
Automotive and highly dependable Networks

TTP/C

Byteflight

FlexRay

Braided Ring

Time Triggered CAN (TTCAN)

TTP/A

LIN





A New High-Performance Data Bus System for Safety-Related Applications

By Josef Berwanger, Martin Peller and Robert Griessbach
BMW AG, EE-211 Development Safety Systems Electronics,
Knorrstrasse 147, 80788 Munich, Germany

http://www.byteflight.com/presentations/atz_sonderausgabe.pdf





Flexible protocol supports synchronous and asynchronous messages

supports high data rates

availability of integrated communications-controller (e.g. Motorola 68HC912BD32)

integral part of FlexRay

Principles:

- **message priorities are associated with node-IDs**
- **time slots, which correspond to certain priorities**
- **priority is enforced by waiting times**



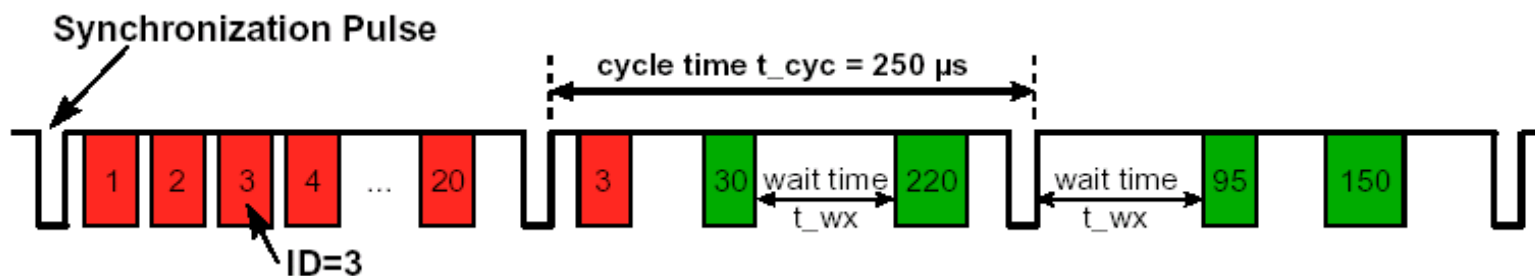
Assumptions

- **Communication is organized in rounds or cycles respectively.**
- **Clock synchronization between nodes is assumed to be better than 100ns.**
- **One (fault-tolerant) sync master responsible to indicate the start of a round by sending a sync pulse.**
- **The interval between two sync pulses determines the cycle time (250 μ s @ 10 Mbps)**

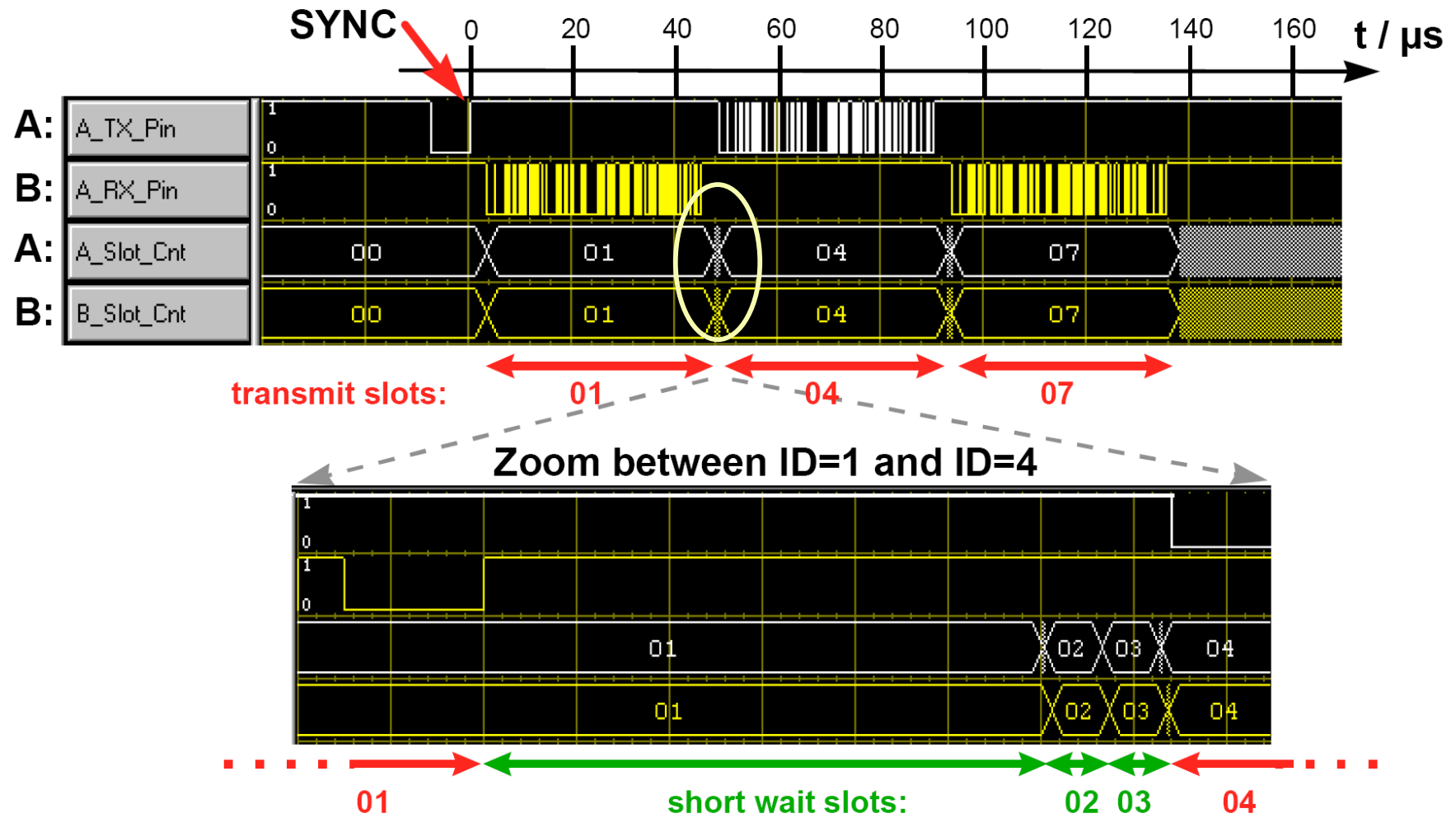


Byteflight: Flexible TDMA

- ➔ **SyncMaster** sends the synchronization pulse to init the cycle.
- ➔ The interval between two sync pulses determines the cycle time ($250 \mu\text{s}$ @ 10 Mbps)
- ➔ Every node has a number of identifiers assigned that define message priorities. The system must ensure that the message IDs are unique.
- ➔ Every communication controller has a counter which counts message slots.
- ➔ The counter is stopped on an ongoing message transfer and will be started again when the transfer has completed.
- ➔ If the counter value corresponds to the priority of a message, this message can be transmitted.



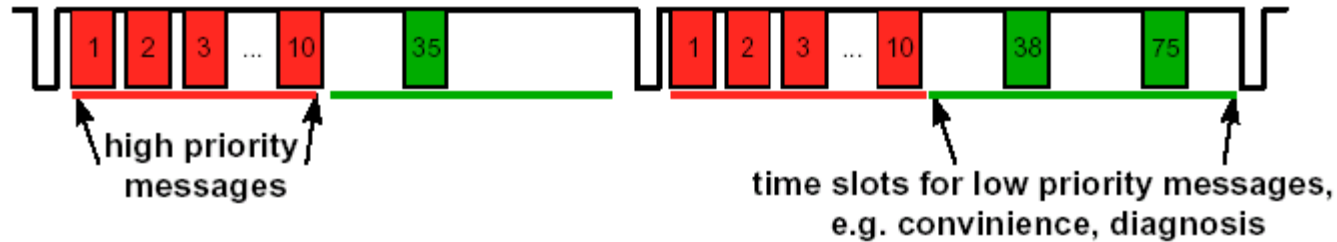
Distributed synchronized "Slot-" counter



Waiting period $t_{wait} = t_0 + t_{delta} * (ID - ID_{t-1})$



Synchronous and asynchronous data transmission

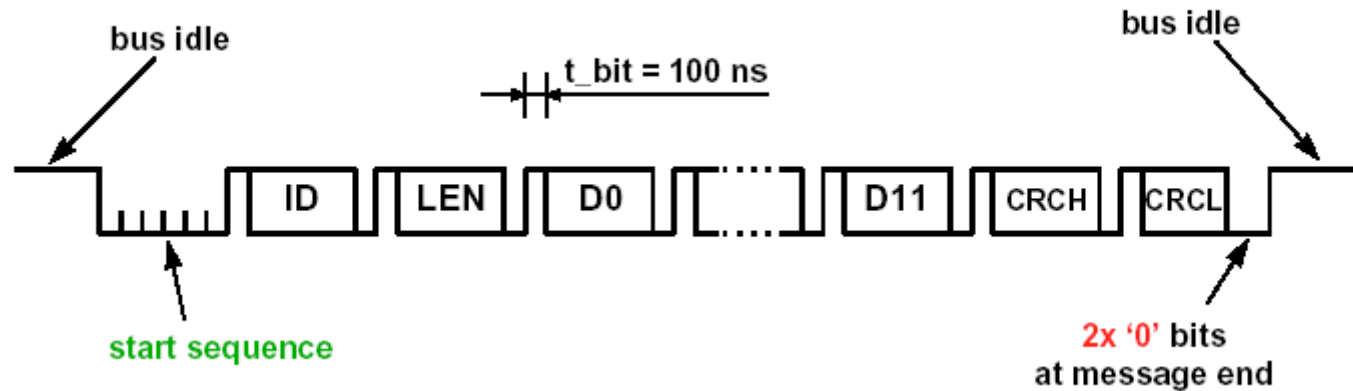


Slots with fixed priorities are reserved for synchronous messages. These slots are assigned in every cycle (1-10) and allow a deterministic analysis of message latencies.

Asynchronous messages have lower priorities. These are dynamically assigned and enforced by the waiting mechanism. To determine message latencies, only probabilistic analysis is possible.



ByteFlight message format



Start sequence: 6 Bits
ID: 8 Bits (1 Byte)
Length: 8 Bits (1 Byte)
Data: 96 Bits (12 Bytes)
CRC: 16 Bits (Hamming distance = 6)



Fault handling in the Byteflight Protocol

Alarm state:

The master can send a special synchronization signal that is recognized by all stations. This signal has no influence on the protocol but the nodes can detect a specific situation locally.

Fault treatment:

Transient transmission faults are not specially treated and no re-transmission is initiated. It is assumed that with the next cyclic transmission this fault is gone.

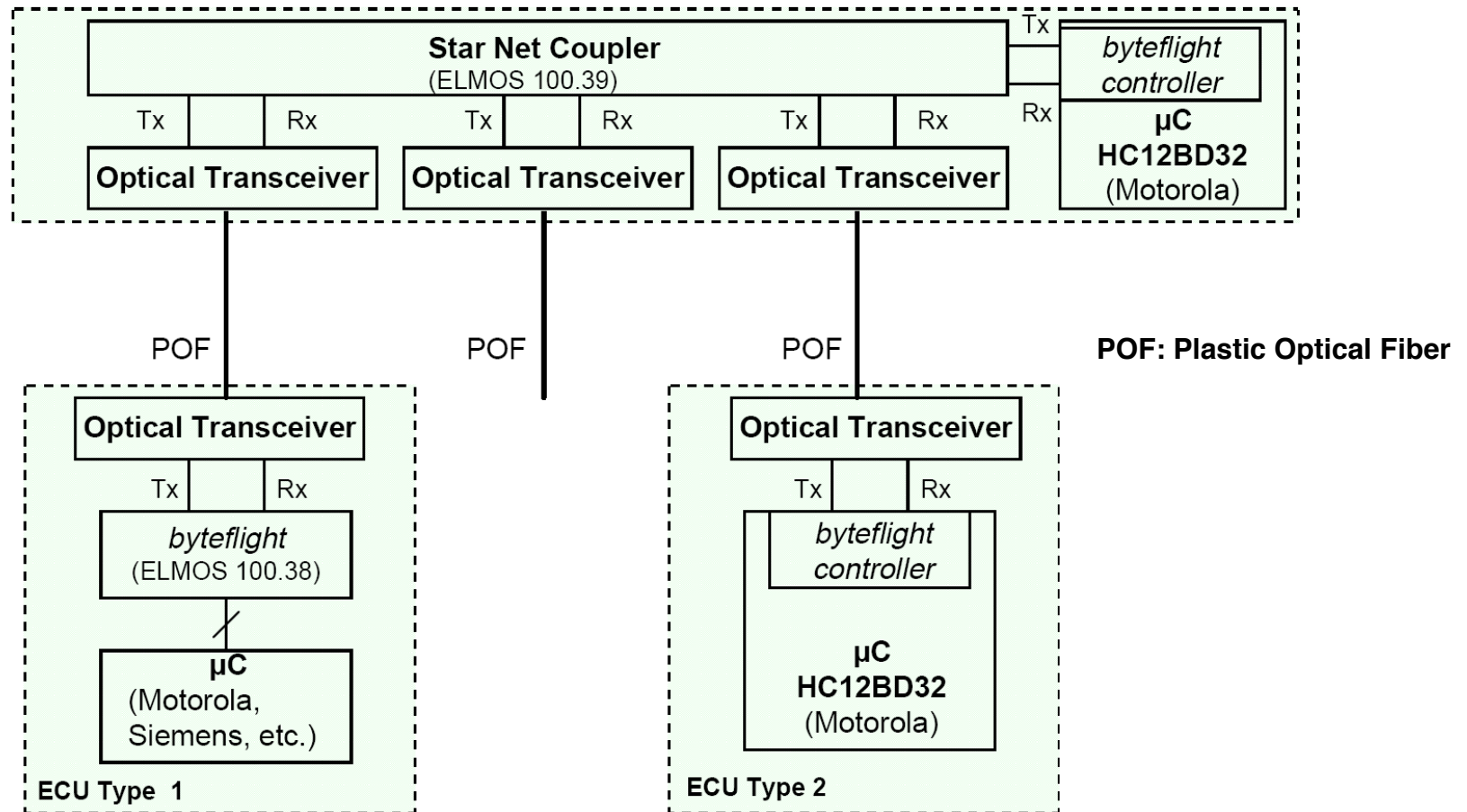
Timing errors are handled by the star coupler.

In a bus structured network, bus guardians are used to enforce a fail silent behaviour. Here the protocol exploits the strict timing discipline.

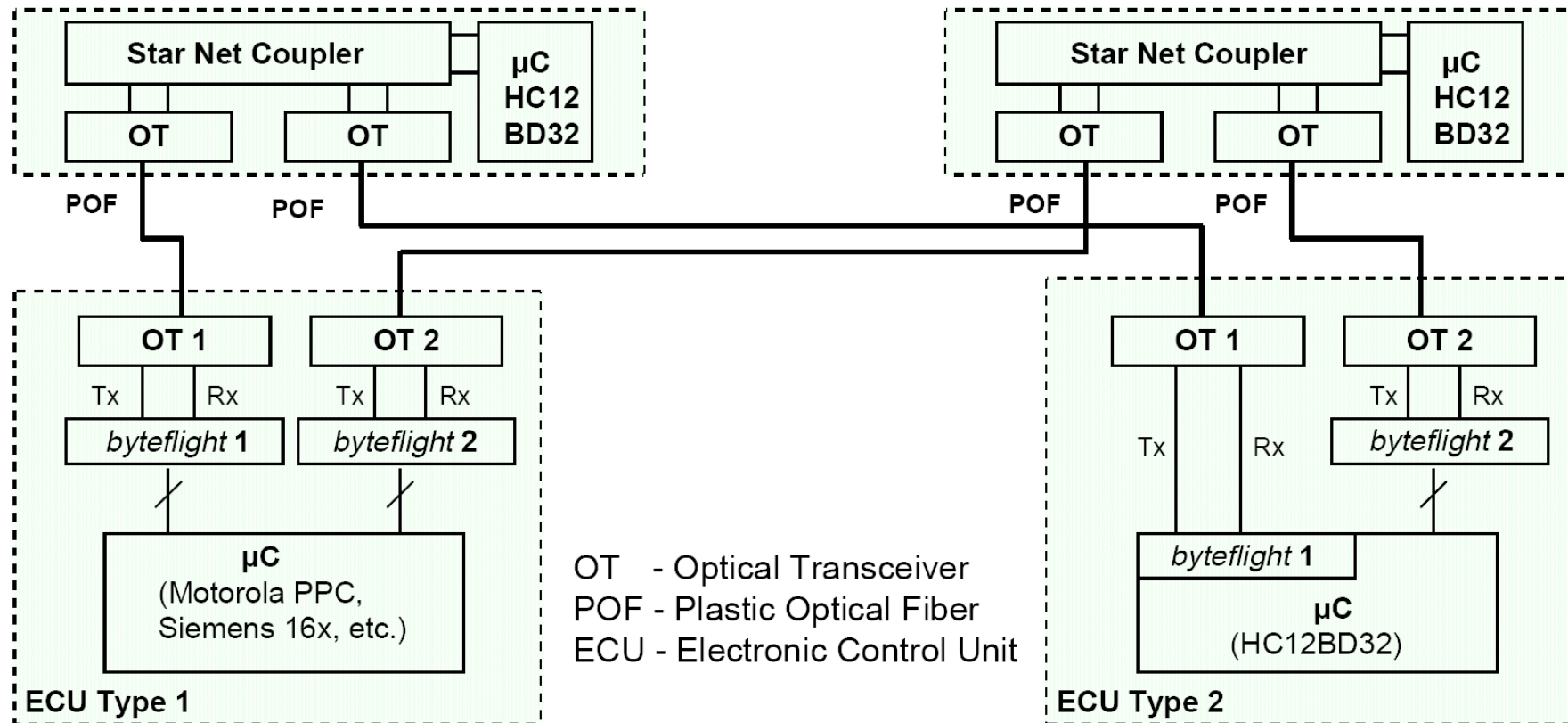
Replacements for a failing sync master are determined a priori.



Example of a Byteflight topology



Byteflight star topology & redundancy concept



Comparison between Byteflight and TTP

byteflight: a new high-performance data bus system for safety related applications,
 J. Berwanger, M. Peller, J. Griessbach,
 BMW-AG, EE211 Development Safety
 Systems Electronic

Feature	CAN	TTP [10]	<i>byteflight</i>
Message transmission	asynchronous	synchronous	asynchronous and synchronous
Message identification	message identifier	time slot	message identifier
Data rate	1 Mbps gross up to 58 % net	2 Mbps gross up to 37 % net	10 Mbps gross up to 53 % net
Bit encoding	NRZ with bit stuffing	modified frequency modulation (MFM)	NRZ with start/stop bits
Physical layer	transceivers up to 1 Mbps	not defined	optical transceiver up to 10 Mbps
Latency jitter	bus load dependent	constant for all messages	constant for high priority messages according t_{cyc}
Clock synchronization	not provided	distributed, in μs range	by master, in 100 ns range
Temporal composability	not supported	supported	supported for high priority messages
Error containment (physical layer)	partially provided	provided with special physical transceiver	provided by optical fiber and transceiver chip
Babbling idiot avoidance	not provided	possible by independent bus guardian	provided via star coupler
Extensibility	excellent	only if extension planned in original design	extension possible for high priority messages with affect on asynchronous bandwidth
Flexibility	flexible bandwidth for each node	only one message per node and TDMA cycle	flexible bandwidth for each node
Availability of components	several μC families and transceiver chips	microcoded RISC chip available, physical transceiver and independent bus guardian not available	HC12BD32, E100.38 <i>byteflight</i> standalone controller, E100.39 star coupler ASIC, optical transceiver available



Combination of TDMA and Byteflight



Belschner et al. : Anforderungen an ein zukünftiges Bussystem für fehlertolerante Anwendungen aus Sicht Kfz-Hersteller

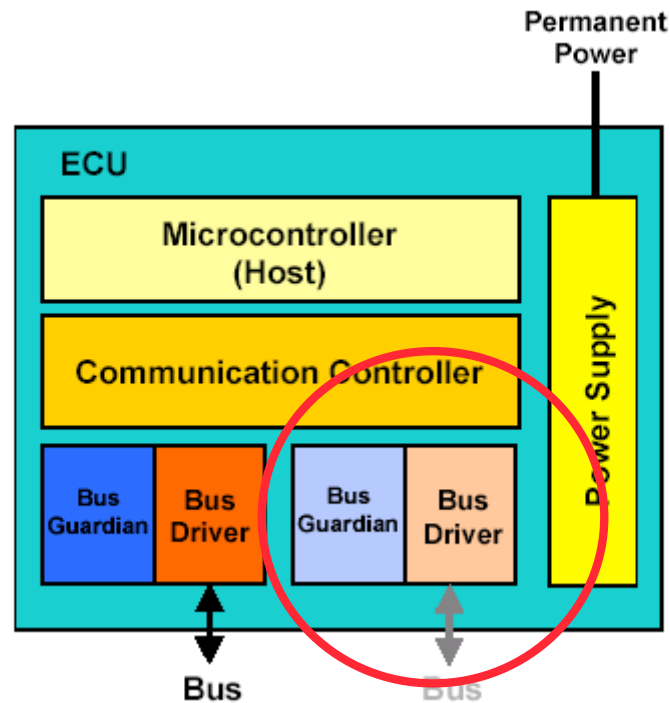




Requirements of the Protocol

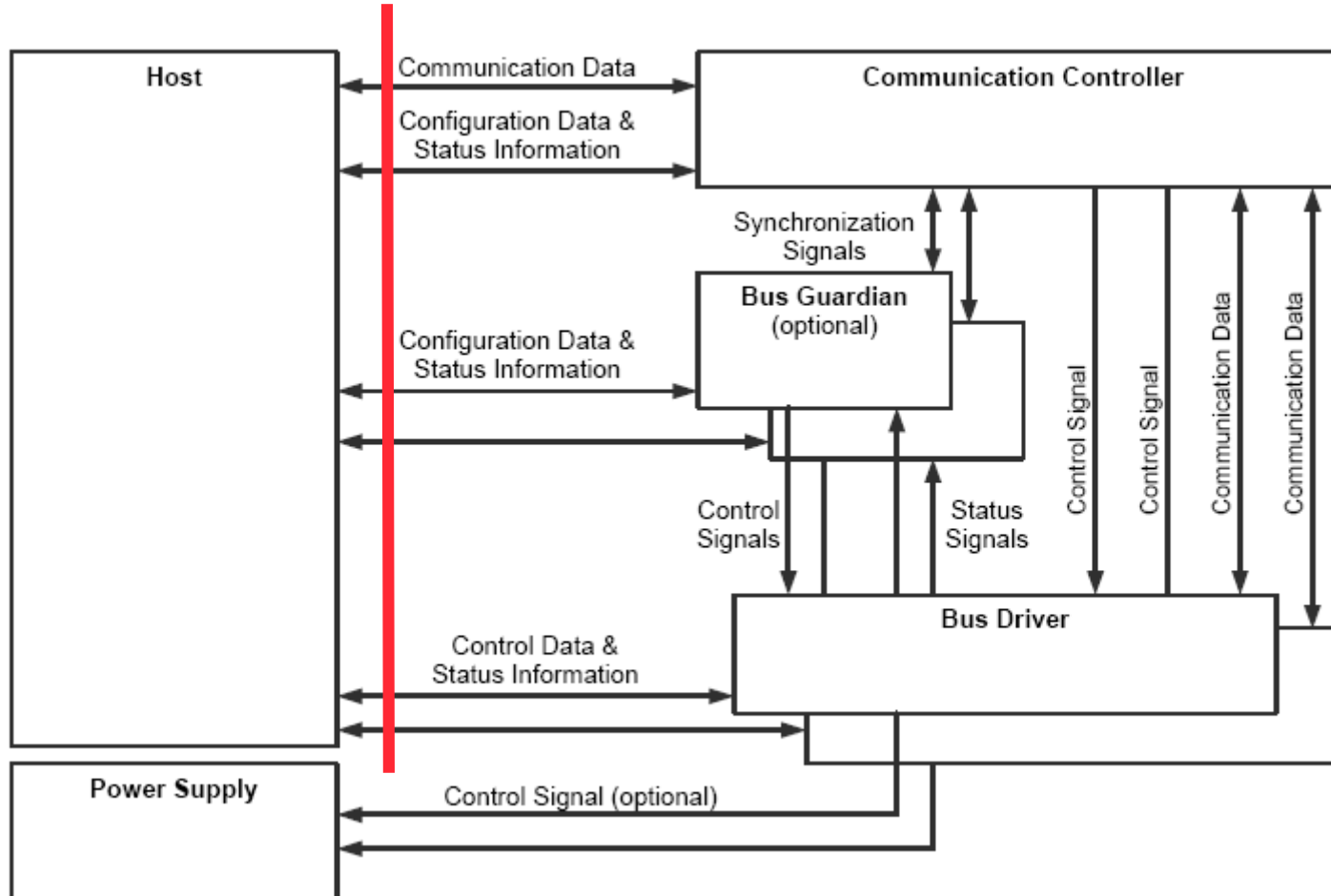
- Synchronous and asynchronous data transmission (scalable)
- Deterministic data transmission, guaranteed message latency
- Fault-tolerant, synchronized global time
- Redundant transmission channels (configurable)
- Flexibility (expandability, bandwidth usage, ...)
- Different topologies (bus, star and multi-star)
- Electrical and optical physical layer
- Communication protocol independent of the baud rate

Architecture of a FlexRay node (ECU: Electronic Control Unit)



Interfacing the communication controller

CNI: no control signals

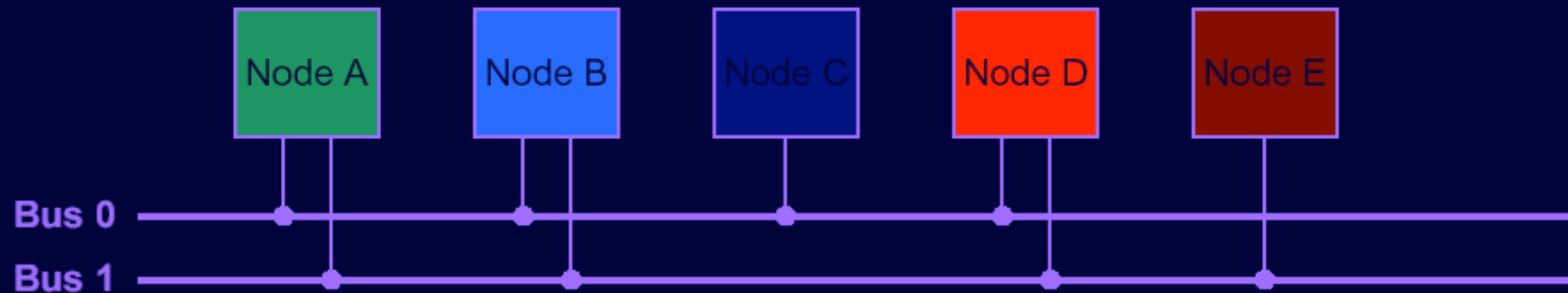


Data- und control flow between Host and CC





FlexRay Basic Concepts



Redundancy

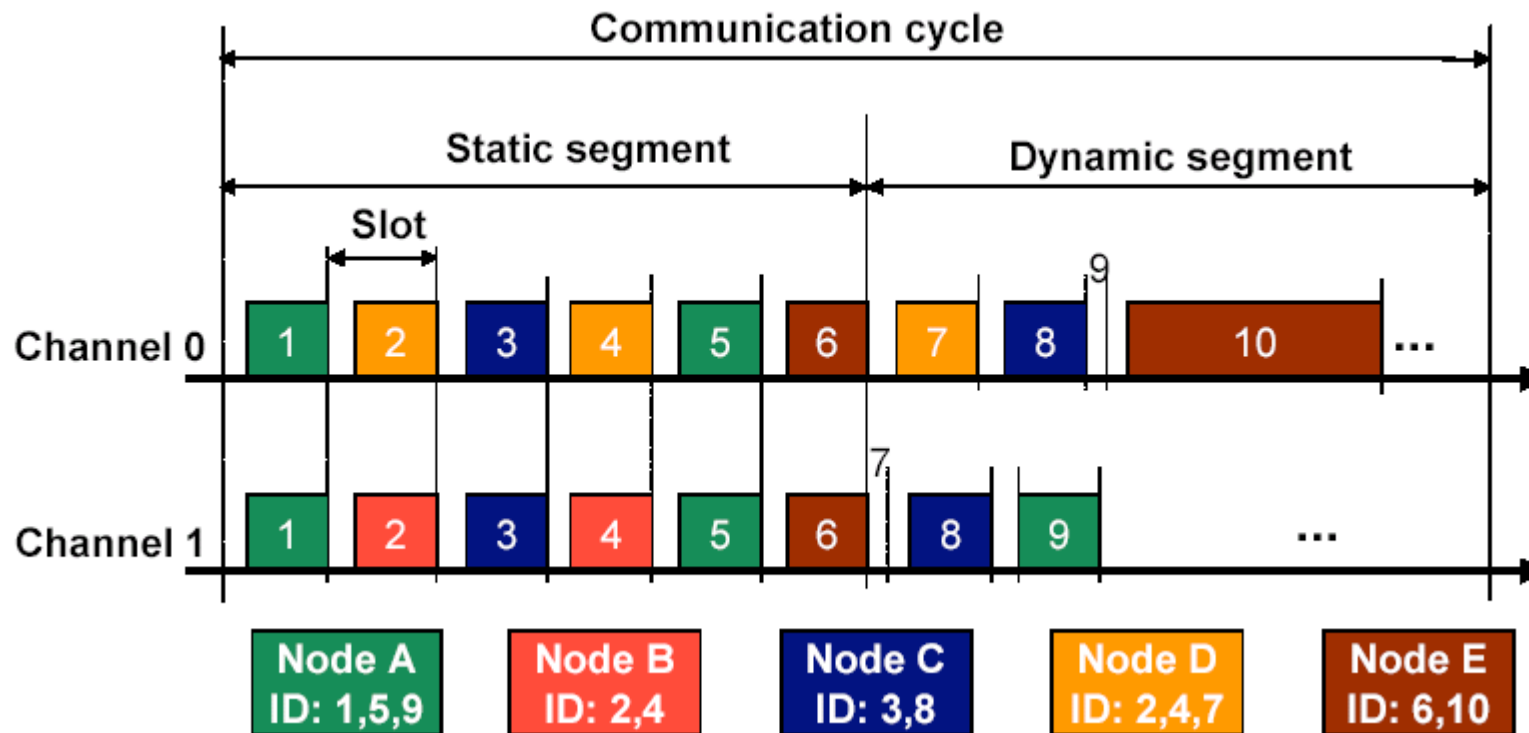
- The protocol supports two serial busses
- A node can either be connected to both or only one of the busses

PHY Bit Coding

- transmission speed up to 10 Mbit/s (gross, optical)
- NRZ 8N1 for optical transmission
- Xerxes (MFM extension) coding for electrical transmission



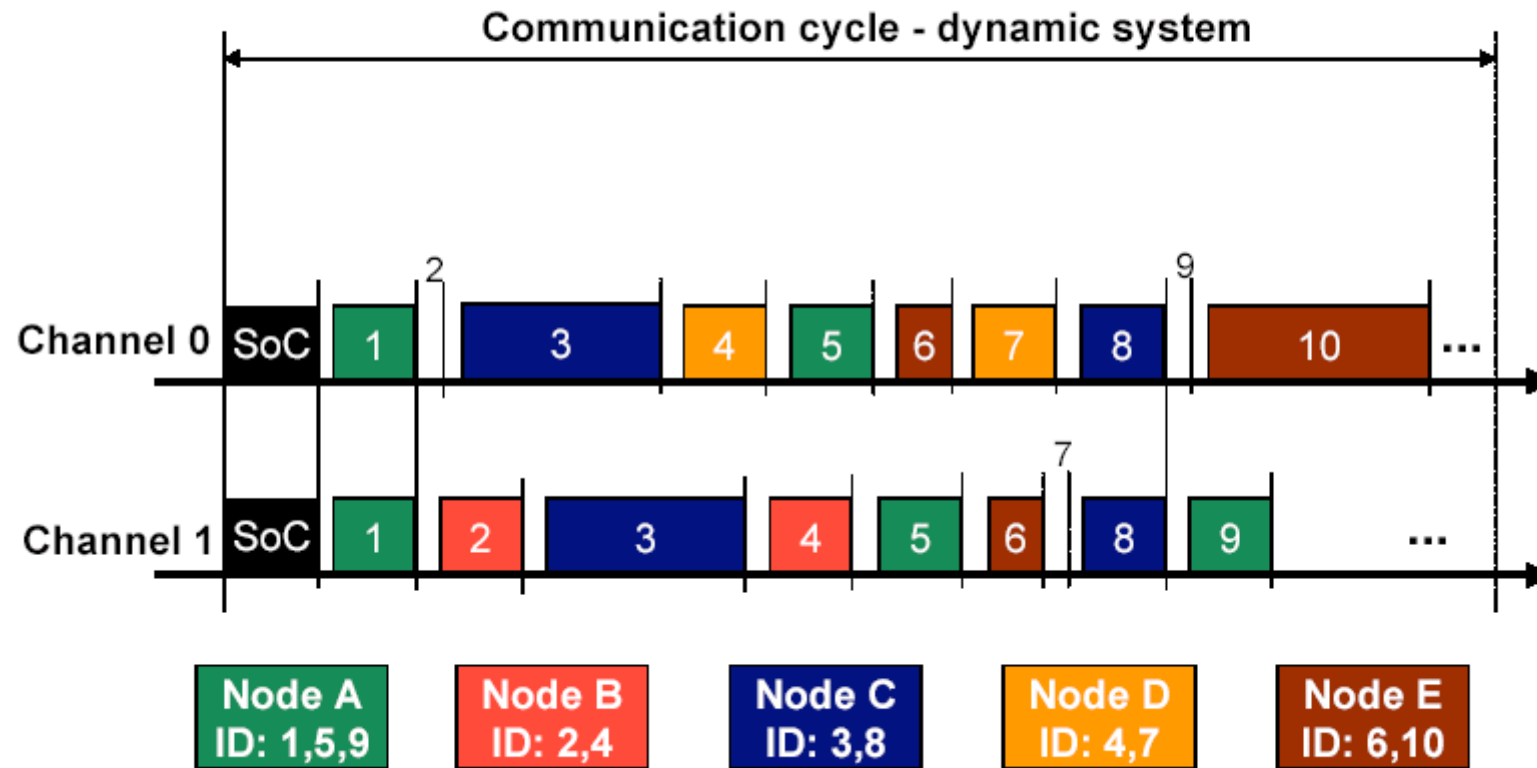
The FlexRay Communication Cycle



Cycle with static and dynamic segment



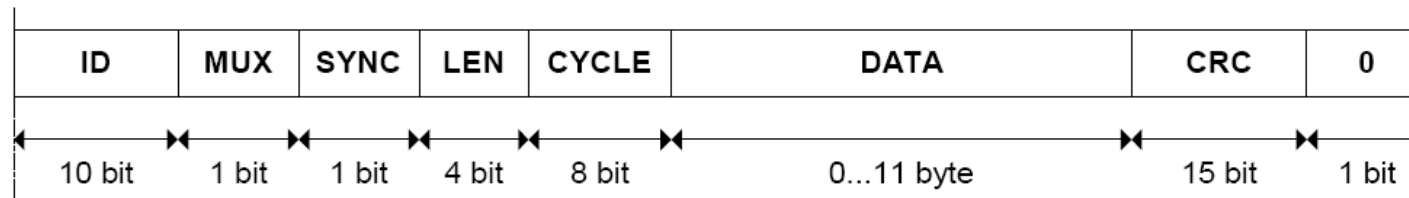
The FlexRay Communication Cycle



Cycle with dynamic segment only



Format of a FlexRay frame



- ID:** Identifier, 10 Bit, value range: (1 ... 1023), defines the slot position in the static segment and the priority in the dynamic segment. A low ID defines a high priority. ID = 0 is reserved for the SYNC-symbol. An identifier must be unique in the network, i.e. two identical IDs would lead to a collision. Every node may use one or more identifiers in the static and the dynamic segment.
- MUX:** Multiplex-field, 1 Bit. This bit enables to send multiple data under the same ID..
- SYNC:** SYNC-field, 1 Bit. This bit indicates whether the message is used for clock synchronization and whether the first byte contains the sync counter (SYNC = "1": message with Frame-Counter and clock synchronization, SYNC = "0": message without counter)
- LEN:** Length field, 4 Bit, number of data bytes (0 ... 12). Any value > 12 will be interpreted as LEN=12. If the cycle counter (in the first byte) is used (SYNC=1) any value >11 is set to LEN=11.
- CYCLE:** The CYCLE-Field can be used to transmit the cycle counter or data. The cycle counter is synchronously incremented at the start of every communication cycle by all communication controllers.
- D0-11:** Data bytes, 0 – 12 bytes
- CRC:** 15 Bit Cyclic Redundancy Check.



Topology Options

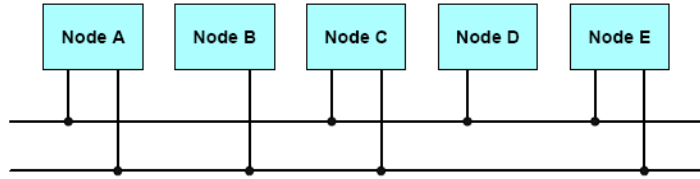


Figure 1-1: Dual channel bus configuration.

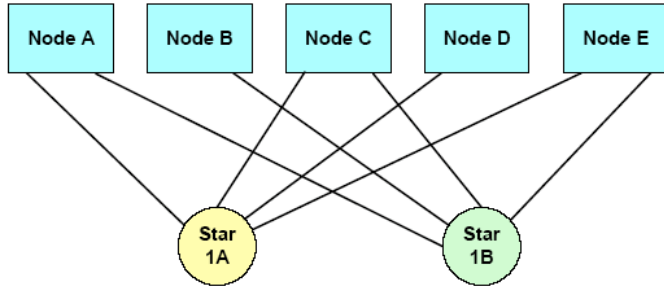


Figure 1-2: Dual channel single star configuration.

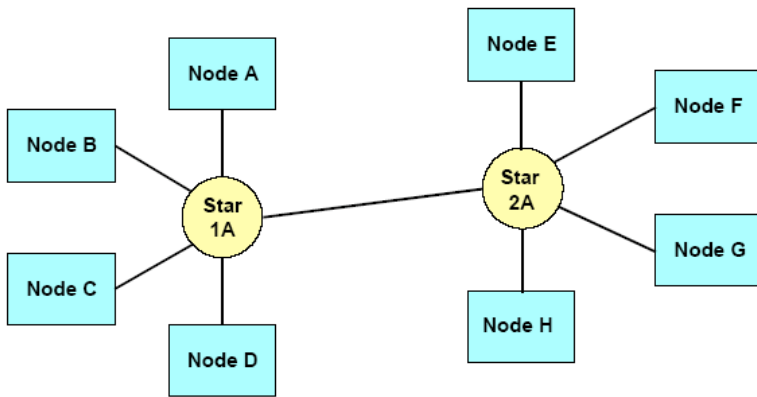


Figure 1-3: Single channel cascaded star configuration.

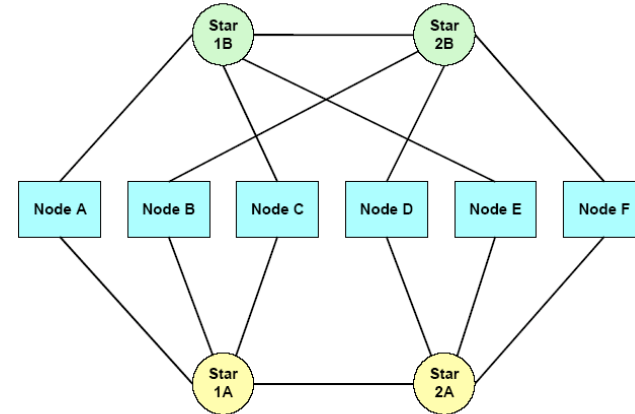


Figure 1-4: Dual channel cascaded star configuration.

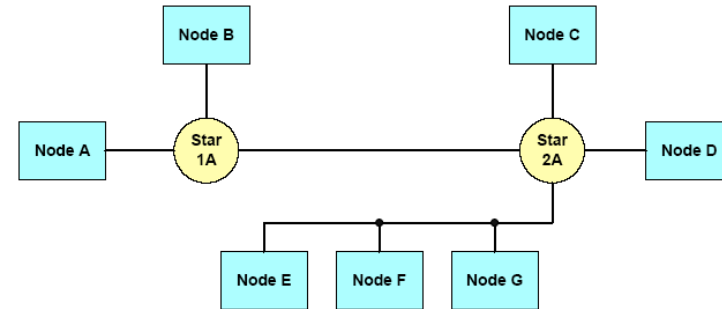


Figure 1-5: Single channel hybrid example.

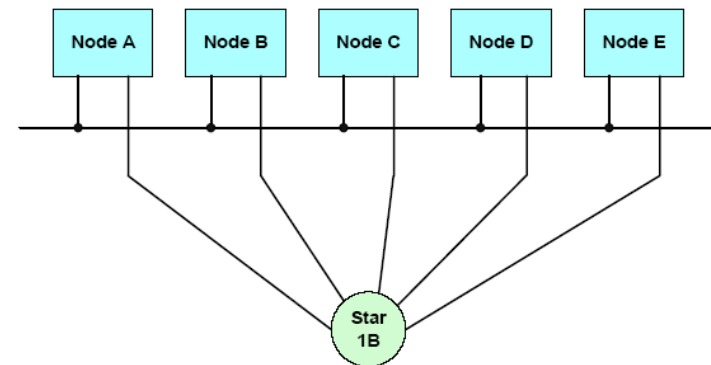


Figure 1-6: Dual channel hybrid example.



Comparison

H. Kopetz

A Comparison of TTP/C and FlexRay
Research Report 10/2001

hk@vmars.tuwien.ac.at
Institut für Technische Informatik
Technische Universität Wien, Austria
May 9, 2001

Characteristic	TTP/C	FlexRay
Designed to meet automotive requirements	yes	yes
Priority in the “safety versus flexibility” conflict	safety	flexibility
Specification in the public domain	yes	no
Composability (precise interface specification in the value domain and in the temporal domain)	yes	no
Fault-tolerant clock synchronization	yes	yes
Replicated communication channels	yes	yes
Time-triggered message channels	yes	yes
Bus guardians to avoid babbling idiots	yes	yes
Bus guardian and protected node in different fault-containment regions	yes	no
Dynamic asynchronous message channels	yes, local	yes, global
Membership service	yes	no
Fault-hypothesis specified	yes	no
Never-give-up (NGU) strategy specified	yes	no
Critical algorithms formally analyzed	yes	no
Handling of outgoing link failures	yes	?
Handling of SOS failures	yes	?
Handling of Spatial Proximity failures	yes	?
Handling of Masquerading failures	yes	?
Handling of babbling idiot failures	yes	?
Transmission speed planned up to	25 Mbits/sec	10 Mbits/sec
Message data field length up to	236 bytes	12 bytes
Physical layer	copper/fiber	copper/fiber
CRC field length	3 bytes	2 bytes
Maximum achievable data efficiency for time-triggered messages in a 10Mbit/second system, interframe gap 5 microseconds.	95.8 %	45.7 %
Scalability: Maximum achievable data efficiency for time-triggered messages in a 100Mbit/second system, interframe gap 5 microseconds.	78 %	14.5%
Number of oscillators in a system with 10 ECUs	12	30
First system available on the market	1998	planned 2002
Architecture validated by fault injection	yes	no
Architecture viable for aerospace applications	yes	?



Braided Ring

Ringling out Fault Tolerance. A New Ring Network for Superior Low-Cost Dependability

Brendan Hall, Honeywell International

Kevin Driscoll, Honeywell International

Michael Paulitsch, Honeywell International

Samar Dajani-Brown, Honeywell International

2005 International Conference on Dependable Systems and Networks (DSN'05) pp. 298-307



Braided Ring: Inspired by the SafeBus properties

Objectives:

Highest integrity of message transmission

Tolerating node and connection crashes

Protection against byzantine failures and monopolization of the network

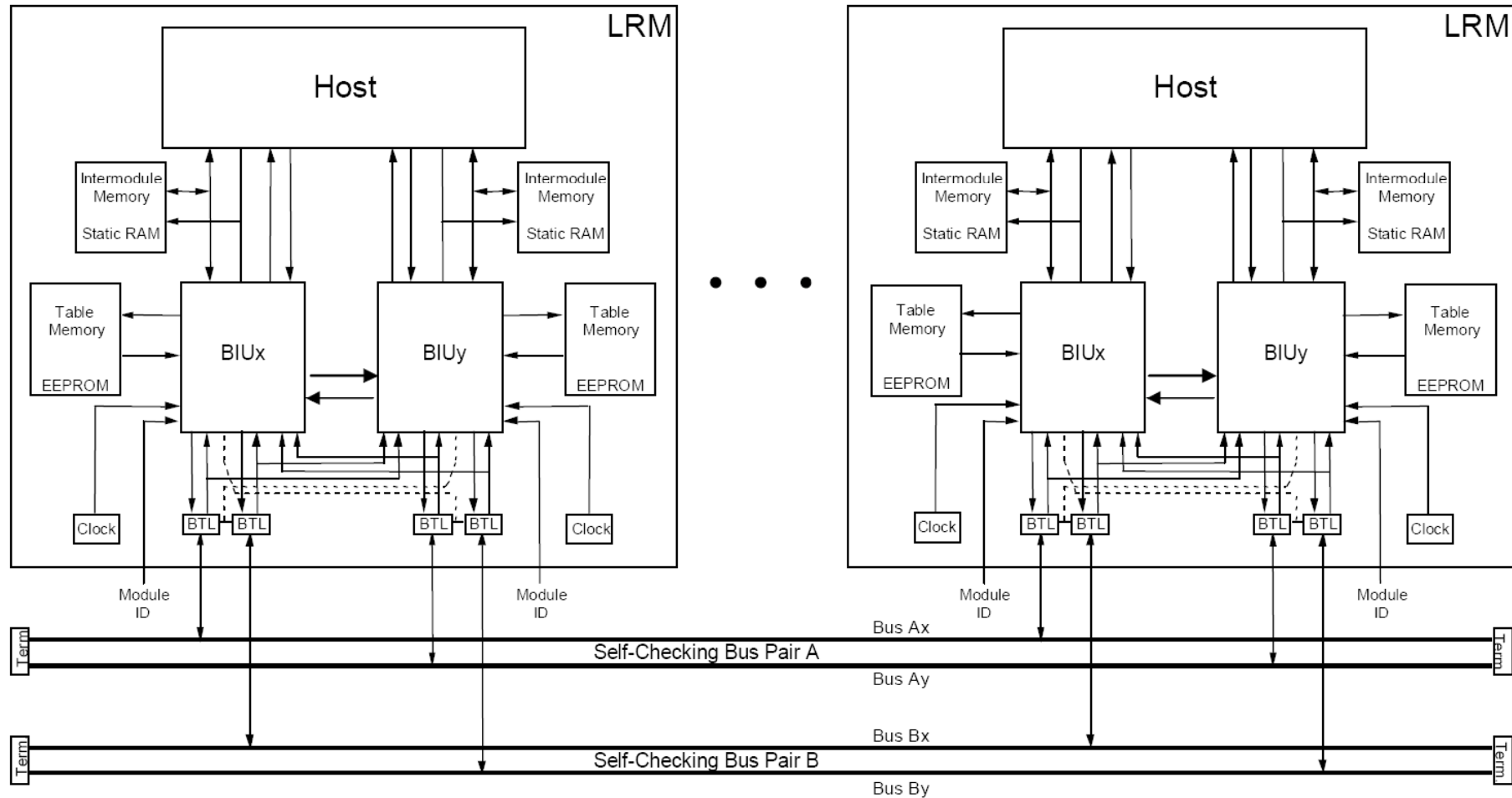
Low cost guardians

Safe start-up und re-integration of nodes

Integrity of source data and support for redundant computations



Hardware-Structure of the SAFEbus



Brendan Hall, Kevin Driscoll, Michael Paulitsch, Samar Dajani-Brown, "Ringing out Fault Tolerance. A New Ring Network for Superior Low-Cost Dependability," dsn, pp. 298-307, 2005 International Conference on Dependable Systems and Networks (DSN'05), 2005



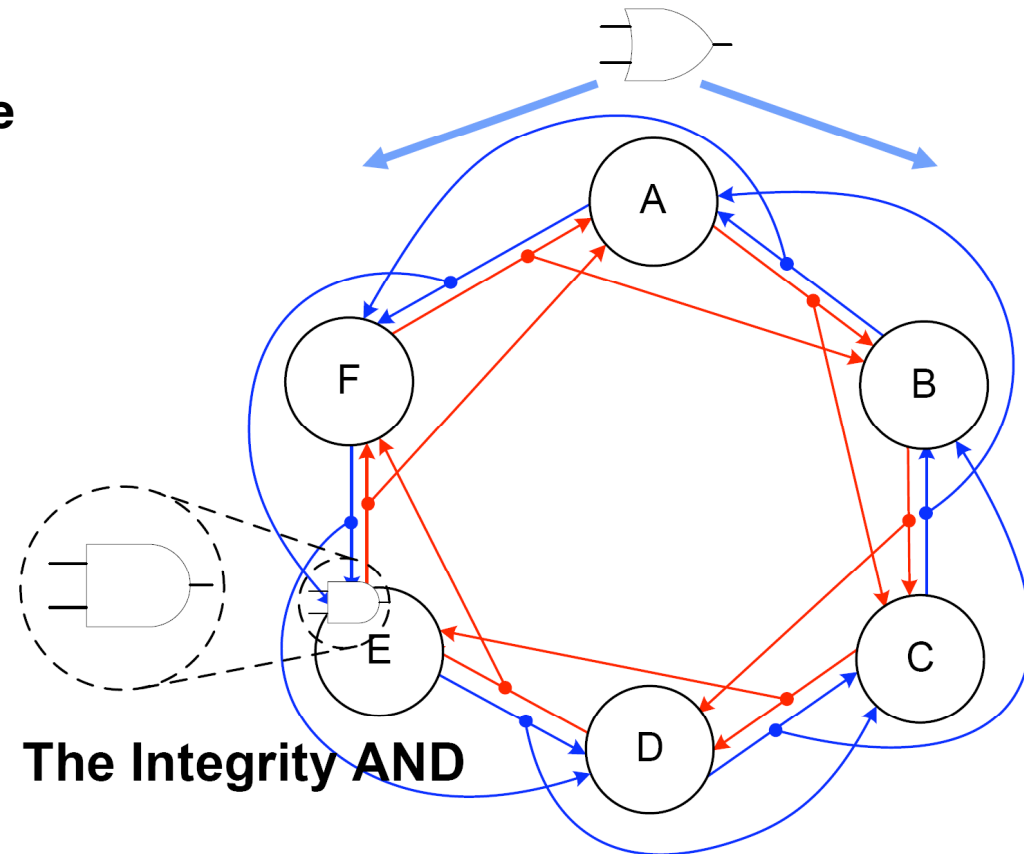
Concept of the Braided Ring

"... the topology supplies the connectivity required to achieve both independence to assure high transport availability and full-coverage to assure high data transport integrity."

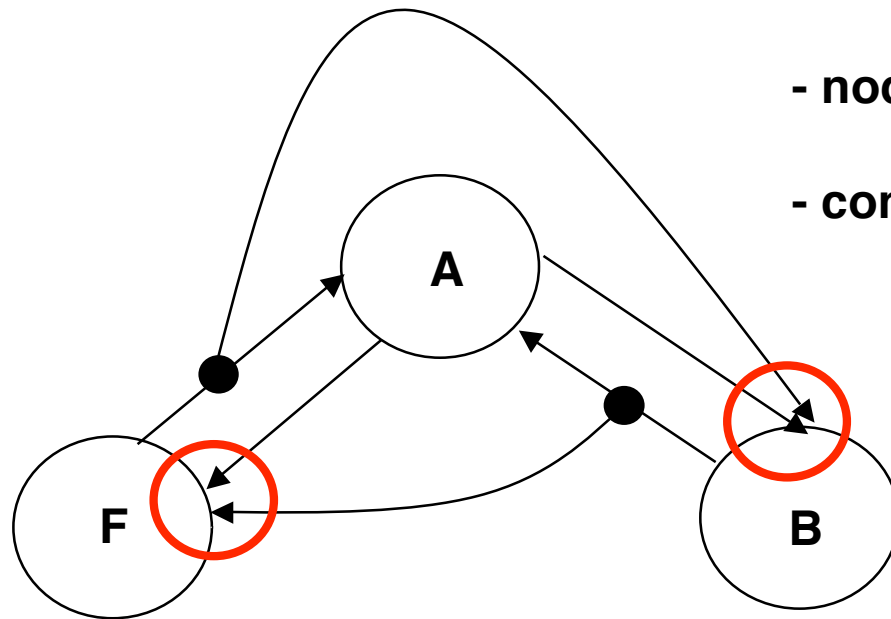
Basic Idea:

Let the neighbors act as guardians. Provide a interconnect structure to tolerate failures of neighbors.

The Availability OR



Availability OR

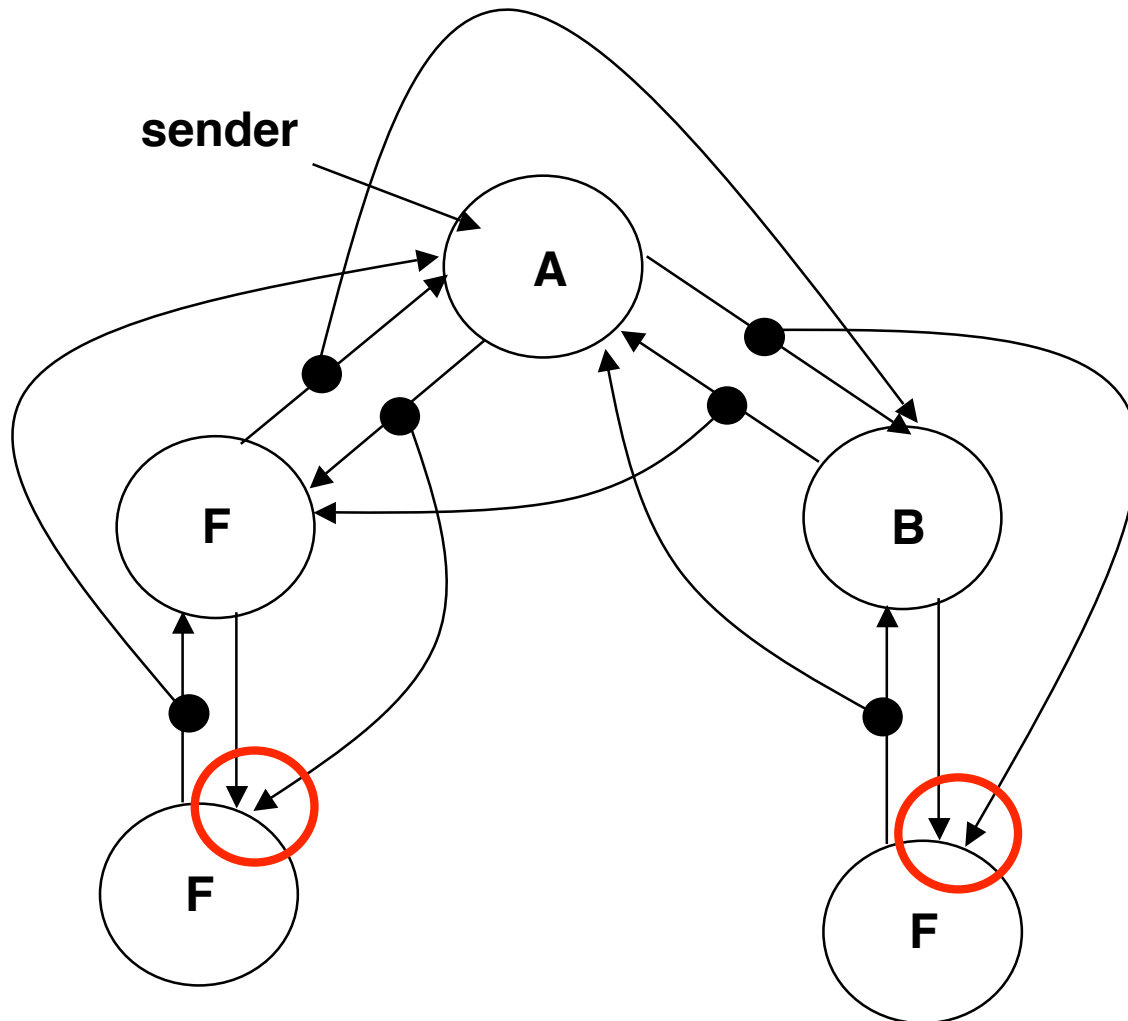


Availability OR tolerates:

- node crashes (no relaying)
- connection failures
 - both directions can be used
 - Babbling Idiot failures can be masked



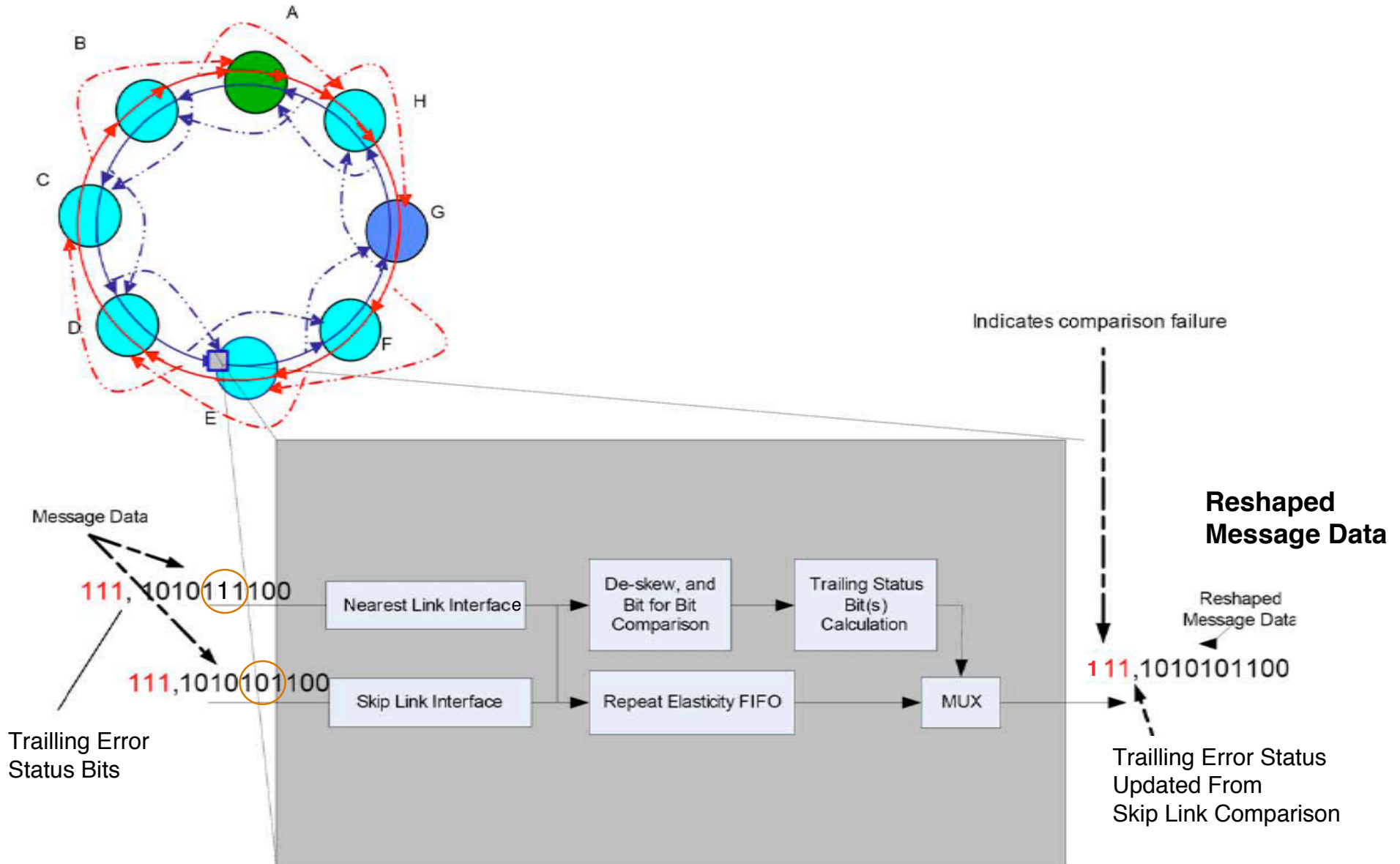
Integrity AND



**detection of
relaying failures**



Braided Ring Propagation and Status Generation and Appending



-
- ➔ **Bit-by-Bit comparison of incoming links**
 - ➔ **All failures, that are caused by neighbor nodes can be detected**
 - ➔ **The outcome (state) of a comparison is included in the "trailing bits"**
 - ➔ **every nodes appends its state to the message.
This enables precise fault localization**
 - ➔ **"Aggregated Error Status" :**
**A node can change the state of a message from valid to invalid
but not vice-versa.**
 - ➔ **All errors induced by a relaying node will be detected.**
 - ➔ **CRC is used for error detection on the "direct links".**
 - ➔ **Dependability figures of 10^{-9} require protection against all kinds of
"unbelievable" failures as masquerade and controlled data corruption.**



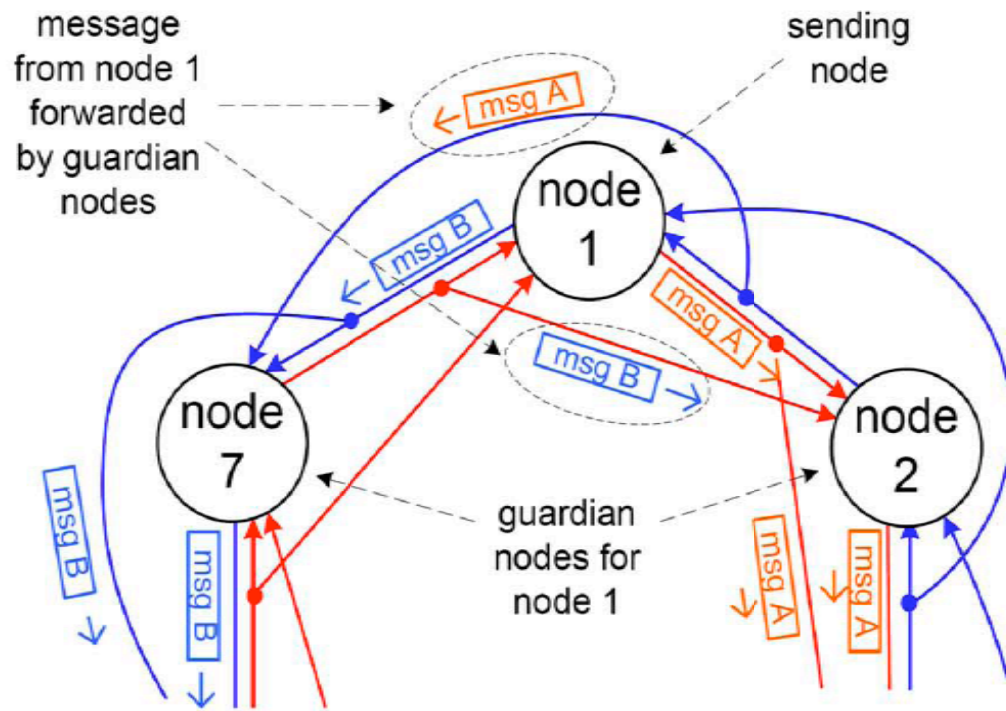


Figure 4. Byzantine Transmission Detection

Guardians guarantee, that for TDMA messages will only be sent in the respective assigned time slot.



4 messages are compared !

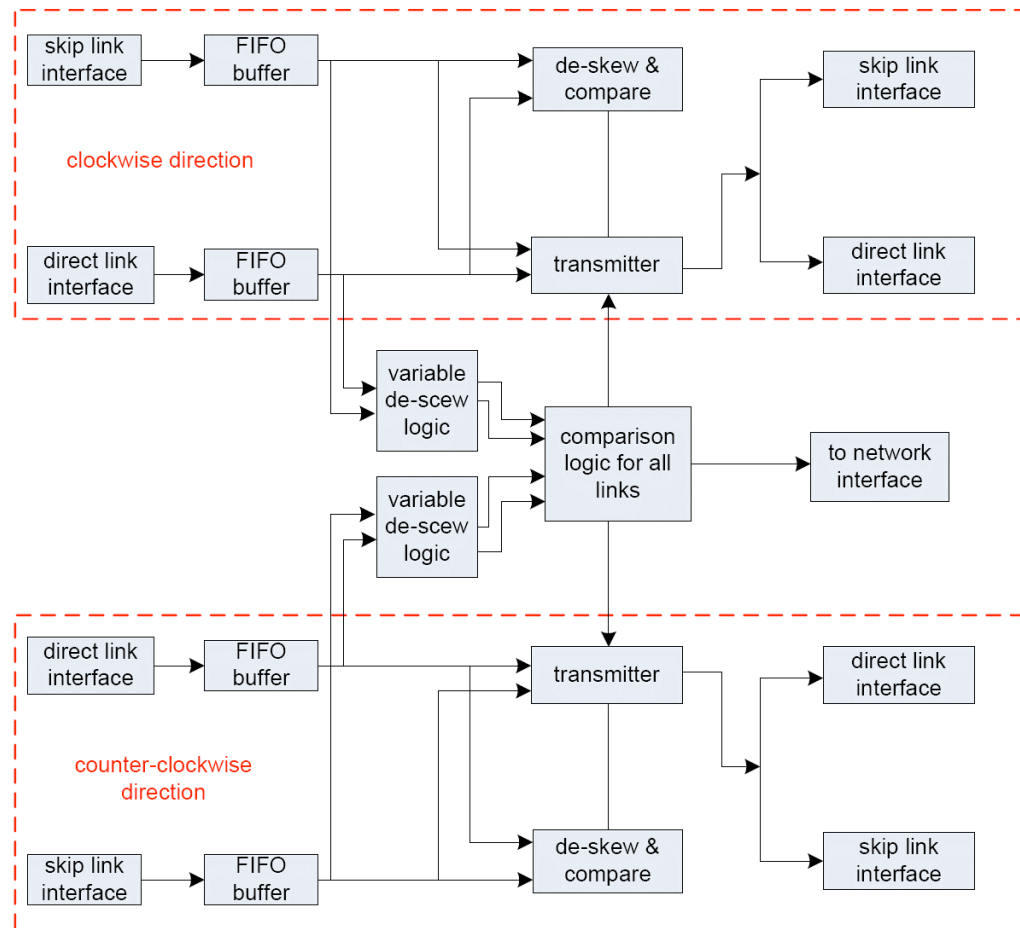


Figure 5. Reconstitution Of Integrity



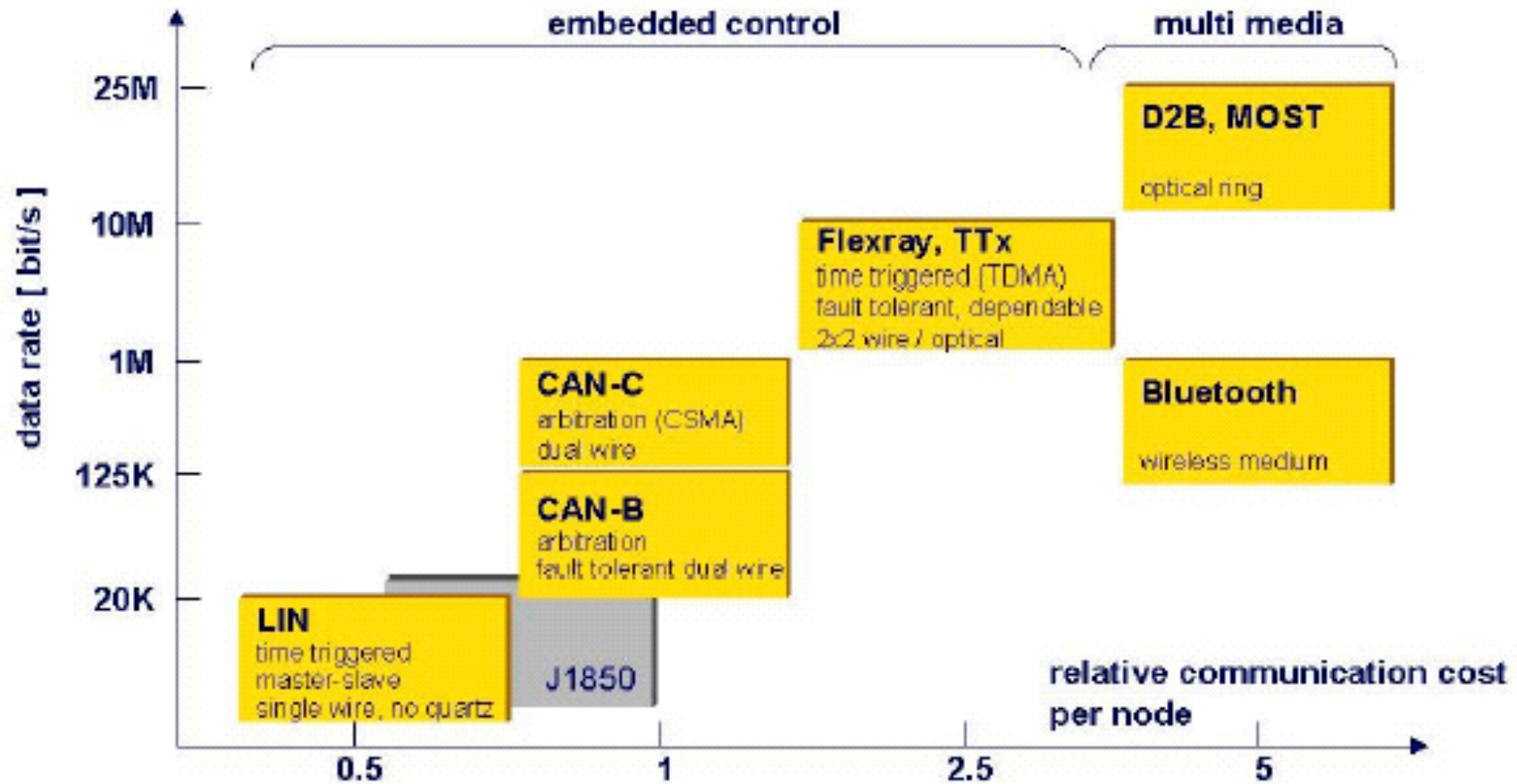


Figure 1: Major Network Protocols in Vehicles

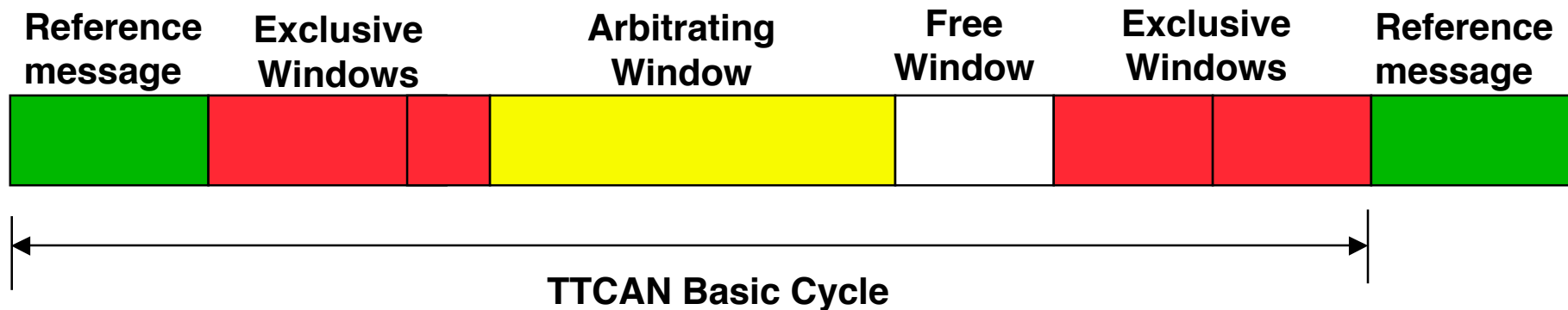


Time Triggered CAN TTCAN

Time Triggered CAN: TTCAN (Führer, Müller, Dieterle, Hartwich, Hugel, Walther,(Bosch))



Basic Cycle and Time Windows




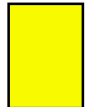

- reference message:** indicates the start of a cycle,
- exclusive window :** used for critical periodic state messages,
- arbitrating window:** used for spontaneous state and event messages,
- free window :** window for further extensions and gap to the next exclusive window.

RETRANSMISSIONS ARE GENERALLY NOT ALLOWED IN TTCAN !!



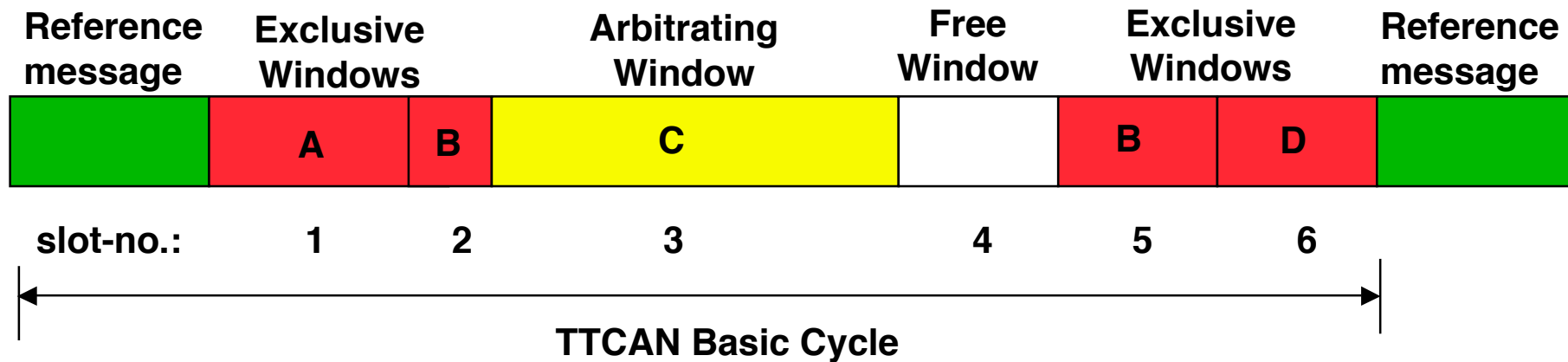
Scheduling a Basic cycle on a node

Node n

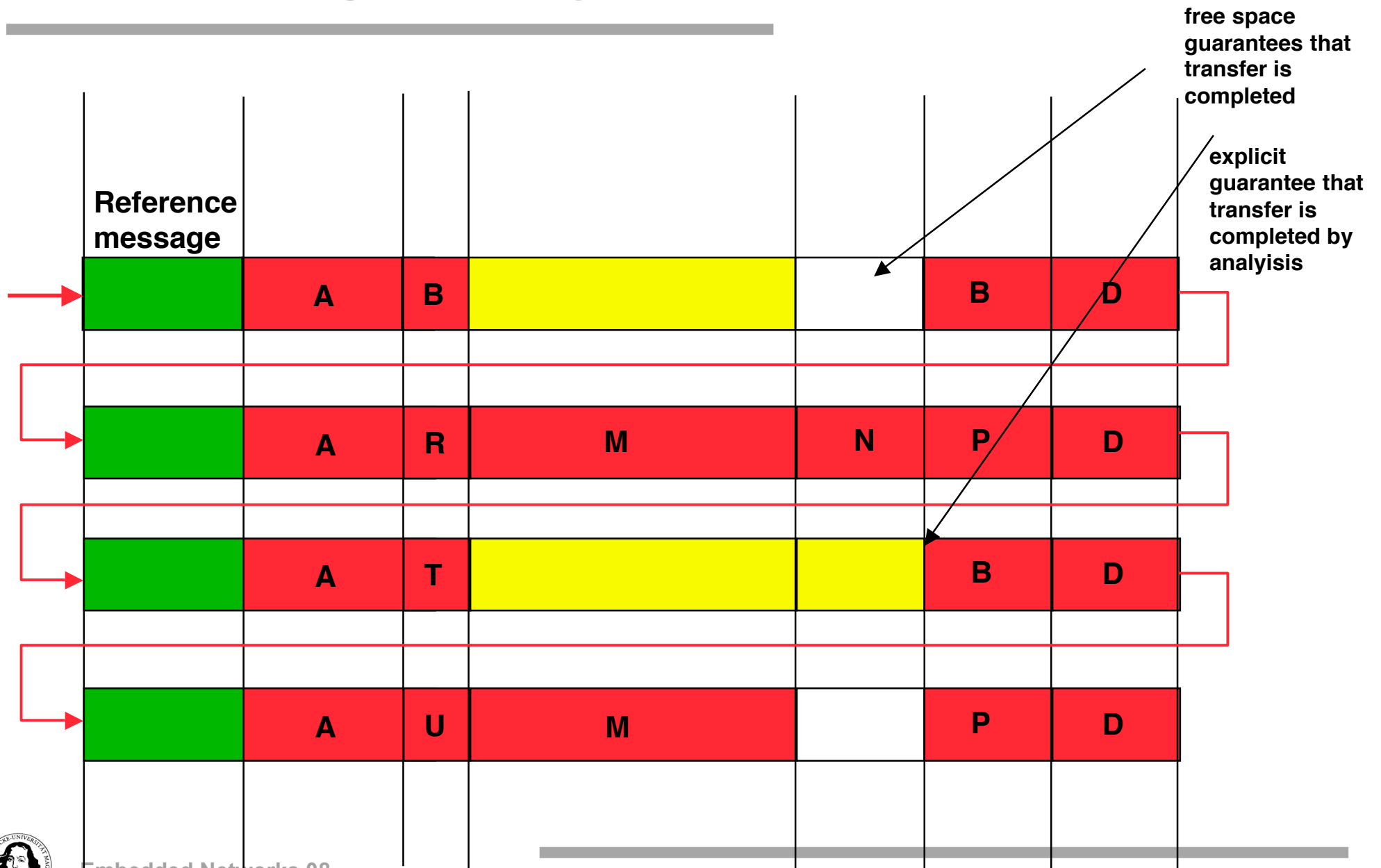
-  Send msg B in slot 2 and 5
-  Send msg F in slot 3
-  Receive msg D in slot 6

Constraint:

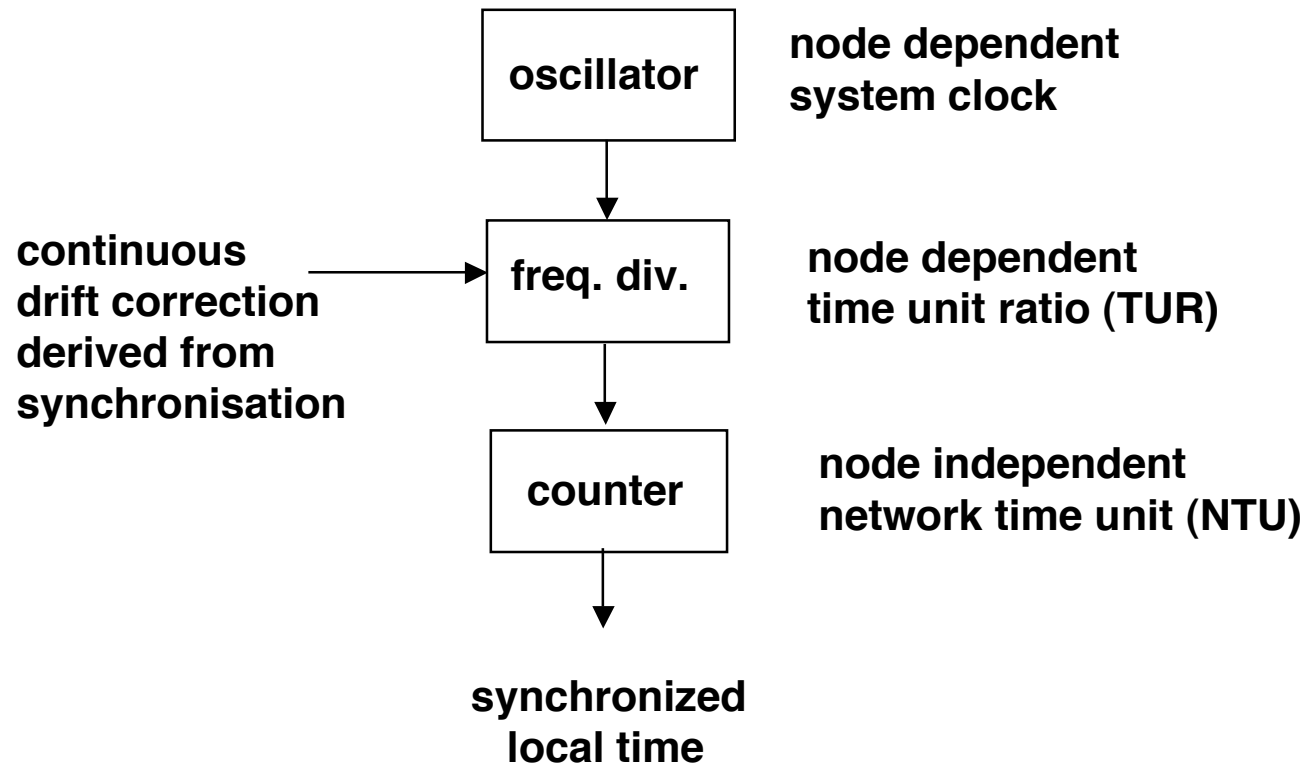
A message transfer in an arbitrating window must be successfully completed before the start of an exclusive window.



Concatenating Basic Cycles to a **MATRIX CYCLE**



Time and clock synchronization in TTCAN



Synchronization based on the existence of a Time Master.

All nodes take a snapshot of their local time at the SoF (Start of Frame) bit of the reference message.

Because of dependability reasons, TTCAN supports redundant Time Masters.

Arbitration among Time Masters is based on the priority scheme of CAN.



Conclusion

TT-CAN adds predictability to CAN

TT-CAN considers periodic message transfer

Fault handling differs substantially from Standard CAN

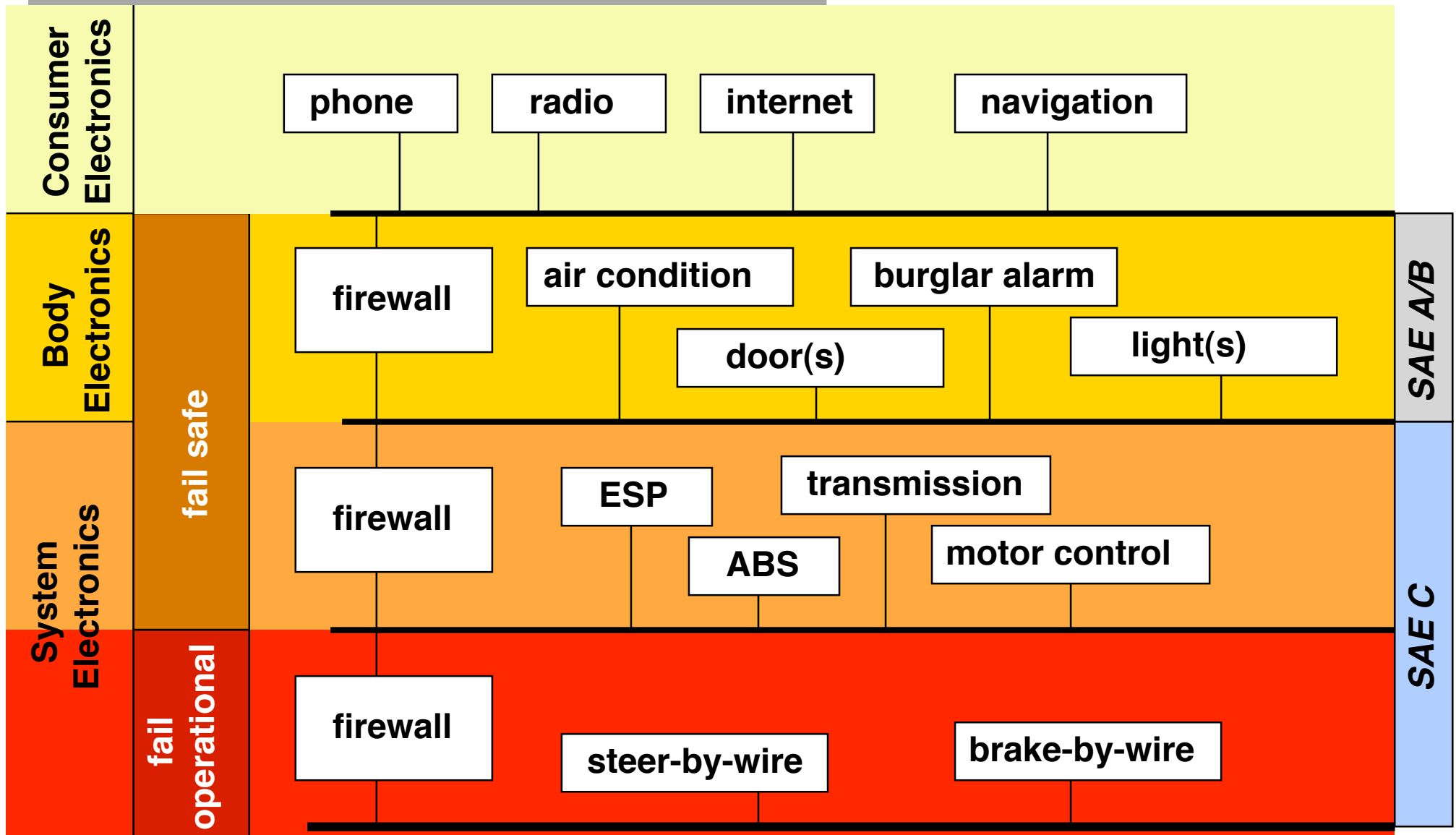
Clock synchronization is supported by hardware

Hybrid approaches are available in the scientific community



Communication levels in a car

(T. Führer, B. Müller, W. Dieterle, F. Hartwich, R. Hugel, M. Walther:
 „Time Triggered Communication on CAN“)



Cost-Performance Trade-off

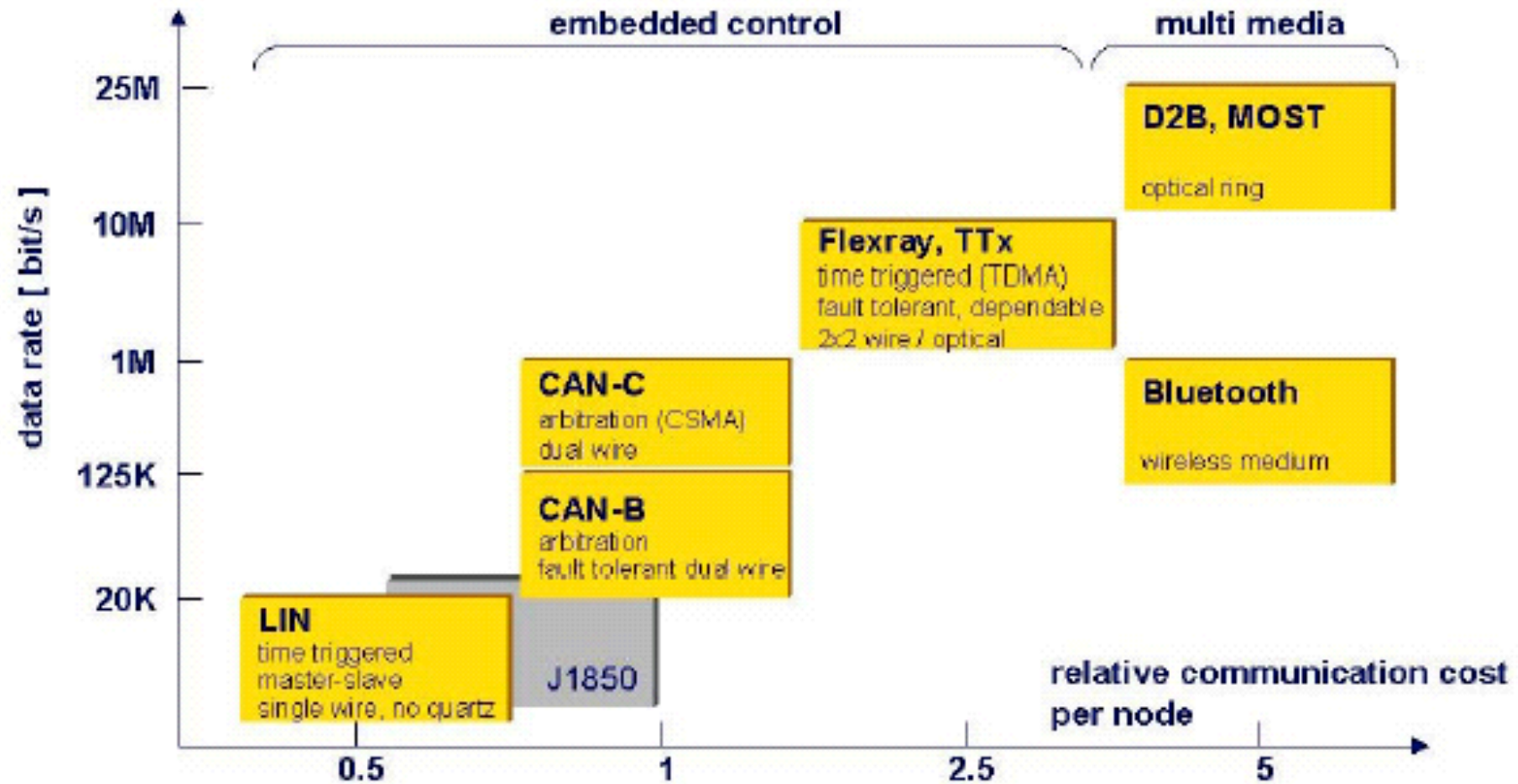


Figure 1: Major Network Protocols in Vehicles



Protocols for less critical, simple sensor-actuator networks:

TTP/A (Time Triggered Protocol for SAE class A applications)

LIN (Local Interconnect Network)



-
- **Master/Slave protocols**
 - **low dependability requirements**
 - **free-running low cost oscillators should be possible**
 - **physical „Single-Wire-Network“ (asynch. serial interface)**
 - **low bandwidth requirements**
 - **low cost**

Transmission speed up to	LIN	TTP/A
20 kbits/second	ISO 9141 (ISO-K)	ISO 9141 (ISO-K)
1 Mbit/second	not specified	RS 485 or CAN
above 1 Mbit/second	not specified	fiber optics

Table 4: Transmission speed of LIN and TTP/A



TTP/A

H. Kopetz: Lit. Einführung,

H. Kopetz, W. Elemenreich, C. Mack: A Comparison of LIN and TTP/A, Research report 4/2000, Institut für Technische Informatik, TU Wien

- real time data
- round: up to 64 byte
- broadcast
- management and configuration data
- diagnostic interface
- point-to-point

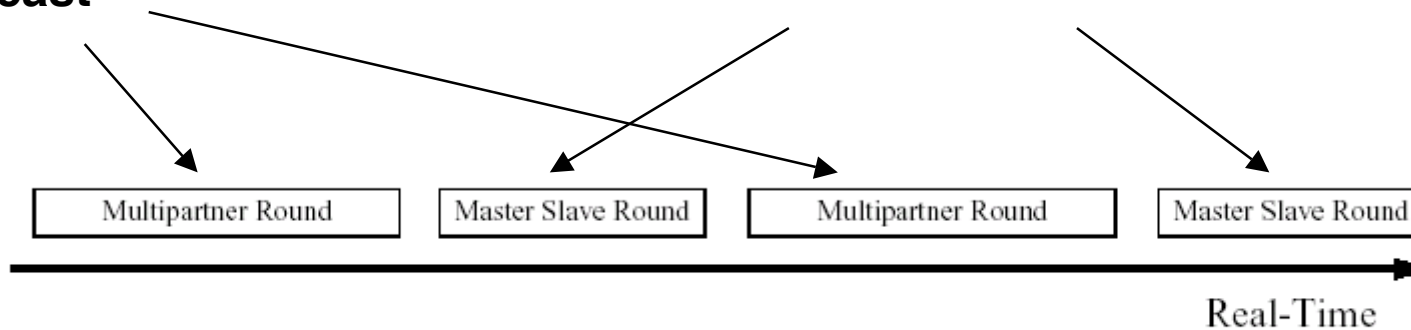


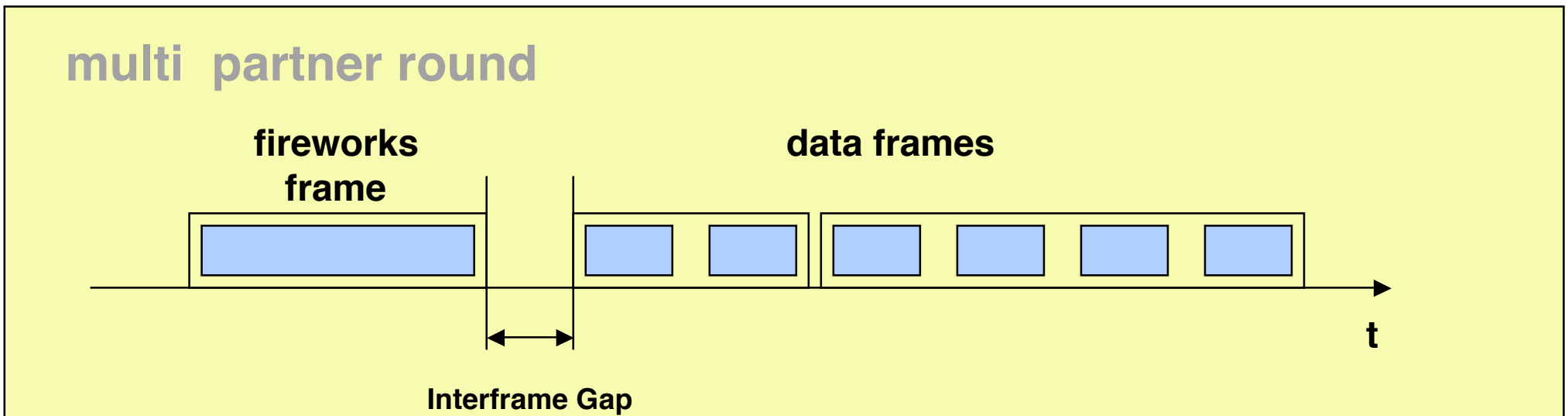
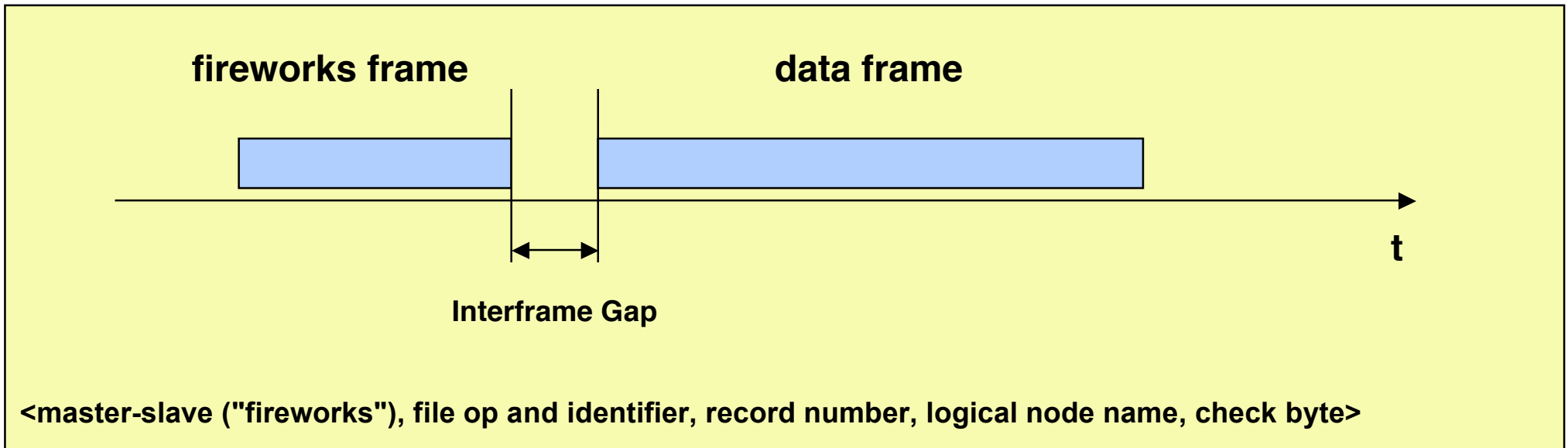
Figure 3: Traffic on the TTP/A Bus

3 different interfaces for slaves:

- RMI : Real-Time message Interface
- DMI: Diagnostic message Interface
- CMI: Configuration Message Interface



master-slave dialogue

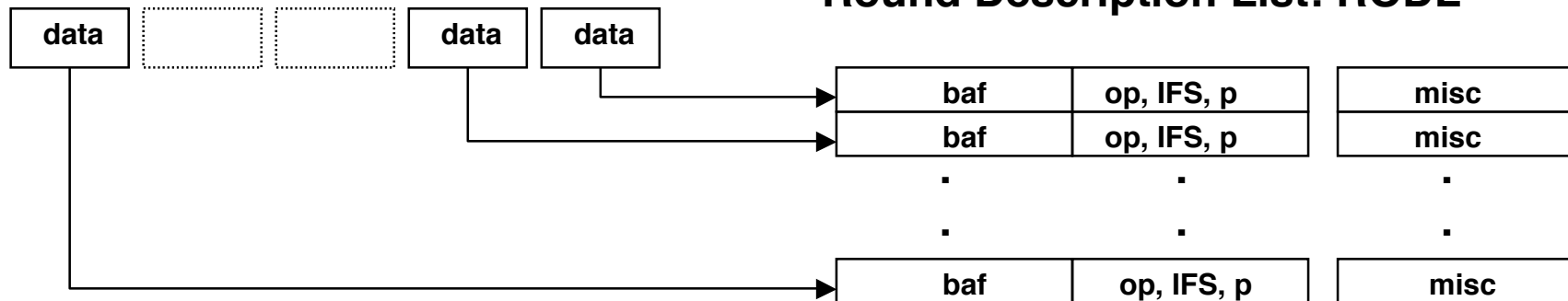


data centric communication model

- real time frames contain data **only!**
- all data is stored in the Interface File System (IFS).
- addresses to data are specified as IFS addresses.
- addresses are specified in the round description list (RODL), i.e. the time slot in which the message is transmitted is fixed according to the TT model.

baf: byte after fireworks
 op: operation
 IFS: IFS-Adresse
 p: protection (checksum)

Multipartner Round

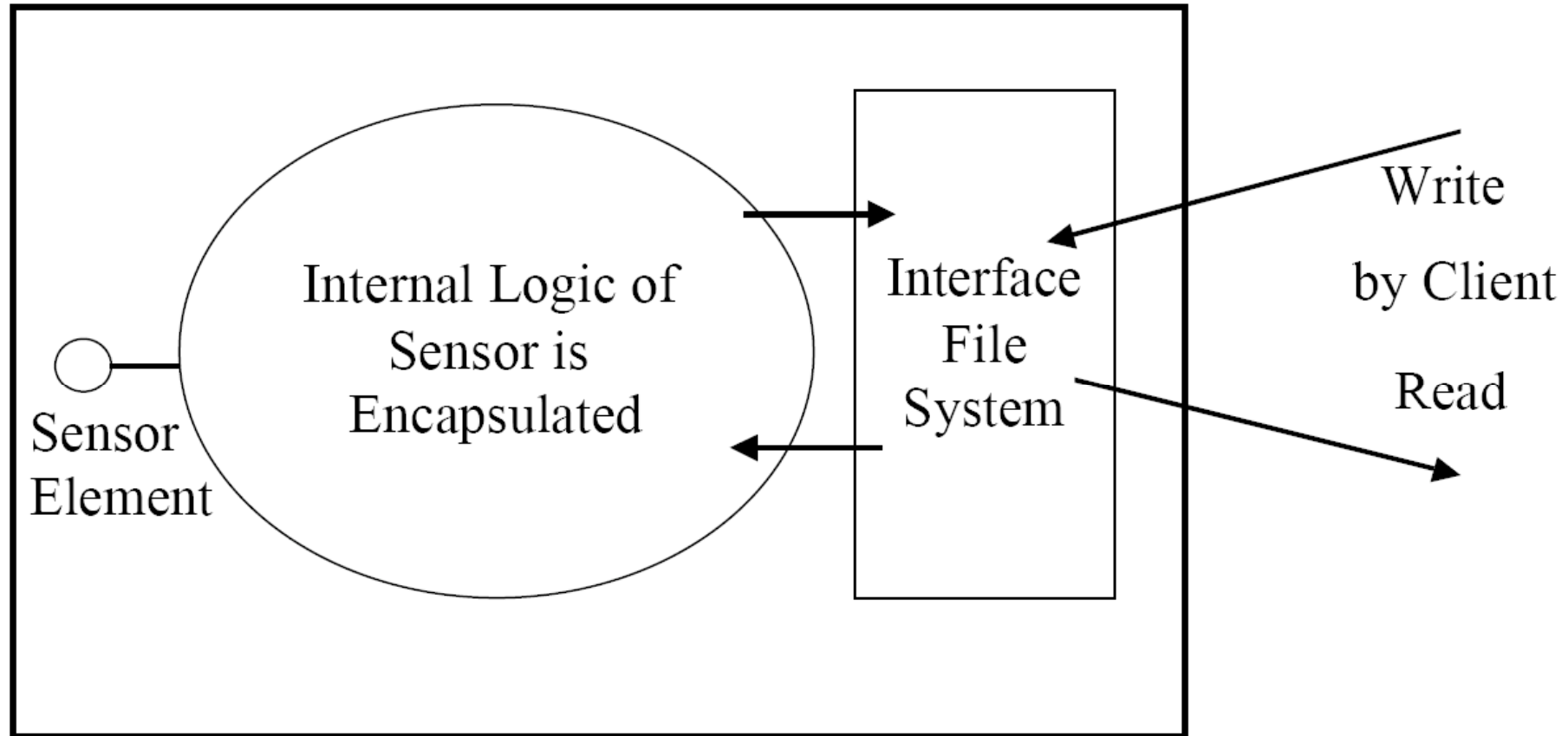


The RODL is also stored in the IFS and can be configured via the CMI.

There are max. 8 RODLs. RODL# is transmitted with a Hamming Distance of 4 (high protection against failures).



Programming model for smart transducers in the IFS



The address space of the „Interface File System“ IFS

Address contains: < file, record, byte, checksum >
 2^6 2^8 2^2

every node in the IFS supports:

up to 64 files
up to 256 records
with 4 bytes each

i.e. an address space of 2^{16} bytes/node.

and how to address the nodes ?



Every Smart Transducer has a unique physical name (8 bytes) consisting of:

- a node type name (series number)**
- a node name within series (serial number)**

During operation a node is addressed by a one-byte logical name that is unique within a cluster (i.e. up to 256 nodes/cluster).

The assignment of a logical name to a node is called baptizing and can be performed on-line. Low cost nodes can have preprogrammed logical names.

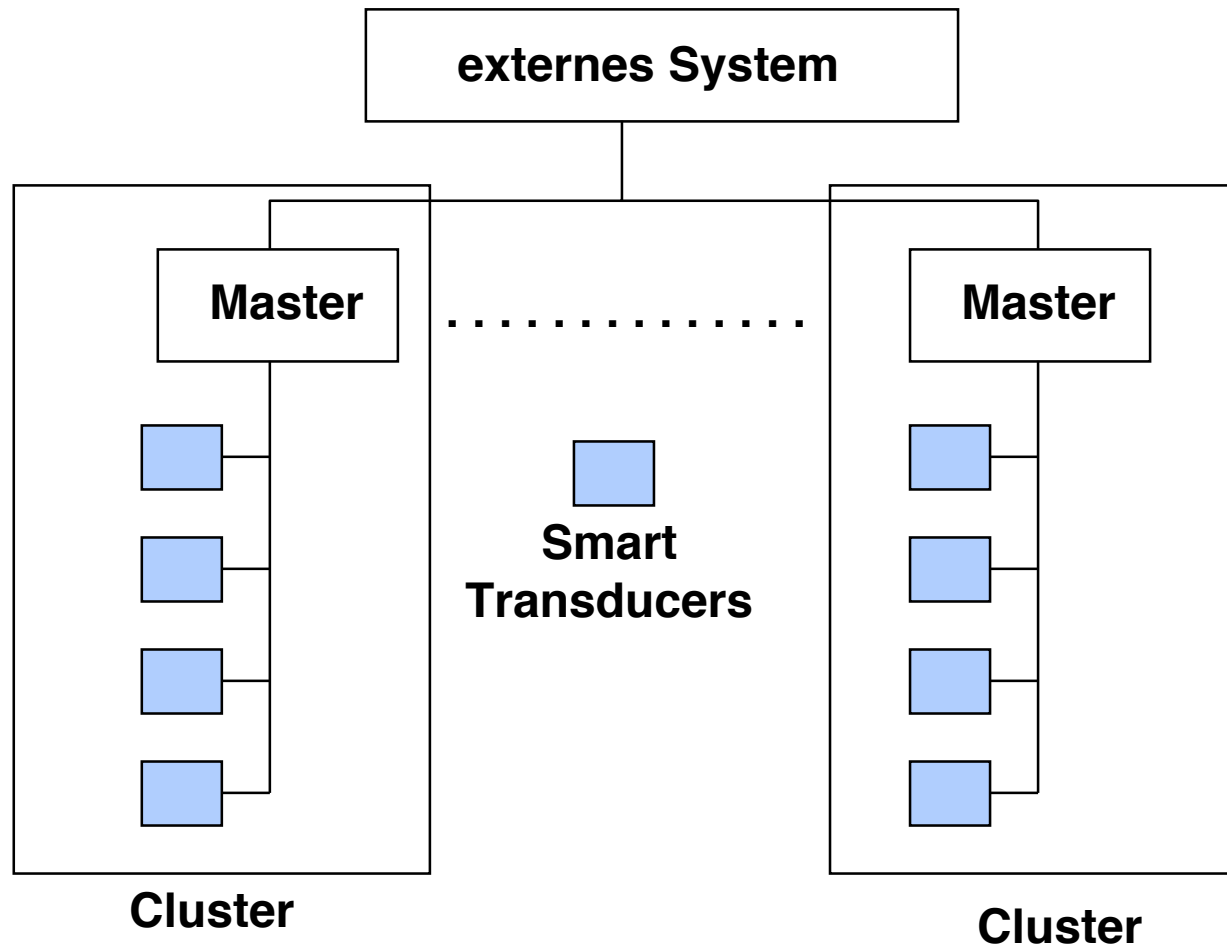
During operation a node is addressed by:

<Cluster Name, Node Name, File Name, Record Name>

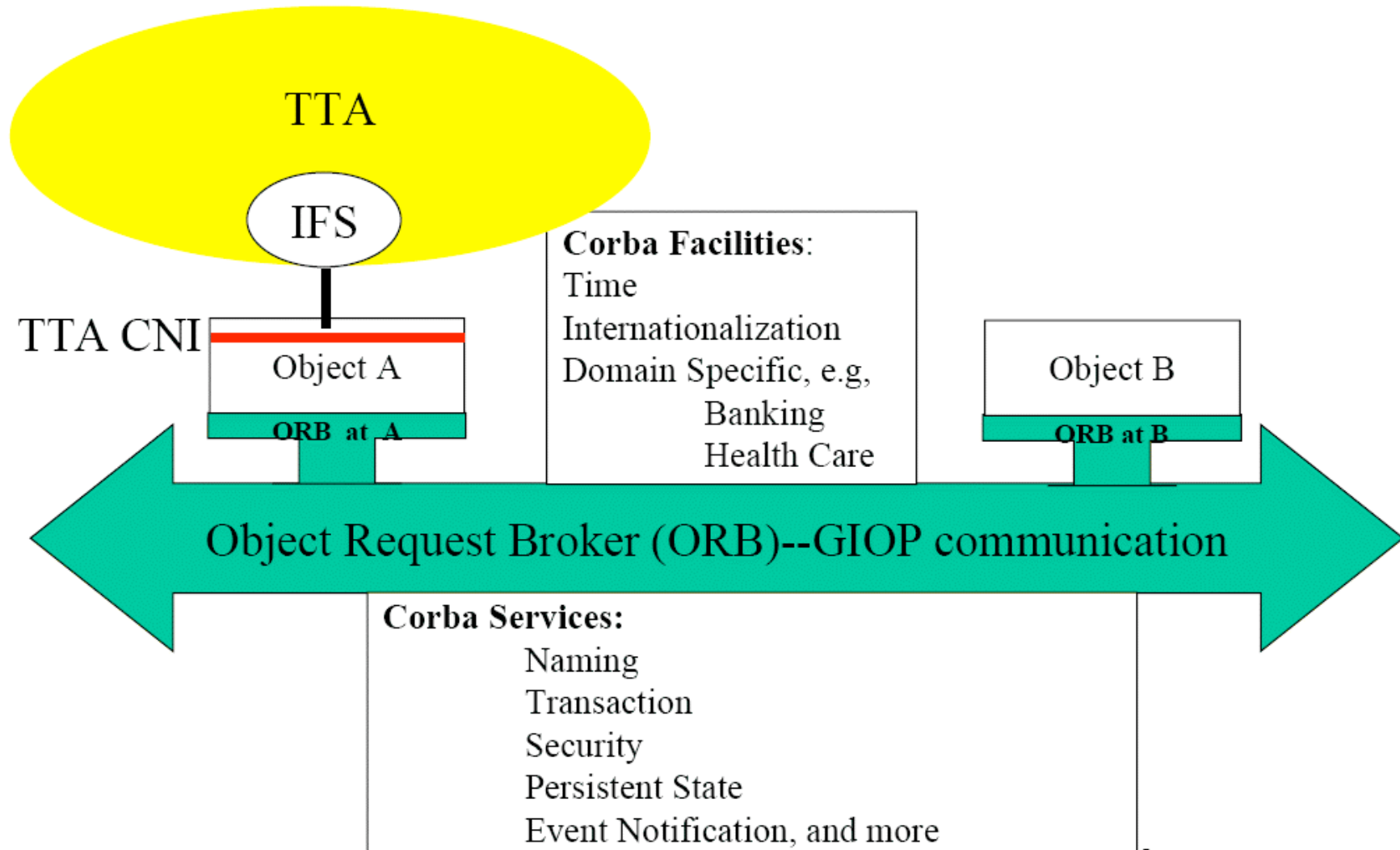


General architecture of a TTP/A system

global name of a data item: <cluster name, node name, file name, record name>



Integrating a TTP/A system in CORBA

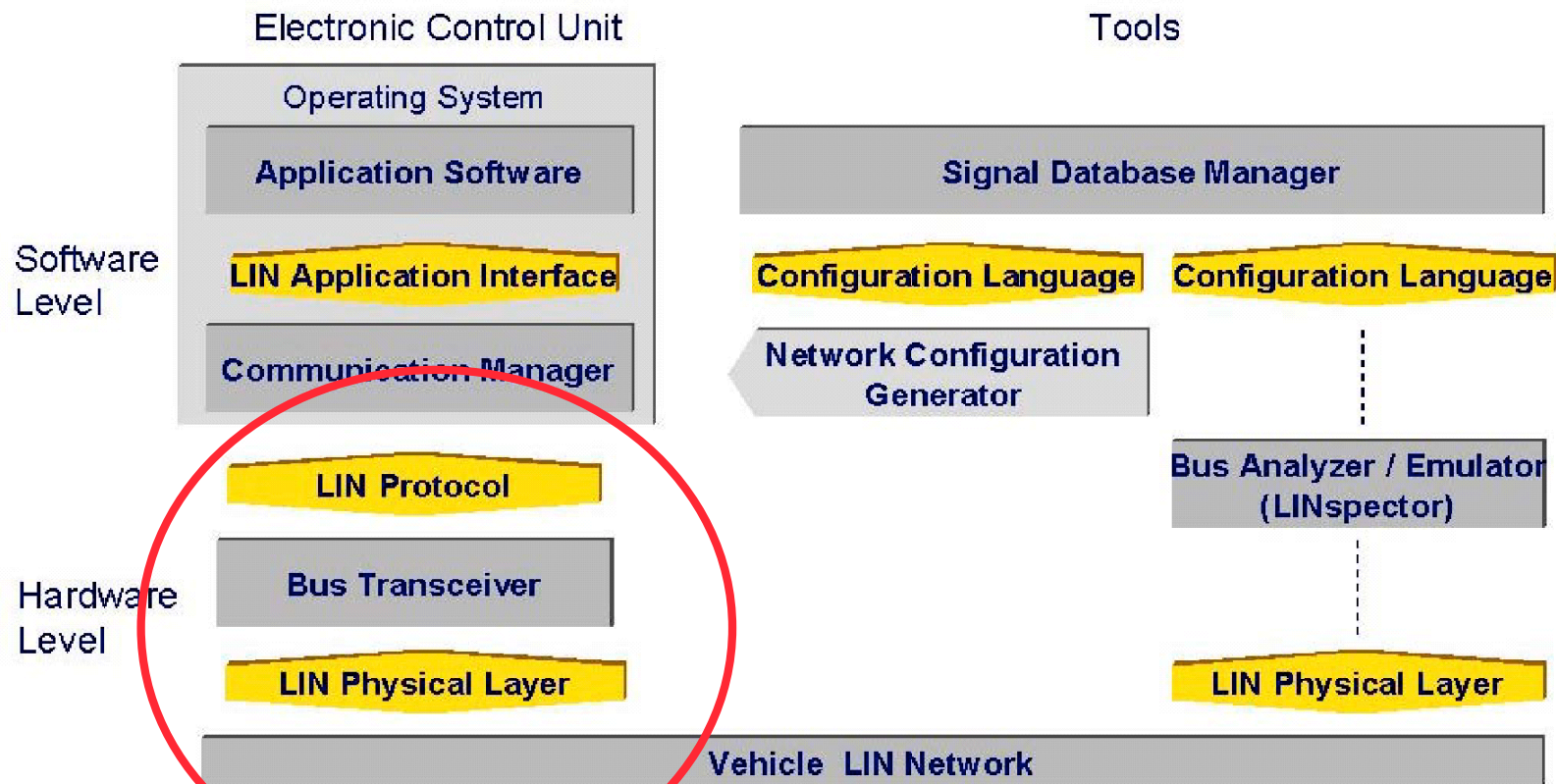


© H. Kopetz 27/11/2001



LIN (Local Interconnect Network)

LIN Specification Package, Revision 1.2, Nov. 17, 2000

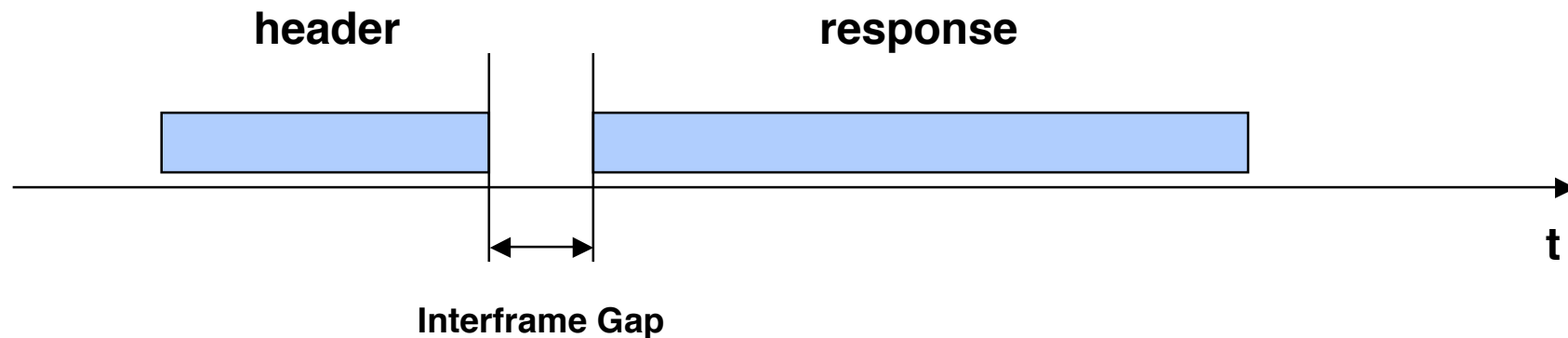


Properties of LIN

- . **single-master / multiple-slave concept**
- . **low cost silicon implementation based on common UART/SCI interface hardware, an equivalent in software, or as pure state machine.**
- . **self synchronization without quartz or ceramics resonator in the slave nodes**
- . **guarantee of latency times for signal transmission**
- . **low cost single-wire implementation**
- . **speed up to 20kbit/s.**



Master-Slave communication in LIN



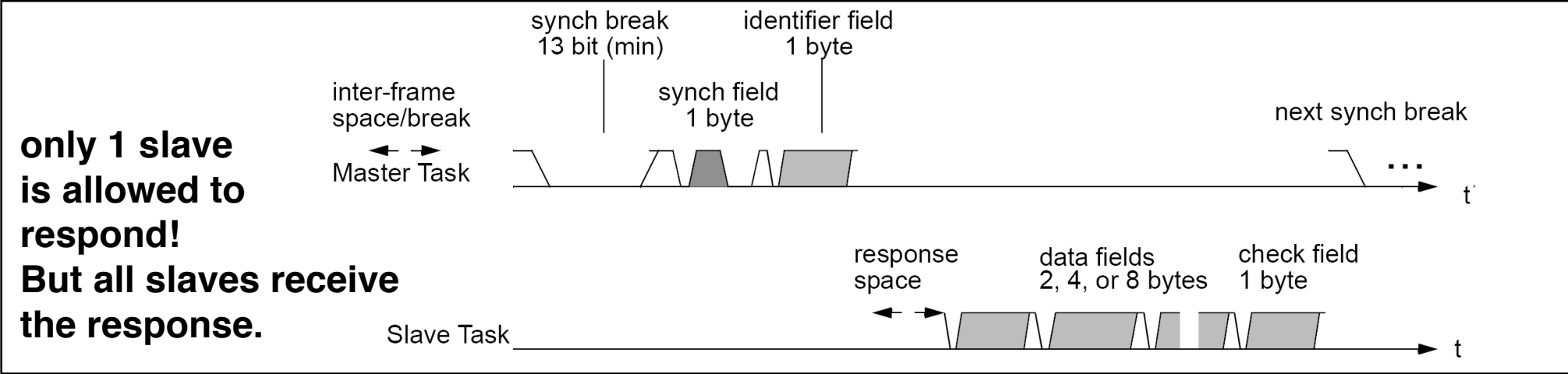
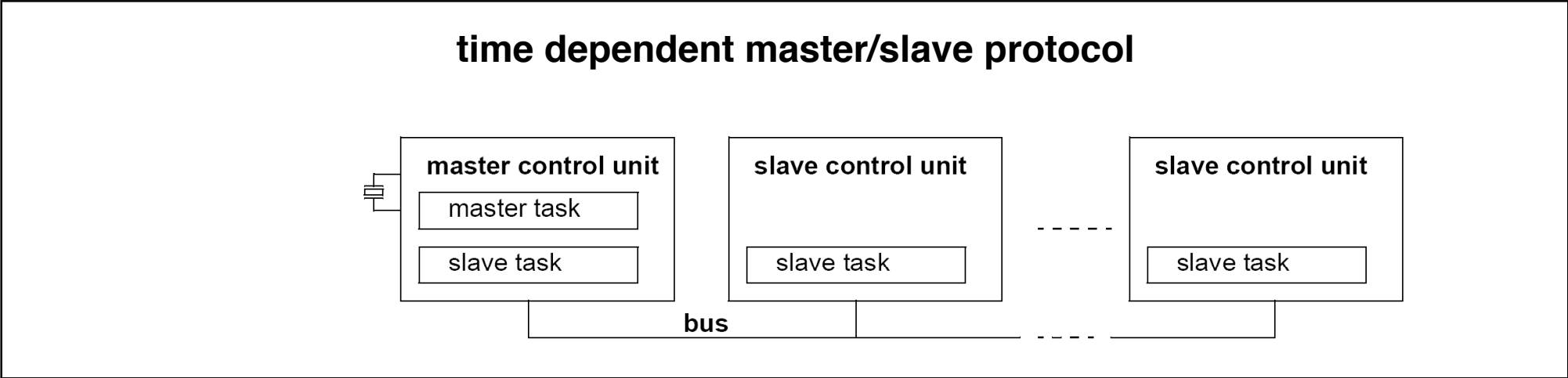
Header:

- serves for the synchronisation of slaves
- specifies the sequence and length of the fields in the data frame

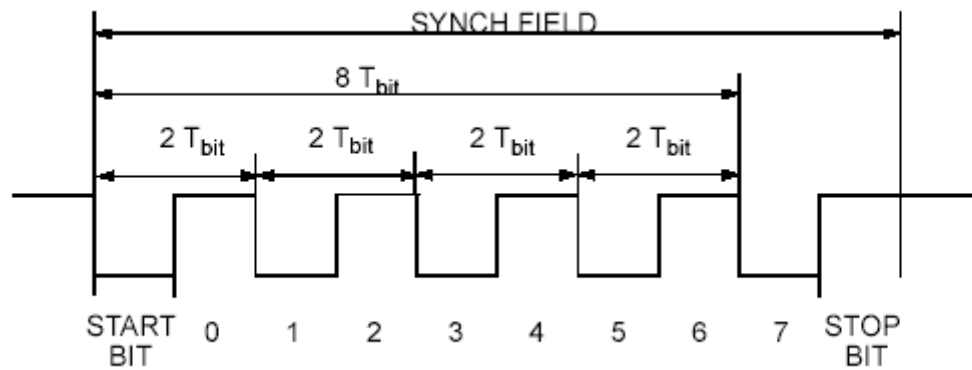


LIN (Local Interconnect Network)

LIN Specification Package, Revision 1.2, Nov. 17, 2000



LIN Specification Package, Revision 1.2, Nov. 17, 2000



**Synch. Feld
0x55**

Figure 9.1: SYNCHRONIZATION FIELD

clock tolerance	Name	$\Delta F / F_{Master}$
master node	$F_{TOL_RES_MASTER}$	$< \pm 0.5\%$
slave node with quartz or ceramic resonator (without the need to synchronize)	$F_{TOL_RES_SLAVE}$	$< \pm 1.5\%$
slave without resonator, lost synchronization	$F_{TOL_UNSYNCH}$	$< \pm 15\%$
slave without resonator, synchronized and for a complete message	F_{TOL_SYNCH}	$< \pm 2\%$

Table 8.1: Oscillator Tolerance



LIN Specification Package, Revision 1.2, Nov. 17, 2000

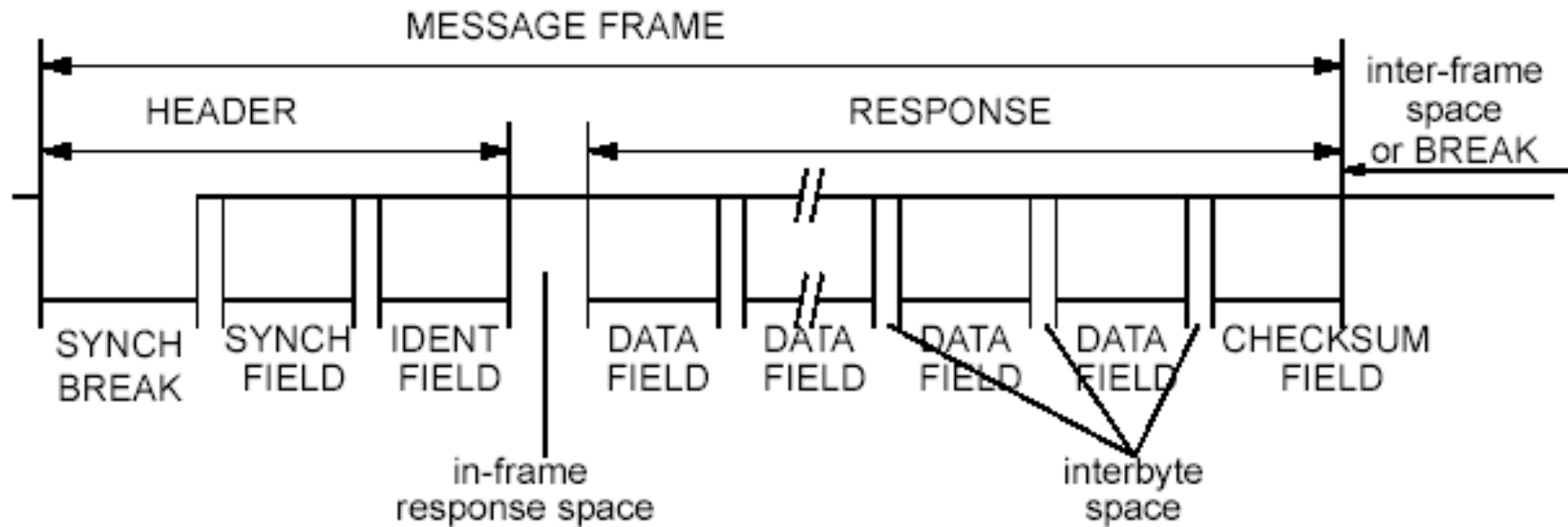


Figure 3.1: LIN MESSAGE FRAME



LIN Specification Package, Revision 1.2, Nov. 17, 2000

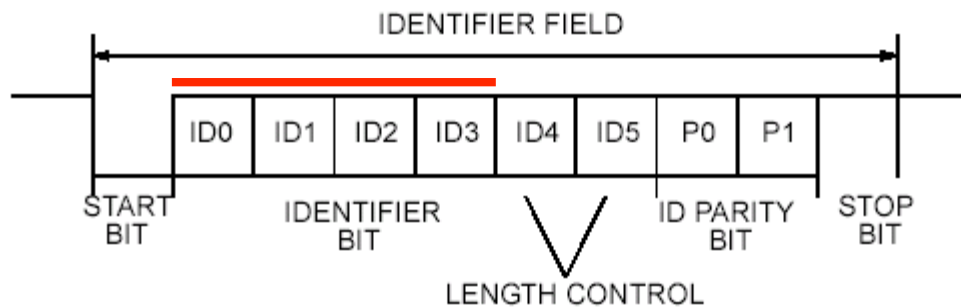


Figure 3.5: IDENTIFIER FIELD

64 identifiers

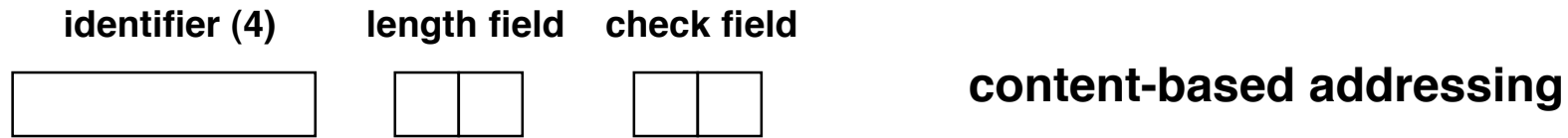
divided in 4 groups of length: 2,4, and 8 bytes

An ID identifies the content of a message, not the sender or receiver !

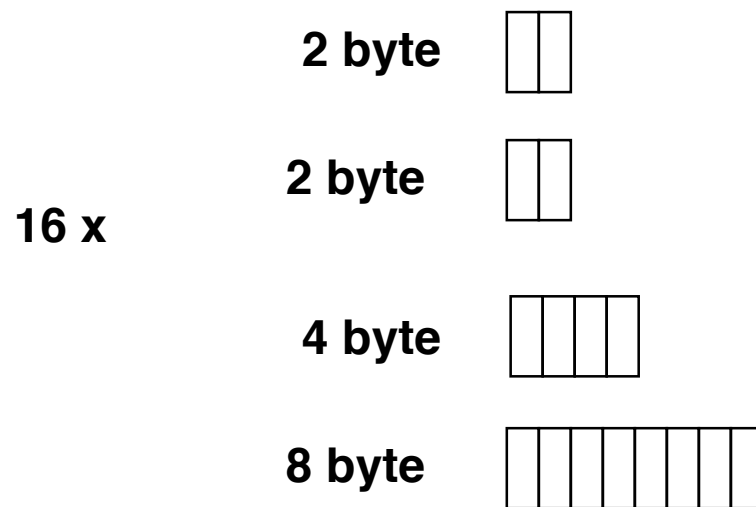
Slaves can be added or removed without changing any software in the other slaves.



LIN frame format



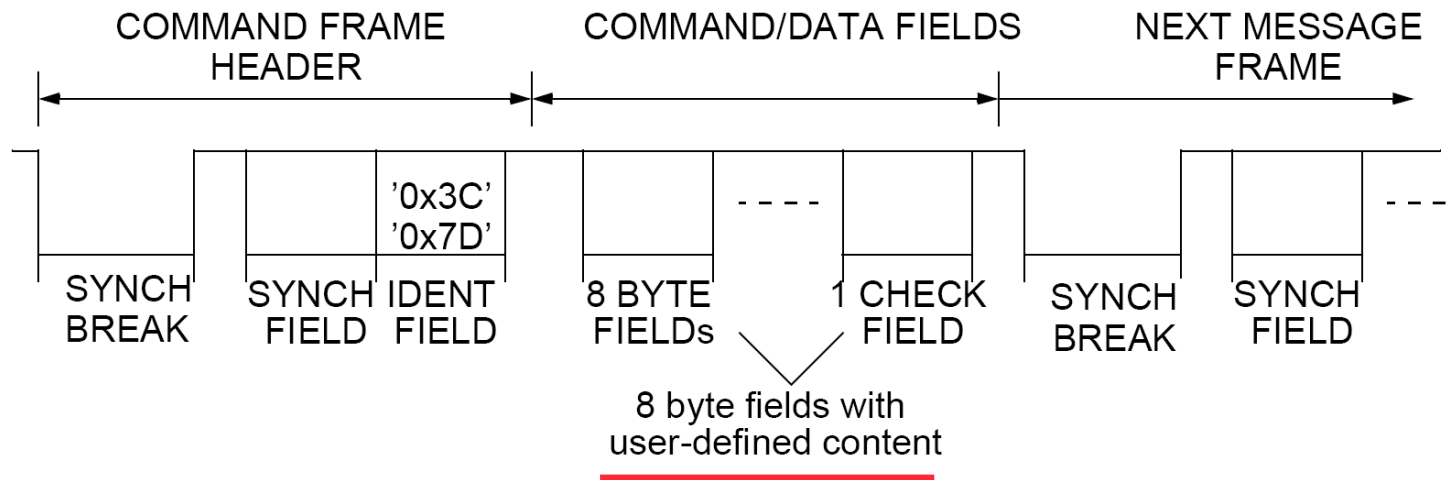
max. 8 Byte response frame



**reserved IDs: Master request Frame (0x3C), Slave Response Frame (0x3D)
Extended Frames (User 0x3E, Reserved 0x3F)**



LIN Master Request Frame

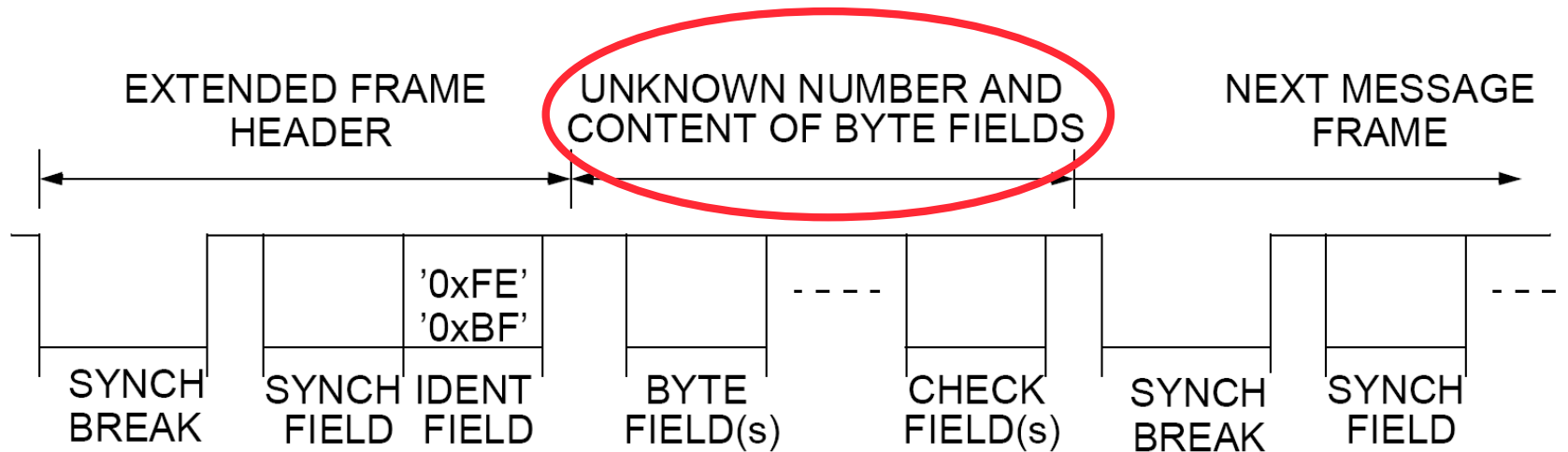


**Download of data to the slave.
Request of data from the slave.**

**Multiple 8 byte fields possible!
Slave address is part of the command fields.**



LIN Extended Frame



**slaves, which are not addressed (interested resp.)
wait until the next SyncBreak!**



Error detection capabilities of LIN:

Bit-Error

Checksum-Error

Identifier-Parity-Error

Slave-Not-Responding-Error

Inconsistent-Synch-Field-Error

No-Bus-Activity



Comparison LIN und TTP/A (response time and protocol efficiency)

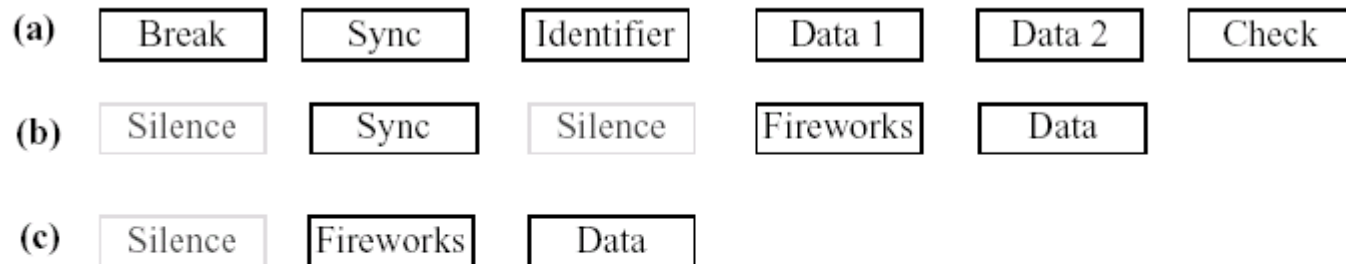
Kopetz, Elmenreich,
Mack, TU Wien, 2000

response
time

10 nodes, response time in milliseconds on a 20 kbit bus	Minimum LIN	Maximum LIN	Minimum TTP/A	Maximum TTP/A
Every nodes sends four bytes of data	46.75 msec	65.4 msec	35.4 msec	35.6 msec
Every nodes sends two bytes of data	35.75 msec	50.05 msec	22.2 msec	22.3 msec
Every node sends one byte of data	35.75 msec	50.05 msec	15.6 msec	15.7 msec
Every node sends four bits of data	35.75 msec	50.05 msec	9 msec	9.1 msec
Every node sends four bits of data, additional master-slave round for DM service between any two multipartner rounds in TTP/A	not supported	not supported	16.8 msec	16.9 msec

Table 2: Achievable response times of LIN and TTP/A

protocol
overhead



Real Time

Figure 5: Byte Sequence of the simplest message in LIN (a), in TTP/A with start-up synchronization (b) and in TTP/A without start-up synchronization (c).



Automotive and highly dependable Networks

TTP/C

Byteflight

FlexRay

Braided Ring

Time Triggered CAN (TTCAN)

TTP/A

LIN

