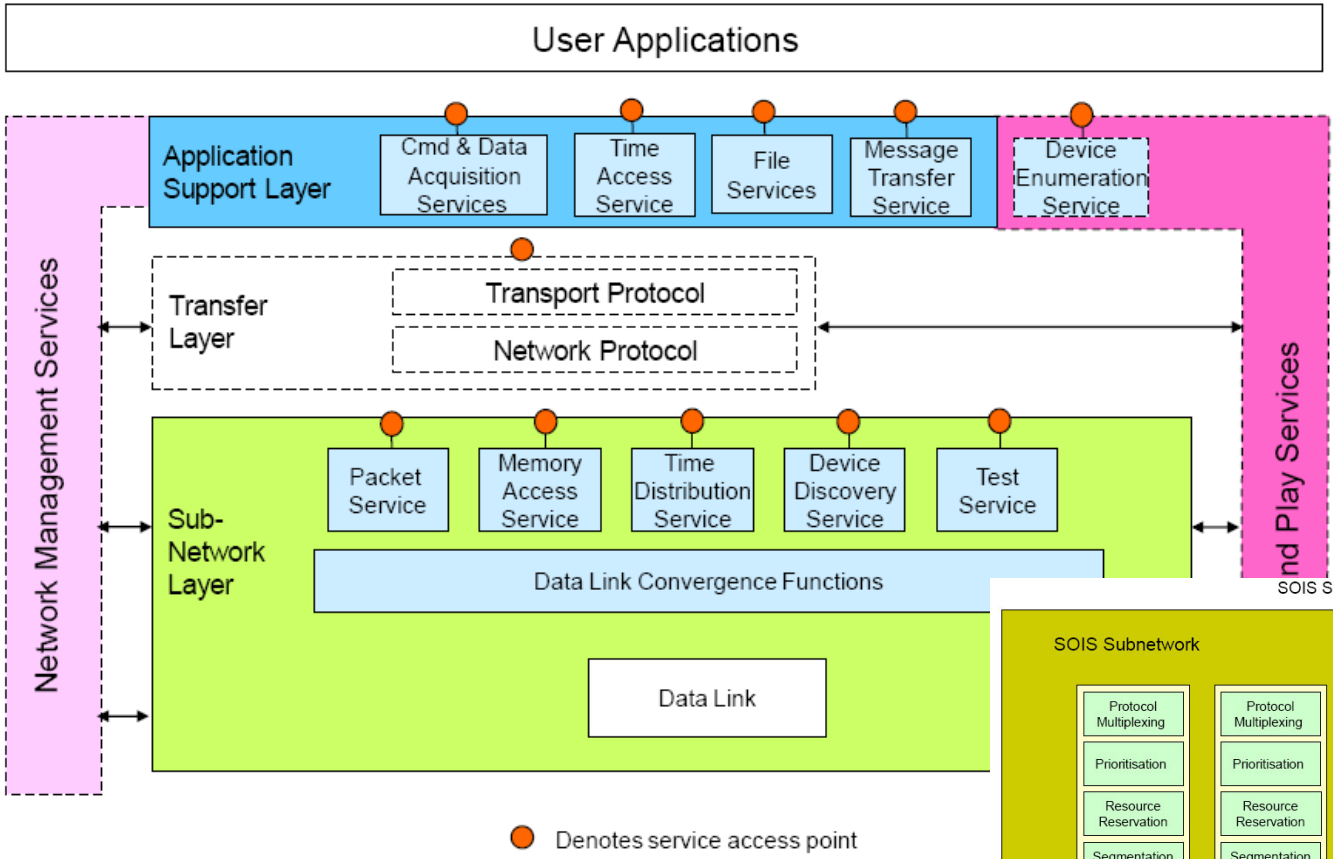
SpaceWire for Command & Control

Refined specifications of required QoS classes and implementation options for SpW networks

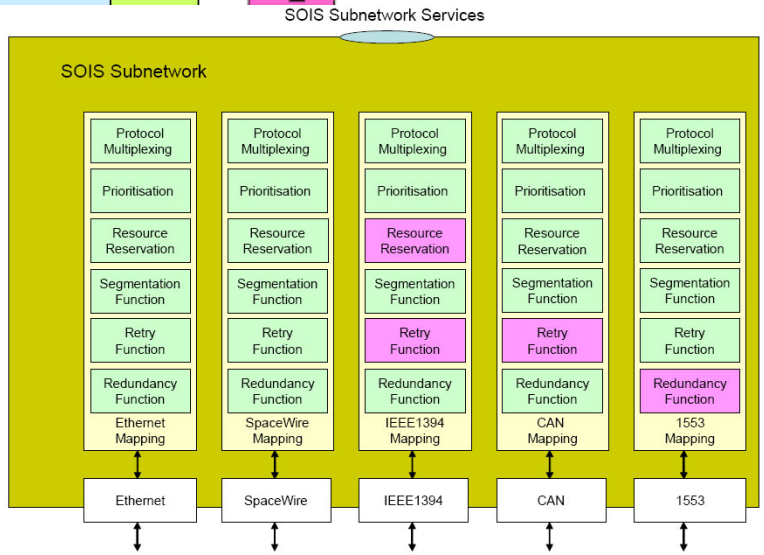
Outline

- Context and purpose
- Mission requirements
- QoS classes specification
- Mapping with SOIS QoS classes
- Implementation options
- Verification of mission requirements
- Conclusions and open issues

SOIS SubNetwork Services and convergence layer



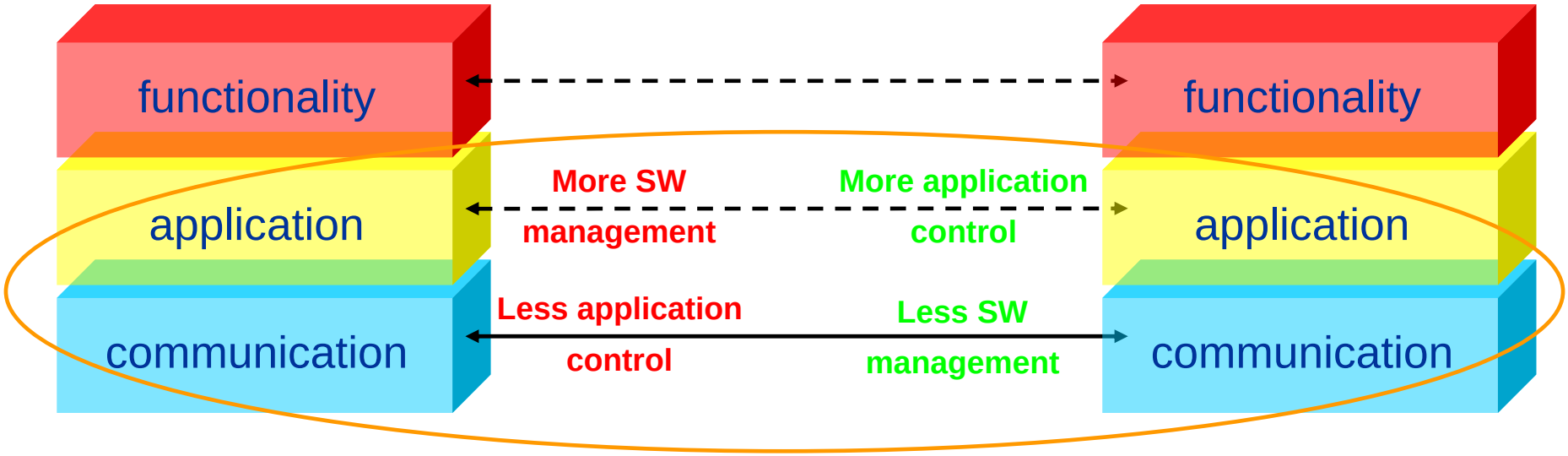
QoS

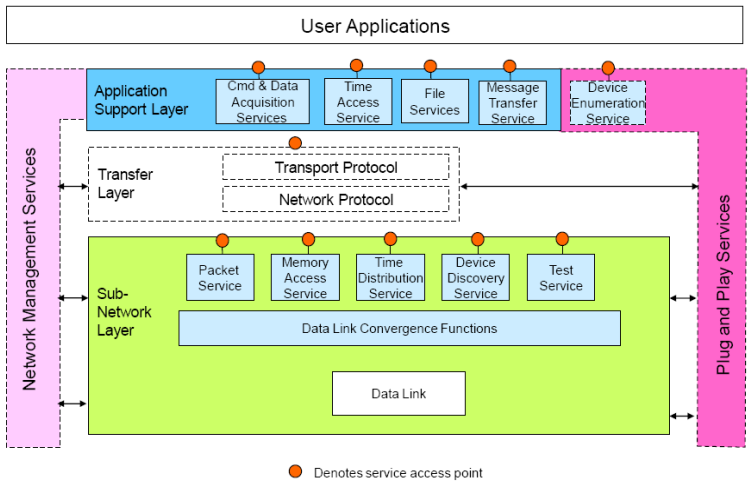


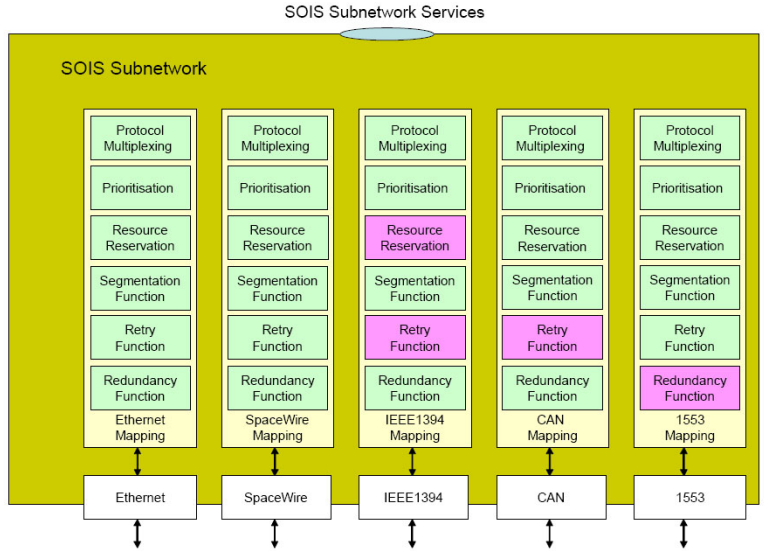
QoS for on-board communications

- definition: communication QoS = communication properties
  - ex: in telecoms, expected communication properties are statistical
- on-board communication properties for space applications:
  - hard properties:
    - Real-Time: a deadline, short or long, must be met
    - Fault-Tolerant (Single Failure Hypothesis): one single failure does not impact the end-to-end communication
    - Assurance: the sender application is assured (through service ACK) that its message has arrived
  - soft properties:
    - priorities: higher priority messages will probably arrive before lower priority ones
    - increased reliability (retries without HW redundancy): a retried message is more likely to arrive than a one shot one (assumes protocol ACK)
- In each category, properties are all a priori independent from each other (soft and hard properties are exclusive).

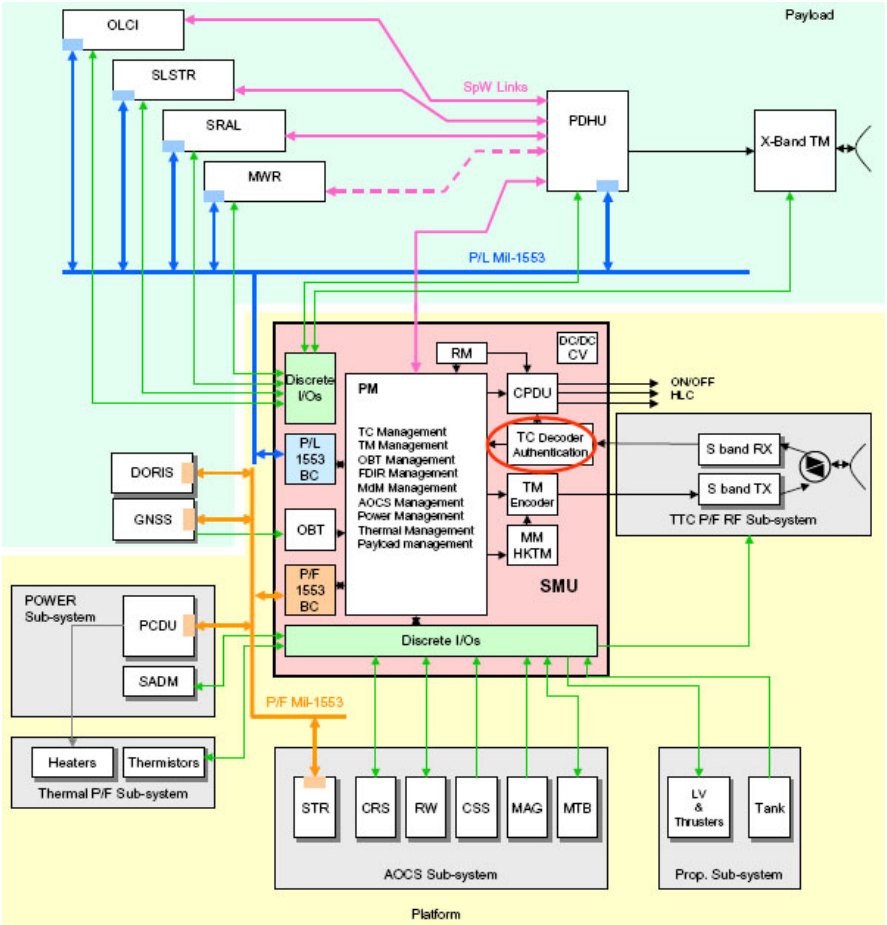
Implementation level for QoS properties

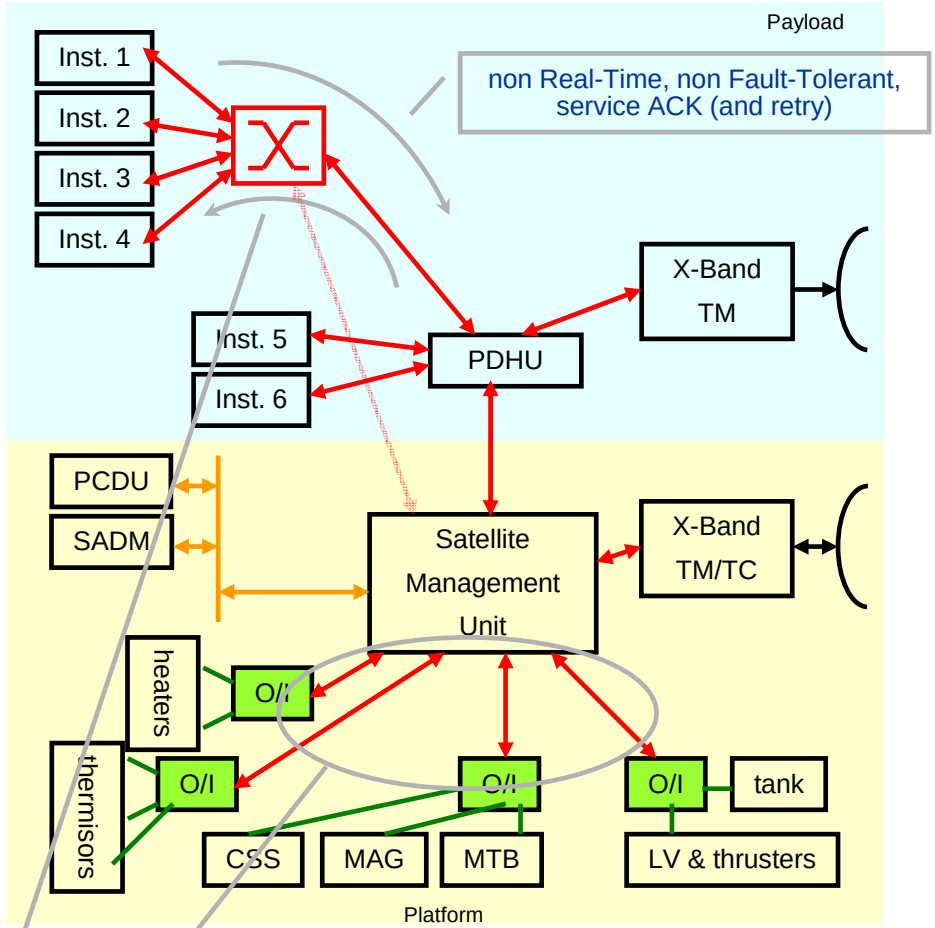






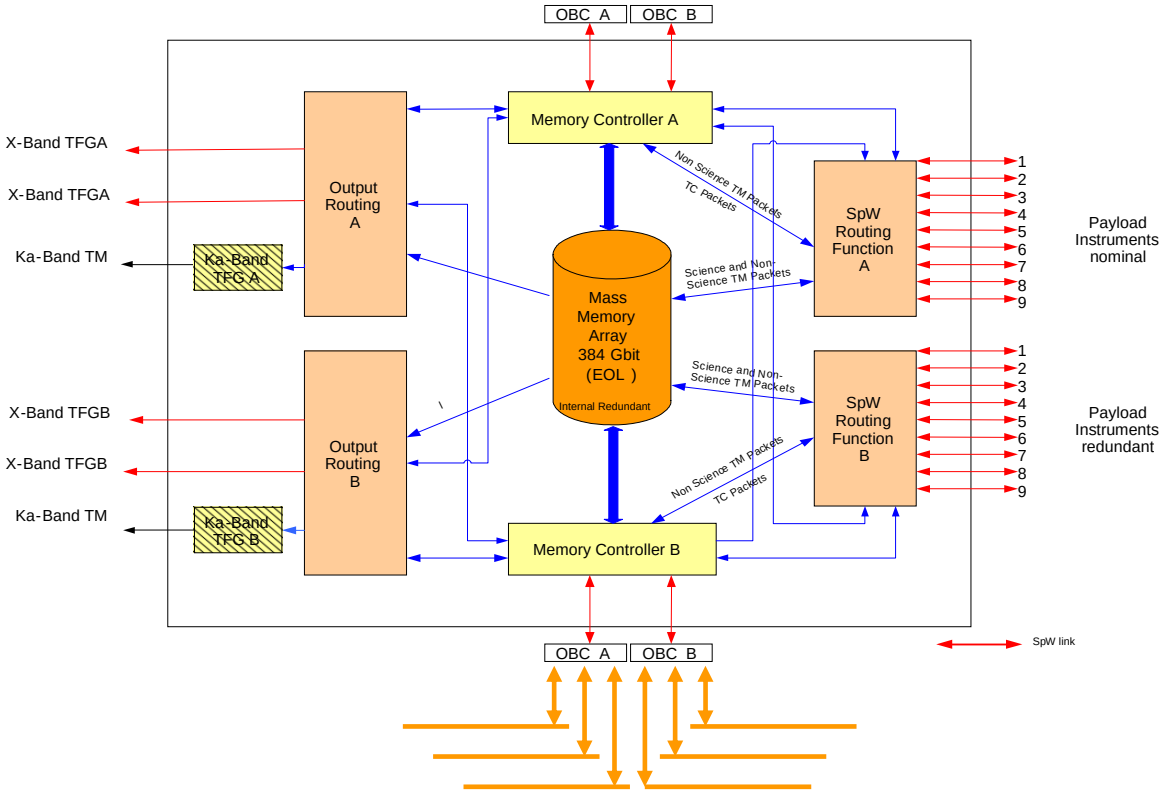
Mission requirements (1) : Earth Observation





1553-like: Real-Time, non Fault-Tolerant, service ACK, no retry (Fault tolerance, supported by HW redundancy, is managed at application level)

Mission requirements (2) : Science (BepiColombo)

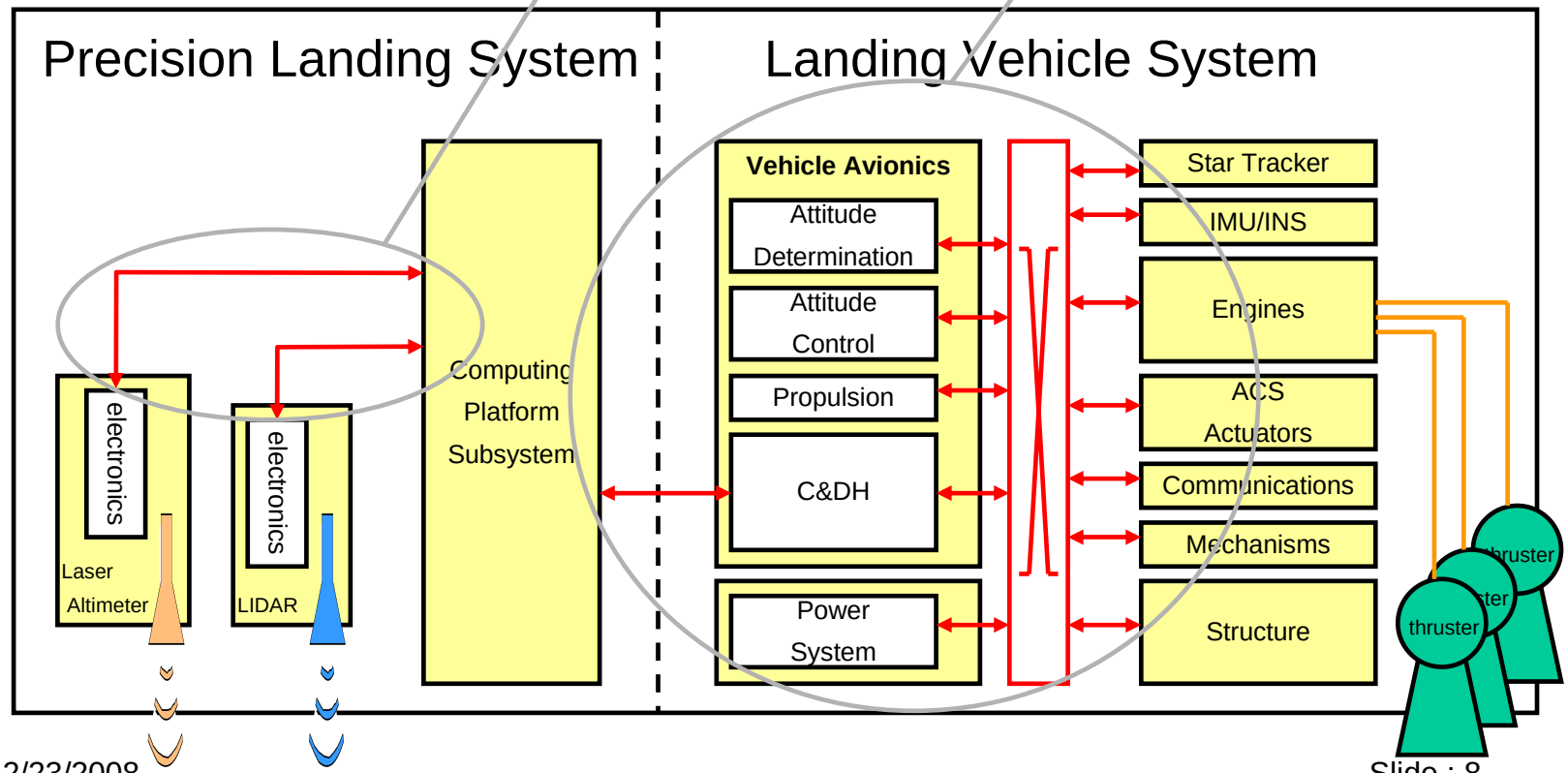


Mission reqmts (3) : High Precision Soft Landing

- mission critical operation
- high speed RT control loop
- all equipments are hot redundant

high-speed Real-Time and Fault-Tolerant (no service ACK, no retry)

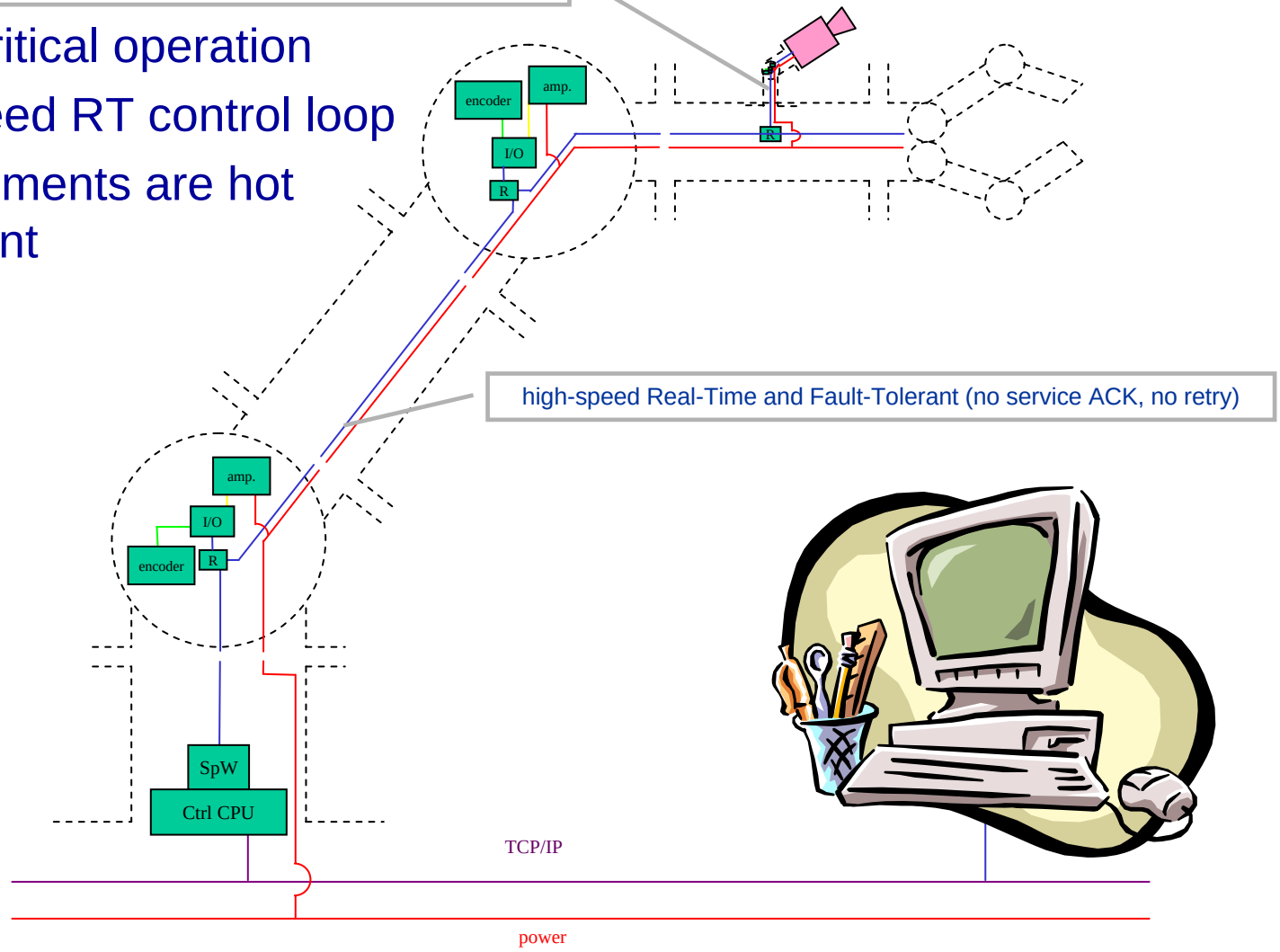
1553-like: Real-Time, non Fault-Tolerant, service ACK, no retry (Fault tolerance, supported by HW redundancy, is managed at application level)



Mission requirements (4) : next generation IIS Robot

non Real-Time, non Fault-Tolerant, no service ACK, no retry, may use priorities

- safety critical operation
- high speed RT control loop
- all equipments are hot redundant



QoS classes for the communication

- Best effort (non Real-Time, non Fault-Tolerant, no service ACK, no retry)
  - may use priorities
- Assured (non Real-Time, non Fault-Tolerant, service ACK, no retry)
  - may use priorities
- Transport-like (non Real-Time, non Fault-Tolerant, service ACK and retry) = Assured + increased reliability
  - may use priorities
- Real-Time (non Fault-Tolerant, service ACK, no retry)
  - Fault tolerance (supported by HW redundancy) is managed at application level
- high-speed Real-Time and Fault-Tolerant (no service ACK, no retry)

QoS classes (2) – SOIS mapping

- Derived from missions
  - Best effort
  - Assured
  - Transport-like
  - Real-Time
  - Real-Time Fault-Tolerant

- SOIS QoS classes
  - Best effort
  - Assured
  - Reserved
  - Reserved + service ACK
  - Guaranteed

~~quality~~

complexity

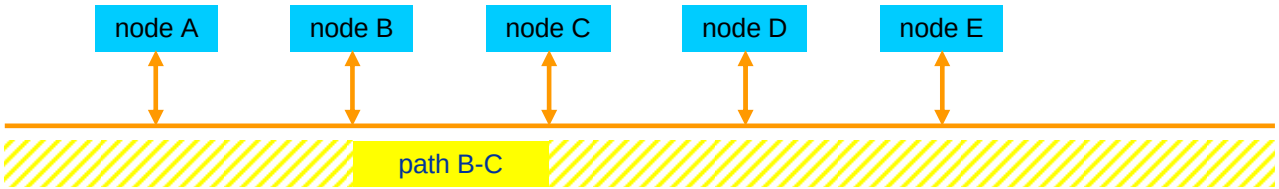
QoS classes (3): Fault-Tolerance ➔Real-Time

- Properties:
  - FT: one single failure does not impact the end-to-end communication (Single Fault Hypothesis)
  - RT : communication can always succeed if not constraint by a deadline

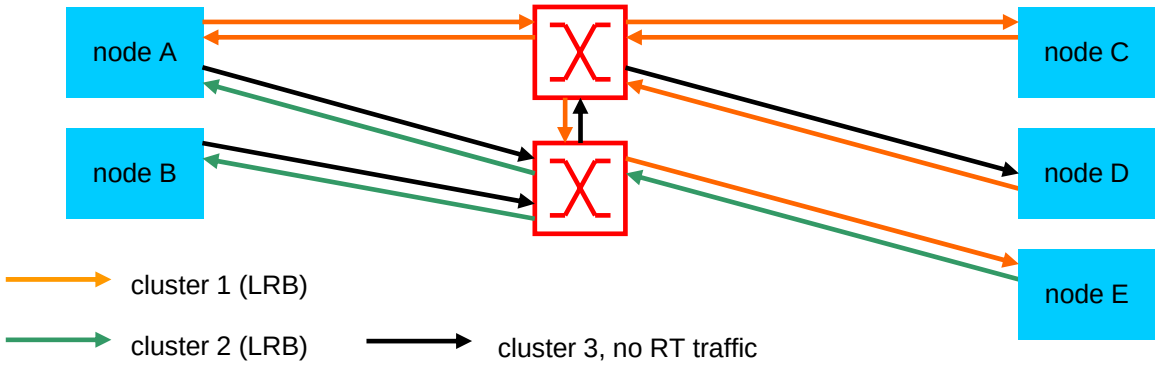
- Solutions
  - FT: A communication path can fail – need for a redundant path.
  - RT: Communication must be orchestrated (according to a schedule or by a master).

QoS classes (4): Real-Time (communication path)

- RT communication = orchestrated (on a given communication path, only one node speaks at a time)
  - For 1553, any path blocks the whole bus.



  - Definition: For SpW, a path blocks a set of half-links from senders to receivers that compete for links: a Realtime Logical Bus (RLB)

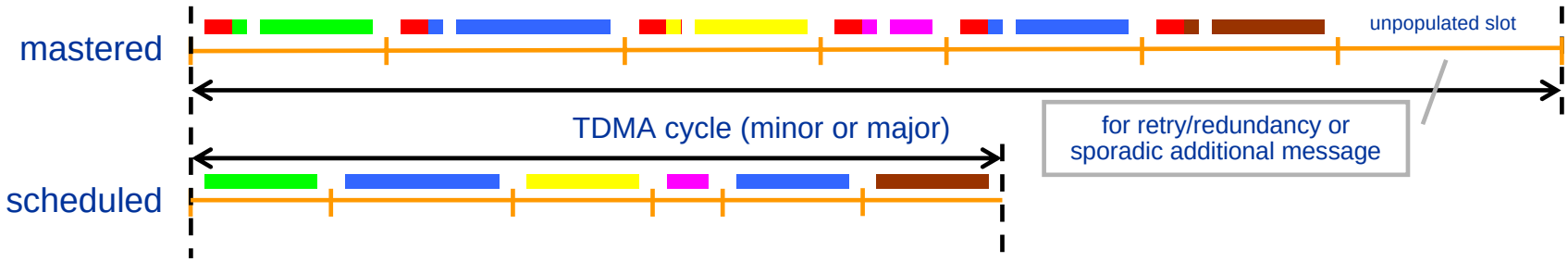


SpaceWire links are full-duplex !! Opposite traffics are Independent.

- Definition: A cluster is a set of half-SpW links connected through routers. A cluster can host either RT traffic (Realtime Logical Bus) or non RT traffic.

QoS classes (5): Real-Time (scheduled vs mastered)

- Nodes can self-orchestrate (follow a common schedule) or obey the maestro (the communication Realtime Logical Bus master)



mastered approach

- can accommodate sporadic additional messages.
- allows the master to change the schedule without informing the slave nodes.

scheduled approach

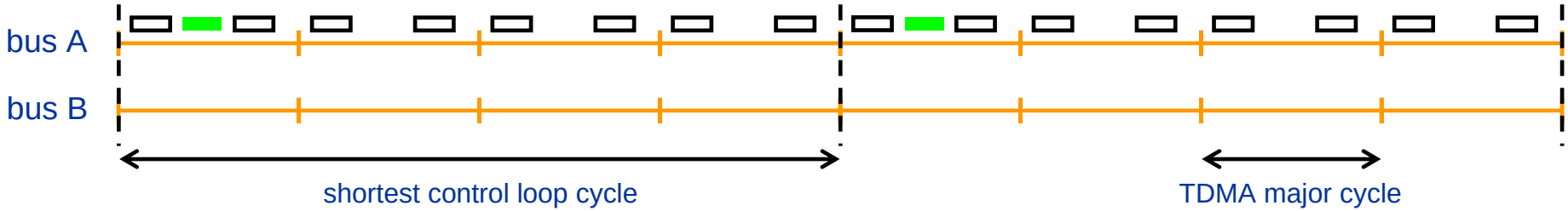
- can bring additional reliability features (membership, implicit acknowledgement, etc.)
- requires that node be time-synchronised
- requires that each node knows the time table
- Requires start-up and clique detection algorithms

- Babbling Idiot: Both solutions allow HW control of communications but require a HW bus guardian for higher reliability.

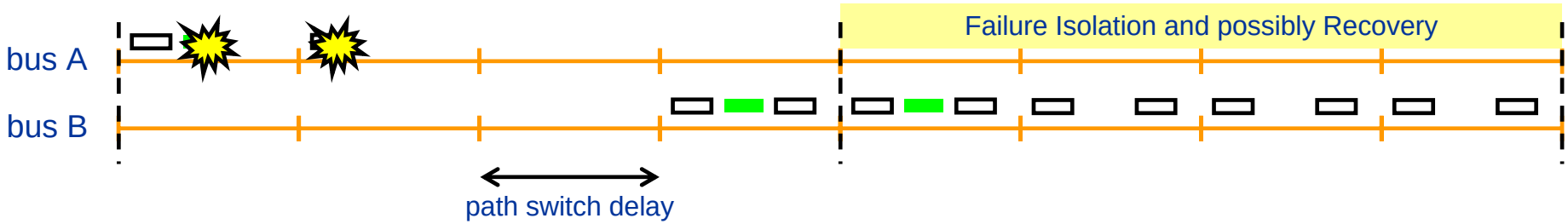
- Preferred option is master-slaves, like MIL-STD-1553.

QoS classes (6): Real-Time and Fault-Tolerant (1)

- Long-cycle RT: the redundant path can be invoked after the failure (application-level retry with HW redundancy)
- Communication QoS = Real-Time (fault tolerance is managed at application level, like in 1553)
  - nominal mode

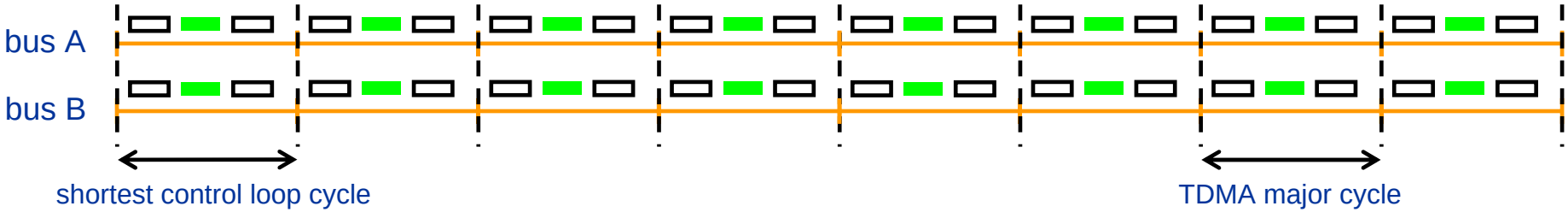


  - failure mode

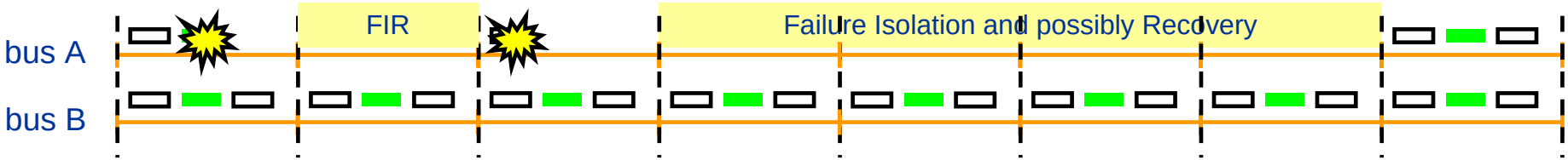


QoS classes (7): Real-Time and Fault-Tolerant (2)

- Short-cycle RT: the redundant path must be invoked at the same time as the nominal one
- Communication QoS = Real-Time and Fault-Tolerant
  - nominal mode



  - failure mode



QoS classes (2) – SOIS mapping

- Derived from missions
  - Best effort
  - Assured
  - Transport-like
  - Real-Time
  - Real-Time Fault-Tolerant

- SOIS QoS classes
  - Best effort
  - Assured
  - Reserved
  - Reserved + service ACK
  - Guaranteed

~~quality~~

complexity

QoS classes (8) : Transport-like

- Properties:
  - non Real-Time, non Fault-Tolerant, service ACK and retry
- Solutions
  - redundant communication path not required
  - protocol ACK and one (TBC) retry with same SpW address (path or logical)
  - ACK or TIMEOUT signal to sender application
  - may support priorities

QoS classes (9) : Assured

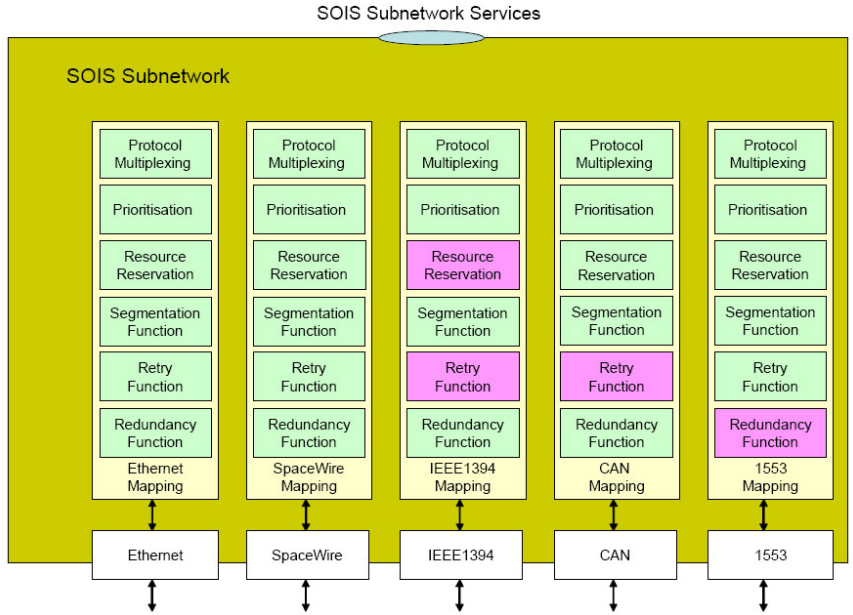
- Properties:
  - non Real-Time, non Fault-Tolerant, service ACK, no retry
- Solutions
  - redundant communication path not required
  - protocol ACK
  - ACK or TIMEOUT signal to sender application
  - may support priorities

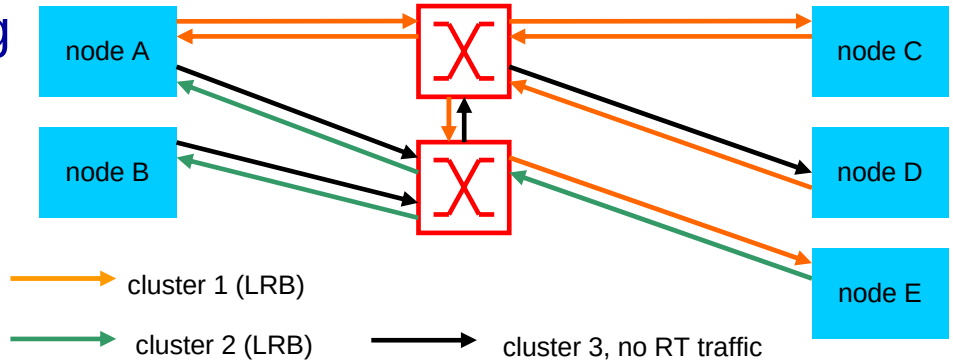
QoS classes (10) : Best effort

- Properties:
  - non Real-Time, non Fault-Tolerant, no service ACK, no retry
- Solutions
  - redundant communication path not required
  - no protocol ACK
  - no ACK or TIMEOUT signal to sender application
  - may support priorities

SpW convergence layer

- general
  - protocol multiplexing: PID
- Data Transfer (non RLB clusters)
  - retry
  - priorities
  - segmentation
- Cmd & Ctrl (RLB clusters)
  - resource reservation
    - at cluster level
    - mastered time sharing
  - full redundancy
    - at cluster level

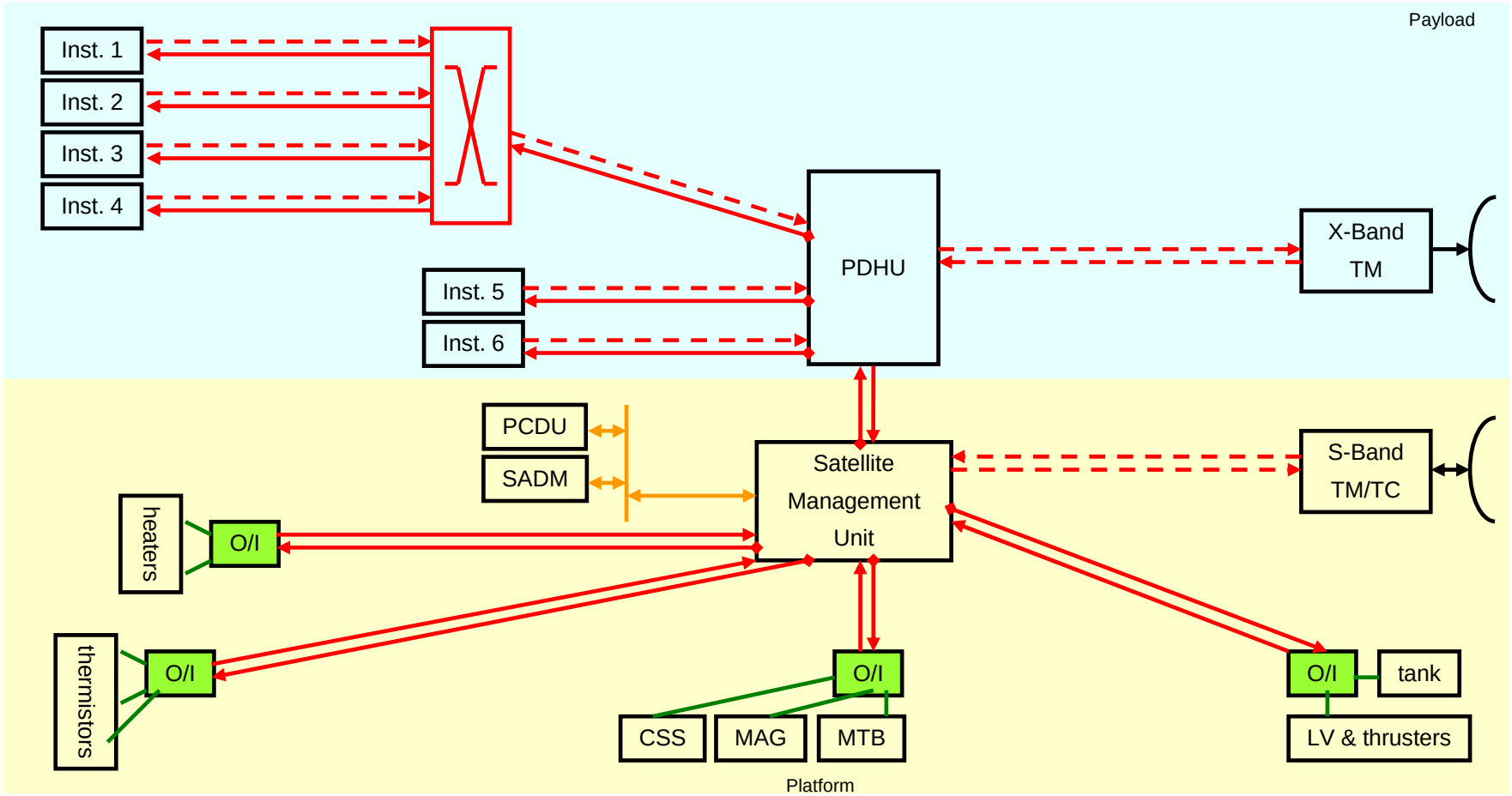




SOIS SubNetwork services

- SOIS QoS classes for the Packet Service to be slightly refined
- SOIS SubNet services:
  - Memory Access Service: RMAP-like protocol to be implemented with SOIS SubNet Packets -> the QoS classes will be the ones of the Packet Service
  - Time Distribution Service: protocol to be implemented with SOIS SubNet Packets and SpW timecodes -> the QoS classes will be the ones of the Packet Service (Cmd&Ctrl type of classes only)
  - Device Discovery Service: protocol to be implemented with SOIS SubNet Packets -> the QoS classes will be the ones of the Packet Service (Data Transfer type of classes only)
  - Test Service (not defined yet)
- All types of SpW Cmd&Ctrl packets (e.g. Packets, Time Distribution, Memory Access) sharing the same RLB must have compatible QoS and be scheduled by the same master.

Back to Earth Observation requirements (1)



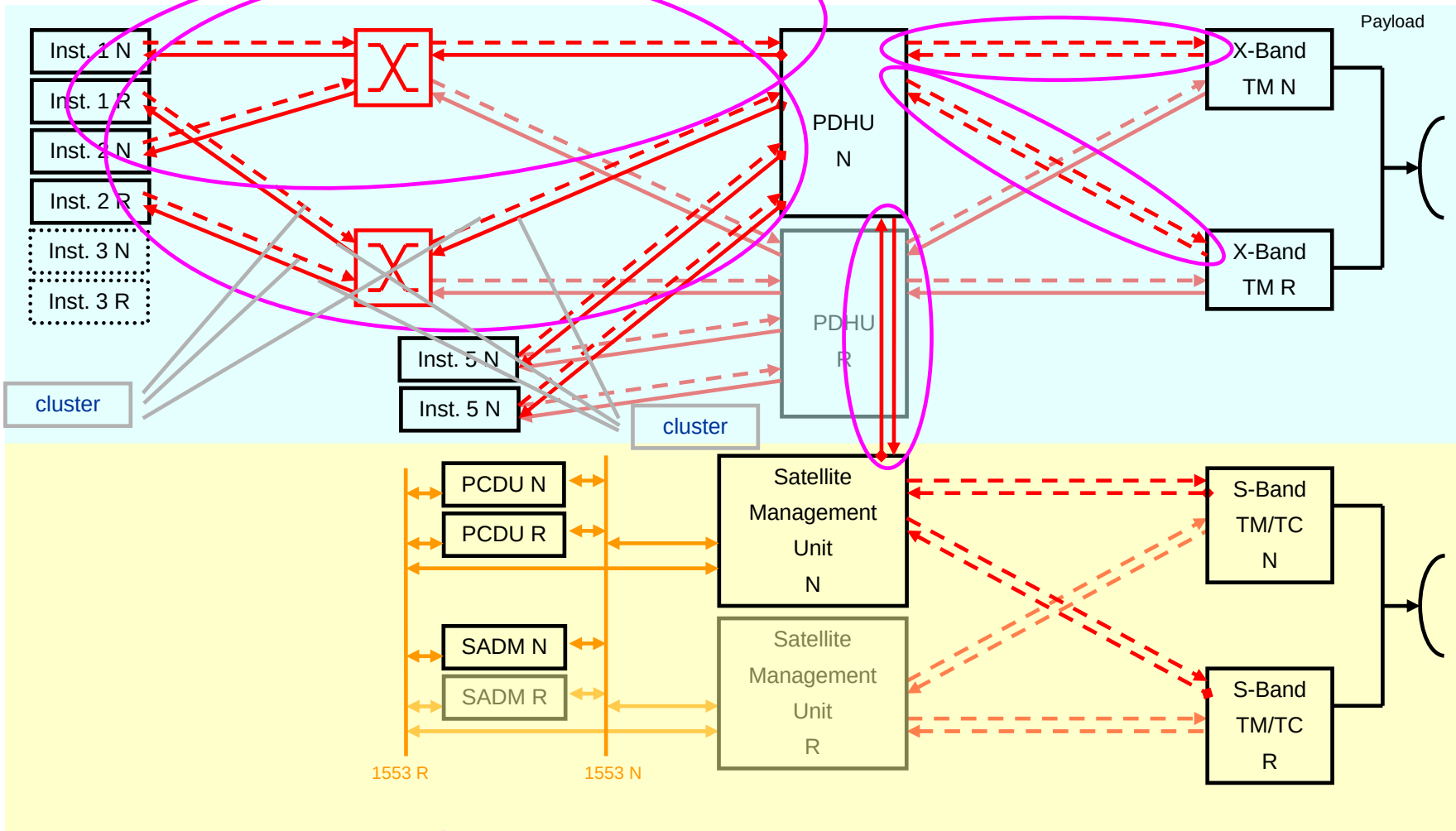
Cmd&Ctrl SpW (TDMA)

Data Transfer SpW

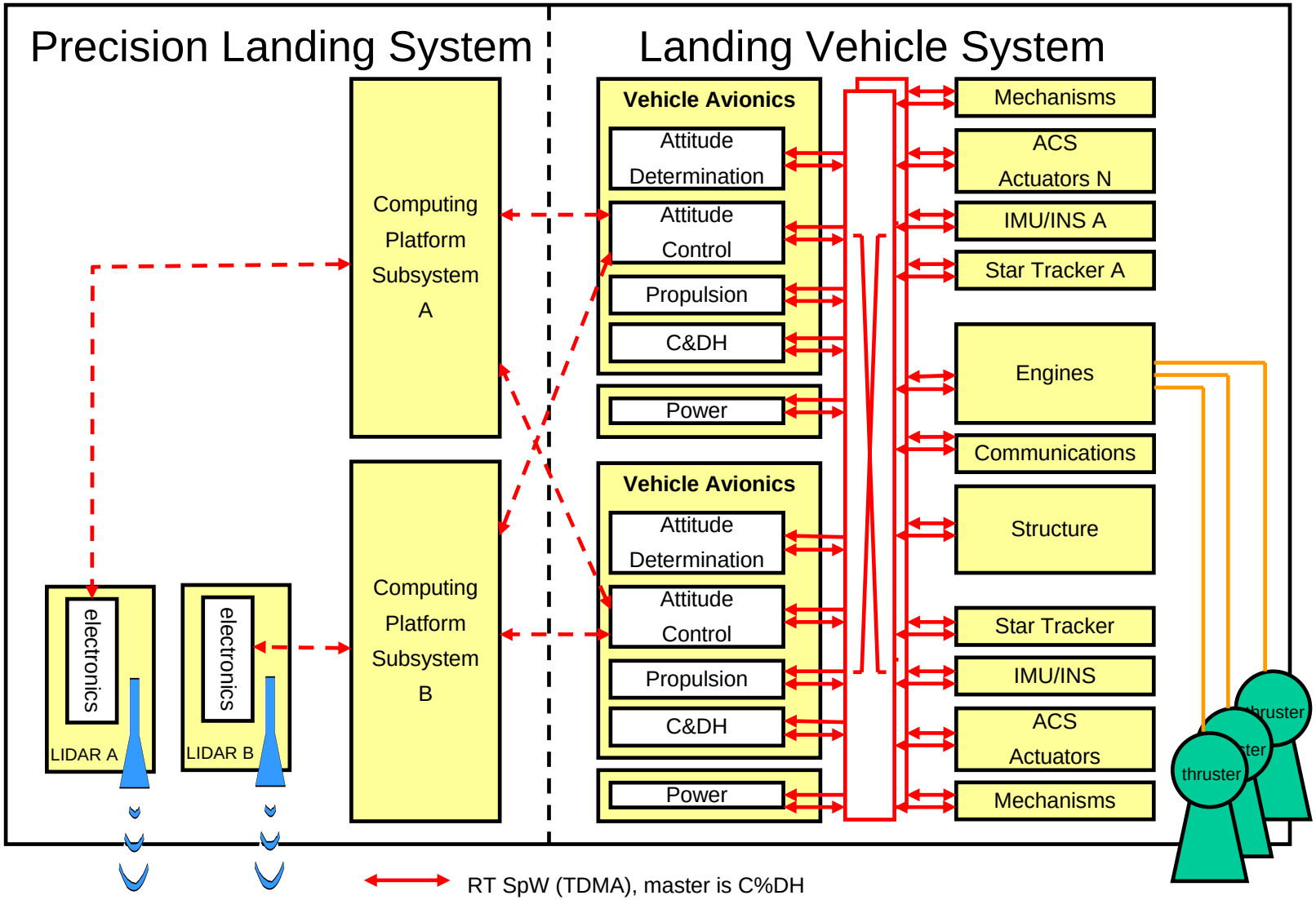
RLB master

analogue

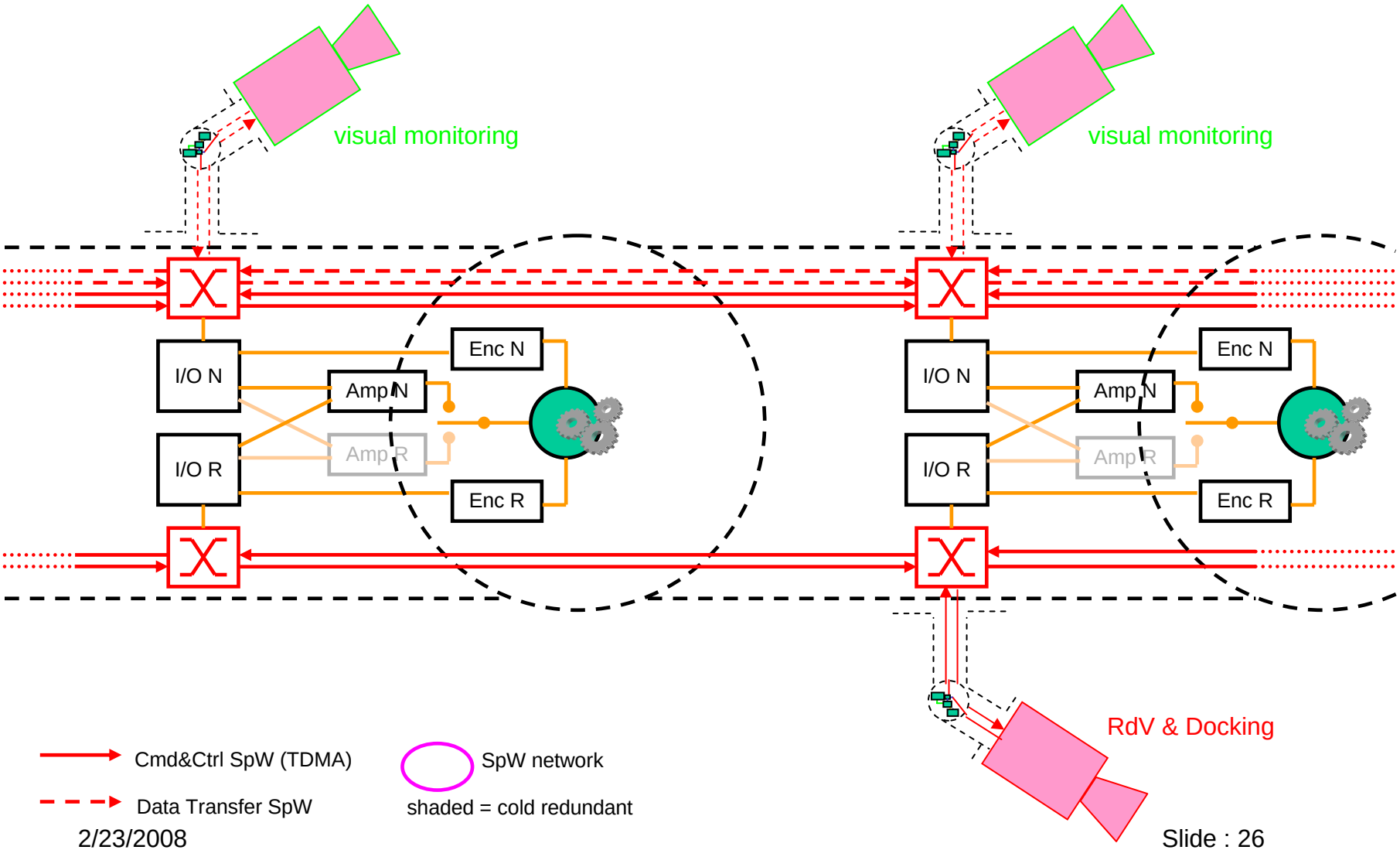
Back to Earth Observation requirements (2)



Back to High Precision Soft Landing reqmts

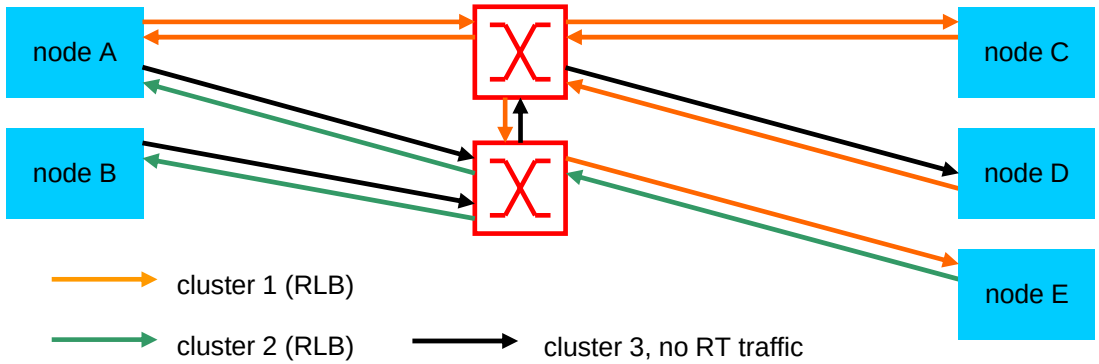


Back to next generation IIS Robot reqmts

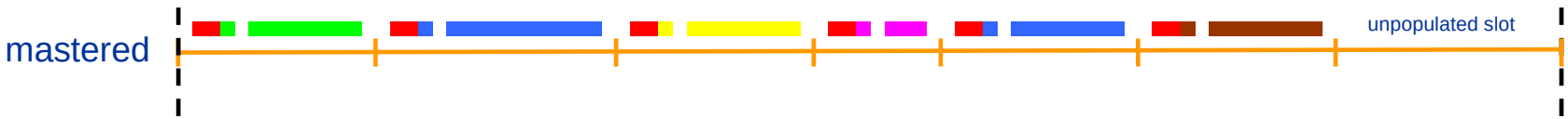


Conclusion (1) - Divide and Conquer

- Divide on-board data systems into SpW networks and SpW networks into clusters (RLB and non RLB)



- Implement on each RLB a master-slave protocol (1553-like)



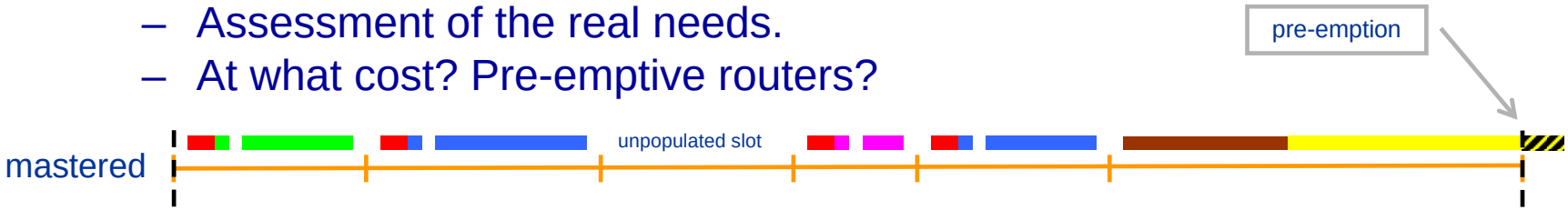
Conclusion (2) – SOIS Sub-network Services

- SOIS QoS classes for the Packet Service to be slightly refined
- Other SOIS SubNet services can be implemented with SOIS SubNet Packets -> the QoS classes will be the ones of the Packet Service
- SOIS convergence layer: confirmation of required functions (protocol multiplexing, retry, priorities, segmentation, resource reservation, redundancy) with refined specifications.

Conclusion (3) – Open issues

- How to implement a 1553-like protocol on a SpW Realtime Logical Bus?
  - Do we need timecodes? What is the added value?

- Mix Cmd&Ctrl and Data Transfer on the same Logical Bus.
  - Assessment of the real needs.
  - At what cost? Pre-emptive routers?



- Full safe Time-Triggered Architecture allowing on-demand traffic?
  - Requires scheduled pre-emptive routers and network guardians
  - Allows membership, implicit acknowledgement, etc.
  - Allows flexibility for non-critical traffic (temporary payloads)
  - Certifiable w.r.t. transport safety regulations; may be required for future manned spacecraft