Embedded Systems

Time-Triggered Protocol (TTP)

EE4673/5673

by

Dr. Maarten Uijt de Haag

So Far

- ...
- Time in Embedded Systems
- Fault-Tolerance
- Communication between Nodes
- Controller Area Network (CAN)
- CAN Performance
- Now: Time-Triggered Protocol (TTP)
- ...

Reference Material

- Many articles on TTP can be found on:

  http://www.tttech.com/technology/articles.htm

- Maier, Reinhard et al., "Time-Triggered Architecture: A Consistent Computing Platform"

- The articles include comparison articles

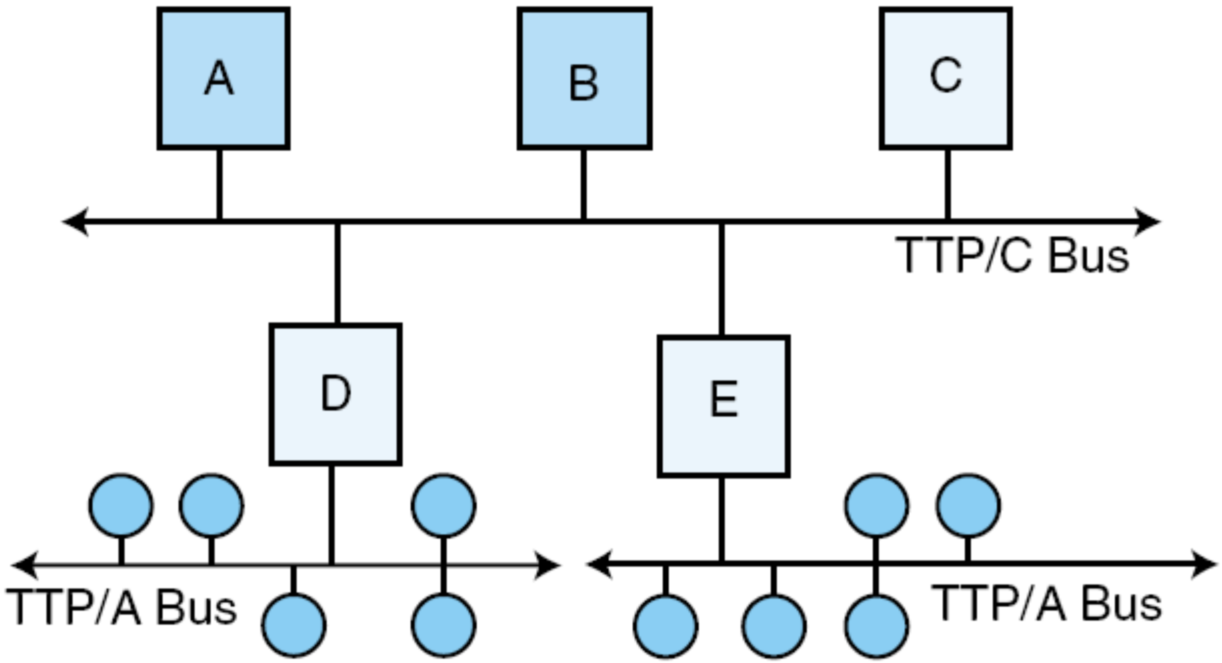
Introduction – History

- **Developed at the Vienna University of Technology in Austria**
- ***Hermann Kopetz***

Two TTP Variations

- TTP/A:
  - Automotive Class A = soft real time
  - A scaled-down version of TTP
  - A <u>cheaper master/slave variant</u>
  - Software on existing hardware
- TTP/C:
  - Automotive Class C = hard real time
  - A full version of TTP
  - A <u>fault-tolerant distributed variant</u>
  - Dedicated hardware + software

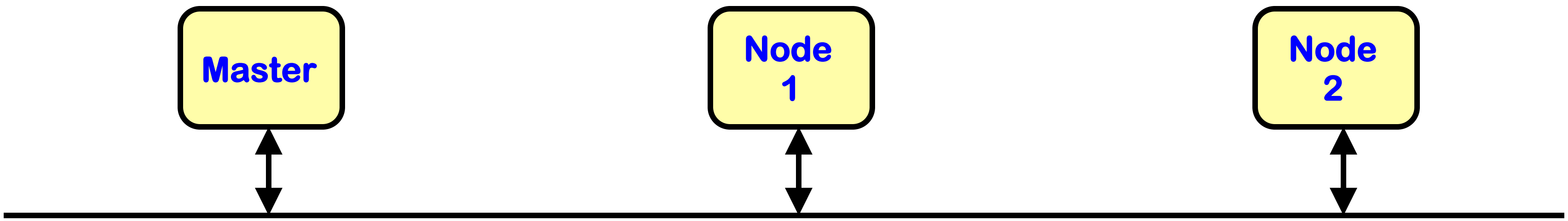
TTP System



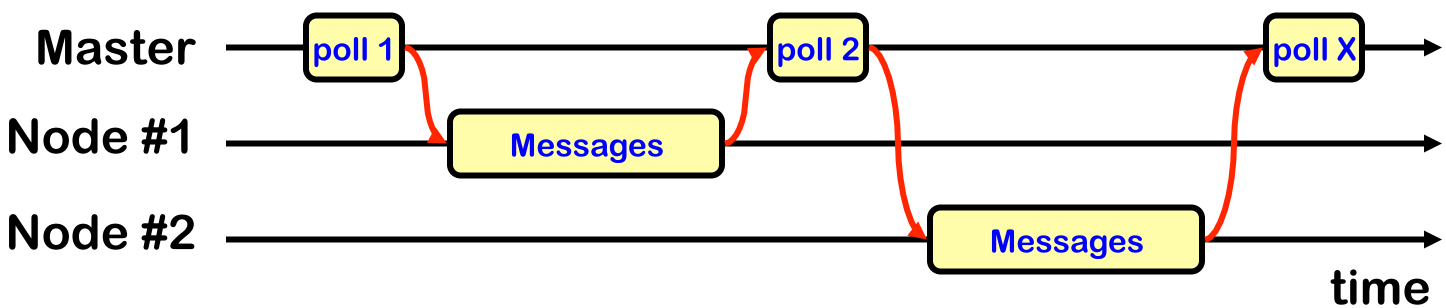
TTP/A intended to provide the non-critical interface of an Embedded Computer Unit (ECU) with a cluster of smart sensors; the fieldbus.

TTP/A

Master/Slave Configuration - Polling



Master polls slaves for messages and waits for response



TTP/A

Master/Slave Configuration - Polling

- Advantage
  - Simple protocol to implement
  - Historically very popular
  - Bounded latency for real-time applications
- Disadvantage
  - Single point of failure from centralized master
  - Polling consumes bandwidth
  - Network size is fixed during installation
    (or master must discover nodes during reconfiguration)

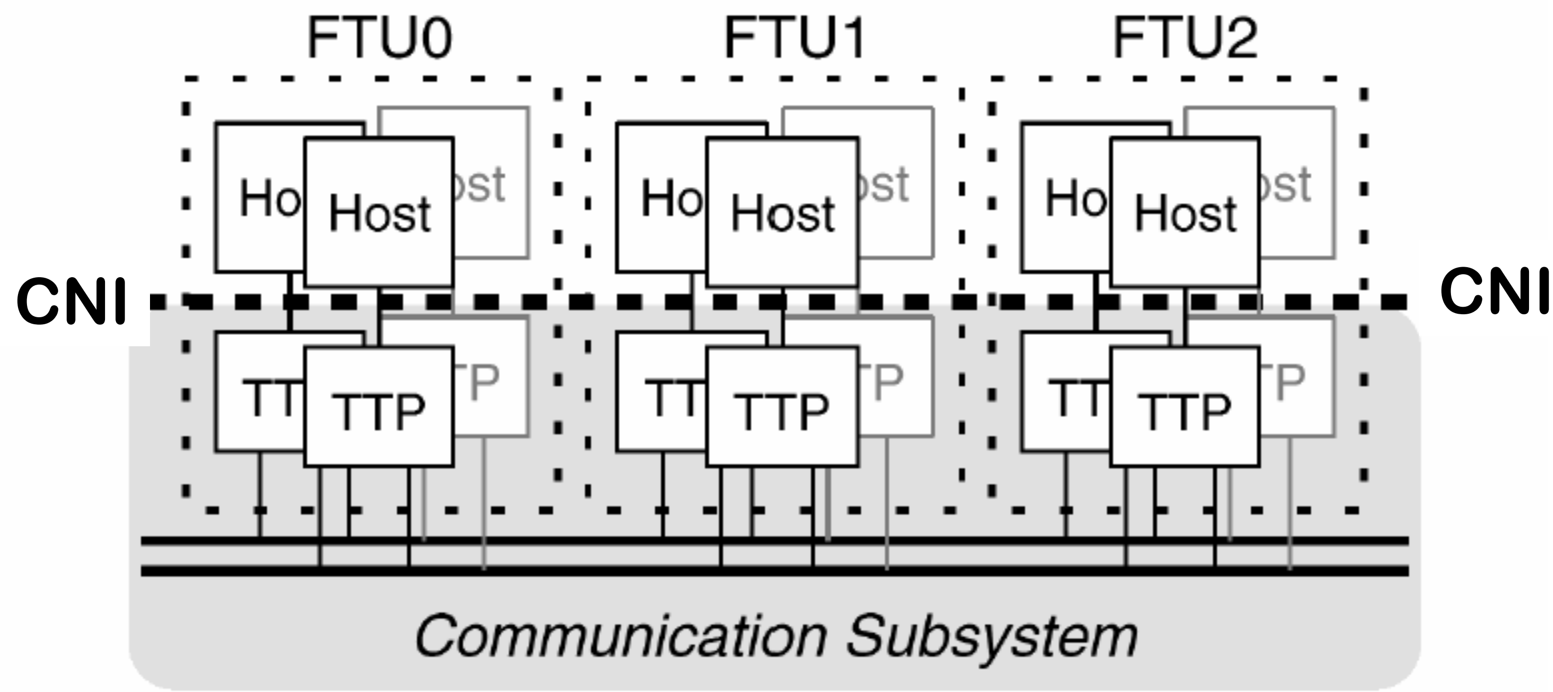
TTP/C

- A time-triggered communication protocol for safety-critical (fault-tolerant) distributed real-time control systems
  – Fault-tolerant Units = redundant nodes
    - Fail-silent nodes
    - Triple-Modular Redundancy (TMR)
  – Replicated communication channels (busses)
- Based on a Time Division Multiple Access (TDMA) media access strategy
- Based on clock synchronization

Comparison of TTP/A and TTP/C

Service	TTP/A	TTP/C
Clock synchronization	Central multi-master	Distributed fault-tolerant
Mode switches	Yes	Yes
Communication error detection	Parity	16/24 bit CRC
Membership service	Simple	Full
External Clock Synchronization	Yes	Yes
Time-redundant Transmission	Yes	Yes
Duplex nodes	No	Yes
Duplex channels	No	Yes
Redundancy management	No	Yes
Shadow node	No	Yes

Computational Cluster (TTP/C)



TTP: TTP Controller

CNI: Communications Network Interface

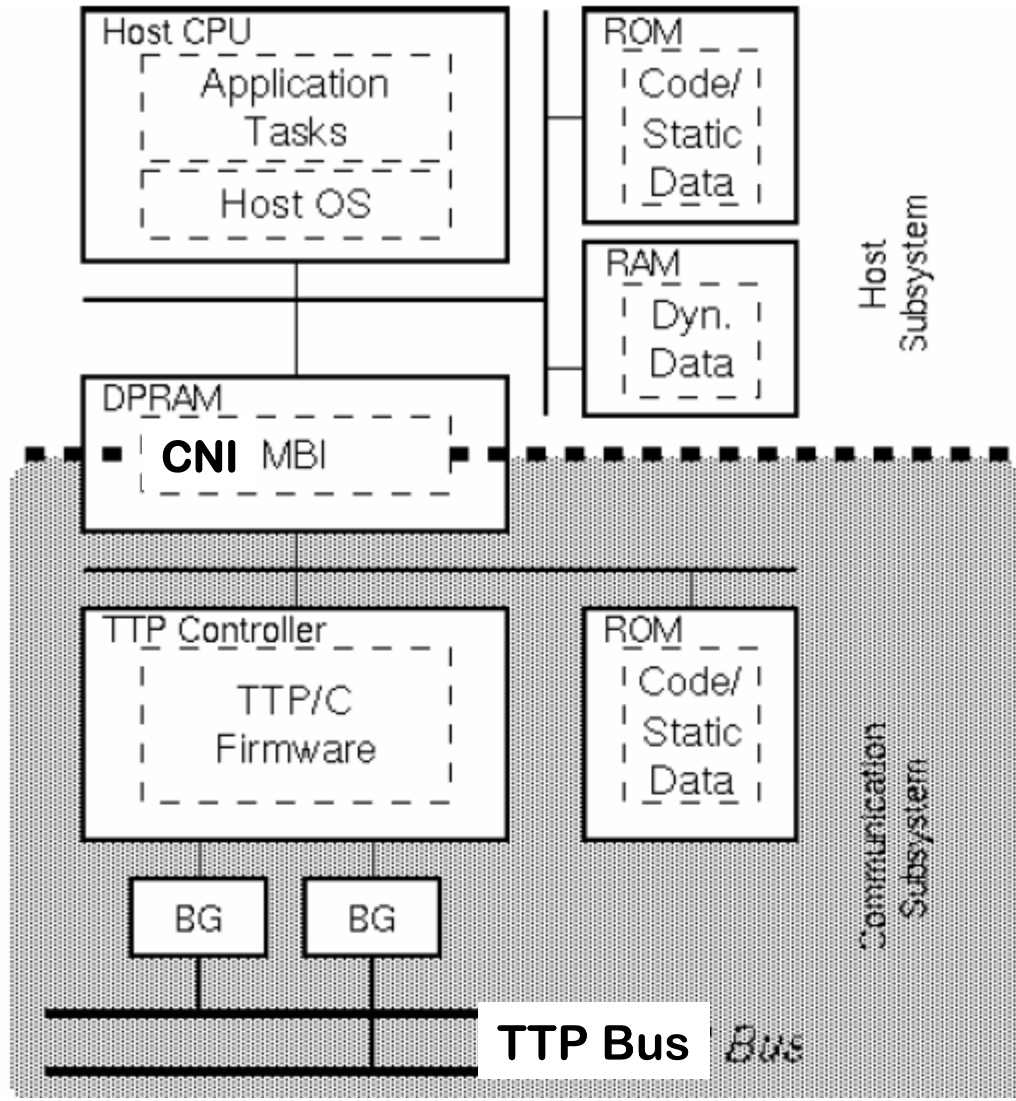
FTU: Fault Tolerant Unit

Consists of multiple hosts or nodes
This node is referred to as the
Smallest Replaceable Unit (SRU)

Hardware Structure of TTP Node

Timer which allows nodes to communicate within their predefined time frame.

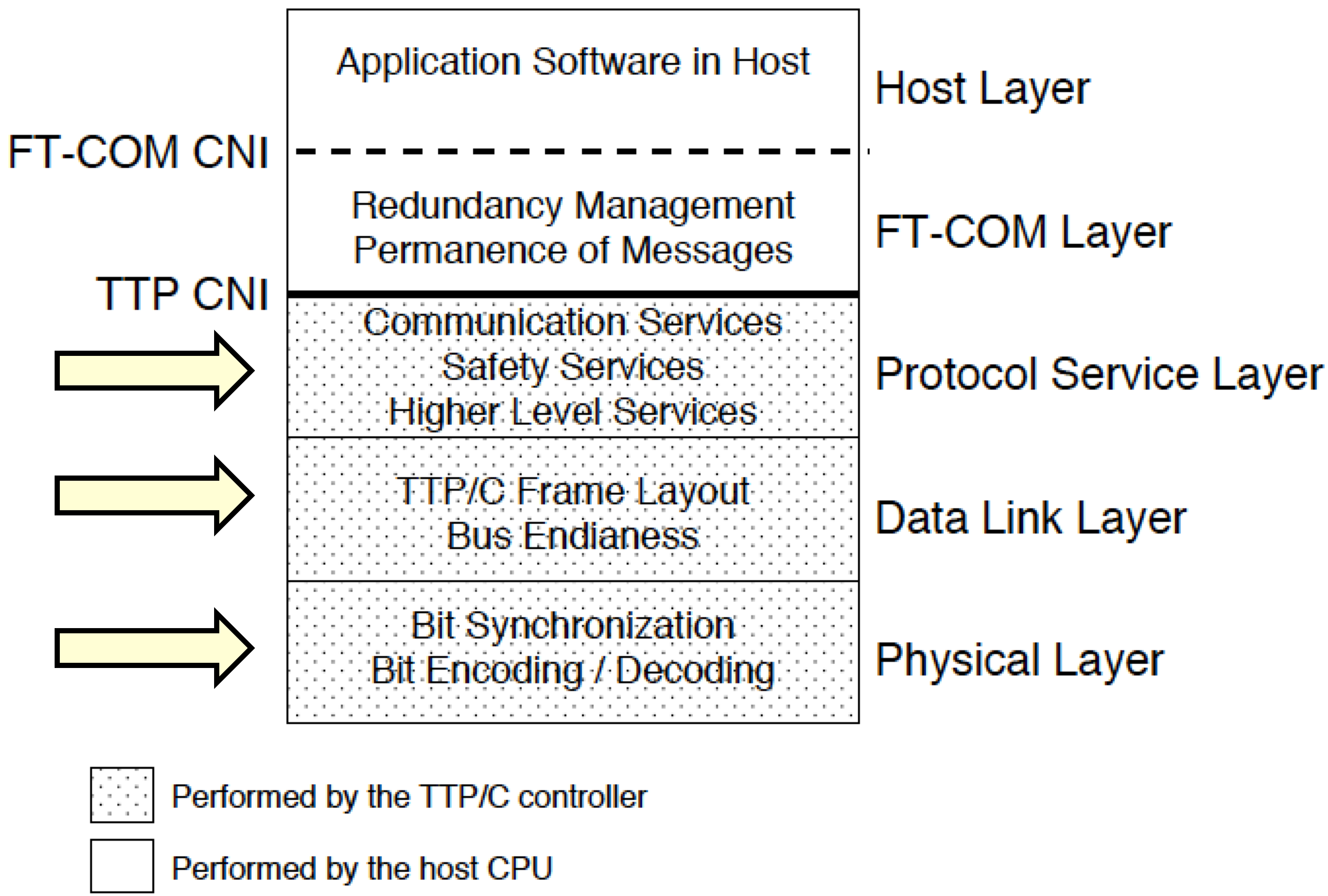
BG: Bus Guardian
DPRAM: Dual Ported RAM



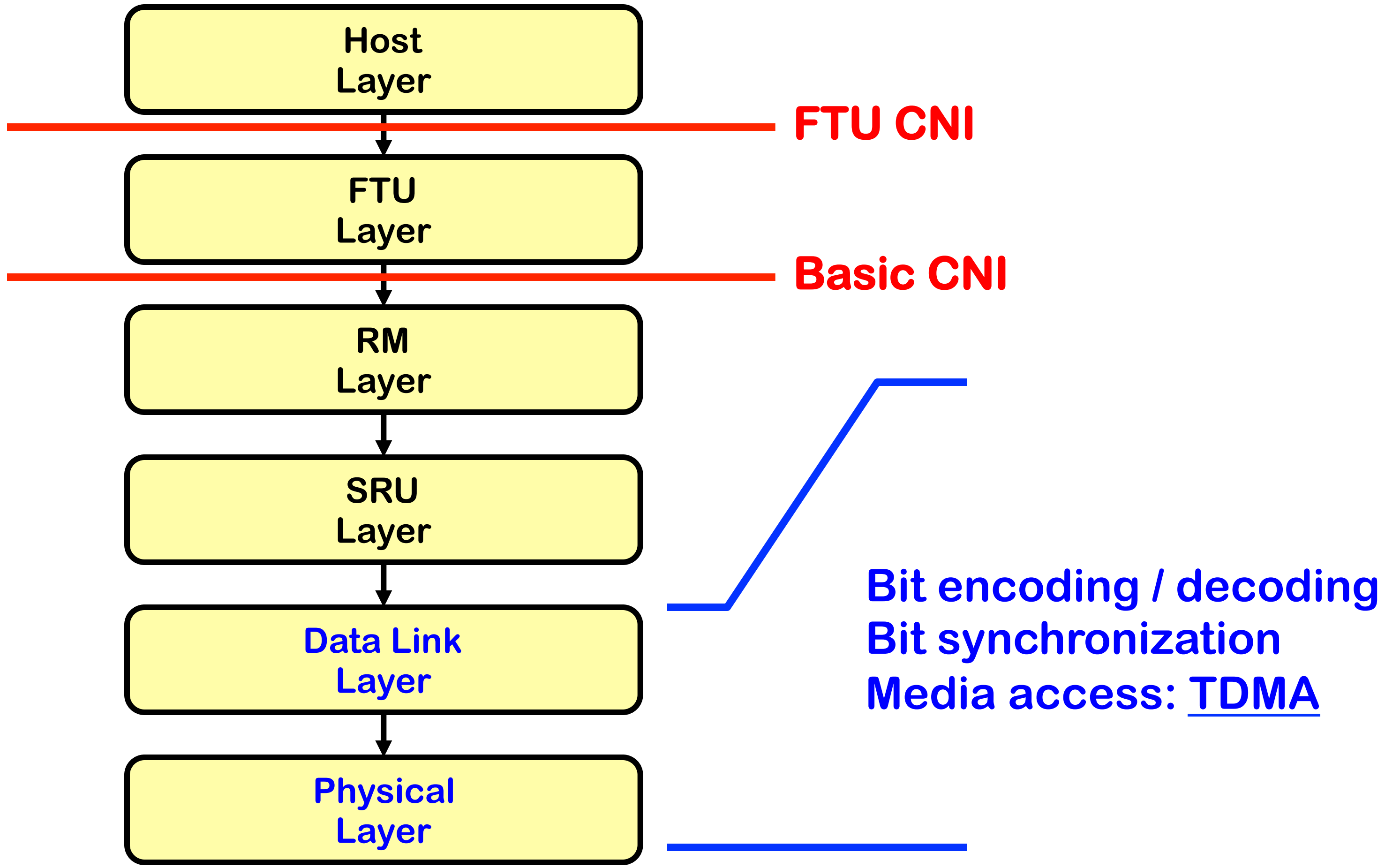
Node Configuration

- Communication Network Interface (CNI):
  - Interface between communication controller and the host computer within a node of a distributed system
- DPRAM (Dual Ported RAM):
  - Memory-mapped network interface
  - Used for data-passing between host and TTP controller
- Bus Guardian:
  - Monitors the bus
  - Protects the bus from being monopolized by a faulty node sending at arbitrary points in time ("babbling idiot" failure).
  - Hardware watchdog to ensure "fail silent"

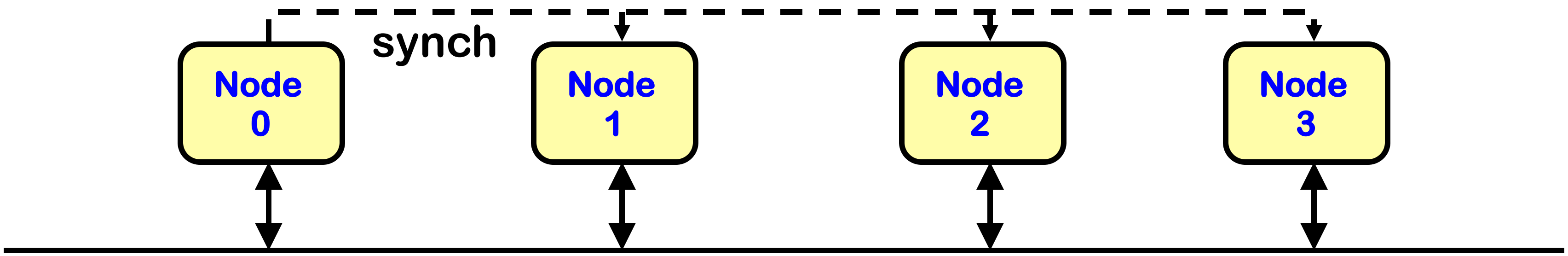
TTP Layers


Application Software in Host
Host Layer
FT-COM CNI
Redundancy Management
Permanence of Messages
FT-COM Layer
TTP CNI
Communication Services
Safety Services
Higher Level Services
Protocol Service Layer
TTP/C Frame Layout
Bus Endianess
Data Link Layer
Bit Synchronization
Bit Encoding / Decoding
Physical Layer
Performed by the TTP/C controller
Performed by the host CPU

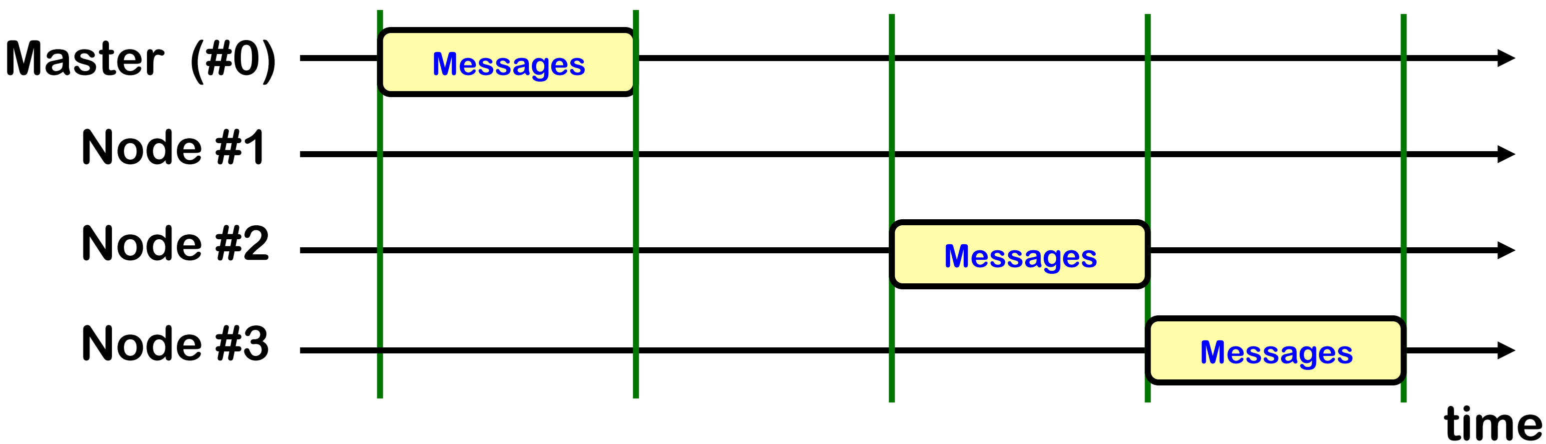
TTP Layers

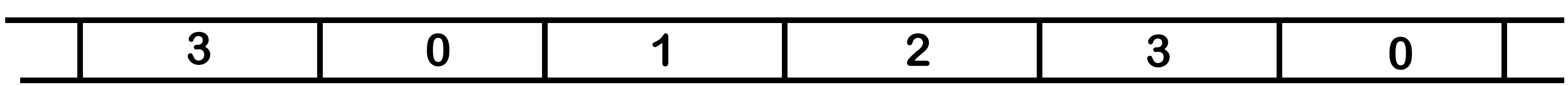

Host Layer
FTU CNI
FTU Layer
Basic CNI
RM Layer
SRU Layer
Data Link Layer
Physical Layer
Bit encoding / decoding
Bit synchronization
Media access: TDMA

TDMA



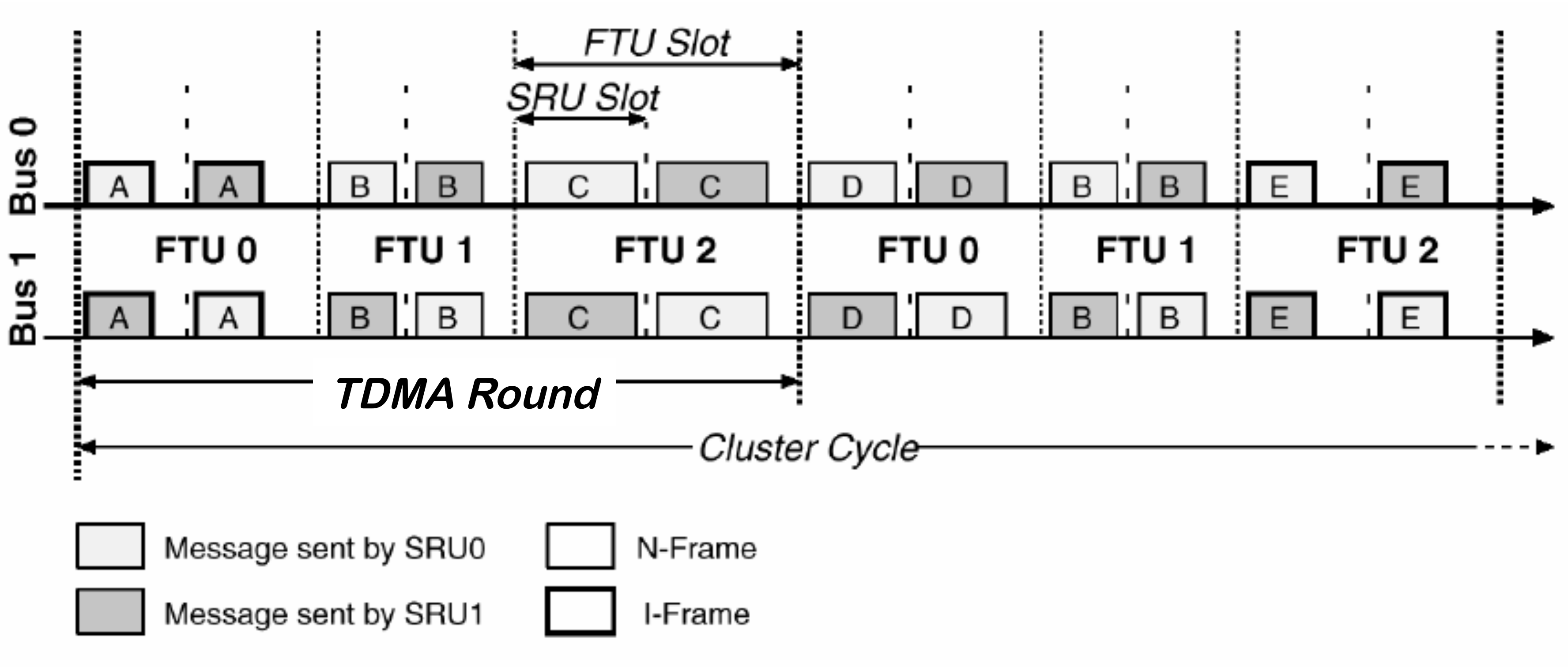
Each node transmits during a specific time slot





timeslot assignment

TTP/C Media Access - TDMA



<u>This figure assumes that</u>:

- One Fault-Tolerant Unit (FTU) consists of two nodes: SRU0 and SRU1
- There are two (redundant) busses

Cycles

- **TDMA Round:**
  - sequence of the periodic TDMA slots
  - each node in the communication system is assigned to one slot (so-called sending slot)
- **Cluster Cycle:**
  - recurring sequence of TDMA rounds with possibly different message length and contents
  - involves scheduling all possible message and tasks

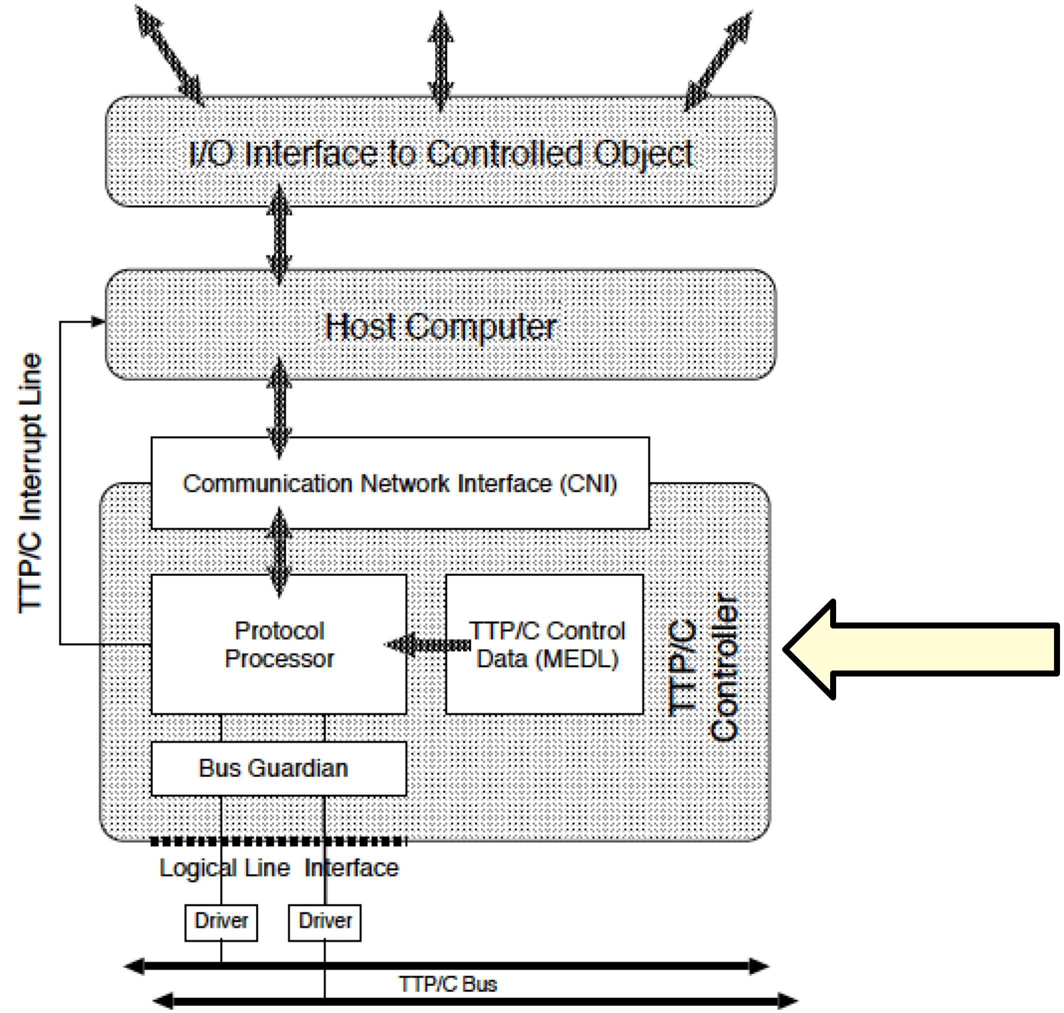
TTP/C
TDMA

- Static schedule for all messages in system
  - Order known *a priori* (at design time) !
  - A completely deterministic TDMA approach
- All tasks synchronized to network TDMA schedule
- The periodic fetch and delivery instances are contained in the message-descriptor list (MEDL)

TTP/C
TDMA

- Message Descriptor List (MEDL)
  - Every node has its own personal MEDL
  - MEDLs of all nodes must be consistent
  - MEDLs are, in general, generated by a software tool for the whole cluster of nodes
- Globally shared schedule of messages and ordering
  - All nodes know the entire message schedule
  - Only one node is permitted to transmit at a time, and only its predetermined message

TTP/C - MEDL



I/O Interface to Controlled Object
Host Computer
TTP/C Interrupt Line
Communication Network Interface (CNI)
Protocol Processor
TTP/C Control Data (MEDL)
TTP/C Controller
Bus Guardian
Logical Line Interface
Driver
Driver
TTP/C Bus

Message Descriptor List (MEDL)

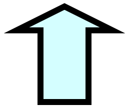
SRU-Time	Address	Attributes			
		D	L	I	A

Contains the point in global time (with SRU granularity) when the message specified in the address field must be communicated

Contains the address of the memory cell (in the CNI) where the data items must be stored or retrieved from

Message Descriptor List (MEDL)

SRU-Time	Address	Attributes			
		D	L	I	A

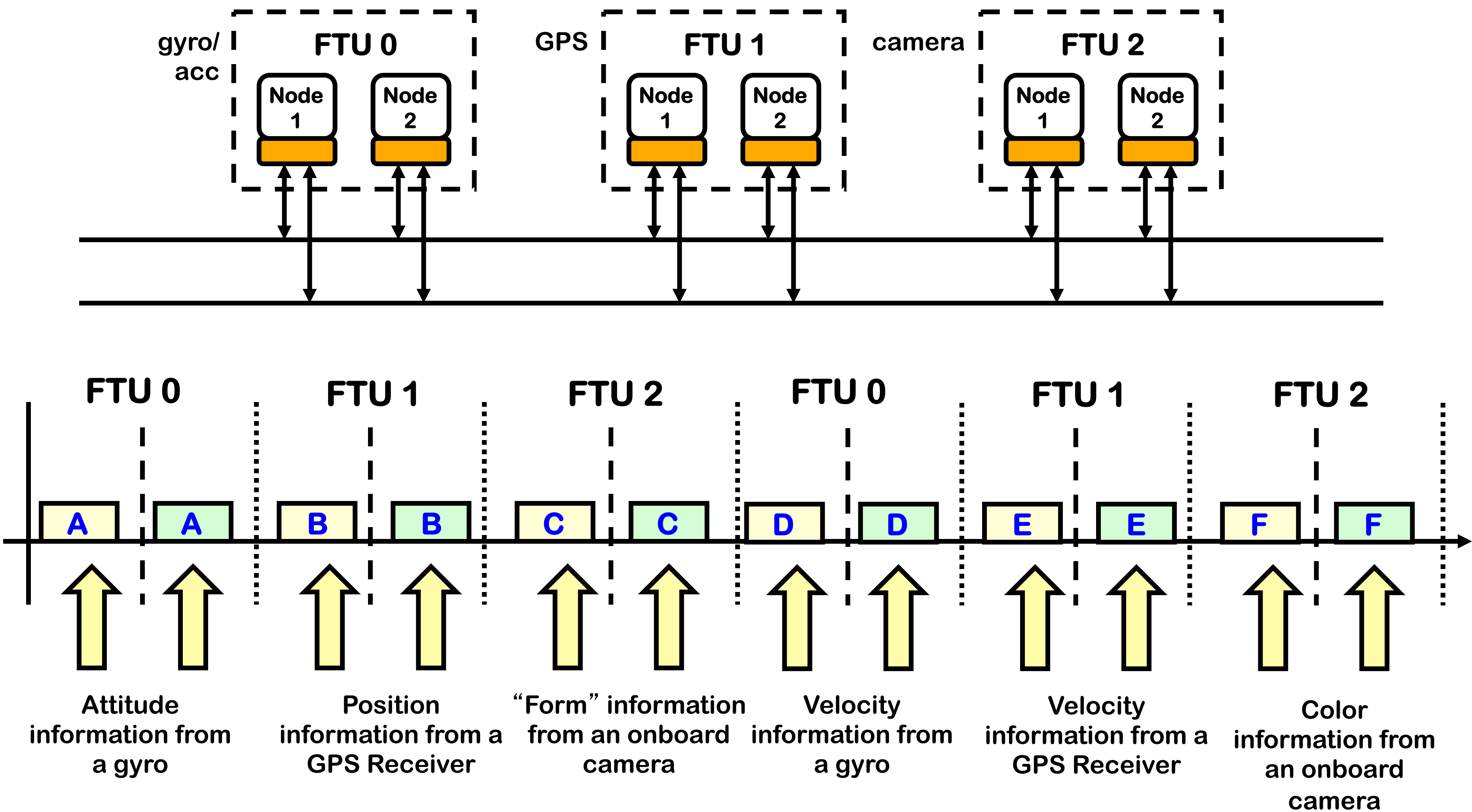


D: direction subfield - input message or output message
L: length subfield - length of the message to be communicated
I: initialization subfield – initialization message or normal message
A: additional protective information

Name Mapping

- Unlike CAN the TTP messages do <u>NOT</u> include an identifier
- Name mapping via:
  - Point in time corresponds to a particular piece of information (name)
    - A particular time corresponds to a particular piece of data
  - CNI memory location and the application software in the host
    - A particular address corresponds to a particular piece on information

Example



gyro/ acc
FTU 0
Node 1
Node 2
GPS
FTU 1
Node 1
Node 2
camera
FTU 2
Node 1
Node 2
FTU 0
FTU 1
FTU 2
FTU 0
FTU 1
FTU 2
A
A
B
B
C
C
D
D
E
E
F
F
Attitude information from a gyro
Position information from a GPS Receiver
"Form" information from an onboard camera
Velocity information from a gyro
Velocity information from a GPS Receiver
Color information from an onboard camera

Example

- **MEDL in the FTU 1 Nodes**

Camera needs gyro information to stabilize

SRU-Time	Address	Attributes			
		D	L	I	A
0	0x0000	I	2	N	
200	0x0002	I	2	N	
400	0x0004	O	4	N	
600	0x0008	O	4	N	
Etc.	…	…	…	…	

In network macroticks

Physical Layer

- TTP is flexible with respect to the transmission medium:
  - ISO11898 – CAN Transceiver
    - up to 2 Mbps
  - RS-485
    - up to 10Mbps
  - Electrical 100BaseTx PHY driver & Optical 100BaseFx PHY driver
    - up to 25Mbps

TTP/C Frames

- Two kinds of frames:
  - I-Frames used for initialization
    - Also sent occasionally to permit recovered nodes to resync to cluster
    - C-state is current state of system (time & position in cluster schedule)
  - N-Frames used for normal messages

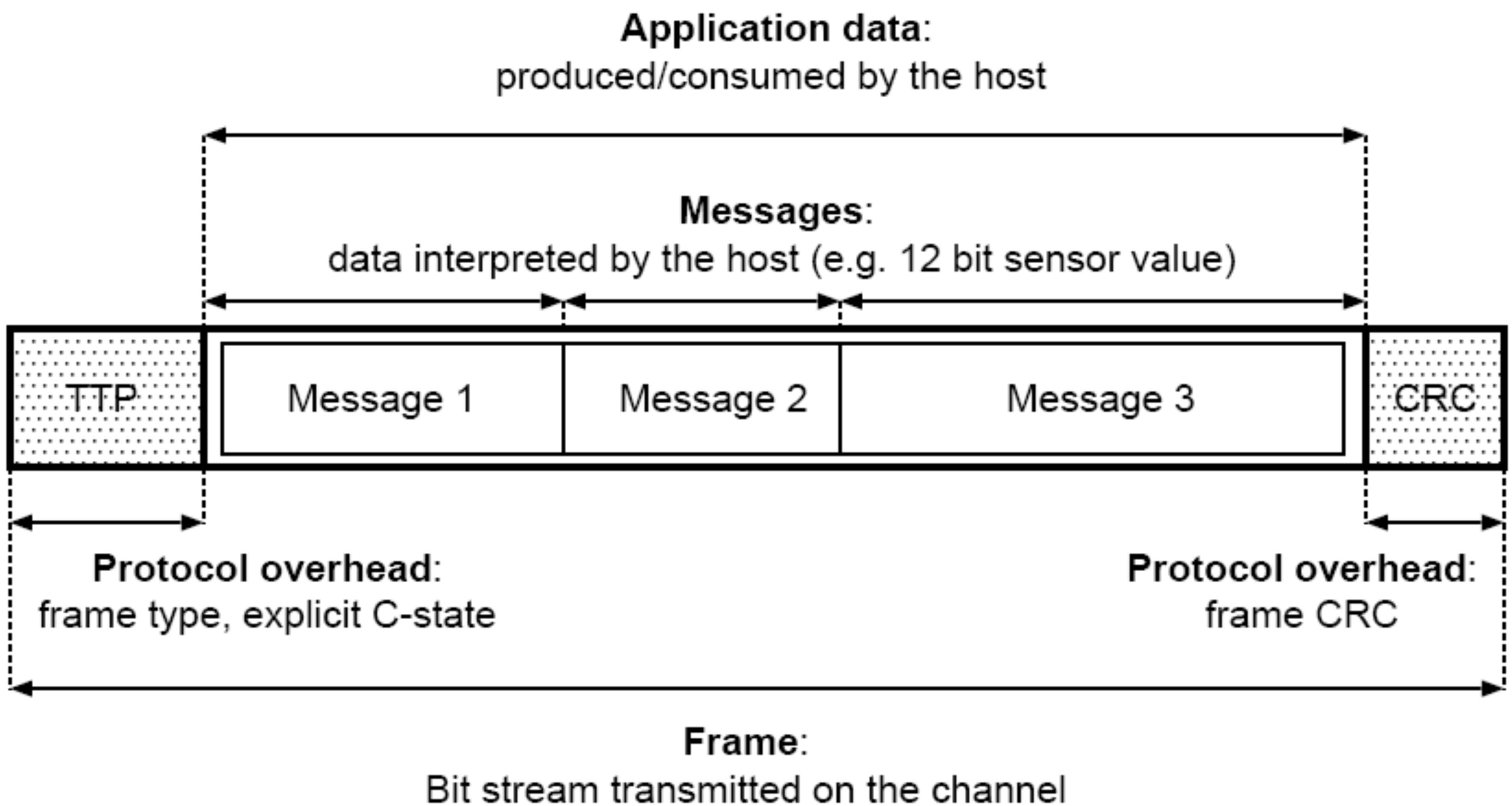
Header	Data Field (2 - 240 bytes)	CRC (24 bits)

I/N Frame	Mode Bit 2	Mode Bit 1	Mode Bit 0	Ack N0 Pre	Ack N1 Pre	Ack N0 PrePre	Ack N1 PrePre

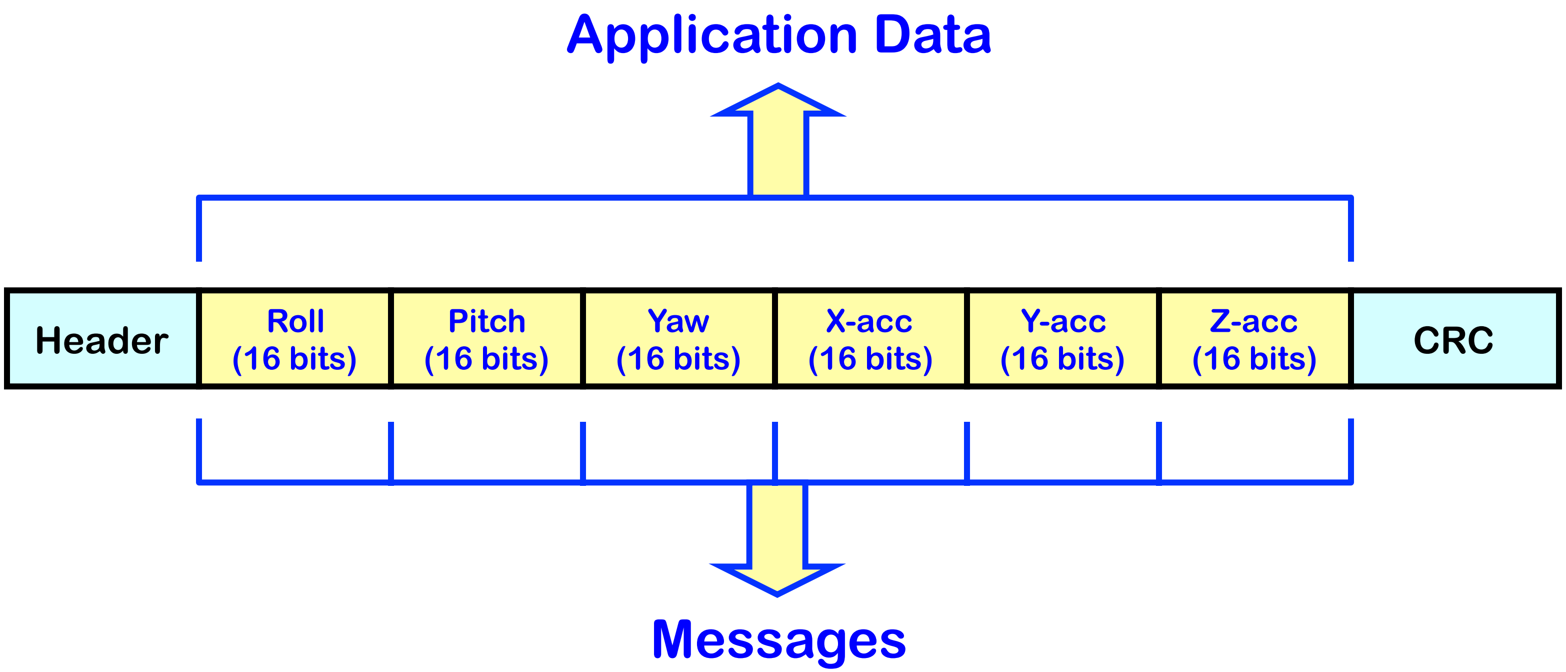
I-Frame

Header	C-State* (6 bytes)	CRC (24 bits)

Frame – Application Data - Message

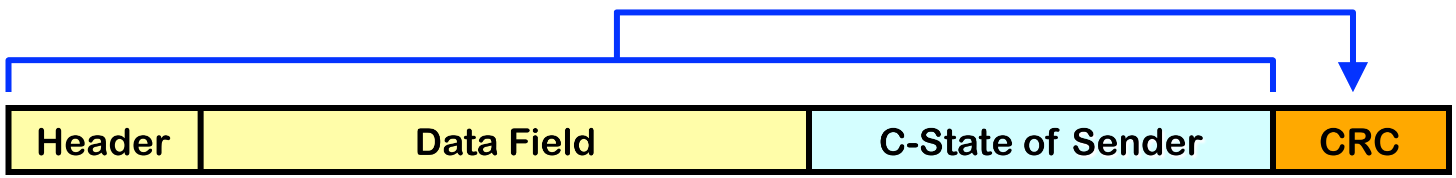


Frame – Application Data – Message
Example



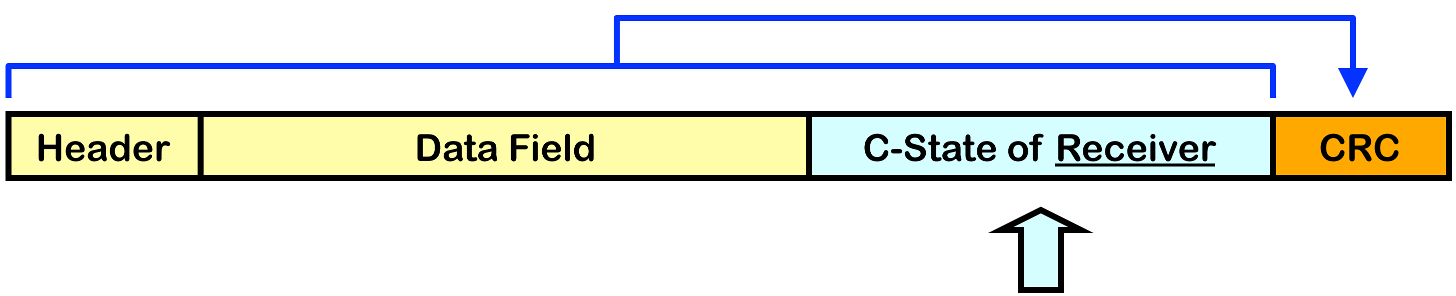
Cyclic Redundancy Check (CRC)

CRC Calculation at Sender:

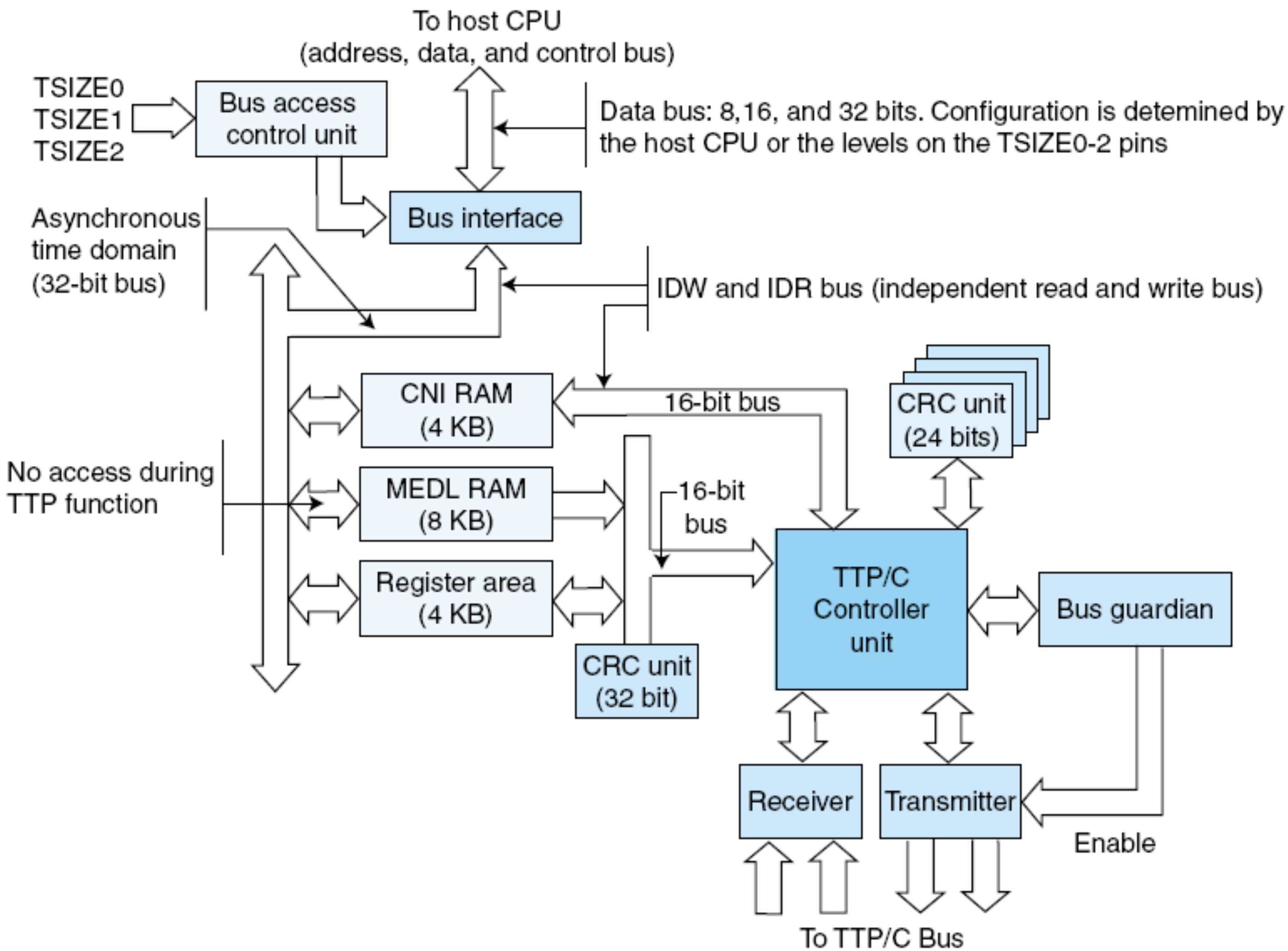


Message on Network

CRC Calculation at Receiver:



Cyclic Redundancy Check



C-State

Header	C-State* (6 bytes)	CRC (24 bits)

- The TTP/C standard states:
  - The *controller state (C-state)* is a collection of state variables which describes the internal state of a TTP/C controller. Although the C-state is calculated locally by each controller, it represents a global view of the cluster and must agree with the calculated C-states of the other nodes in a correctly synchronized TTP/C cluster.
- Consists of:
  - Global time
  - Round slot position
  - Cluster mode
  - Membership information
  - Etc.

C-State

- **Global time**
  - “*The global time of the transmission of the current node slot in node granularity (macroticks), updated at the start of the node slot.*”
- **Round slot position**
  - *“The current slot in the cluster cycle (currently processed entry in the static schedule), updated at the start of the node slot”*
- **Cluster mode**
  - *“The current active cluster mode the controller is operating in, updated at the start of the node slot”*
- **Membership information**
  - *“Consistent view of the activity of all nodes in the cluster. A node is in the membership after having correctly sent in its last slot. A node is outside the membership, if having not sent or sent incorrectly. The membership is updated after the acknowledgment algorithm is performed.”*

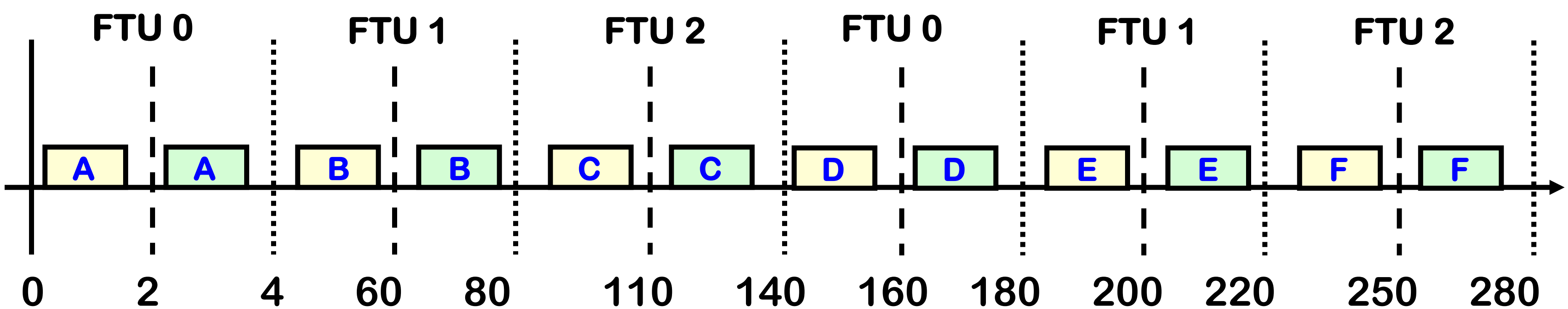
C-State

Header	C-State* (6 bytes)	CRC (24 bits)

- A C-state disagreement between a node and the majority of the other nodes will mark this node as faulty. Thus the exchange of the C-state between the nodes is one of the basic concepts of TTP/C to support fault detection.

TTP/C

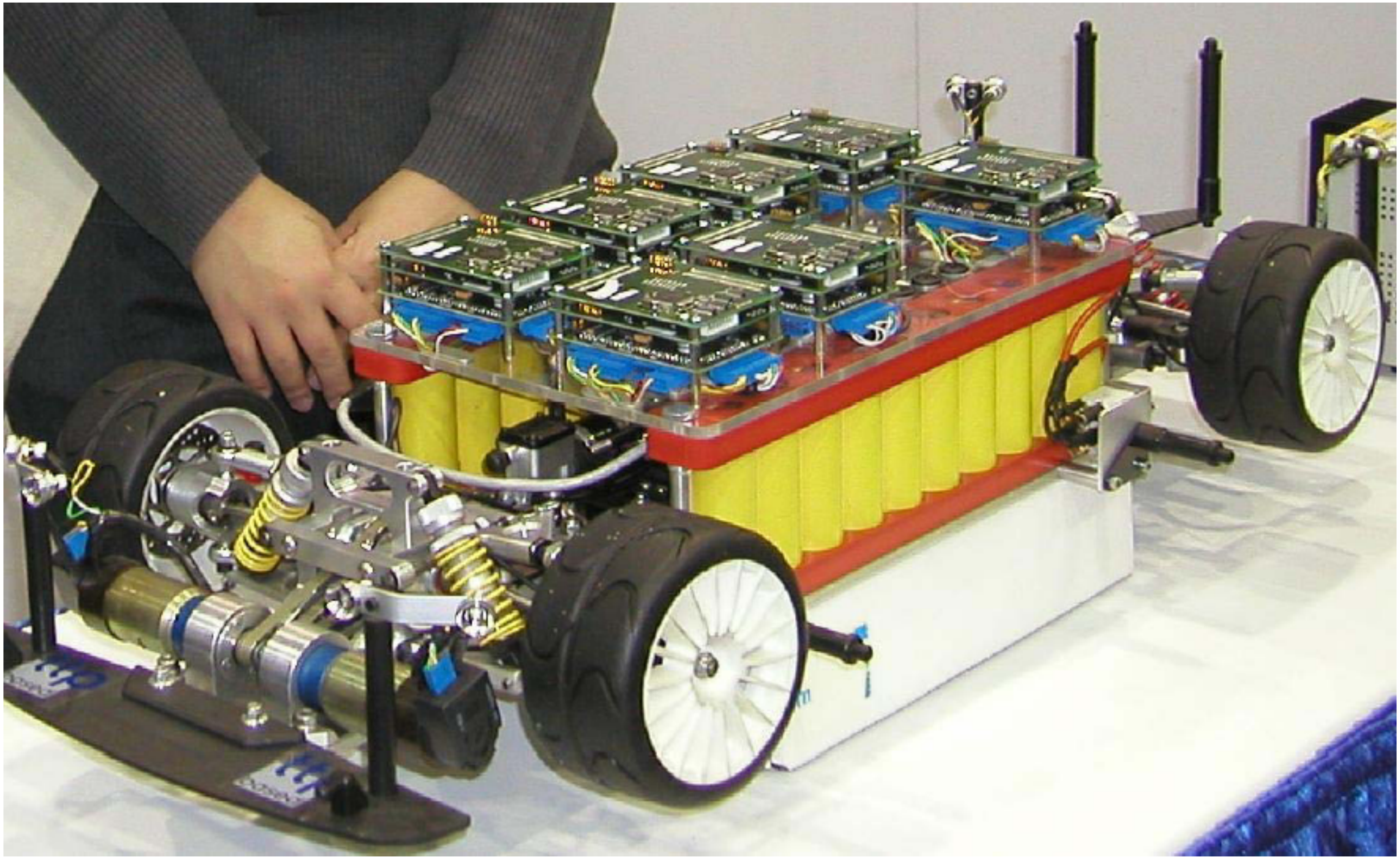
- TTP/C is time-triggered =>
- TDMA causes TTP/C to be deterministic in nature



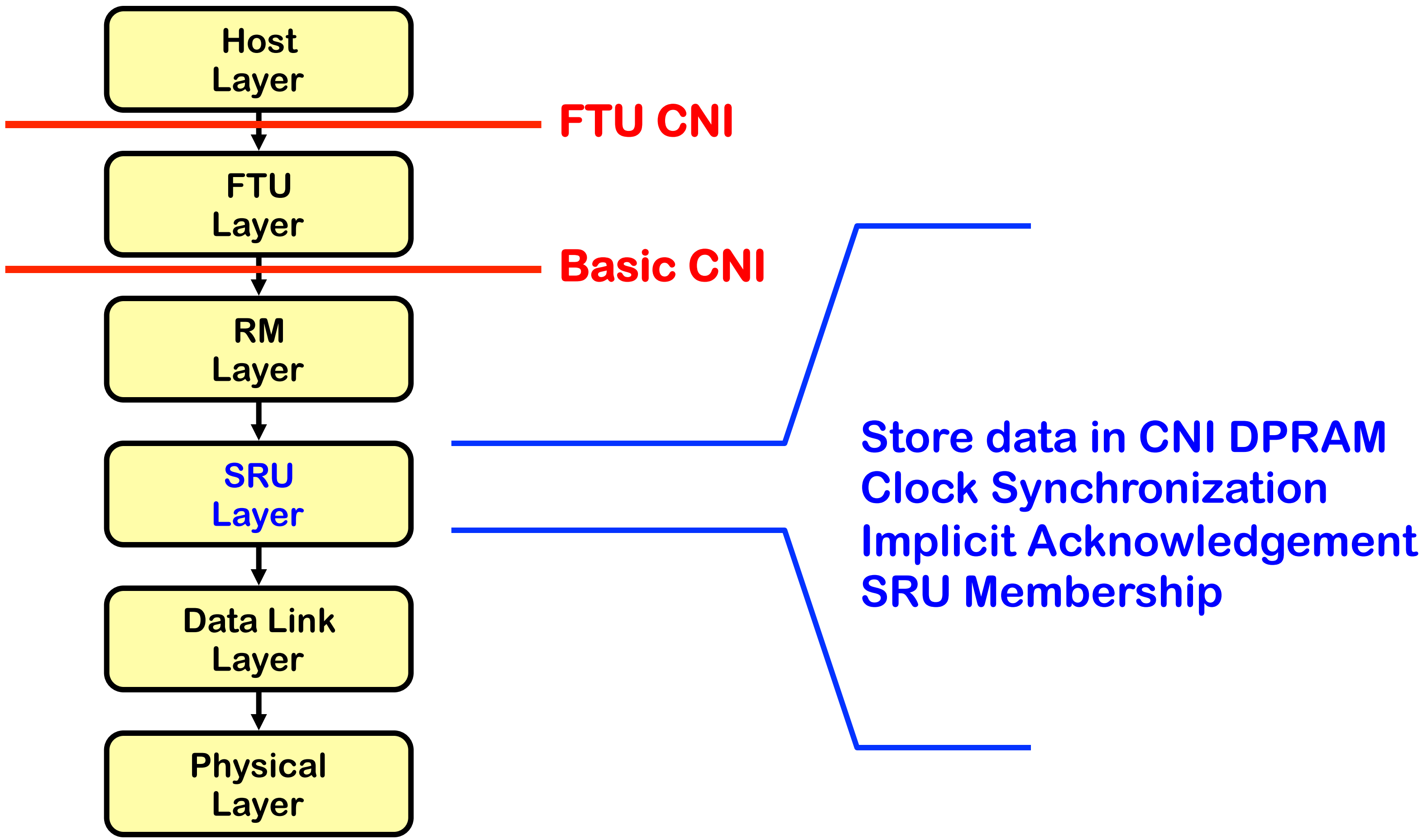
@ 1Mbps => 1 bit = 1μsecond

@ 4 bytes data => 1 message takes 1+4+3 = 8 bytes = 64 bits = 64 μ seconds

TTP/C Demonstrator Vehicle (2000)



TTP Layers


Host
Layer
FTU CNI
FTU
Layer
Basic CNI
RM
Layer
SRU
Layer
Data Link
Layer
Physical
Layer
Store data in CNI DPRAM
Clock Synchronization
Implicit Acknowledgement
SRU Membership

Clock Synchronization

Fault-Tolerant-Average (FTA) Algorithm

At every node:

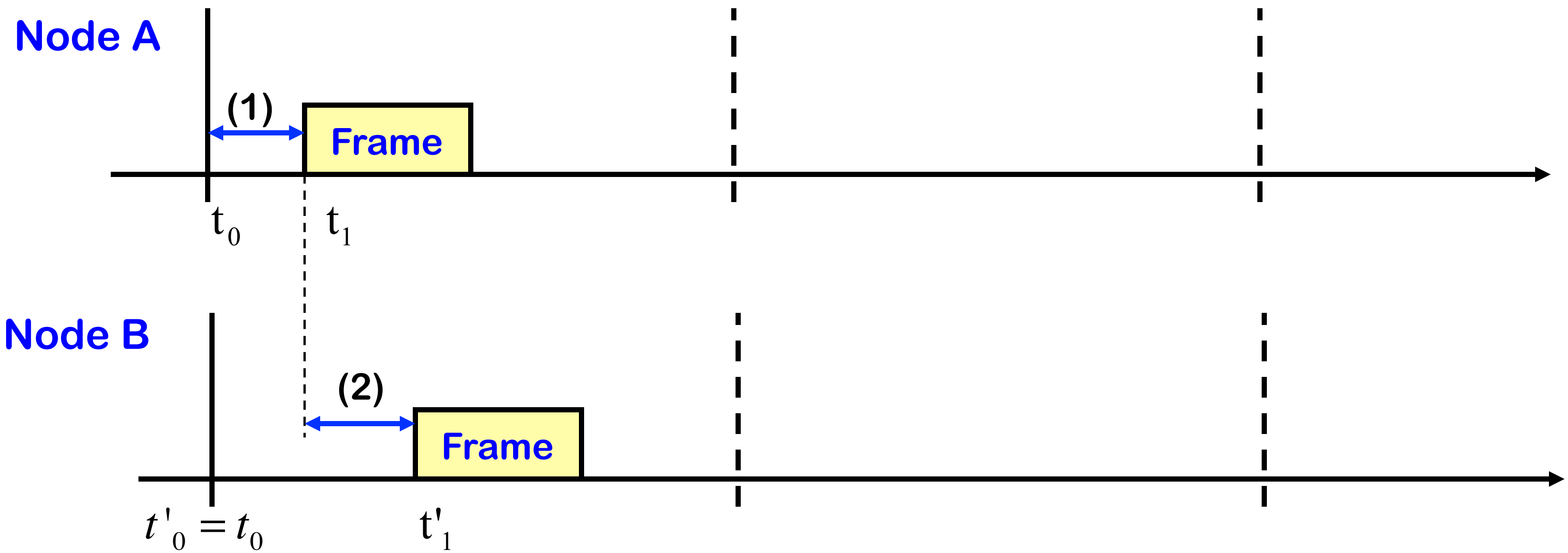
Step 1: Measure the N time differences between the node's clock and the clocks of all other nodes

Step 2: Sort the time differences by size

Step 3: Remove the 'k' largest and 'k' smallest time differences

Step 4: Remaining N-2k time differences will be within the precision window: take the average to obtain the node's clock correction

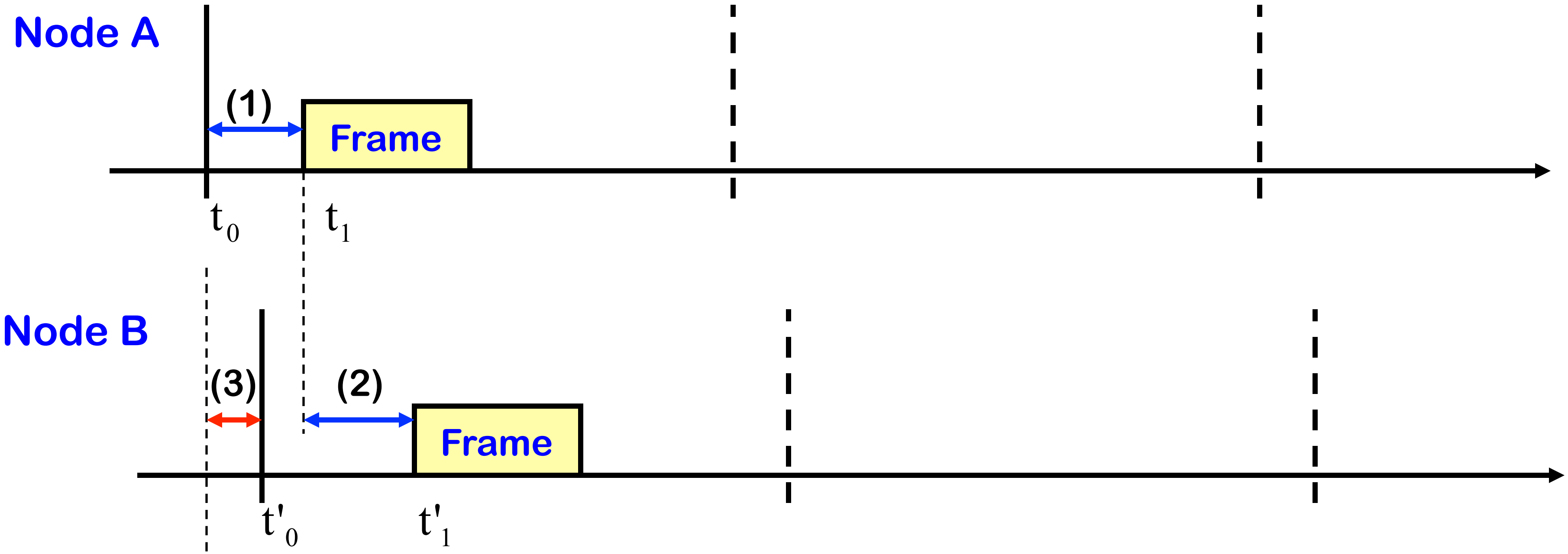
Clock Synchronization



(1) - Intentional delay so the error is observable Δt_{delay} (in MEDL)
(2) - Propagation delay Δt_{prop}

If there were <u>no offset</u> then: $t'_1 - t'_0 = t'_1 - t_0 = t_1 - t_0 + \Delta t_{prop} = \Delta t_{delay} + \Delta t_{prop}$

Clock Synchronization



(3) - Clock difference Δt_{diff}

Node expects: $t'_1 - t_0 = \Delta t_{delay} + \Delta t_{prop}$

But, if there is an <u>offset</u> then: $t'_1 - t'_0 = \Delta t_{delay} + \Delta t_{prop} - \Delta t_{diff}$

Clock Synchronization

Example: **According to Node B's MEDL Node A should transmit its frame in its slot starting at t_0 = 300* with a Δt_{delay} of 10 and Δt_{prop} of 0.**

Node B receives the Node A transmission at its frame at t'_1 = 314 (assume Δt_{prop} = 0).

$$t_1 = t_0 + \Delta t_{delay} = 300 + 10 = 310$$

Thus, $$\Delta t_{diff} = t'_1 - t_1 + \Delta t_{prop} = 314 - 310 + 0 = 4$$

**in macroticks*

Basic CNI Data Storage

- Status Registers
- Control Register
- Message Registers
  - Received messages and messages to be transmitted

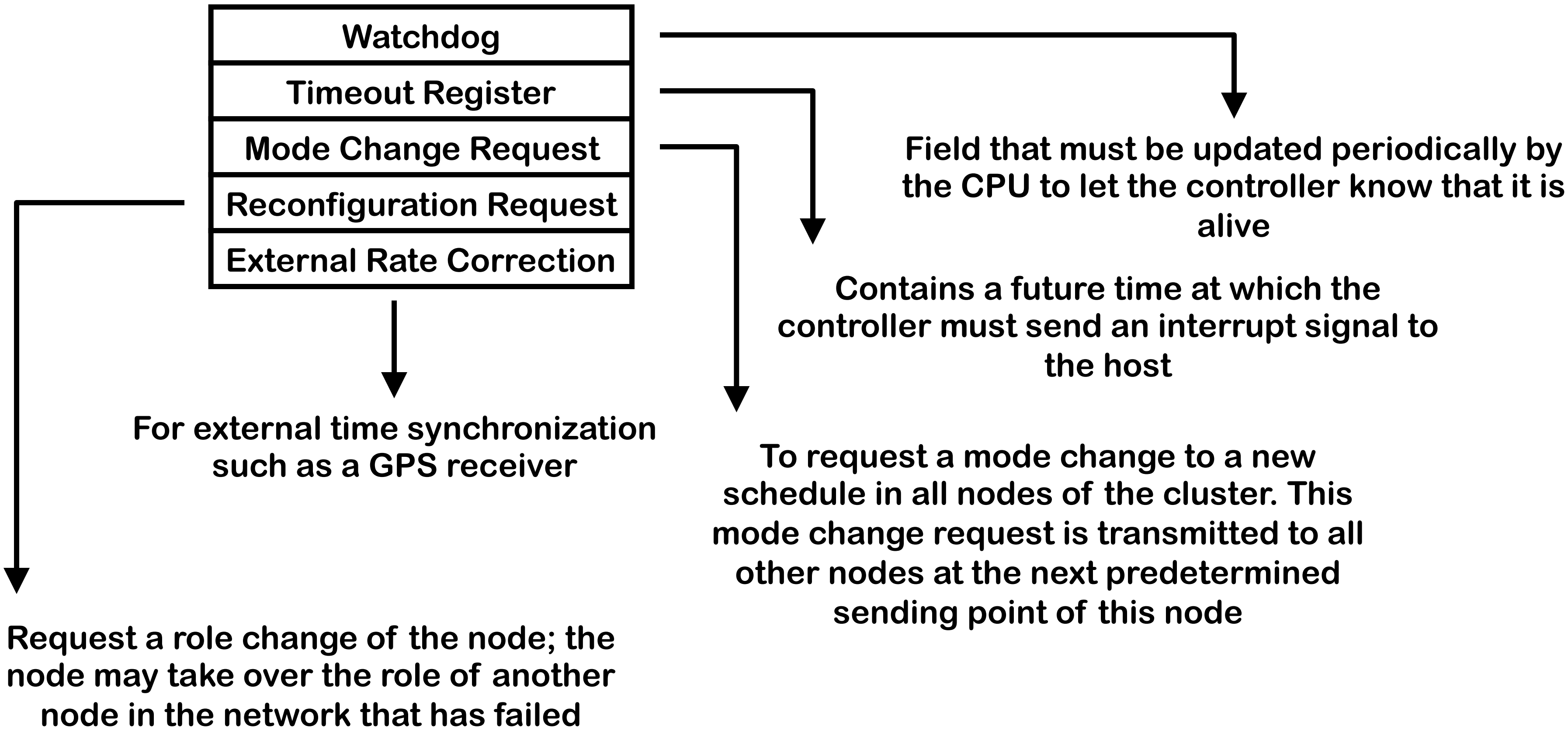
Status Registers:

Global Internal Time	
SRU-Time	Current global time in slot granularity
MEDL	
Membership	Vector containing a bit for every node in the cluster “1” – Node was operation during its last sending slot “0” – Node was not operation during its last sending slot
Status Information	

part of C-state (Controller-State)

Basic CNI Data Storage

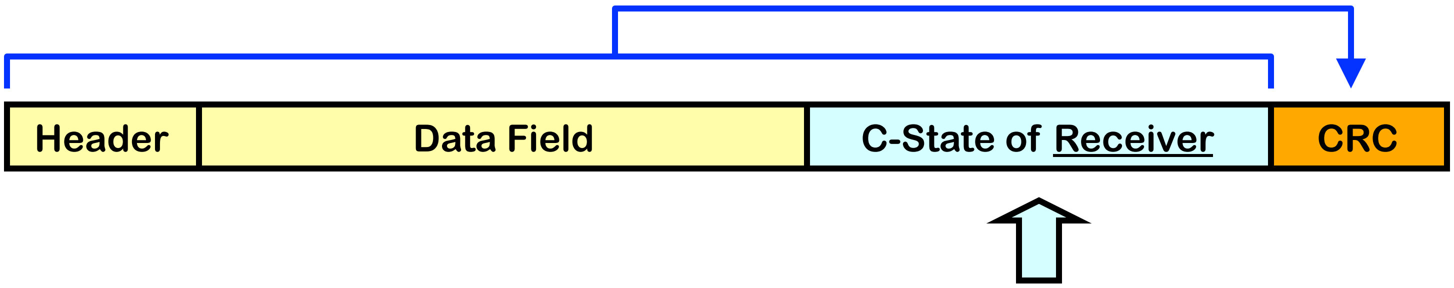
Control Registers:



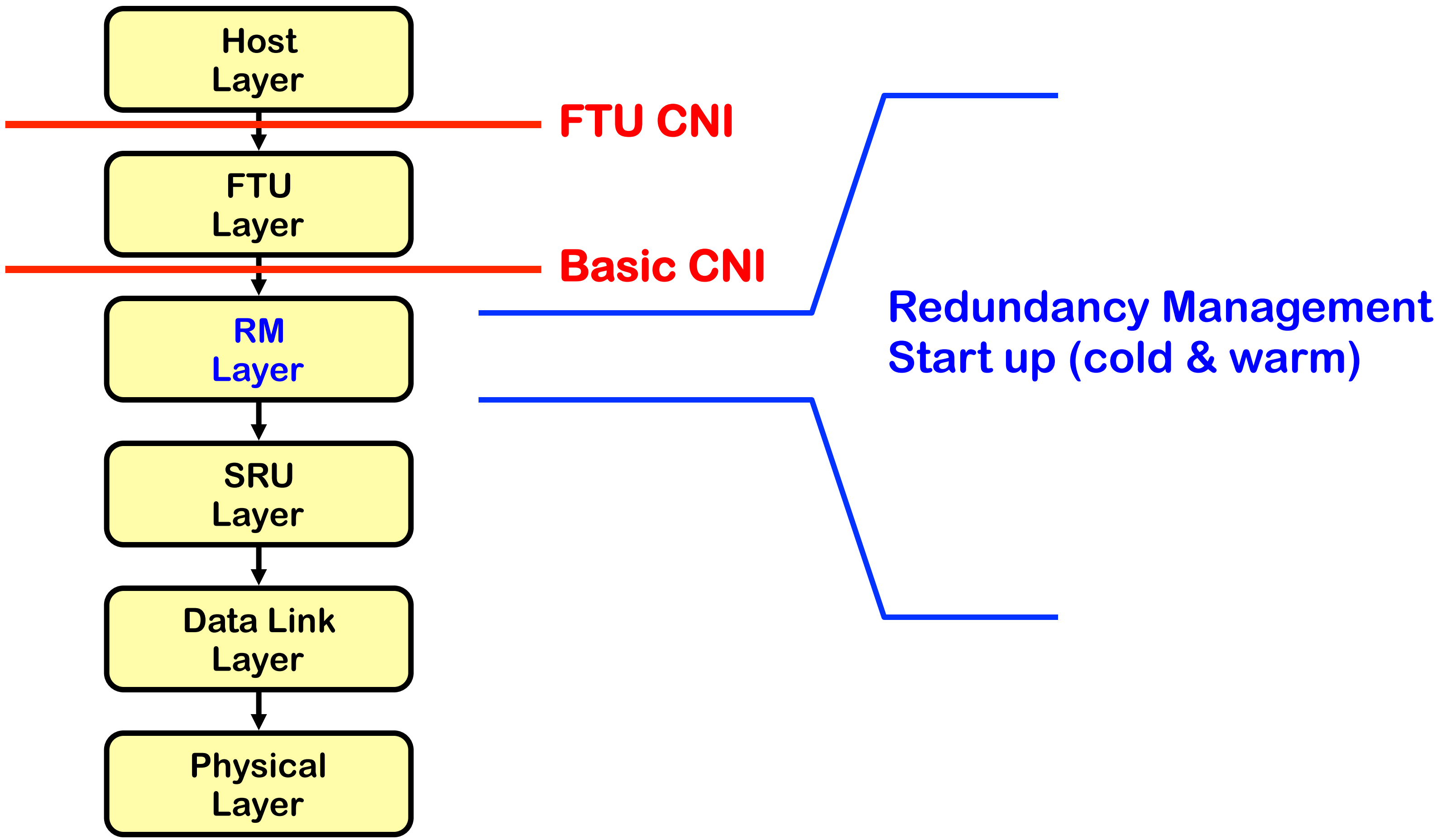
SRU Membership Mechanism

- Membership is updated locally according to a successful or unsuccessful data transmission
- With every transmission, each receiver sees and checks the sender's membership consistency
  - Is sender's membership equal to receiver's membership.
- Every sender with a different membership is assumed to be incorrect.

CRC Calculation at Receiver:



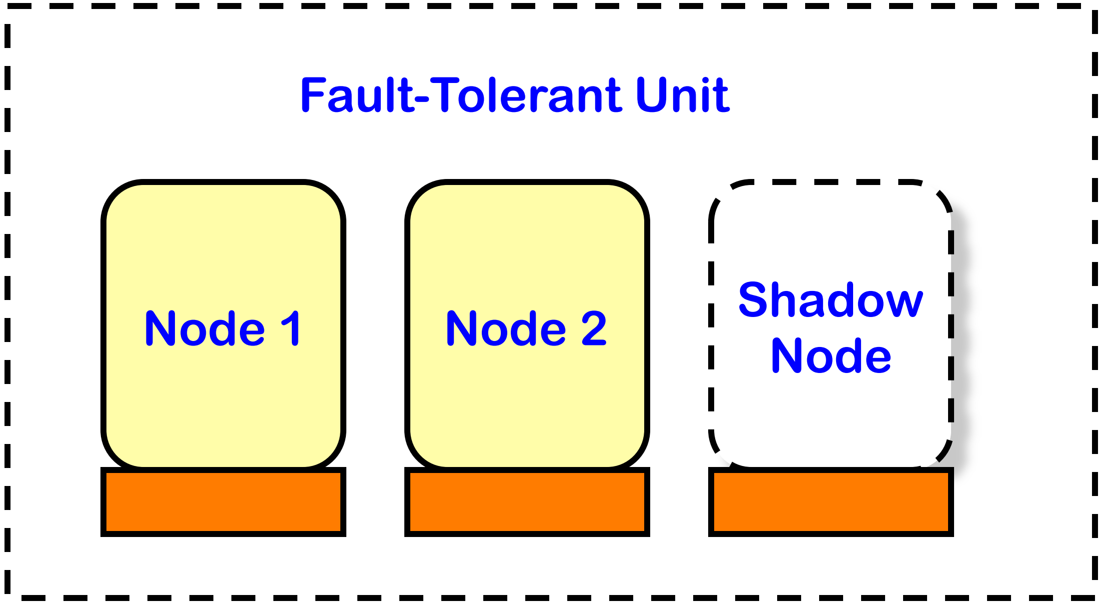
TTP Layers


Host Layer
FTU CNI
FTU Layer
Basic CNI
RM Layer
SRU Layer
Data Link Layer
Physical Layer
Redundancy Management
Start up (cold & warm)

RM Layer

- Tasks include:
  - Mode changes
    - a particular node can operate in various modes (i.e take-off, cruise, landing)
  - Dynamic redundancy management
    - the replacement of a failed node by a shadow node (standby)
  - Reintegration of a repaired node

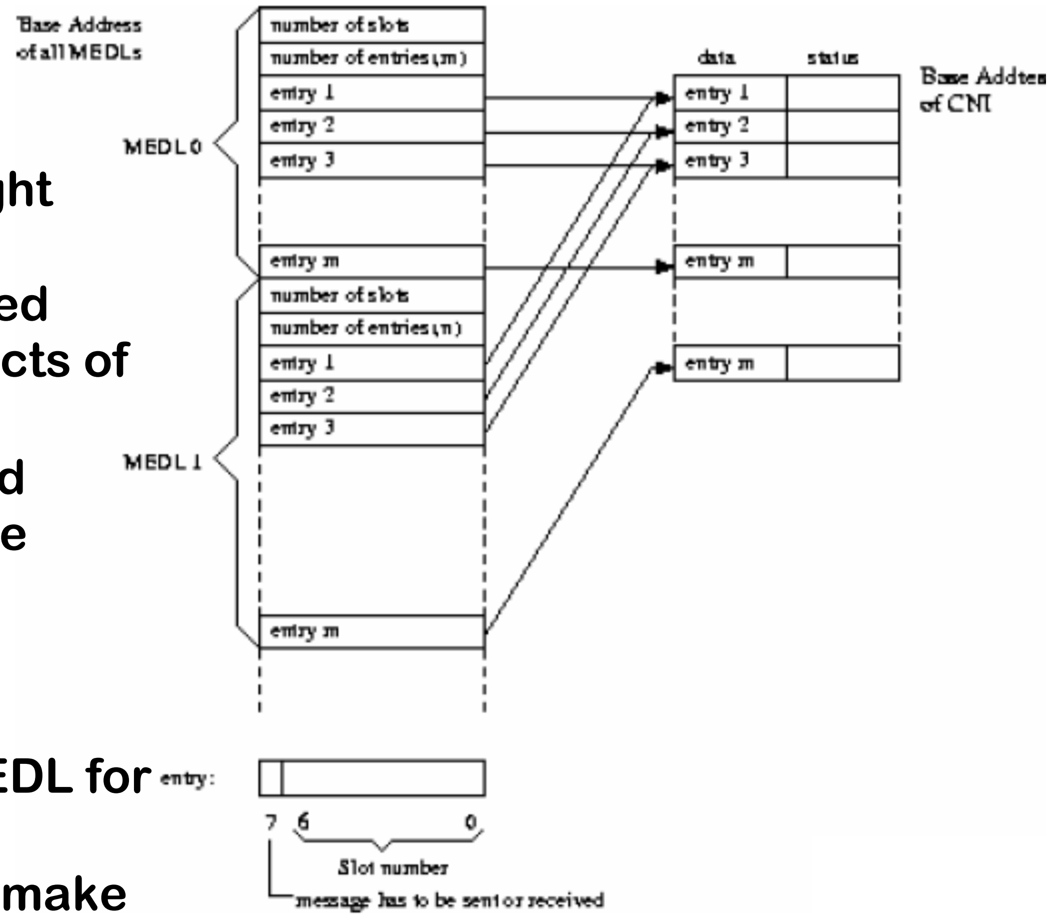
Redundancy Management



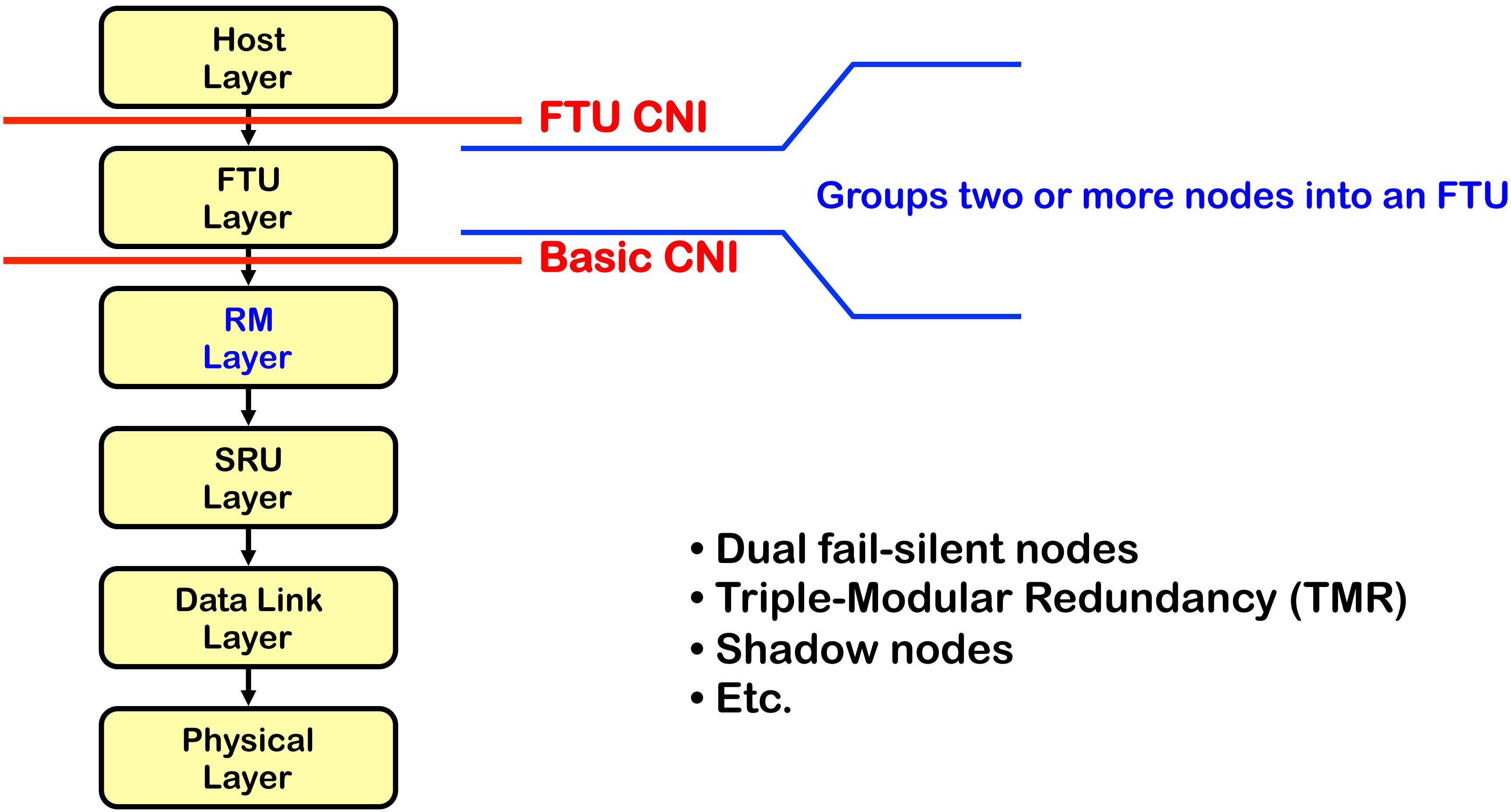
Node #2 may break down, in that case the RM layer of its TTP controller may send a message to activate the shadow node. The reconfiguration register of the shadow node will indicate this role change.

Operating Modes

- Different operating modes require different message schedules
  - Accelerating vs. cruise might need different information
  - Operation vs. diagnosis need emphasis on different aspects of the vehicle
  - Failure recovery might need access to different message traffic
- TTP solution: use multiple schedules
  - Pre-compute a different MEDL for every possible situation
  - (And invent tool support to make this feasible)



TTP Layers



- Dual fail-silent nodes
- Triple-Modular Redundancy (TMR)
- Shadow nodes
- Etc.