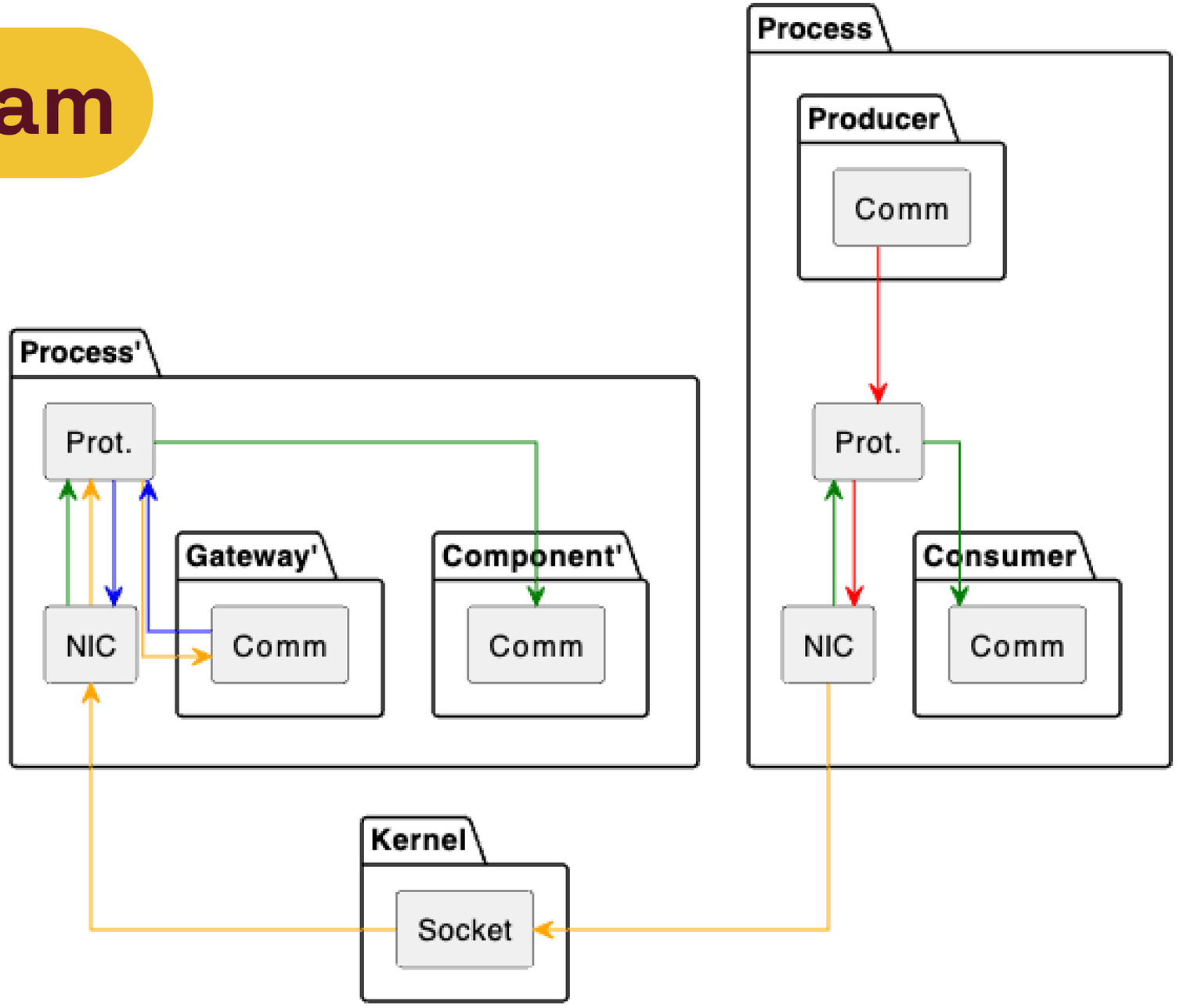
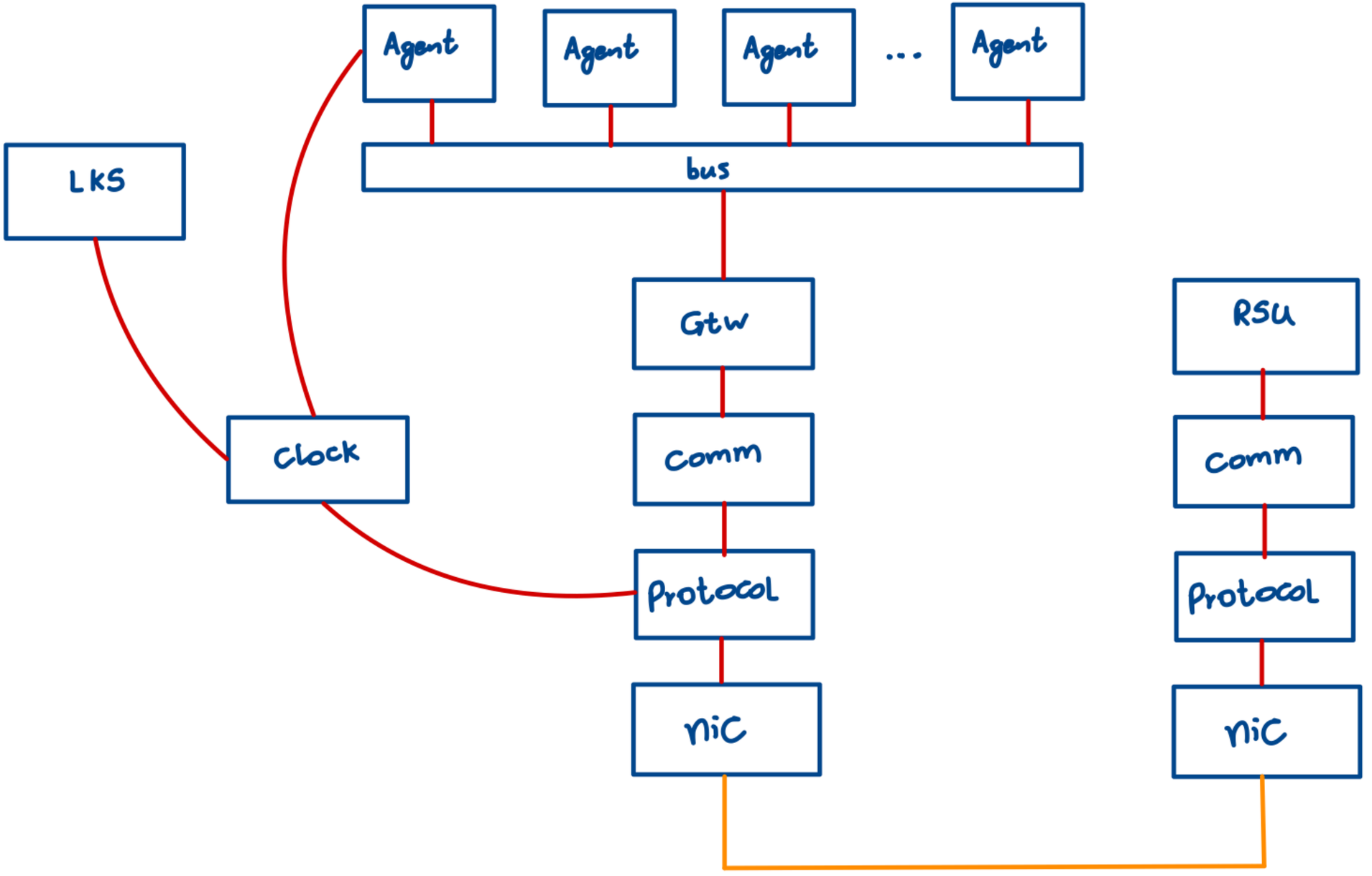
Reliable and secure communication library for critical autonomous systems

CÉSAR AUGUSTO PEREIRA DE SOUZA
ENZO NICOLÁS SPOTORNO BIEGER
JOÃO PEDRO PEREZ RESMER
JOÃO PEDRO SCHMIDT CORDEIRO

P4 28/05/2025

Process Diagram



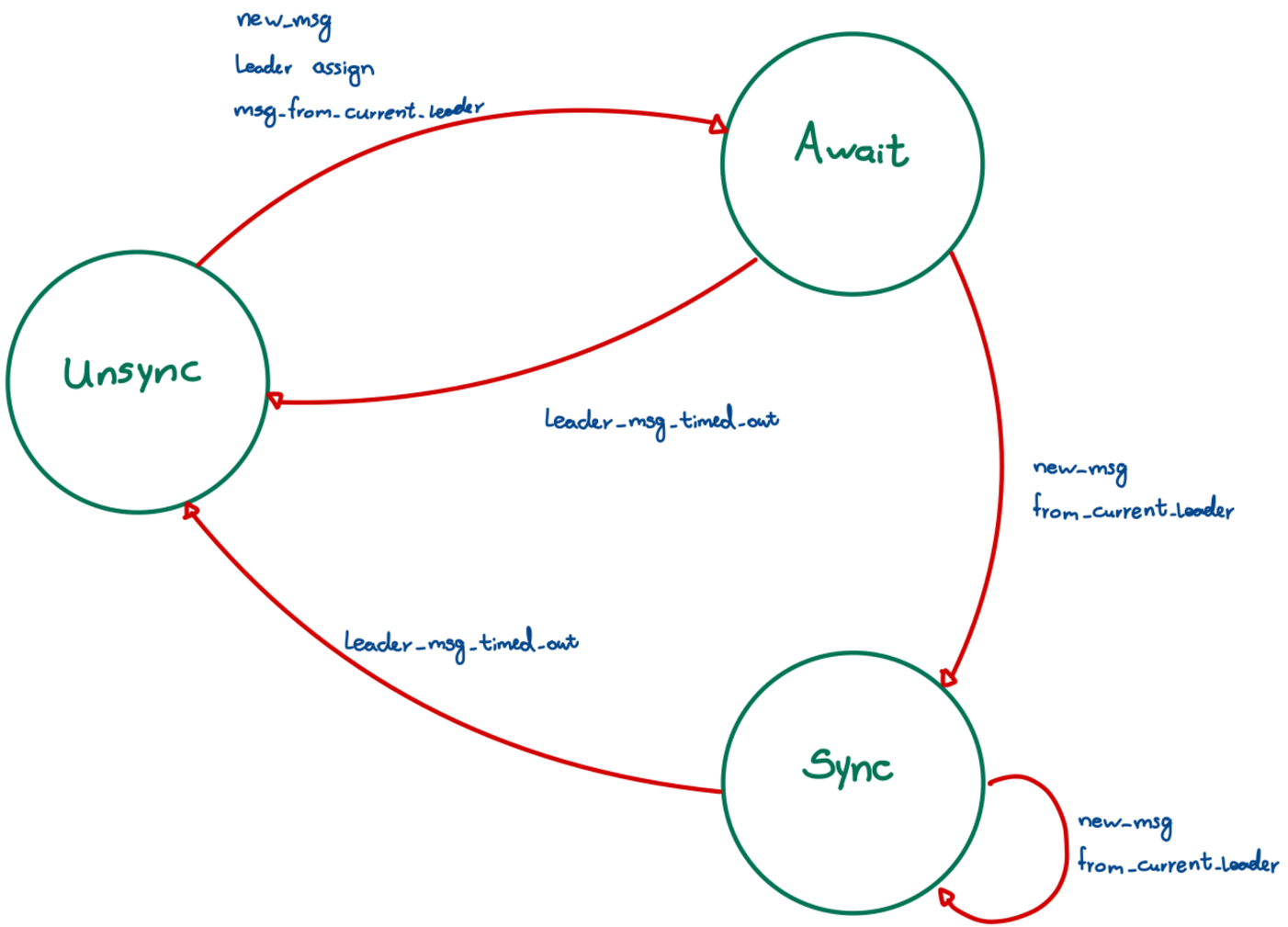

Agent
Agent
Agent
...
Agent
bus
LKS
Clock
Gtw
comm
Protocol
NIC
RSU
comm
Protocol
NIC

Clock

- **Message transmission time:** 2µs per message (tested)
- **Cumulative error limit:** 10ms (10× the 1ms precision for relaxed safety margin)
- **Assumed oscillator drift:** 20 parts per billion (ppb) Standard Crystal (HPET)
- **Message capacity:** ~250,000 messages possible during timeout period (500ms ÷ 2µs)

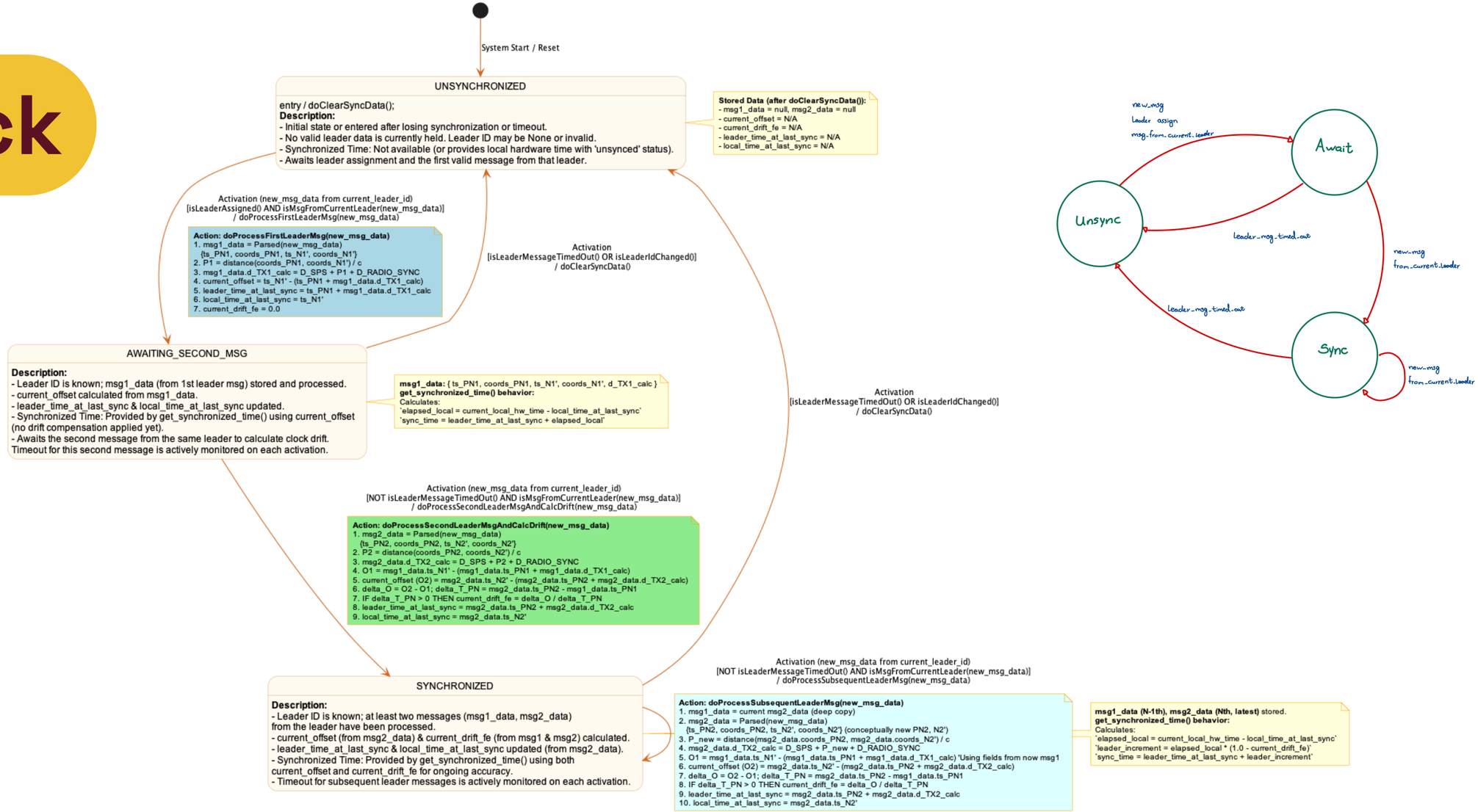
$$\text{Formula: } \text{MAX\_SILENCE} = \frac{\text{ERROR\_LIMIT}}{\text{DRIFT\_RATE}} = \frac{10\text{ms}}{20\text{ppb}} = 500\text{ms}$$

Clock


new_msg
Leader assign
msg_from_current_leader
Await
Unsync
Leader_msg_timed_out
new_msg
from_current_leader
Leader_msg_timed_out
Sync
new_msg
from_current_leader

Enhanced SPTP Clock Component State Machine

Clock



Clock Component State Machine (v2 with Activation-based Timeout)

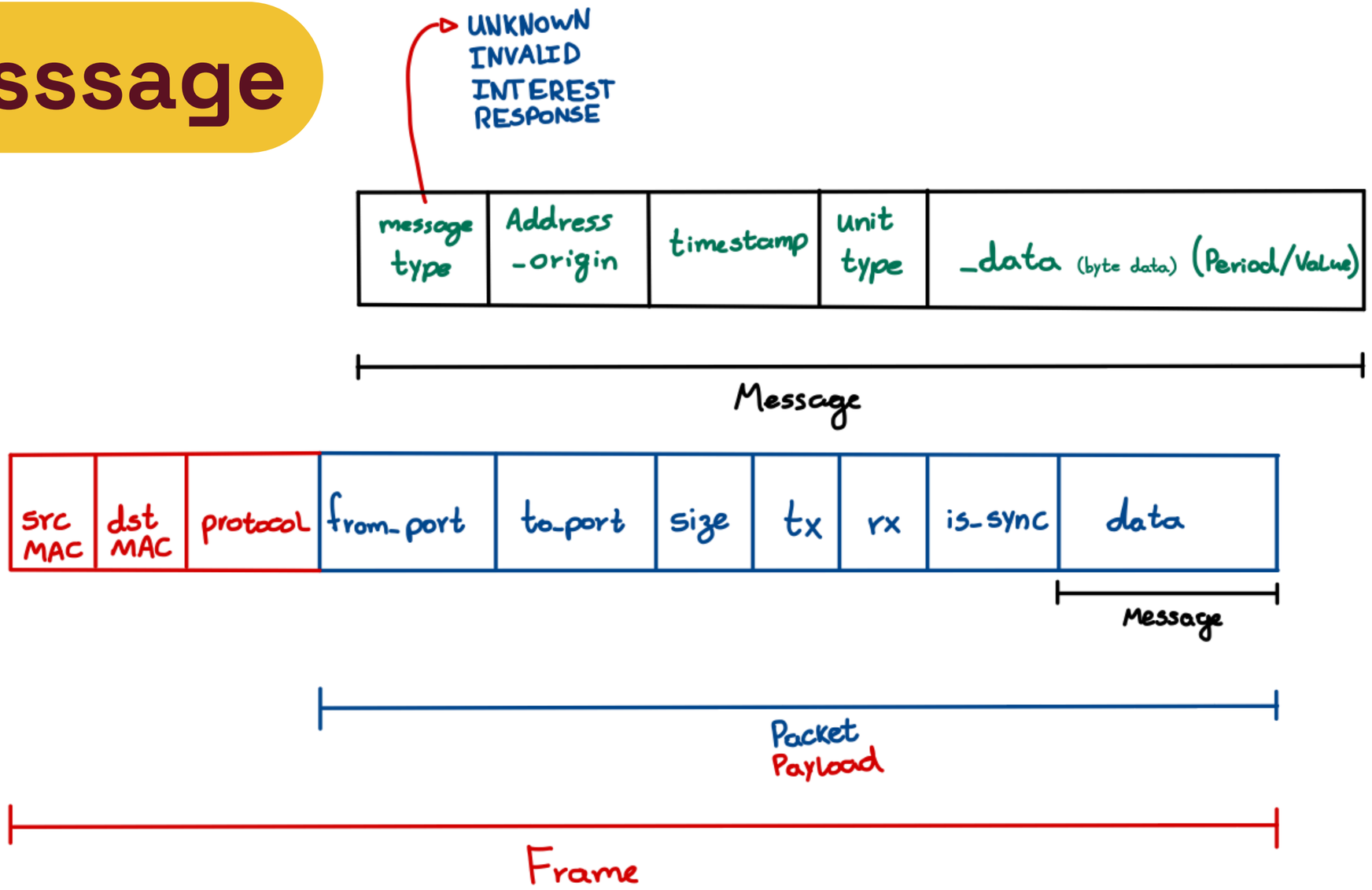
Activation Model:
- The component is activated (e.g., by any NIC message arrival, or a periodic internal check).
- During any activation, if in AWAITING_SECOND_MSG or SYNCHRONIZED state, it first checks `isLeaderMessageTimedOut()` and `isLeaderIdChanged()`. If true, it transitions to UNSYNCHRONIZED.
- Otherwise, if the activation was due to a message from the current leader, the relevant `doProcess...Msg()` action is performed.

Guard Conditions (in brackets []):
- `isLeaderMessageTimedOut()`: (hw_now - local_time_at_last_sync) > MAX_LEADER_SILENCE_INTERVAL
- `isLeaderIdChanged()`: current_leader_id differs from externally managed leader ID.
- `isMsgFromCurrentLeader(msg)`: msg.sender_id == current_leader_id.
- `isLeaderAssigned()`: current_leader_id is valid.

Constants & Functions: As defined in previous discussions.
(D_SPS, D_RADIO_SYNC, c, Parsed(msg), distance(), get_synchronized_time(), etc.)

(v2: Activation-based Timeout Check)

Messsage


UNKNOWN
INVALID
INTEREST
RESPONSE
message type
Address -origin
timestamp
unit type
_data (byte data) (Period/Value)
Message
src MAC
dst MAC
protocol
from_port
to_port
size
tx
rx
is_sync
data
Message
Packet Payload
Frame

Reliable and secure communication library for critical autonomous systems

CÉSAR AUGUSTO PEREIRA DE SOUZA
ENZO NICOLÁS SPOTORNO BIEGER
JOÃO PEDRO PEREZ RESMER
JOÃO PEDRO SCHMIDT CORDEIRO

P4 28/05/2025