TTEthernet Communication

Addressing Open System Requirements in addition to Safety and Fault-Tolerance

IFIP 10.4 Meeting Chicago
June, 27th

Stefan Poledna
stefan.poledna@tttech.com

What is TTEthernet?

TTEthernet =

Ethernet + Clock Synch. + Time-Triggered Communication + Rate Constrained Communication + Safety

Ethernet
- Established dominant standard
- IEEE 802.3

Clock Synch.
- coordination
- distributed control
- SAE AS6802
- IEEE 1588

Time-Triggered Communication
- real-time control (chassis, engine, active&passive safety systems)
- determinism

Rate Constrained Communication
- audio/video streaming
- sensor fusion
- ARINC 664, AVB

Safety
- ISO26262 ASIL D
- IEC 61508 SIL 4
- DO 254 Level A
- „By-wire“

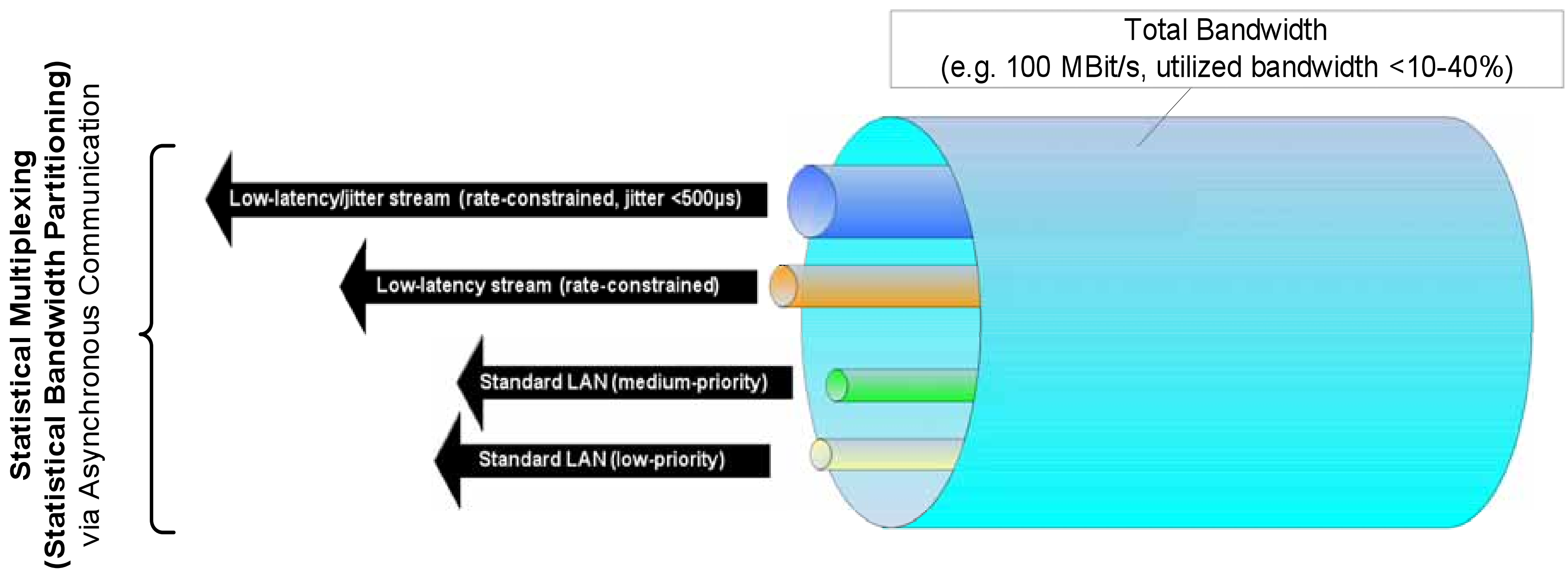
Integration of *all* data flows in one single network

- 100% compatible with Ethernet standard IEEE 802.3
- Scales from low to high speed (10 Mbit/s, 100 Mbit/s, 1 Gbit/s, …)
- Scales from simple to safe and high-availability systems

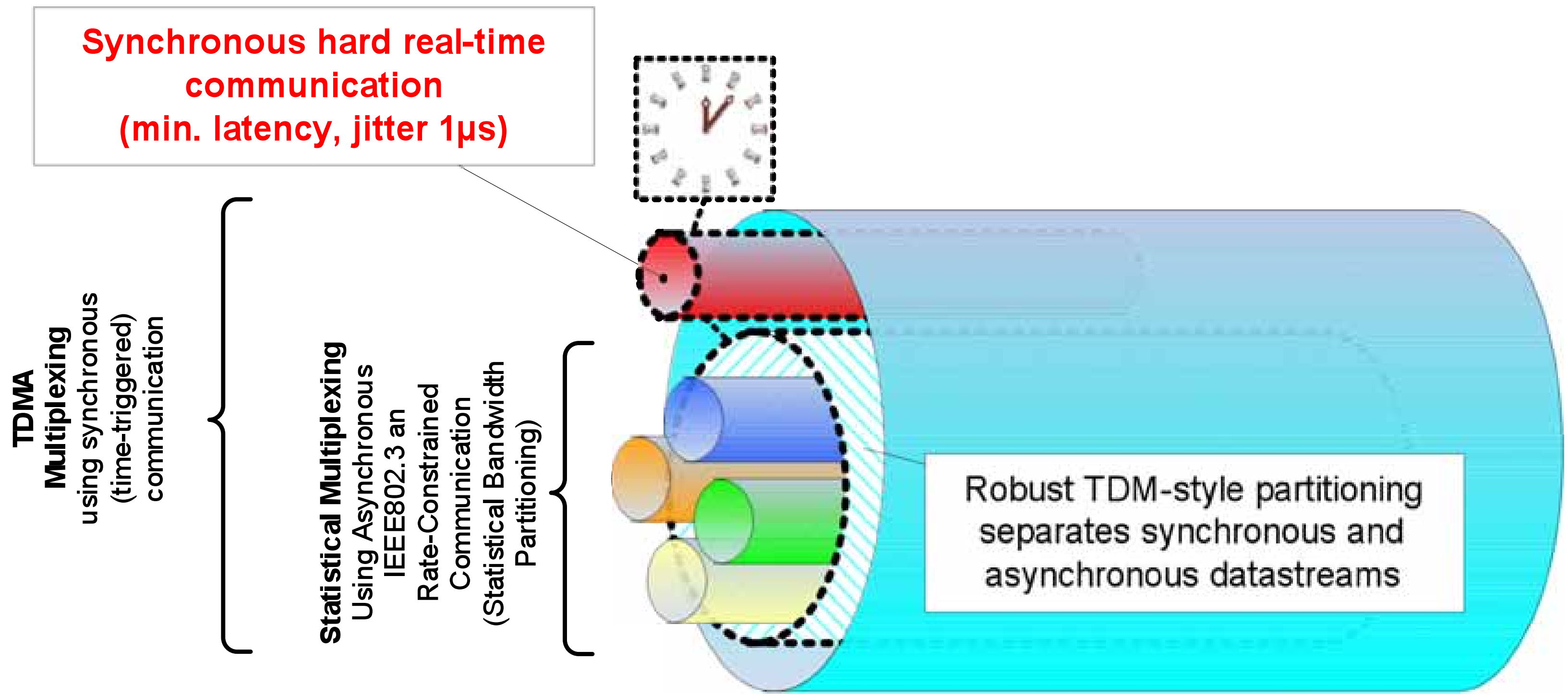
Ensuring Reliable Networks TTTech

Asynchronous (!): Statistical bandwidth partitioning

- Best effort communication - no absolute QoS guarantees
- Data traffic congestions or delays of critical communication possible
- No robust partitioning of communication bandwidth among functions

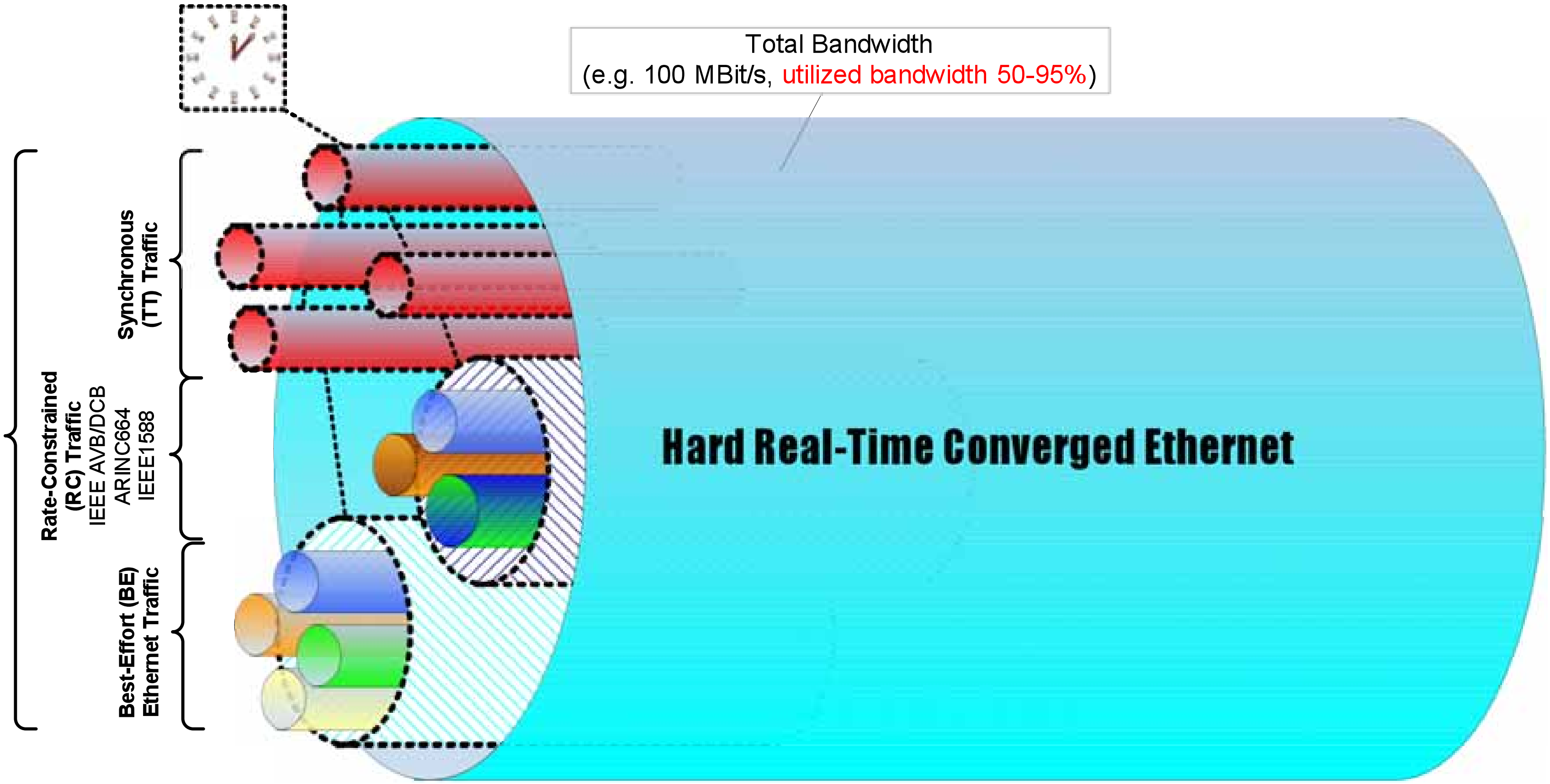


TTEthernet adds Time-Triggered Services



TTEthernet adds Rate-Constraint (Streaming) Services

- Bandwidth allocation / partitioning per virtual link (MAC address)

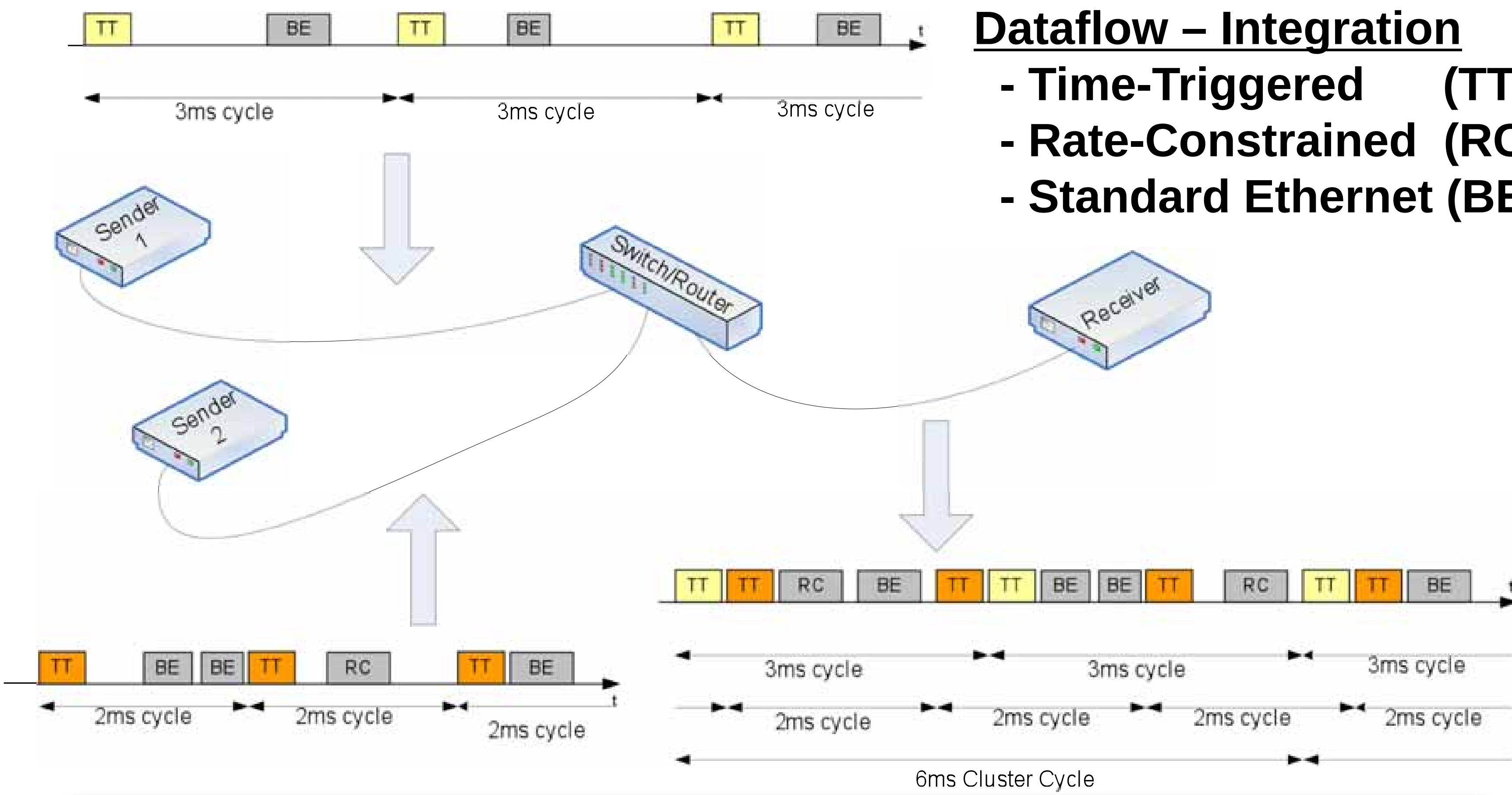


Dataflow in TTEthernet

Ensuring Reliable Networks TTTech

Dataflow – Integration

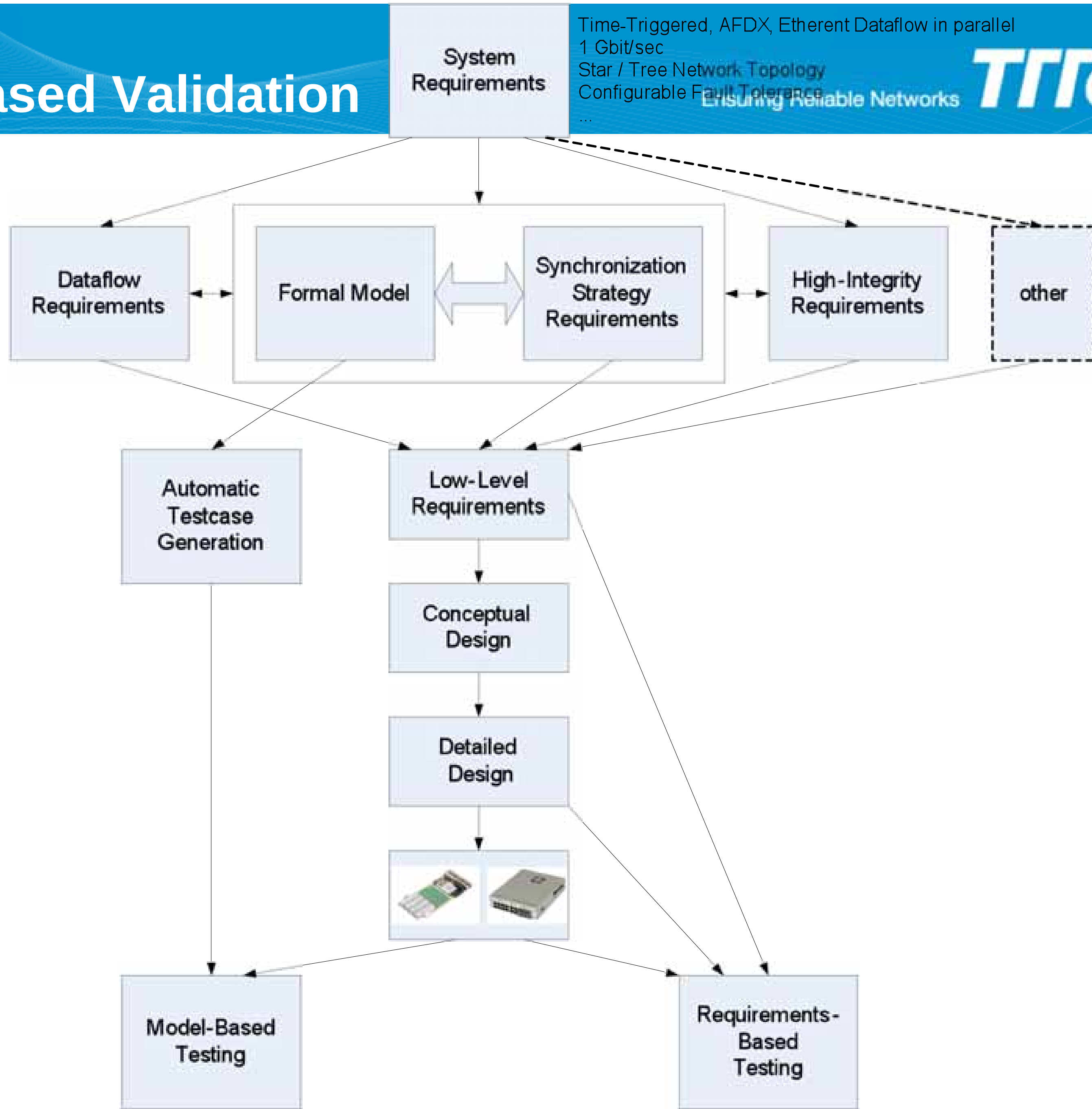
- Time-Triggered (TT)
- Rate-Constrained (RC)
- Standard Ethernet (BE)



TTEthernet Switch is also capable of changing traffic types, e.g. a message received as RC can be relayed as TT

Model-Based Validation

Time-Triggered, AFDX, Etherent Dataflow in parallel
1 Gbit/sec
Star / Tree Network Topology
Configurable Fault Tolerance
...



Formal Verification Activities

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
  - verified with the infinite-bounded model checker *sal-inf-bmc*
  - using disjunctive invariant and k-induction
- Compression Function
  - verified with the infinite-bounded model checker *sal-inf-bmc*
  - using abstraction and 1-induction

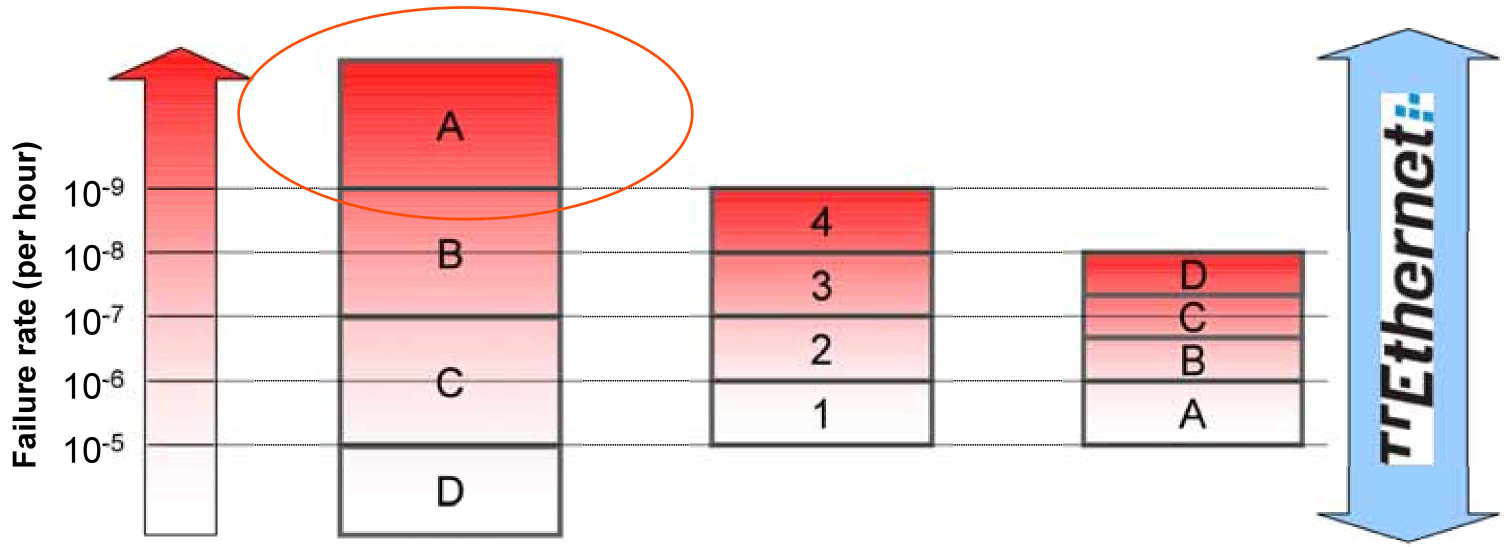
Formal Methods have been applied as early as in the requirements capturing phase

Finalization and Completion of the formal assessment within the CoMMiCS Project

- Complexity Management for Mixed-Criticality Systems
- European Communities FP7 project [FP7/2007-2013] no. 236701

CoMMiCS

DO 254 Level A Certification



Aerospace
DO254
DO178B

Industrial
IEC 61508
SIL

Automotive
ISO 26262
ASIL

TTEthernet Standard

SAE Home > News & Awards > News

SAE International Standard Enabling Ethernet for Critical Embedded Systems

WARRENDALE, Pa., Oct. 15, 2009 - SAE International's AS-2 Embedded Computing Systems Committee is developing a new standard to establish Ethernet as a high-bandwidth network protocol for time-, mission-, and safety-critical systems. It is expected that broader use of Ethernet will reduce costs and enhance design of open and scalable electronics architectures for space, aerospace, defense, ground vehicles and other industry applications.

SAE AS6802 Time-Triggered Ethernet (TTEthernet) describes a set of powerful services to meet the requirements of reliable, hard real-time data delivery in advanced integrated systems. With TTEthernet, critical control systems, audio/video and standard LAN applications can safely coexist in one Ethernet network.

Initial supporters of SAE AS6802 standardization project are Lockheed Martin, Bombardier, Embraer, General Dynamics, Sikorsky Aircraft, Honeywell, BAE Systems, Ultra Electronics, GE Fanuc Intelligent Platforms, TTA-Group and TTTech. First production program that plans to use COTS components compliant with SAE AS6802 will be NASA's Orion crew exploration vehicle in the scope of the U.S. human spaceflight program. Lockheed Martin also works on several advanced integrated system programs using this technology.

SAE International's AS-2 Embedded Computing Systems Committee addresses all facets of embedded computing systems – design, maintenance and in-service experience. The committee is part of SAE International's Avionic Systems Division.

SAE International provides some of the key system architecture, design and networking standards; reports; and recommended practices for commercial and military avionics.

SAE International is a global association of 121,000 engineers and related technical experts in the automotive, aerospace and commercial-vehicle industries. SAE International's core competencies are life-long learning and standards development. SAE International's charitable arm is the SAE Foundation, which supports many programs, including *A World in Motion®* and the Collegiate Design Series.

- www.sae.org -

Reference NASA Orion Space Shuttle

Ensuring Reliable Networks TTTech

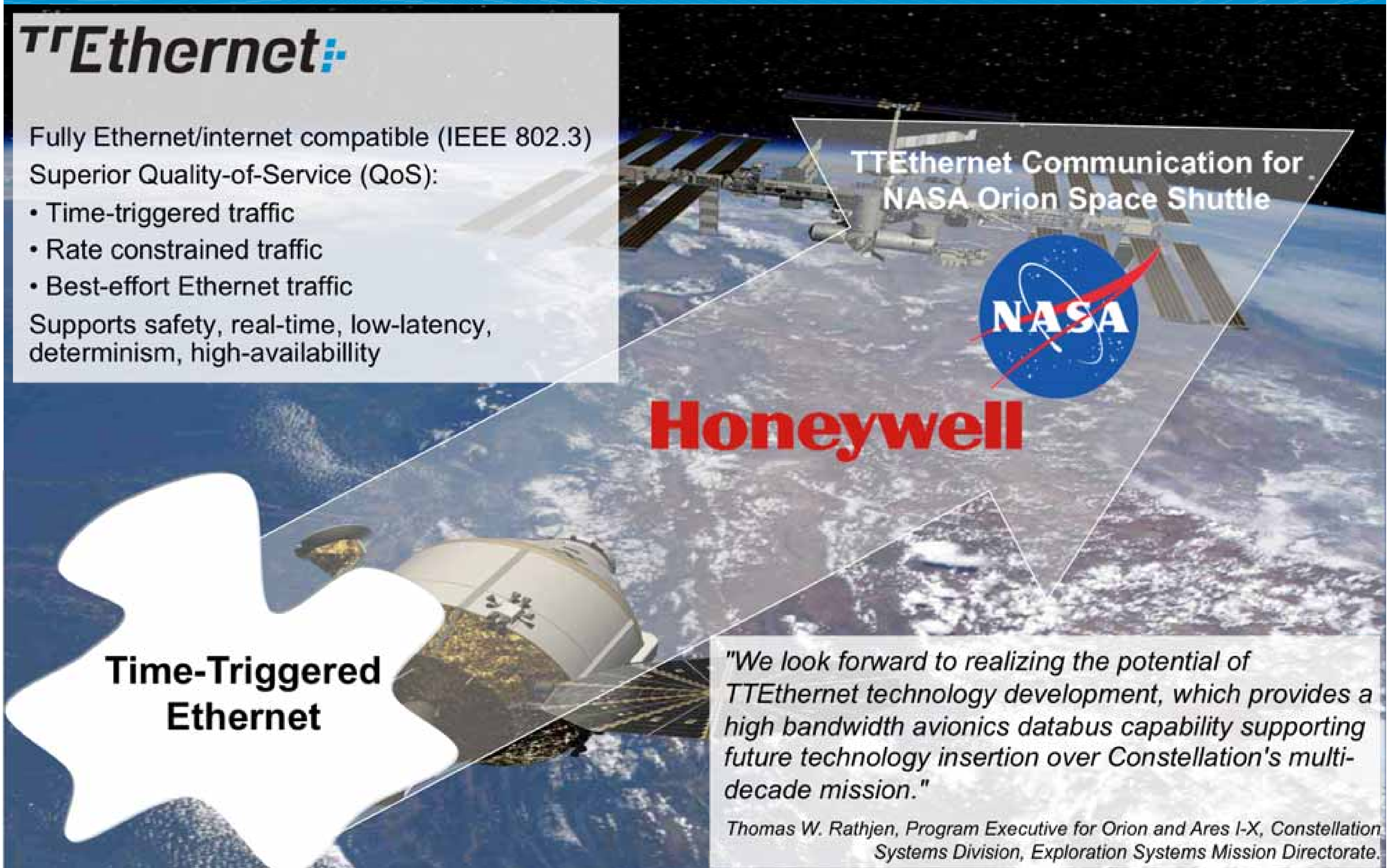
TTEthernet

Fully Ethernet/internet compatible (IEEE 802.3)

Superior Quality-of-Service (QoS):

- Time-triggered traffic
- Rate constrained traffic
- Best-effort Ethernet traffic

Supports safety, real-time, low-latency, determinism, high-availabillity



"We look forward to realizing the potential of TTEthernet technology development, which provides a high bandwidth avionics databus capability supporting future technology insertion over Constellation's multi-decade mission."

Thomas W. Rathjen, Program Executive for Orion and Ares I-X, Constellation Systems Division, Exploration Systems Mission Directorate.

Ensuring Reliable Networks TTTech

Current TTEthernet R&D Activities

Closed-World Open-World Integration

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, ...

High cost

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, …

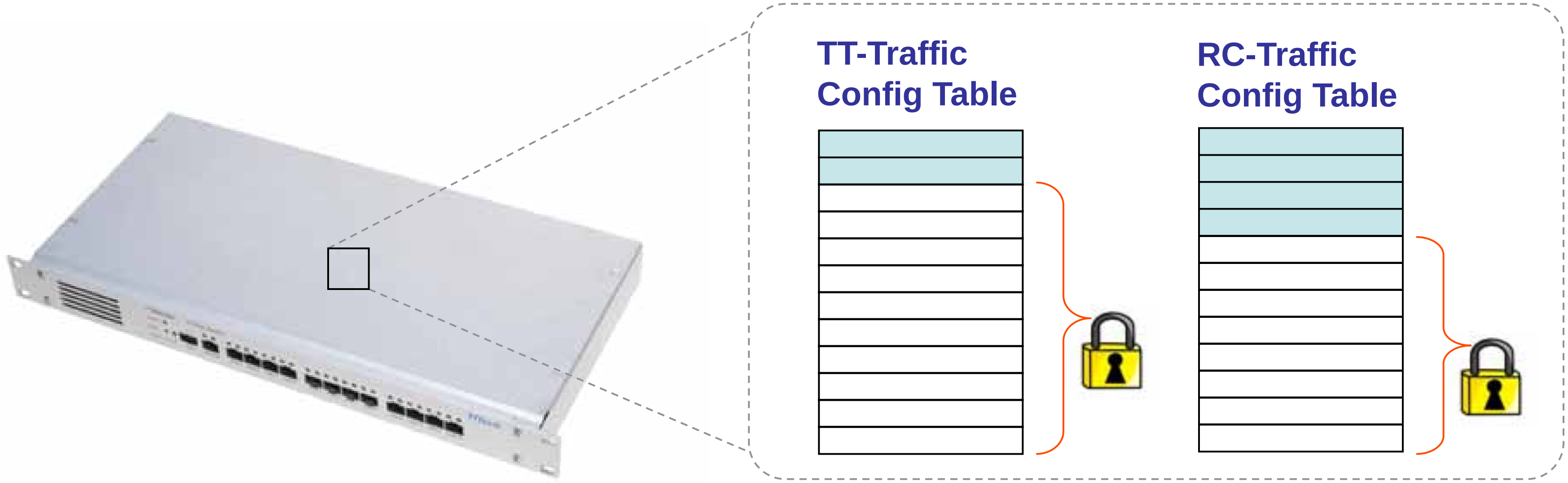
Validation & verification:
No certification, test, simulation, ...

Low cost

Clear need for integration of open and closed world allowing for flexibility an security

Motivation for Dynamic Configuration

- Increase system availability (dispatchability) by supporting generic stand-by computational ressources
- Offer bandwidth guarantees (quality of service) even in non-closed-world environments
- Support of dynamic environments (e.g. switching between different video sources)
- Interoperability with existing and emerging standards (e.g. AVB)



Rate-Constrained On-Line Configuration

Ensuring Reliable Networks TTTech

- **Non-protected, write-enabled VL IDs**
  - source port(s) and destination port(s)
  - assignment to (shared) BAG
  - BAG and jitter parameters of (shared) BAG
  - priority level, maximum length, assignment to memory pool

  can be changed at runtime
- **Traffic type can be changed to time-triggered at runtime**

Time-Triggered On-Line Configuration

Ensuring Reliable Networks TTTech

- **For non-protected, write-enabled VL IDs**
  - source port(s)
  - expected arrival time
  - priority level
  - maximum length

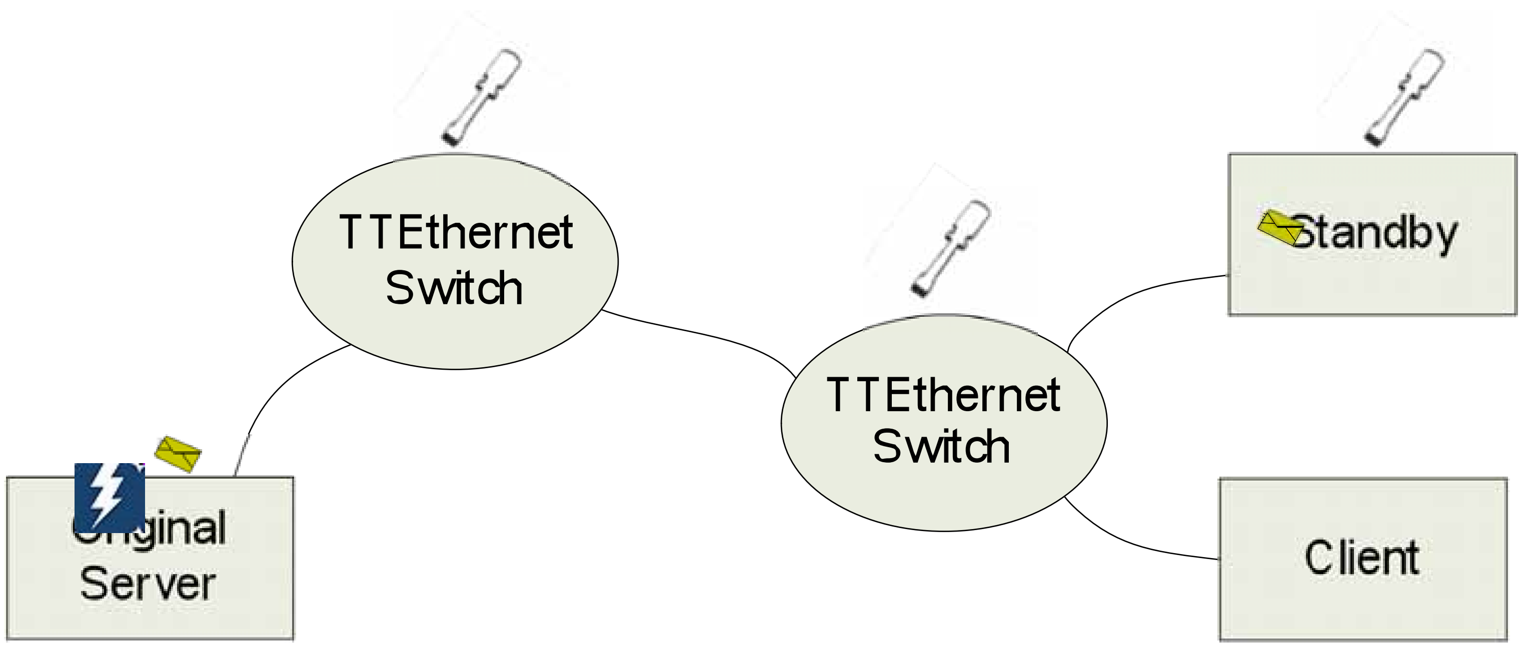
  can be changed at runtime
- **For write-enabled schedule entries**
  - destination port(s)
  - media reservation

  can be changed at runtime
- **Traffic type can be changed to rate-constrained at runtime**

Partitioning Argument

- **Non-protected, write-enabled VL IDs cannot**
  - exceed configured maximum priority level
  - share memory pools with statically assigned VL IDs
  - share BAGs with statically assigned VL IDs
- **Write-enabled schedule entries cannot**
  - exceed configured maximum priority level
  - have their VL ID changed
  - have their action time changed
- **If a write access violates any of these rules, it will be rejected by hardware**

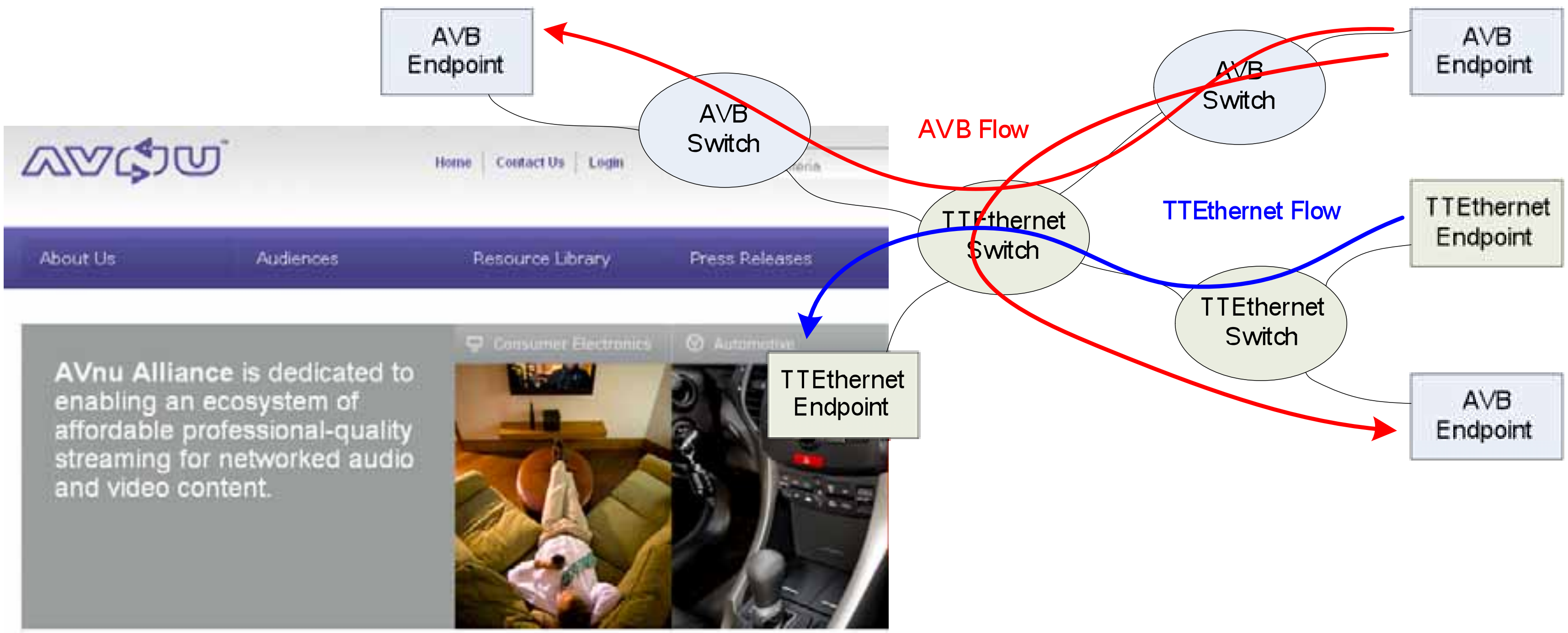
Ensuring Reliable Networks TTTech



TTTech Confidential and Proprietary Information

Integration of TTEthernet and AVB

- Reservation protocol planned to be compliant with *P802.1Qat* (SRP – Stream Reservation Protocol as used by AVB)
- Upscale AVB networks: Run TTEthernet in AVB networks: From multimedia to critical real-time and high-availability apps
- Liaison between TTA-Group and AVnu



Idea: „Extending MILS over the Network“

- Formally verified partitioning properties
- Strong encrypted data transmission
  - long asymmetric keys during network start-up
  - followed by using shorter keys that are changed with high frequency (based on network schedule)
- Encryption scheme for dynamic bandwidth allocation
- Trusted network authority
  - allocate bandwidth at run-time.

TTTech

Ensuring Reliable Networks

www.tttech.com

TTEthernet Products Today

TTEthernet Chip IP
- Switches and End Systems
- Certification Package

TTEthernet Development Switches
- TTEDevelopment Switch 1Gbit/s
- TTEDevelopment Switch 100Mbit/s

TTEthernet End Systems
- TTEPCIe Card
- TTEPMC Card
- TTEXMC Card

TTEthernet Test Equipment
- TTEMonitoring Switch 1Gbit/s
- TTEMonitoring System

TTEthernet Evaluation Systems
- TTEEvaluation System 1Gbit/s
- TTEEvaluation System 100 Mbit/s

TTEthernet Software Products
- TTEBuild, TTE Build Network Config.
- TTELoad
- TTEView
- TTEVerify (certification)

Middleware Software
- TTEProtocol Layer
- TTEDriver and TTEAPI Library
- ARINC 653 COM Layer
- IMA OS Synchronization Library