Automotive and highly dependable Networks

TTP/C
Byteflight
FlexRay
Braided Ring

Time Triggered CAN (TTCAN)
TTP/A
LIN

Time Triggred Protocol (TTP)

H. Kopetz, TU Wien (see references in the introduction)

Excellent surveys:

TTP:
Hermann Kopetz, Günther Bauer:
"The Time-Triggered Architecture"
http://www.tttech.com/technology/docs/history/HK_2002-10-TTA.pdf

Networks for safety critical applications in general:
John Rushby:
"Bus Architectures for Safety-Critical Embedded Systems"
http://www.csl.sri.com/users/rushby/papers/emsoft01.pdf

Products:
http://www.tttech.com/

Automotive and highly dependable Networks

TTP/C
Byteflight
FlexRay
Braided Ring
Time Triggered CAN (TTCAN)
TTP/A
LIN

Time Triggred Protocol (TTP)

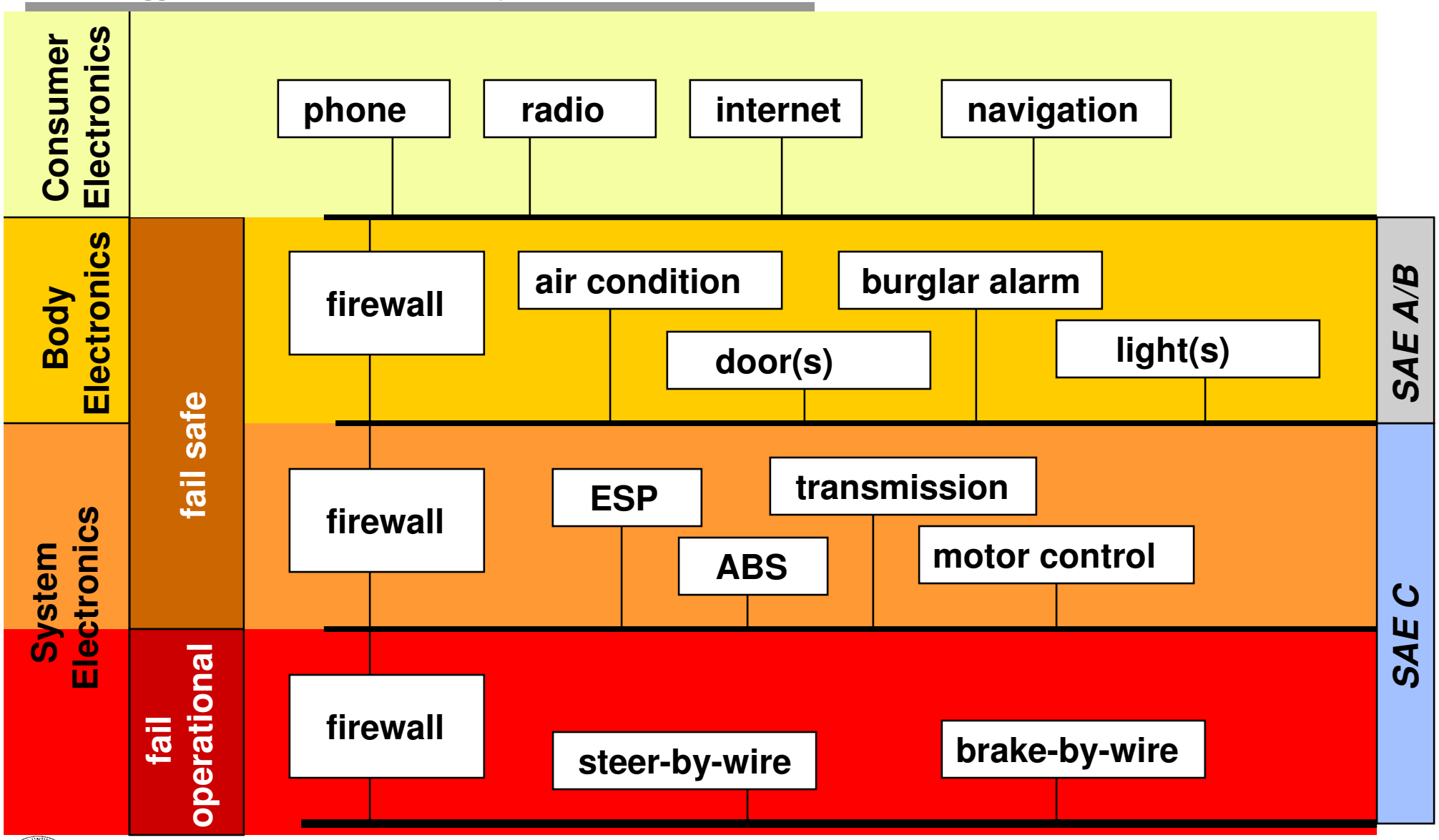
Objectives:

- **Predictable, guaranteed message delay**
- **No single fault should lead to a total network failure**
- **Fault-Tolerance**
  - **- Fault detection on the sender and the receiver side**
  - **- Forward error recocery**
  - **- Treating temporary faults (Black-out)**
  - **- Distributed redundancy management**

- **Clock synchronization**
- **Membership-service (basis for atomic multicast)**
- **Support for fast consistent mode changes**
- **Minimal protocol overhead**
- **Flexibility without sacrifycing predictability**

Communication levels in a car

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

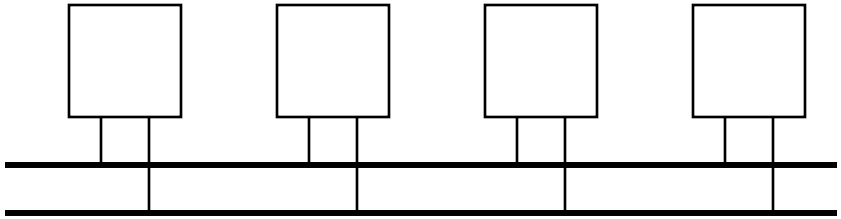


Design principles

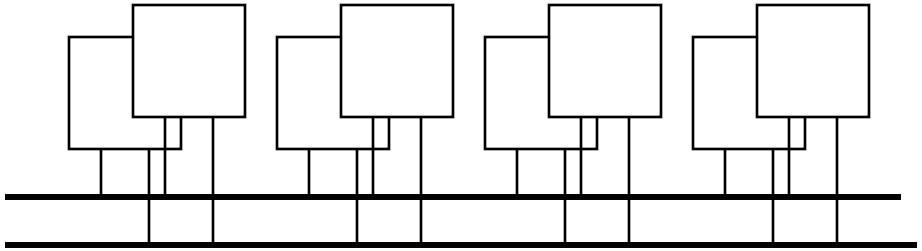
- Exploiting a priori knowledge (static message schedule)
- Implicit flow control
- Fail silence
- Continuous supervision and consistent view of system state

Fault-Tolerant Network Configurations

Class 1:
1 node/FTU
2 frames/FTU

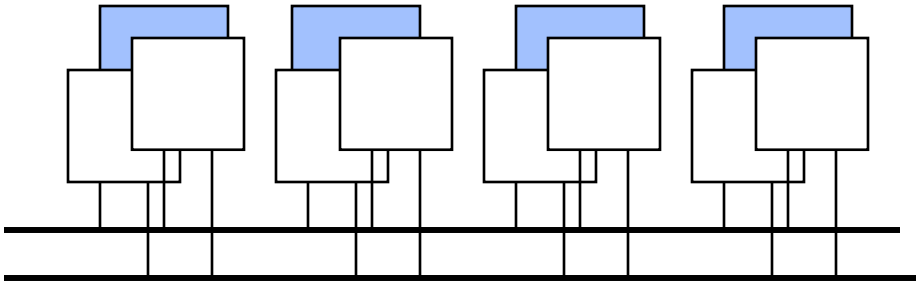


Class 2:
2 active node/FTU
2 frames/FTU



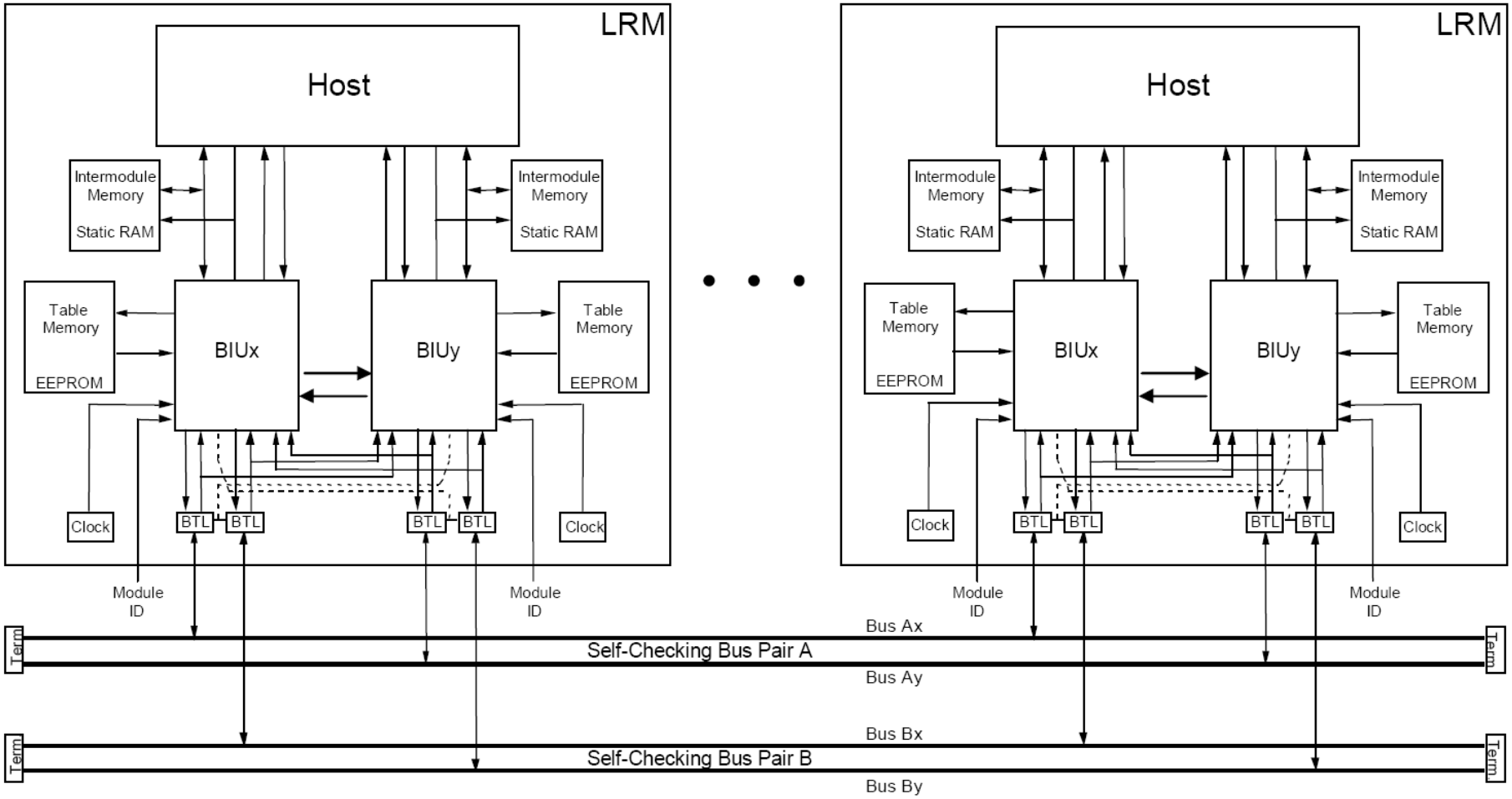
Class 3:
2 active nodes/FTU
4 frames/FTU

Class 4:
2 active nodes/FTU
+ 1 spare/FTU
4 frames/FTU



component redundancy + time redundancy

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

Magic reliability parameter:

10^{-9} failures/h

for a mission time of 10h

Fault-tolerance parameters

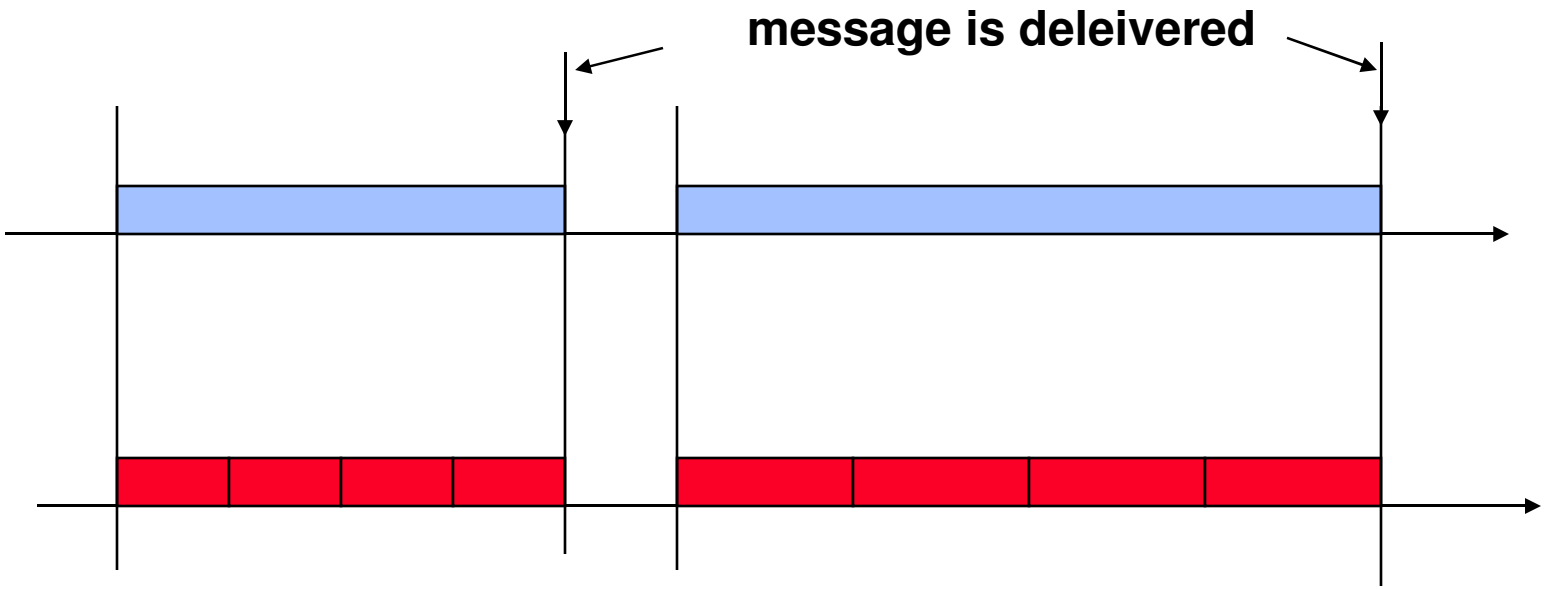
failure type	failure probability
permanent node failure	10^{-6}/h
permanent channel failure	10^{-5}/h
transient node failure	10^{-4}/h
transient channel failure	10^{-3}/h

what is the relation: faulty messages / overall number of messages ?

type of failures	Class 1	Class 2	Class 3	Class 4
Perm. node failure	0	1	1	2
Perm. comm. failure	1	1	1	1
Trans. node failure	0	1/Rec.interv.	1/Rec. interv.	1/TDMA-round
Trans. comm. failure	1 of 2	1 of 2	3 of 4	3 of 4

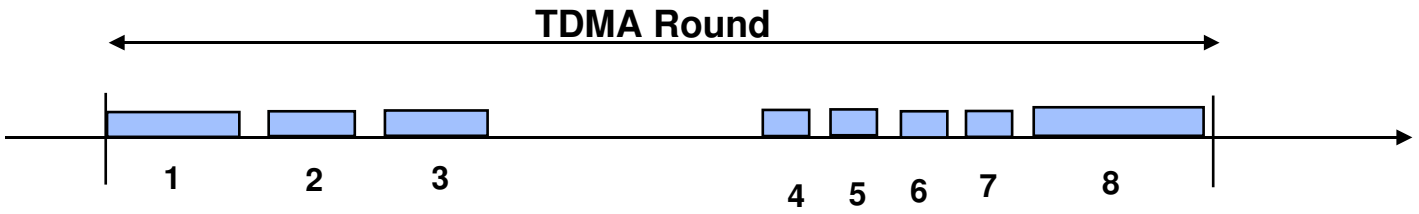
„forward“- error recovery

Predictability means that recovery has to be integrated !



exploit time redundancy → multiple message transmissions

Exploit a priori knowledge: Off-line Scheduling



	time	address	Attributes D	L	I	A
1						
2						
3						
4						
5						
6						
7						
8						

Message Description List

MEDL

time: defines the point in time when the message has to be transmitted

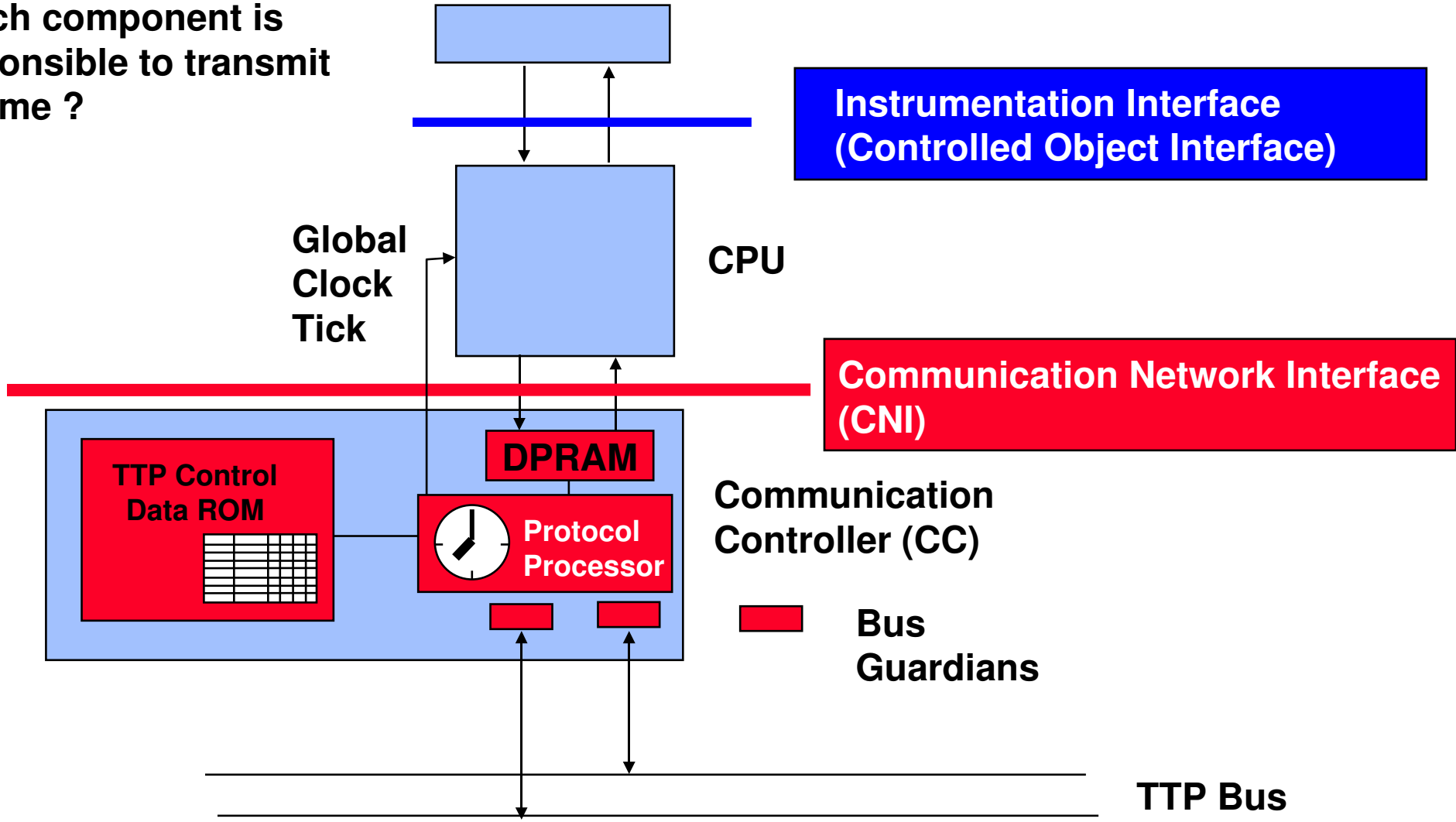
Address: Defines the local address where the messagels to be transmitted are stored in the node's memeory

D: Direction Input or Output
L: frame length
I: Init or normal message
A: "Additional" Parameter Field

TDMA Round (Cluster Cycle): Every FTU has at least transmitted once in a round.

Fail silence und strict enforcement of transmit times

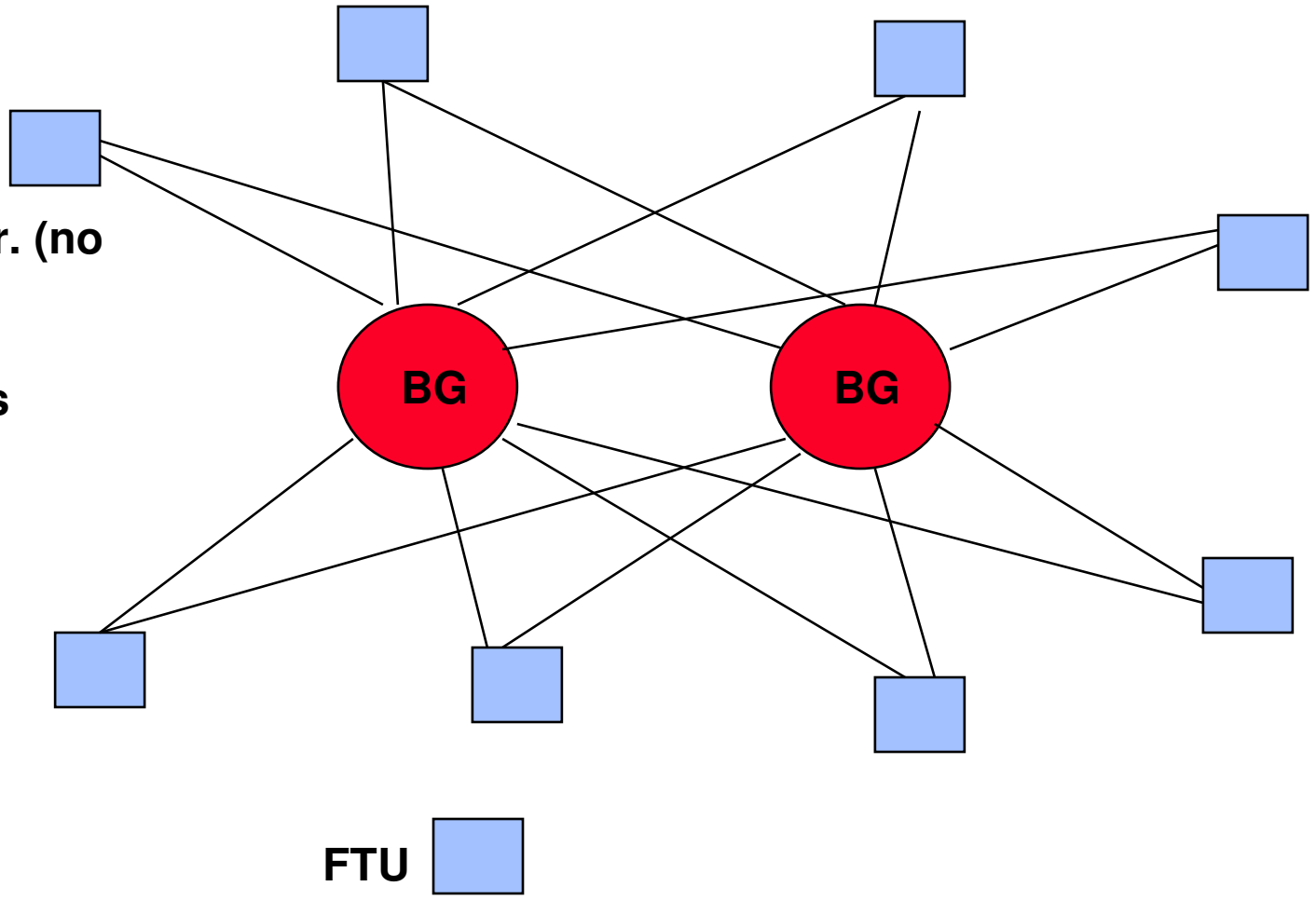
Which component is responsible to transmit a frame ?



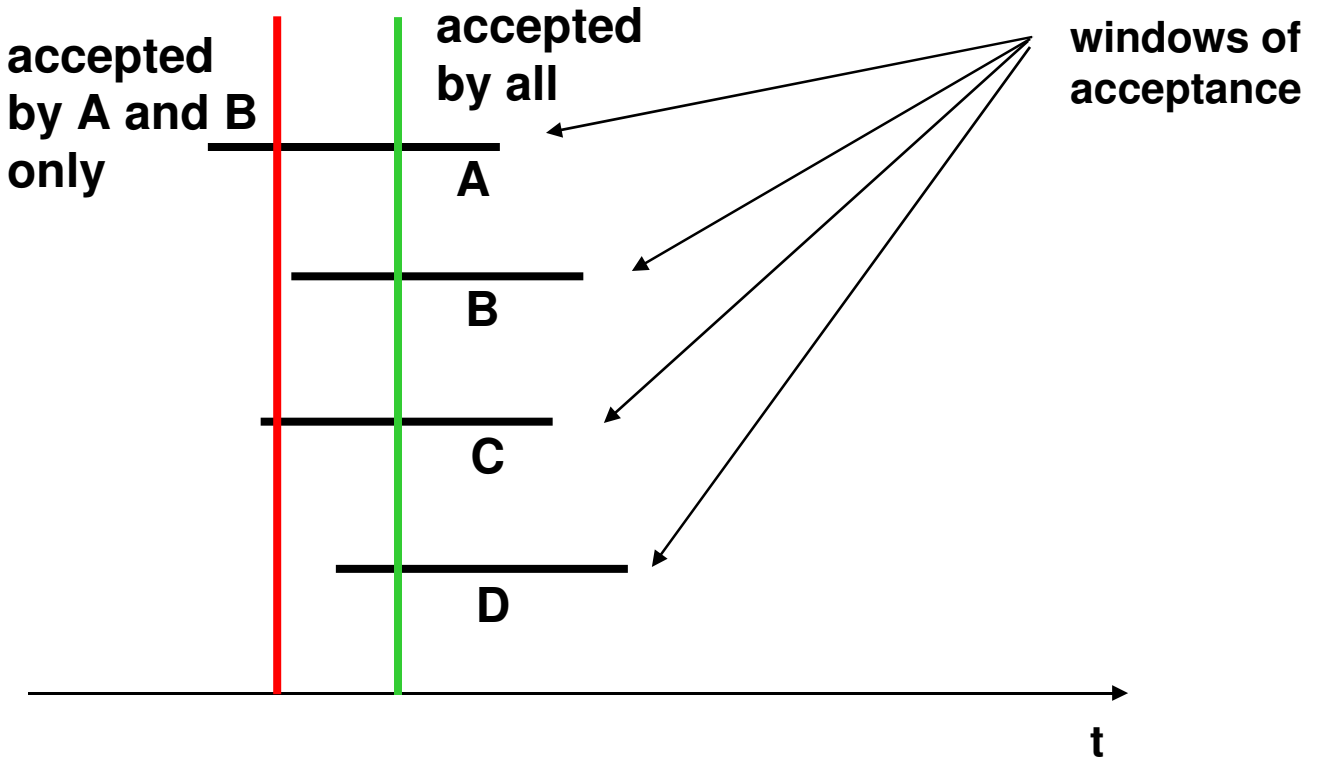
Migration of Bus-Guardians: Star-Topology

Motivation:

- **Re-shaping and synchr. (no SOS failures)**
- **Isolation of faulty FTUs**
- **Physical separation of Bus guardians from hosts (less common mode failures)**

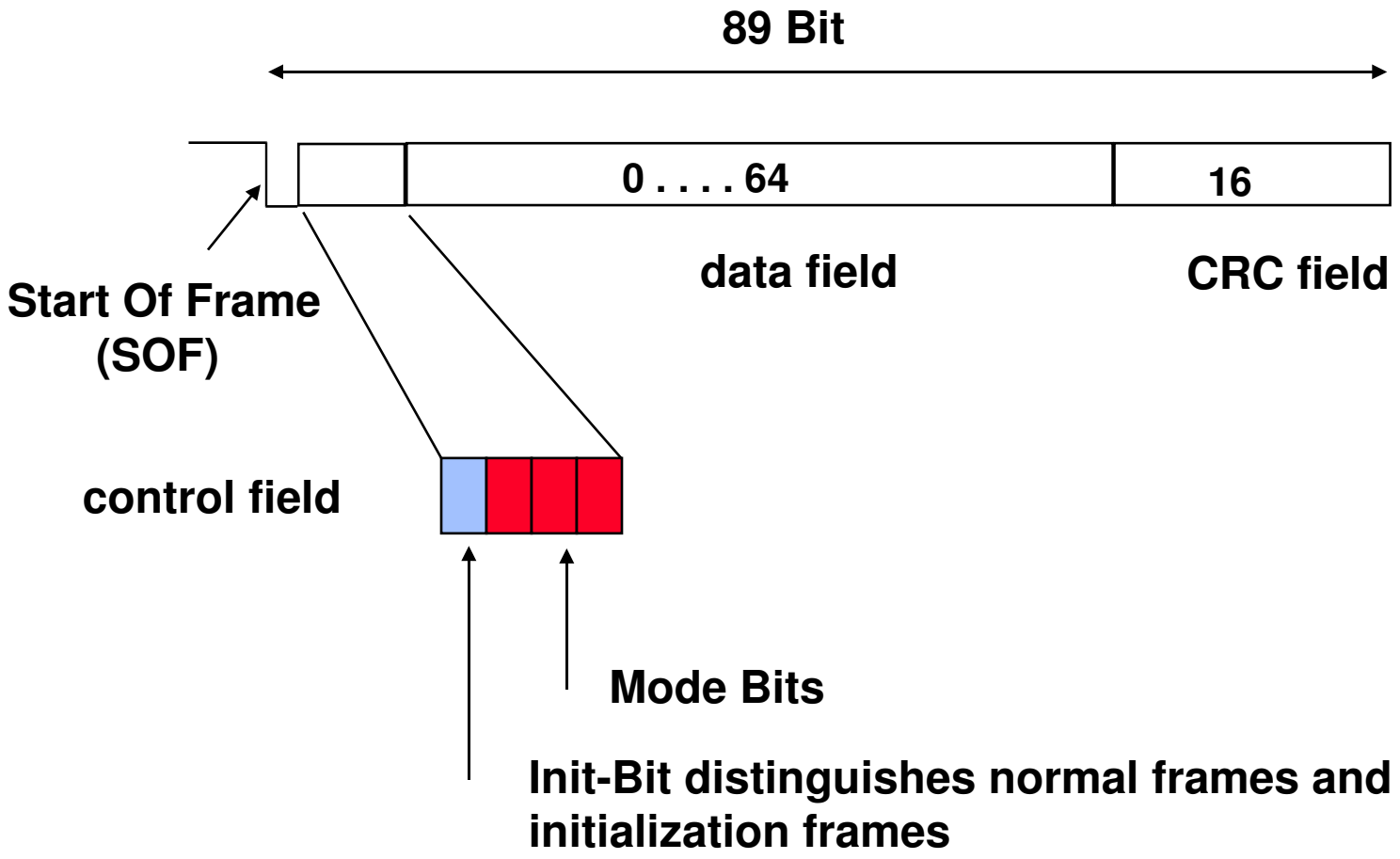


Slightly-off-specification failures



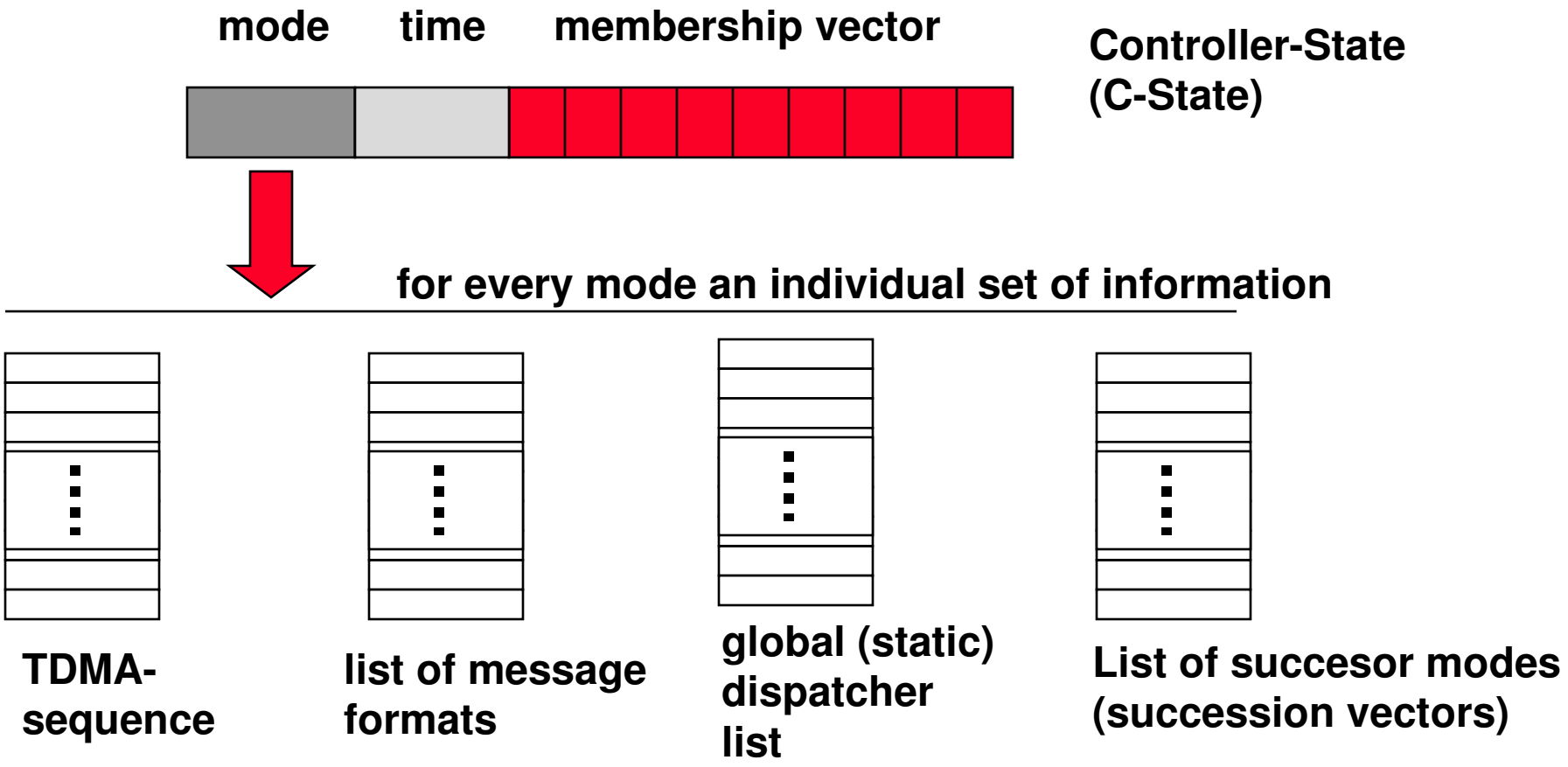
Slightly-off-specification failures can occur at the interface between the analog and the digital world.

Format of a TTP frame



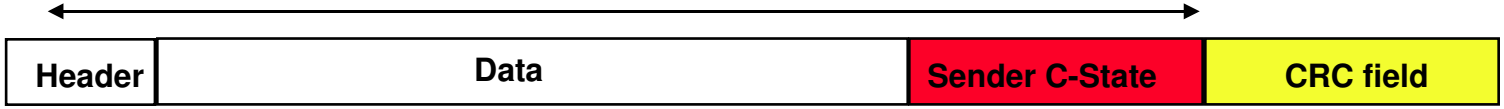
MFM Coding: Constant frame length (not data dependent)

Continuous supervision of the global state



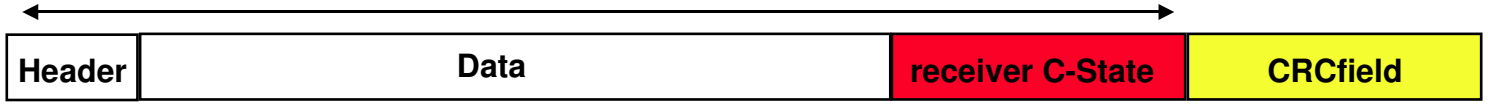
Continuous supervision of the global state

CRC-generation on the sender side



Nachricht

CRC-generation on the receiver side



Handling mode changes

At every point in time, all nodes are in a specific mode.

→ needs consensus

Mode changes:
FTU signals mode changes in the control field by setting the position of the succession vector (index into the respective table).

→ Flexibility: Succession vector can be changed.

Critical functions:

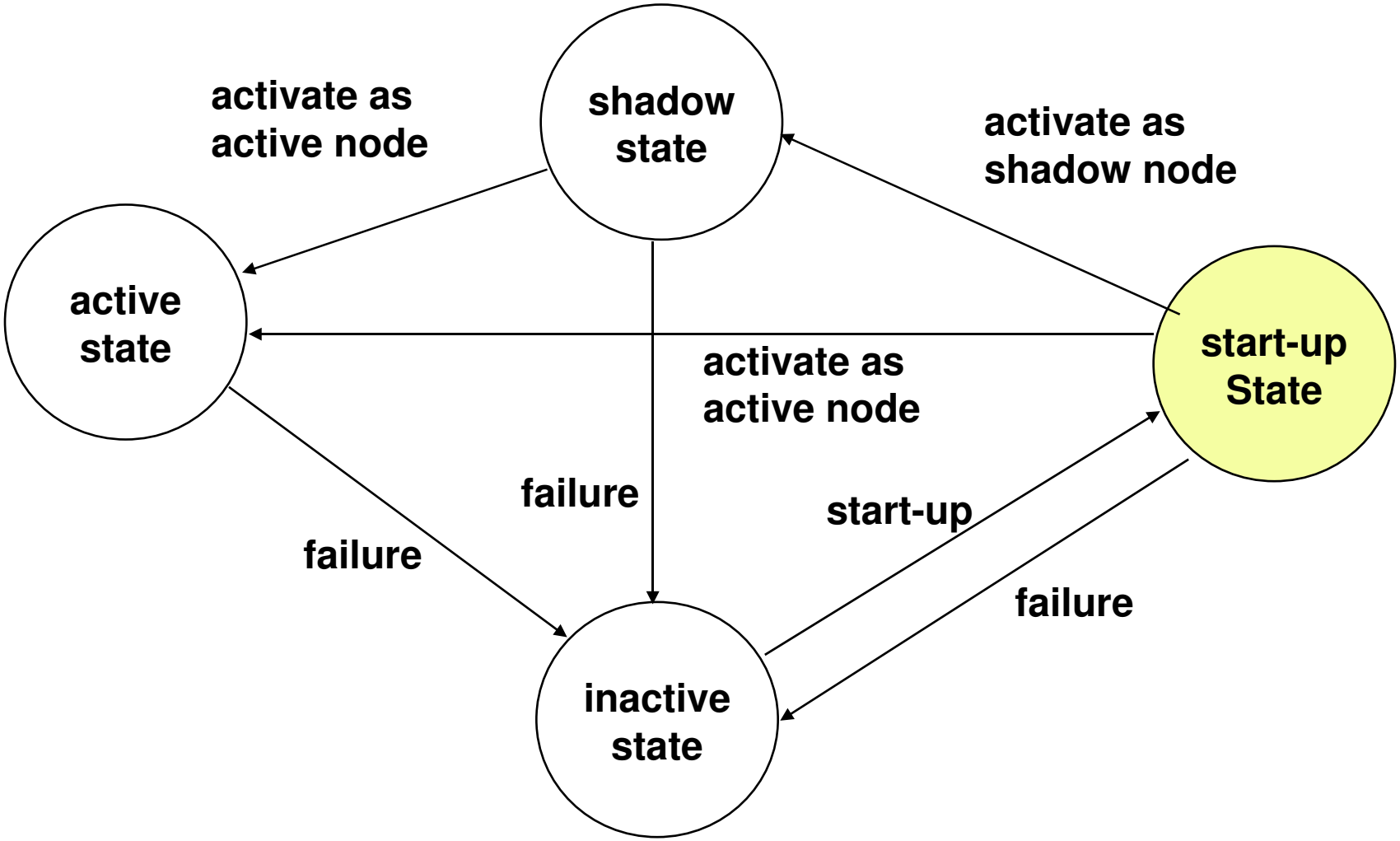
- Initialization
- Membership
- Black-out Handling

Redundancy management and initialization

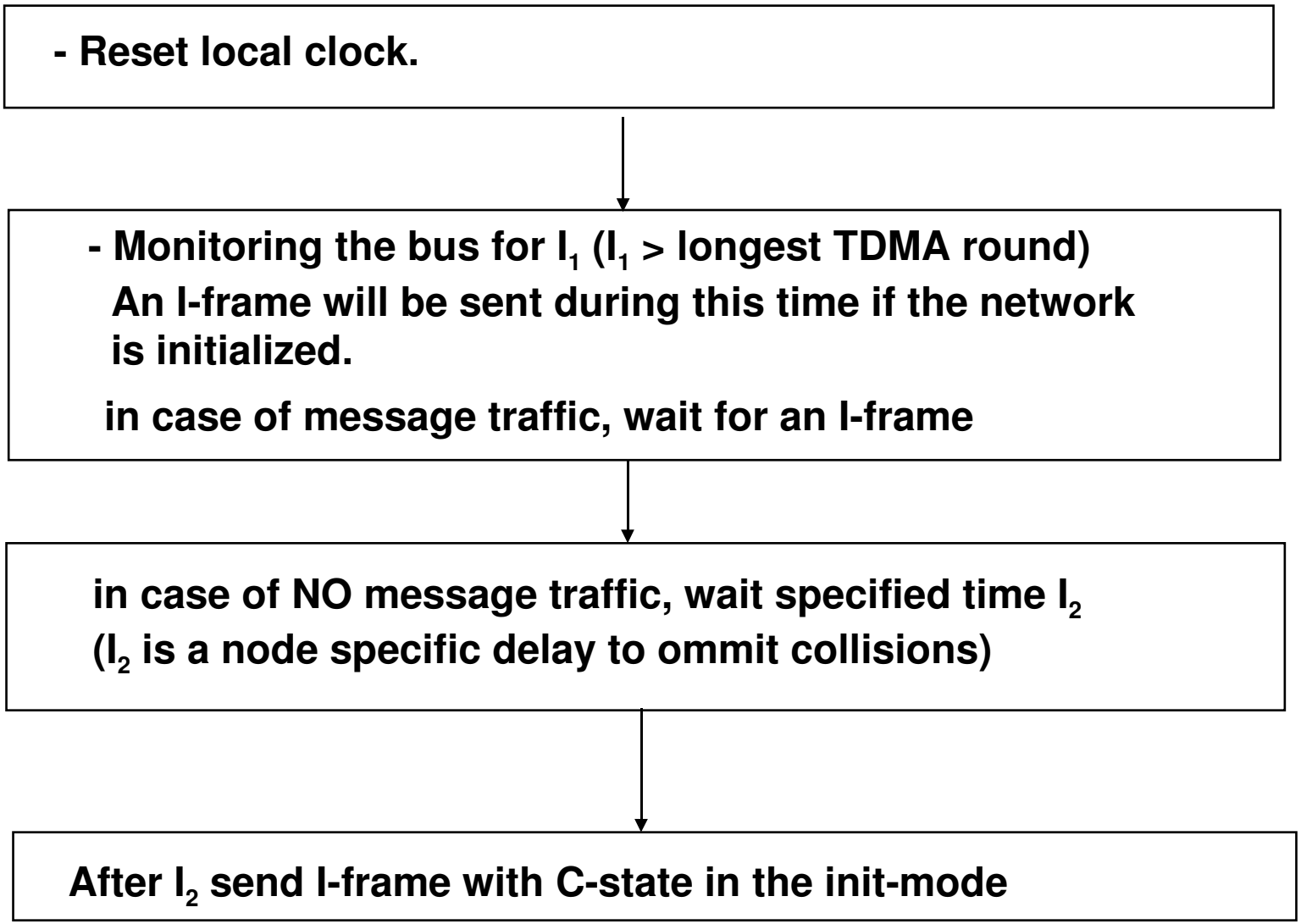
- **Every node has a unique name that defines its position in the TDMA round.**
- **Some special nodes are enabled to send initialization frames (I-frame).**
- **Initialization frames comprise the complete state of the entire system.**
- **The longest interval between two I-frames determines the minimal waiting time for a node before it can be re-integrated.**

Redundancy management and initialization

Local states of an FTU:



Redundancy management and initialization



Membership Service

Sender sets membership bit (MB) to "1"

All receivers set MB to "1"

If no correct frame is received, all receivers set MB = 0 directly after the TDMA-slot

When reaching the membership-point (an a priori known point in time, when the FTU sends a message), the sender checks whether it still is member in the group. The sender uses the state information in the received messages.

Membership Service

A node is member if:

1. the internal check is ok.

2. at least one frame which has been sent during the round has been acknowledged from one of the FTUs, i.e. the physical connection is ok.

3. the number of correct frames which were accepted by the FTU during the last TDMA round is bigger than the number of discarded frames.

If this is not the case, then the local C-state is not in compliance with the majority of other nodes and the node looses its membership. This avoids the formation of cliques, which have different views on the whole group.

Black-out handling

"Black-out" denotes a global distortion, e.g. if the physical communication channel is distorted by external electromagnetic fields.

Black-out detection:

A node continuously monitors the membership field.
If membership dramatically decreases a mode change is triggered to black-out handling.

Black-out mode: nodes only send I-Frames and monitor the bus

When external distortion vanishes, membership will stabilize again.

Return to "normal mode"

Discussion

Synchrony (Jitter, Steadyness, Thightness)

Automatic clock synchronization

Fault masking

Monopolization- (Babbling Idiot-) faults are omitted

Replica Determinism

Composability and extensibility

Summary TTP

- **Protocol execution is initiated by the progression of global time. The sending point in time for every message is a priori know by all receivers.**
- **The maximum execution time corresponds to the average execution time (with a small deviation only)**
- **Error detection is possible for the recievers because they know when a message can be expected.**
- **The protocol is unidirectional. No acknowledgements are required.**
- **Implicit flow control is needed.**
- **No arbitration conflicts can occur.**

Desirable Features

More Flexibility:

- **Accomodating a range of criticality requirements**
- **Accomodating more messages than slots**
- **Dynamic assigment of transmission slots**
- **Event-triggered message dissemination**

What will be the price to pay?

More Flexibility ?

Federating networks with different properties.