SpaceWire-RT Initial Protocol Definition

Preliminary comments on version 2.1

Christophe Honvault / Olivier Notebaert
Astrium Satellite Central Engineering

All the space you need

EADS astrium

General facts

Transfer types

- Asynchronous
  - Asynchronous communications but priority of packets are managed.
  - Three QoS: *Basic*, Best effort, Assured
- Scheduled
  - All the traffic within the system must respect time slots
  - Time slots are defined in a schedule table
  - Five QoS: *Basic*, Best effort, Assured, Resource-reserved, Guaranteed

Services

- SOIS oriented services
  - For packet, memory access, device discovery
- SpaceWire packet transfer
- RMAP
- PnP (soon)

Scheduled type

- Transfer managed by a schedule table
  - All the devices must have this table available and respect it
- Some points are not addressed in the document:
  - How are initialized the schedule tables within the system:
    - Static definition at the level of each device?
    - Dynamic definition through configuration (as routers routing tables are initialized)?
  - Are they **reconfigurable** to handle persistent failures?
  - How is handled time synchronization?
    - By SpaceWire-RT, SpaceWire or CTM for instance?
  - Table construction is a “relatively straightforward exercise” (§3.8.1.4) but “has to take account of the timeliness requirements of possible retries” (§3.9.3.2.2).

EADS astrium

Who is the killer?

- P78: « The “killing” of packets still being sent when the time-code arrives is done to prevent fault propagation. ». Who is the killer?
  - SpaceWire-RT himself
    - Has to manage received time-codes and control the current status of the SpaceWire codec.
  - SpaceWire
    - Require a modification of the current implementation of SpaceWire codecs.
  - A dedicated « guardian »
    - Could be able to manage other errors, e.g. to ensure a fail-silent behaviour of devices.

What is the fault model?

- Managed errors are limited to the content of the packets:
  - Error in header
  - Error in address (that is not protected by CRC, which may lead to use unauthorized path!)
  - Error in data
  - Error in the sequence
  - Duplication error
  - Error in end of packet (EEP)
- No error linked to time is taken into account:
  - Communication during unauthorized slot
  - Non « fail silent » error modes of a node
  - Time-code reliability

EADS astrium

SpaceWire routers could help

- The proposed protocol attempts to ensure the network reliability without taking into account SpaceWire routers.
- Many fault detection and propagation avoidance functions could be implemented by the routers
  - Communication time-out (watch dog) as implemented in SpW-10X router is not sufficient.
  - Verification of the traffic with respect to schedule tables:
    - Blocking the communication from an unauthorized source.
    - Detection of error in addressing.
  - Such concepts are implemented on other RT protocols such as AFDX and FlexRay

Asynchronous type

- Scheduled system needs strong fault containment.
- Proposed asynchronous type does not support timeliness.
- Other timely asynchronous system exists relying on consensus and coordination of the nodes. It makes possible to optimize the bandwidth use.
- Experimented in the frame of the A3M study:
  - time codes used as “ I’m alive” messages ensuring failure detection with silent-failed users,
  - two services developed: task synchronization and datapool update in a distributed system

EADS astrium

Implementation complexity

- All the devices must respect the communication model:
  - Manage one or both types
  - Manage up to 256 channels potentially associated to several buffers
  - Manage retries and flow control
  - …
- Implementation in full HW will be complex and will require large amount of resources (memory and logic) making devices more expensive and difficult to validate.

Evaluation of overheads

- Splitting all the traffic into small messages leads to increase the overheads and limit the bandwidth. This may be not acceptable for high-data rate instruments.
  - Even if all the time slots are reserved for a channel, the maximum data throughput on the corresponding path will not reach the maximum capacity of the path.
- Possibility to use reserve paths that are not managed by SpaceWire-RT?
  - In Figure 3-13, channel 41/70/1 could use reserved path A,E/F that will be no more managed by SpaceWire-RT.

Recommendations

- SpaceWire-RT should be improved with focus on:
  - Determinism: have more consideration for the time aspects
  - Fault model: cover the entire range of errors and identify hypothesis.
  - Simplicity: do not try to implement all SOIS required QoS at the level of SpaceWire-RT
- Define different classes of applications illustrated by Use Cases (preferably coming from future users)
  - Organisation by size (small to complex systems), by criticality, …
- From these Use Cases, identify main drivers and necessary features

Conclusion – SpW RT protocol

- The currently proposed RT-Protocol definition looks to us (engineering feeling as potential users):
  - Taking some of our needs into account but maybe not all
  - To propose features that may probably never be used
  - Highly complex, maybe fragile with probably weak points
  - Difficult to manage at system level
  - Difficult to validate with all its features
  - Difficult to implement in building block

Conclusion - Approach

- The current approach seems:
  - Not focused on application needs:
    - Reference application and system user requirements for the SpW-RT-Protocol are not clearly established and agreed
  - Constrained by existing protocols, devices, standards,…
    - Lots of constraints are taken into account from the space heritage
    - But existing concepts from non-space domain are not considered
  - Not being enough considering implementation aspects (design, validation, operations…)
  - Not taking into account sufficient elements to ensure rationale decisions from an engineering trade-off

Way forward

- Aim at simplification
- Redefine the approach
  - A new protocol shall take into account (at least…)
    - User goals for requesting it (focus the requirements on the user applications and reference system architecture)
    - Existing items and constraints to take into account (e.g. existing protocols, devices, standards,…) but maybe with adaptations/tailorisation
    - Implementation aspects (design, validation, operations…)
  - Eventually a trade-off defines a solution which is the result of a rational compromise

➢ A specific “task-force” could implement this approach

- Minor comments follow…

General comments

- Some elements are used before their definition:
  - Page 43 last paragraph:
    - « A time-slot is defined by SpaceWire-RT to be long enough to allow six packets of maximum permitted length to be sent in one time-slot ».
    - Why six packets? What is the maximum length? See page 48.
  - Page 45:
    - « This is set up by the network manager. […] During a master time-slot a network manager can send network configuration packages.».
    - What is the network manager? See p 119 (and this is not really a definition).

General comments

- Some elements are not clear and/or require precisions:
  - P78: The “kill”, ACK, wait, BFCT and wait intervals are then **reasonably deterministic in length**, so that no other traffic is flowing when the Data PDU interval starts.
  - P42-43: The traffic generated by SpaceWire FCT is not taken into account. The FCT consumes a part of the bandwidth that cannot be used (and may introduce latency).