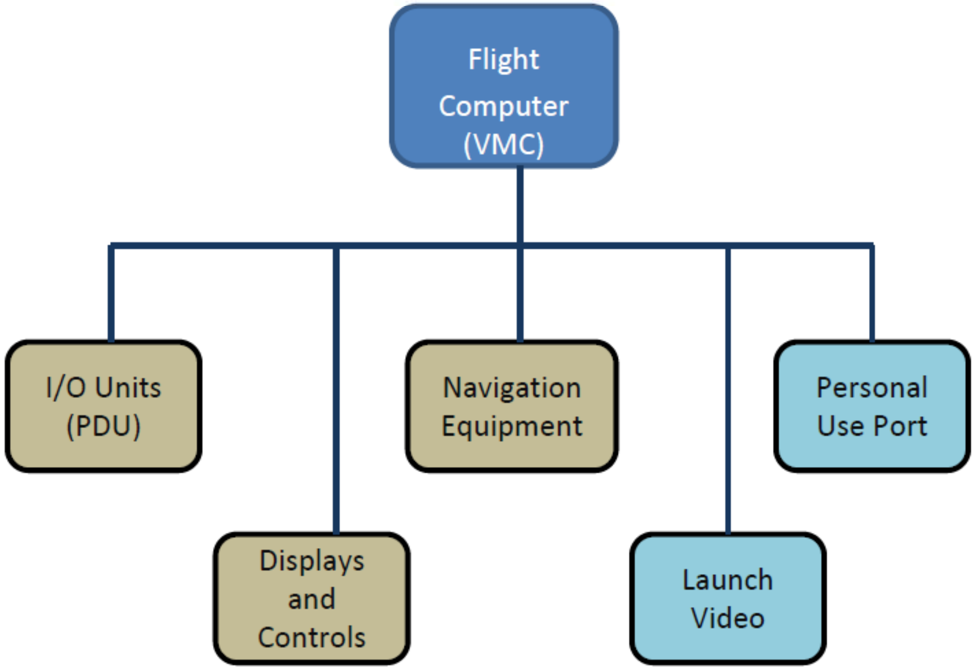
- The original Orion architecture contained two Ethernet-based data networks:



- A flight-critical control bus that handled time-sensitive and/or safety critical commands
- A general-purpose data bus that handled non-critical traffic such as video and personal crew equipment

Orion Network Unification

- However, to reduce vehicle size, weight, and power while maintaining acceptable reliability, Orion collapsed both networks into one, TTEthernet-based infrastructure



- Critical or time-sensitive data utilized time-triggered or rate-constrained TTEthernet traffic classes
- Video and personal crew data utilized the best effort TTEthernet traffic class

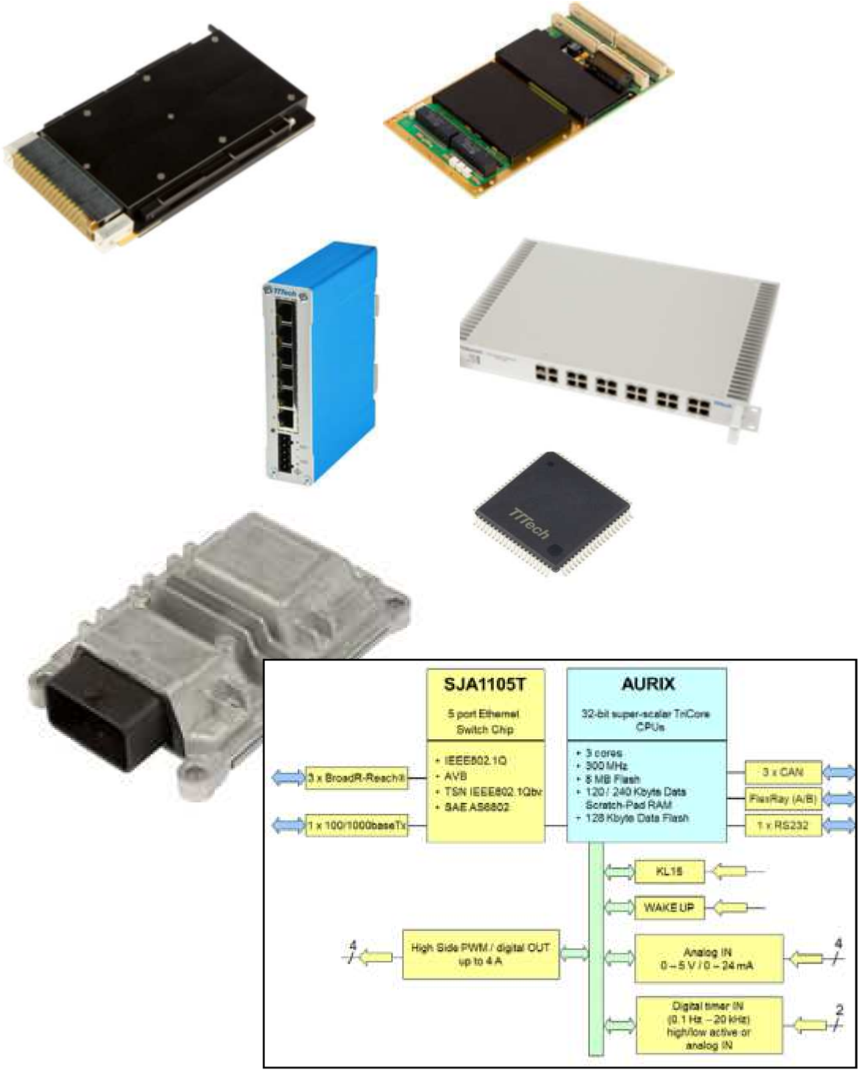
Clint Baggerman, NASA – Johnson Space Center, TTA Group Open Forum, Nov. 4th 2010

TTTech

Technology Portfolio

Cross-industry applicability

- Space programs
- Avionics programs
- Renewable energy
- Automotive
- Railway
- Industrial automation
- Process control


TTTech
SJA1105T
5 port Ethernet Switch Chip
• IEEE802.1Q
• AVB
• TSN IEEE802.1Qbv
• SAE AS6802
AURIX
32-bit super-scalar TriCore CPUs
• 3 cores
• 300 MHz
• 8 MB Flash
• 120 / 240 Kbyte Data Scratch-Pad RAM
• 128 Kbyte Data Flash
3 x BroadR-Reach®
1 x 100/1000baseTx
3 x CAN
FlexRay (A/B)
1 x RS232
KL15
WAKE UP
High Side PWM / digital OUT up to 4 A
4
Analog IN 0 – 5 V / 0 – 24 mA
4
Digital timer IN (0.1 Hz – 20 kHz) high/low active or analog IN
2

www.tttech.com

Product Variants

- Different number of ports
- Different speeds
- Different form factors
- Different safety standards
- Stand-alone switches vs. integrated switch/node
- Different functionality (Standards!!)

IT-OT Convergence

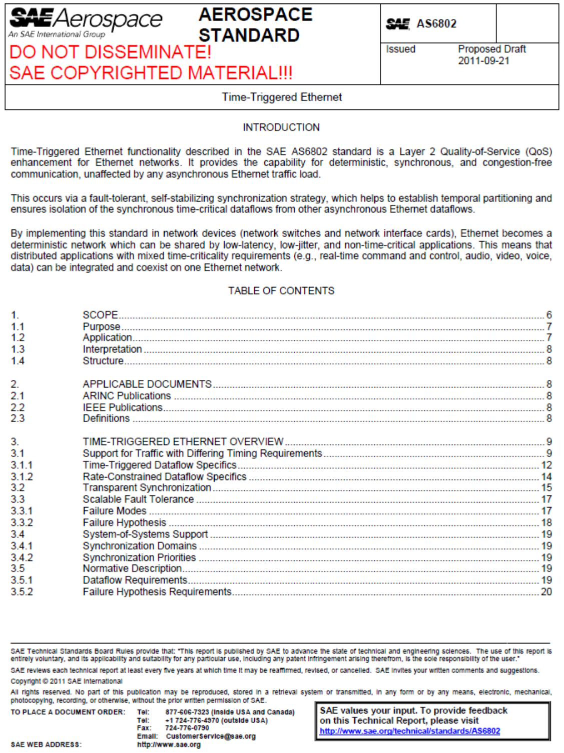
- Information Technology and Operations Technology converge
- Motor that drives smart* developments

- For us “OT networking people” this means: like Ethernet, more and more IT standards enter the OT domain.

Standardization

- The initial use cases for SAE AS6802 have been in the aerospace and space domain. SAE Aerospace has been a good fit as a standardization body, therefore.

- IEEE 802.1 and 802.3 is the natural home of Ethernet. In parallel to TTEthernet, there have been some interesting technology developments.



SAE Aerospace
An SAE International Group

AEROSPACE STANDARD

DO NOT DISSEMINATE!
SAE COPYRIGHTED MATERIAL!!!

SAE AS6802

Issued — Proposed Draft 2011-09-21

Time-Triggered Ethernet

INTRODUCTION

Time-Triggered Ethernet functionality described in the SAE AS6802 standard is a Layer 2 Quality-of-Service (QoS) enhancement for Ethernet networks. It provides the capability for deterministic, synchronous, and congestion-free communication, unaffected by any asynchronous Ethernet traffic load.

This occurs via a fault-tolerant, self-stabilizing synchronization strategy, which helps to establish temporal partitioning and ensures isolation of the synchronous time-critical dataflows from other asynchronous Ethernet dataflows.

By implementing this standard in network devices (network switches and network interface cards), Ethernet becomes a deterministic network which can be shared by low-latency, low-jitter, and non-time-critical applications. This means that distributed applications with mixed time-criticality requirements (e.g., real-time command and control, audio, video, voice, data) can be integrated and coexist on one Ethernet network.

TABLE OF CONTENTS

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be reaffirmed, revised, or cancelled. SAE invites your written comments and suggestions.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

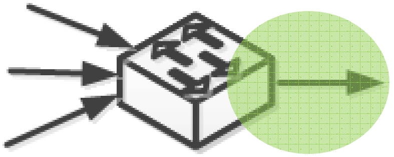
SAE values your input. To provide feedback on this Technical Report, please visit http://www.sae.org/technical/standards/AS6802

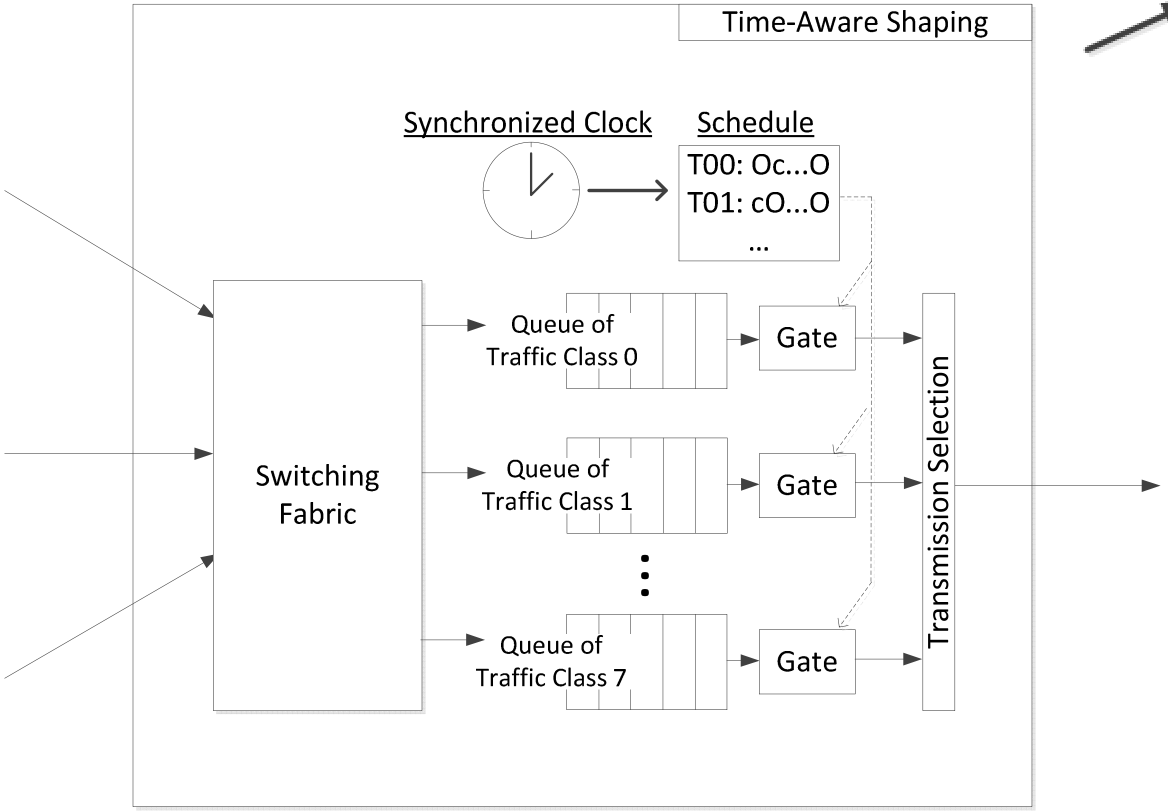
http://standards.sae.org/as6802

IEEE 802.1 standards

- With AVB (Audio/Video Bridging), IEEE 802.1 moved into the area of real-time communication
- With TSN (Time-Sensitive Networking), IEEE 802.1 moves into the area of hard real-time and reliable communication, e.g.,
  - 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.

Example: 802.1Qbv
Time-Aware Shaper





From the most recent draft standard IEEE 802.1Qbv-D.2.0

IEEE 802.1 standards

- TTTech engages in the IEEE standardization process since Jan/2012
- Deterministic Ethernet solutions are and will support the evolving TSN standard in its chip IP offering.
  - A clear focus will be put on features that are requested by and used in the market.

TTTech

Current & Future Pursuits

Electronic Robustness for a More Electric and Connected World

Autonomous & Near Autonomous Operations

$1.9 Trillion

Economic impact of near autonomous cars by 2025

Real-Time Internet of Things

25+ Billion

Embedded and intelligent systems by 2020

Every 2nd

Embedded device will be safety relevant by 2020

Safety & Reliability

Research Agenda

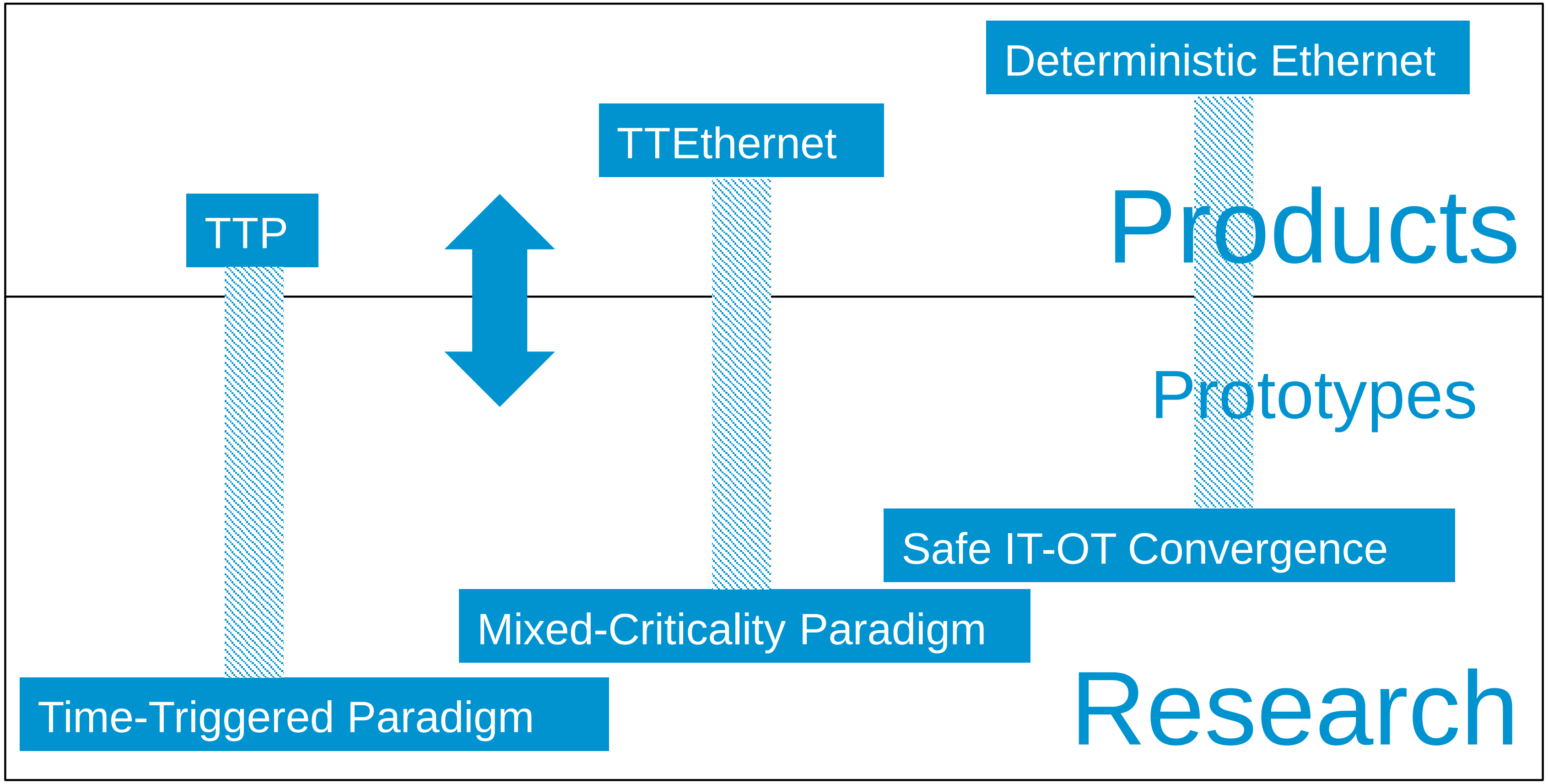
- Deterministic Wireless Communication (Pablo Gutierrez Peon)
  - Apply the time-triggered paradigm to wireless communication media, e.g., IEEE 802.11 (WiFi)
- Configuration and Management (Francisco Pozo, Marina Gutierrez)
  - Scheduling and performance analysis of extremely large networks (e.g., smart cities)
  - Increase flexibility and reconfiguration capabilities of time-triggered systems
- Security (Elena Lisova)
  - Development of a generic threat model for wired/wireless time-triggered systems and integration of security mechanisms (e.g., IPsec).
- Deterministic Computer Vision (Ayhan Mehmed)
  - Improve determinism and safety of computer vision systems via offline safety measuring/assessment and online safety monitoring

REA grant agreement no.607727

RETNET Real-Time Networks

Deterministic Ethernet Development Summary

TTTech



Conclusions

- Research in time-triggered communication and time-triggered architectures has *produced a broad base of knowledge.*
- Solutions that build on this knowledge are successfully deployed today.
- Steady and continuous research is essential to provide a strong theoretical foundation for new product generations.

TTTech

Thank you!
Questions?

Deterministic Ethernet Forum
October 23, 2015 – Vienna, Austria

https://www.de-forum.com/

Mixed-Criticality forum

http://www.mixedcriticalityforum.org

Become a TTTech University & Research Partner

www.tttech.com

TTTech

Ensuring Reliable Networks

Vienna, Austria (Headquarters)
Phone +43 1 585 34 34-0
office@tttech.com

USA
Phone +1 978 933 7979
usa@tttech.com

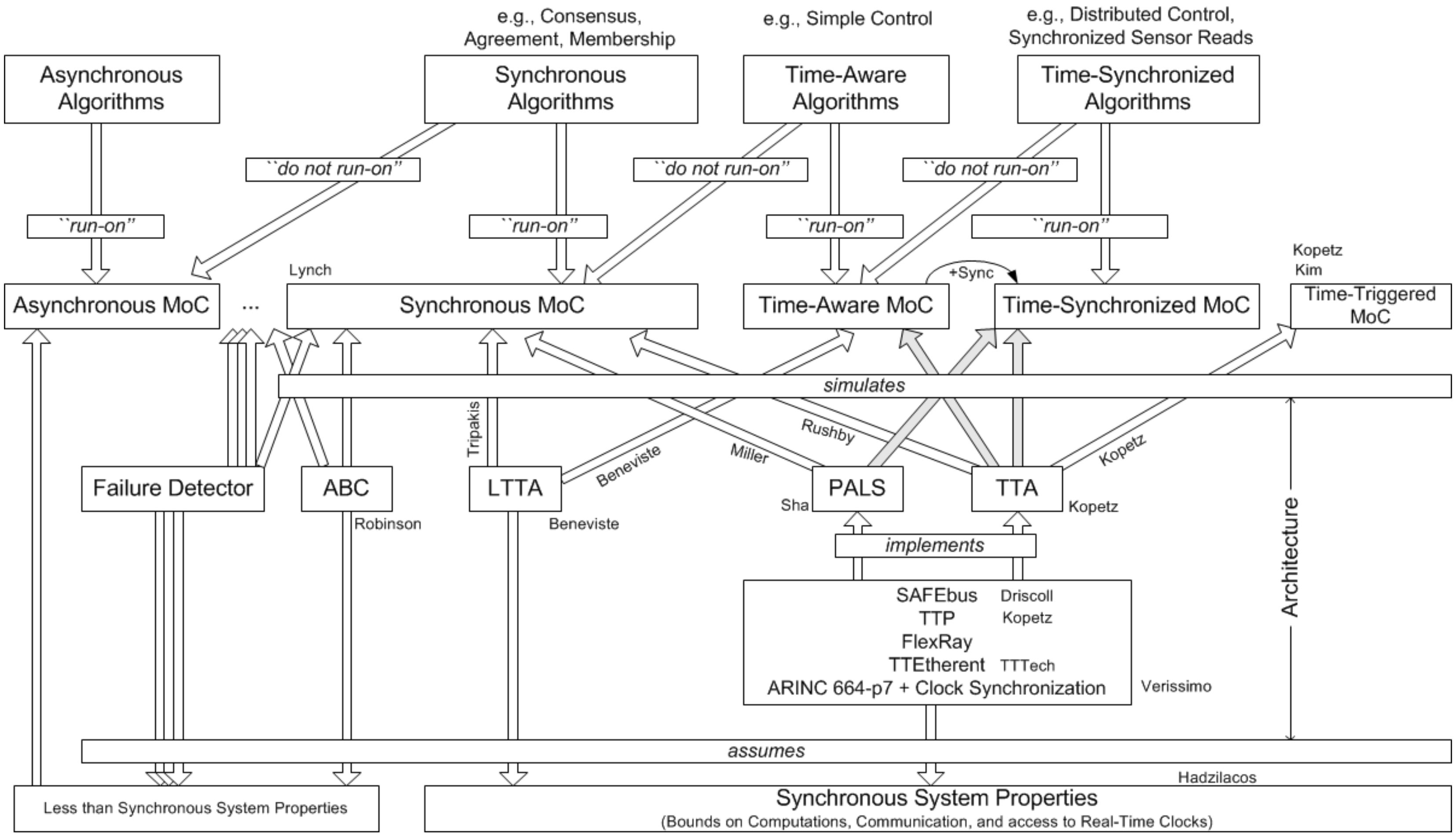
Japan
Phone +81 52 485 5898
office@tttech.jp

China
Phone +86 21 5015 2925-0
china@tttech.com

www.tttech.com

Backup

Common Architectures



www.tttech.com