Network Management and FDIR for SpaceWire Networks (N-MaSS FDIR)

Astrium Satellites

John Franklin

10th April 2013

All the space you need

ASTRIUM
AN EADS COMPANY

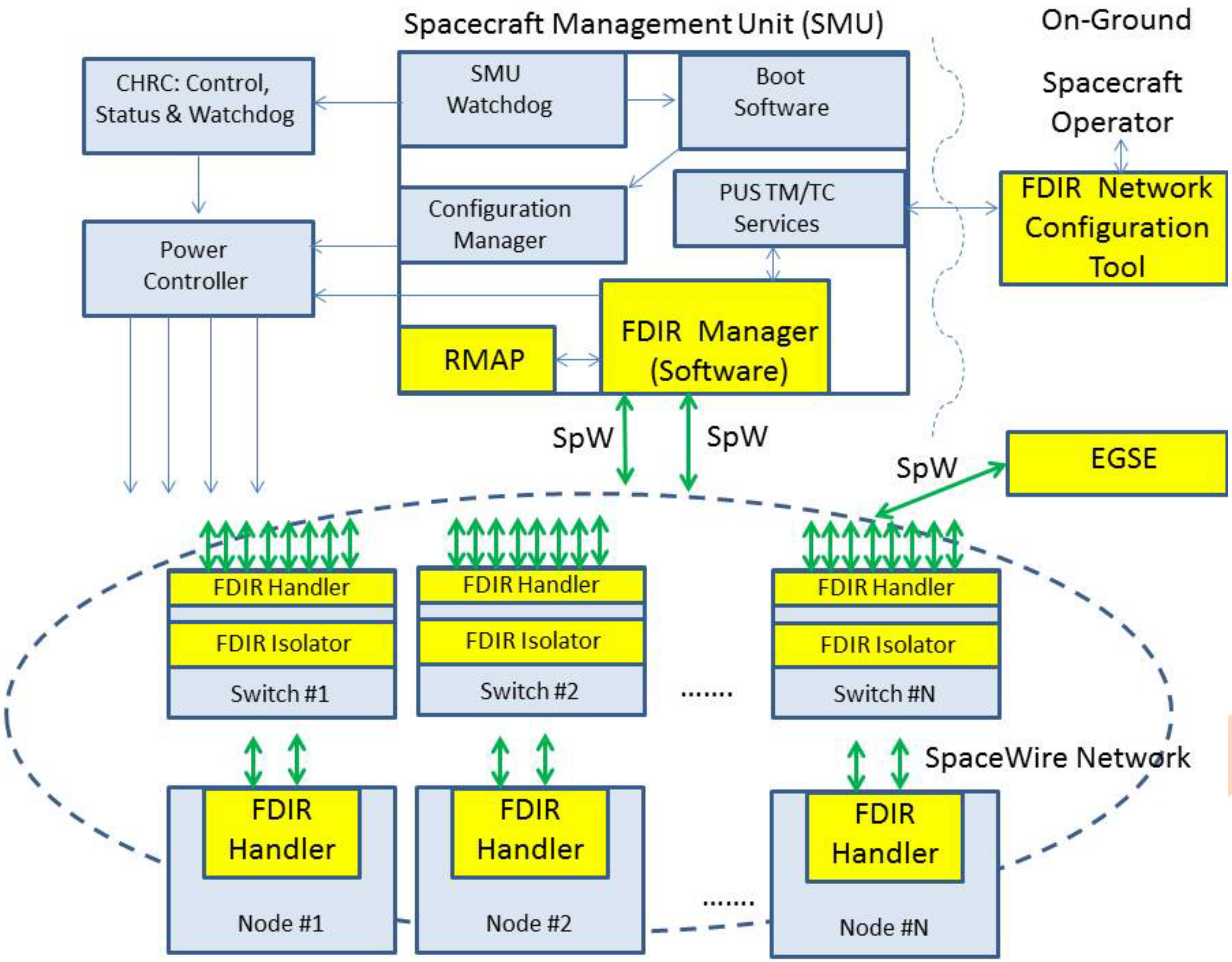
What is N-MaSS FDIR?

- Standardised service suite and protocol, providing autonomous Fault Detection, Isolation and Recovery solution for SpaceWire networks
- N-MaSS manages network topology and configuration, plus node identities and configurations
- N-MaSS FDIR autonomously maintains connectivity and performance of data handling networks in the presence of failures.
- Produce Demonstrator showing FDIR on a network
  - Network topology and scale captures the features of target space missions
  - Simulates the relevant failure mechanisms
  - Demonstrates fault-recovery with reliability, performance, resources
  - Breadboard based on COTS test-equipment hardware, with N-MaSS firmware & software

What is N-MaSS Project?

- ESA-sponsored study started Sep 2012, completing Mar 2014
- Produces draft ECSS Standard for N-MaSS SpW FDIR
- Team is led by Astrium Ltd
  - Responsible for specification & architecture;
  - System integrator; and FDIR Manager Software
- Astrium GmbH
  - Requirements capture from Bepi Colombo mission, and RAMS experience
- 4Links Ltd
  - Design & manufacture of Demonstrator hardware
  - Implementation and integration of N-MaSS firmware
  - Integration of verification system
- Teletel SA
  - Design & manufacture of PVS test-kit showing N-MaSS node in software

N-MaSS System Architecture



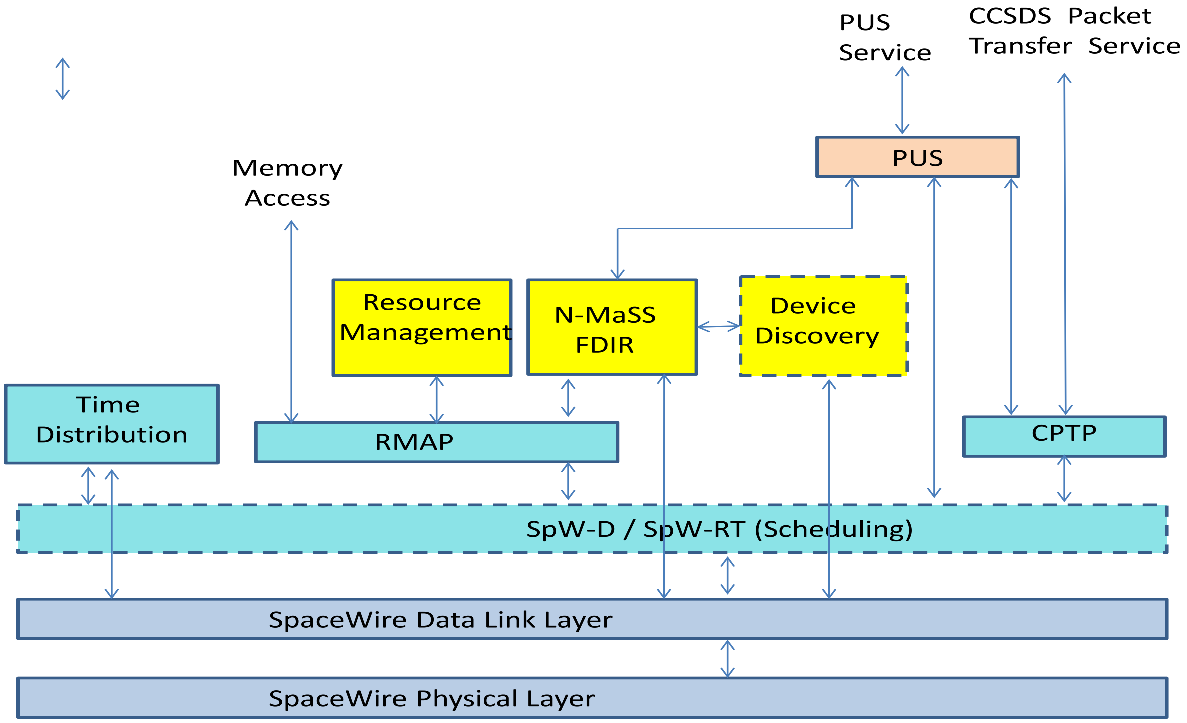
System Level Behaviour

- N-MaSS protocol –
  - Defines the *means*
  - Fully *standardised*
  - Implemented in firmware in Node and Router

- FDIR Manager
  - Defines the *System Level Behaviour*
  - Implemented in software (typ.) in On Board Computer (typ.)
  - Not standardised, but has user requirements e.g. *speed, fault coverage, reliability, telemetry volume, resource usage*

Context of N-MaSS

- Defined at the network layer to achieve efficient re-use for missions, whilst allowing incorporation of legacy equipment
  - Interwork with Plug and Play, SpW-RT and RMAP



Network Failure Modes Handled

- SpaceWire link failure (disconnection)
- SpaceWire link corruption (too frequent parity-error, or EEP)
- “Babbling idiot”, blocking the network at several layers –
  - Transmitting without flow-control credit
  - Transmitting endless packet
  - Transmitting too many packets
  - Specific support to prevent OBC overload with high packet rate
- Failure of component – switch, node or power-supply
  - Including “silent” failure – transmits NULLs but no data
- Switch configuration error – Routing Table, or other link configuration
  - Single Event Upset or permanent failure.
  - Prevent circulating packets on routing-loops
- Time Code Distribution failure
  - Not distributed to a section of the network
  - Corrupted, or incorrectly acts as a Time Code Master

Performance Needs

- Performance
  - Recovery Time 0.5 -1 seconds usually wanted
  - Can be quicker (5 ms) for command and control applications
  - Only Recovery speed is relevant (not Detection) – except sometimes fast Isolation is wanted which is the Recovery Configuration (Safe Configuration)
  - Determined by scheduling period of messages, & load on Onboard Computer software
- Non-Availability
  - Platform <10 seconds per year; large payload <1min / yr
  - Given the hardware fault reliability rate (FITS), drives the Recovery Time
  - Given sufficient redundancy resource, determines function of FDIR Manager
- Reliability
  - 95% over 5 years => 100 yr MTBF
  - Very conservative link BER = 10^{-12} => typical network one per 10 mins (never seen)
  - Given sufficient redundancy resource, drives specification of FDIR Manager
- Size of network
  - Typically~12 nodes + 6 switches, two hops.
  - Up to 60 nodes, 40 routers, 4-8 hops
  - N-MaSS protocol does not limit, only network loading consideration

Functional Needs

- Redundancy strategy
  - Support of Cold & Hot Redundancy is needed
  - Mostly 2:1, but also M:N
  - Single root-cause fault tolerant; two successive faults; multiple faults with intervention
  - Consider elements that are tied together (shared module or power-supply)

- Network Addressing
  - Logical addressing => reconfiguration of switch routing-table
  - Path addressing => command use of redundant path in node
  - Mixed logical & path addressing
  - Group Adaptive Routing is used for FDIR, not congestion control
  - GAR FDIR supports monitoring physical links, not logical arbitration.

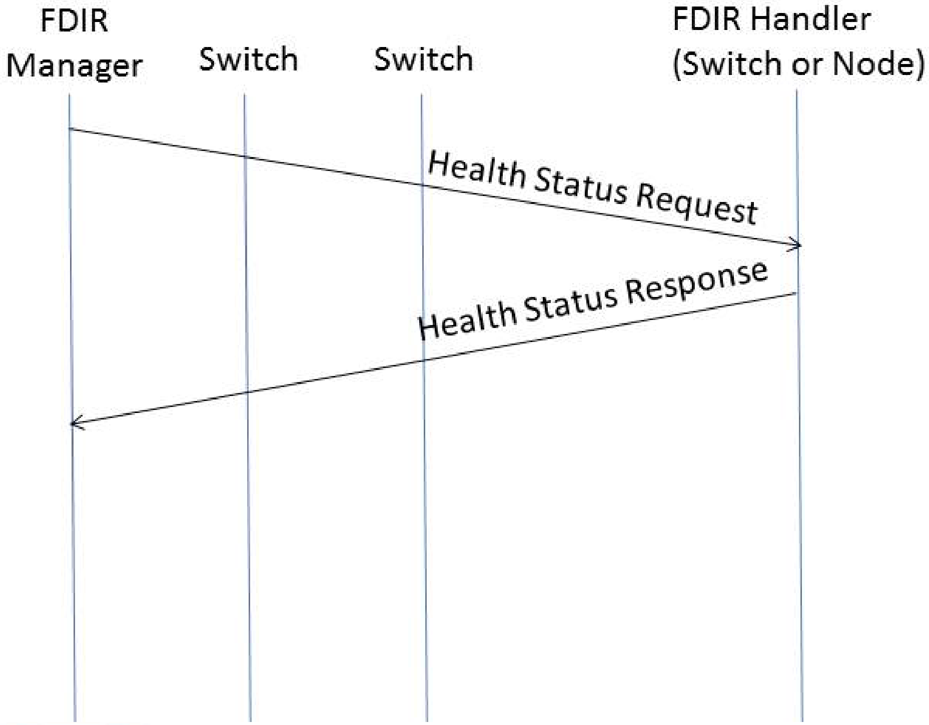
- Level of Autonomy must be configurable
  - Statically determined to give architect / operator confidence & visibility
  - E.g. isolation only rather than recovery
  - Not autonomously swap OBC
  - Configurable to swap C&C links
  - Power-cycling *may* be delegated to OBC Central S/W

Resource Allocation

- Physical footprint
  - FDIR Manager in OBC cyclically scheduled 8-10 Hz; 1 MIPS; 1 MB RAM
  - Reduced capability 0.1 MIPS, 10 kB version wanted by one prime
  - Node IP core must fit easily into FPGA Actel RTAX1000 (300 FF, 600 LUT)
  - Switch IP core should be ~500 FF, 1000 LUT
- Network
  - Network bandwidth load <2% => limits message size & frequency
  - Typical housekeeping telemetry data-rate allowance 50 bps – 10 kbps
  - Statistical Network Health Report
  - +Action Report with full network state and diagnosis (one fault per minute)
- Implementation performance
  - Define “Fast” and “Slow” class of Node for each Recovery Speed need
  - Slow = 25 ms = achievable in hardware or software
  - Fast = 1 ms = achievable in hardware only
  - Switch Configuration & Isolation should be Fast

Failure Detection mechanism

- FDIR Manager verifies network connectivity by periodically pinging Health Status Request messages to each component
- Each component returns a Health Status Response, from FDIR Handler



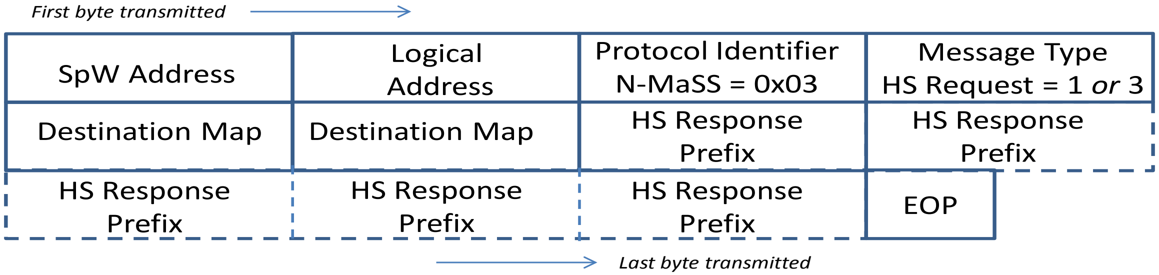
Failure Detection mechanism

- Network health can be determined by the FDIR Manager by
  - Missing HS Responses indicate either failed component or blocked or failed link
  - Delayed HS Responses indicate a blocked or congested link
  - Health flags within HS Response indicate either an intermittent link failure, or a network or node problem detected locally

- FDIR Manager must send HS Request messages
  - To every network component
  - Traverse every link, testing via Path Address
  - Plus every Logical Address (*not* just read-back what the switch thinks it is doing)
  - If a message is lost, repeat at least once before concluding that a link has failed

HS Request / Response formats

- HS Request:
- = HS Req header
- + HS Rsp prefix

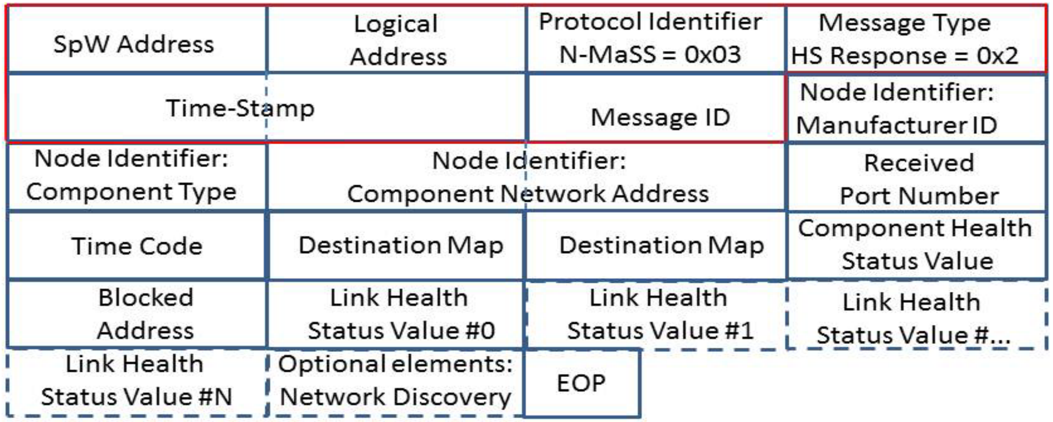


First byte transmitted

SpW Address	Logical Address	Protocol Identifier N-MaSS = 0x03	Message Type HS Request = 1 *or* 3
Destination Map	Destination Map	HS Response Prefix	HS Response Prefix
HS Response Prefix	HS Response Prefix	HS Response Prefix	EOP

Last byte transmitted

- HS Response
- Strips off header
- Appends HS fields
  - No buffering
  - Minimal storage



SpW Address	Logical Address	Protocol Identifier N-MaSS = 0x03	Message Type HS Response = 0x2
Time-Stamp		Message ID	Node Identifier: Manufacturer ID
Node Identifier: Component Type	Node Identifier: Component Network Address		Received Port Number
Time Code	Destination Map	Destination Map	Component Health Status Value
Blocked Address	Link Health Status Value #0	Link Health Status Value #1	Link Health Status Value #...
Link Health Status Value #N	Optional elements: Network Discovery	EOP	

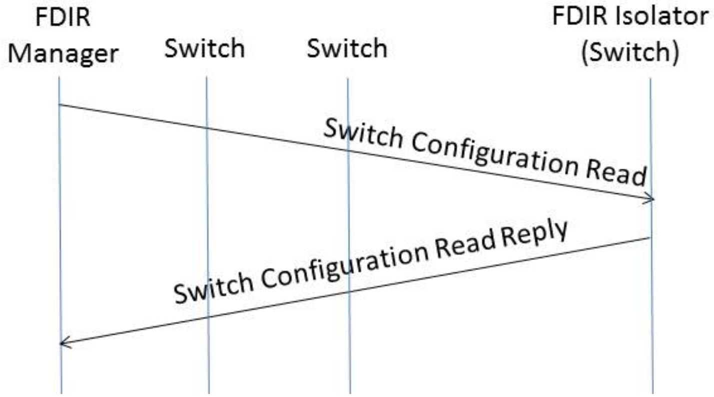
- Multiple SpW messages per route =>high processing load on OBC (ISR)
- Prefix mechanism can daisy-chain between devices, to combine messages

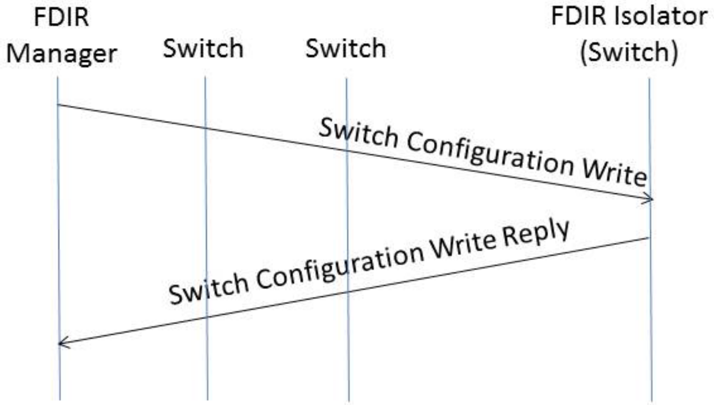
Recovery

- Define Initial Recovery action(s) and Recovery Configuration for each potential Diagnosed Fault
  - Pre-computed, uploaded to FDIR Manager from Network Configuration Tool
  - Execute actions starting from minimum impact; verify effect in Fault Detection mode
  - Operator pre-configures which type of actions and configurations are allowable
- Initial Recovery actions do not permanently change network state –
  - Free a network port by disabling and re-enabling a relevant switch port
  - Refresh the configuration of a switch (single register or full), from secure storage
  - Soft reset a switch or end-point
  - Power-cycle a switch
- Recovery Configurations provide recovery for Permanent faults
  - Swap network route(s) to different link(s): reconfigure routes in switch, or inform node
  - Both hot and cold redundancy are catered for – refresh configuration of components
  - Redundant power-supply swapped for a nominal power-supply
  - Safe Mode Configurations supported to Isolate critical components or routes

Recovery: Reconfiguration

- To recover a switch-configuration upset, protocol to Read and Write configuration must be standardised
  - Use subset of RMAP (reduced resource footprint)
  - Standardise register format for managed functions (e.g. routing table)
- N-MaSS refreshes, but does not manage, non-standardised configuration

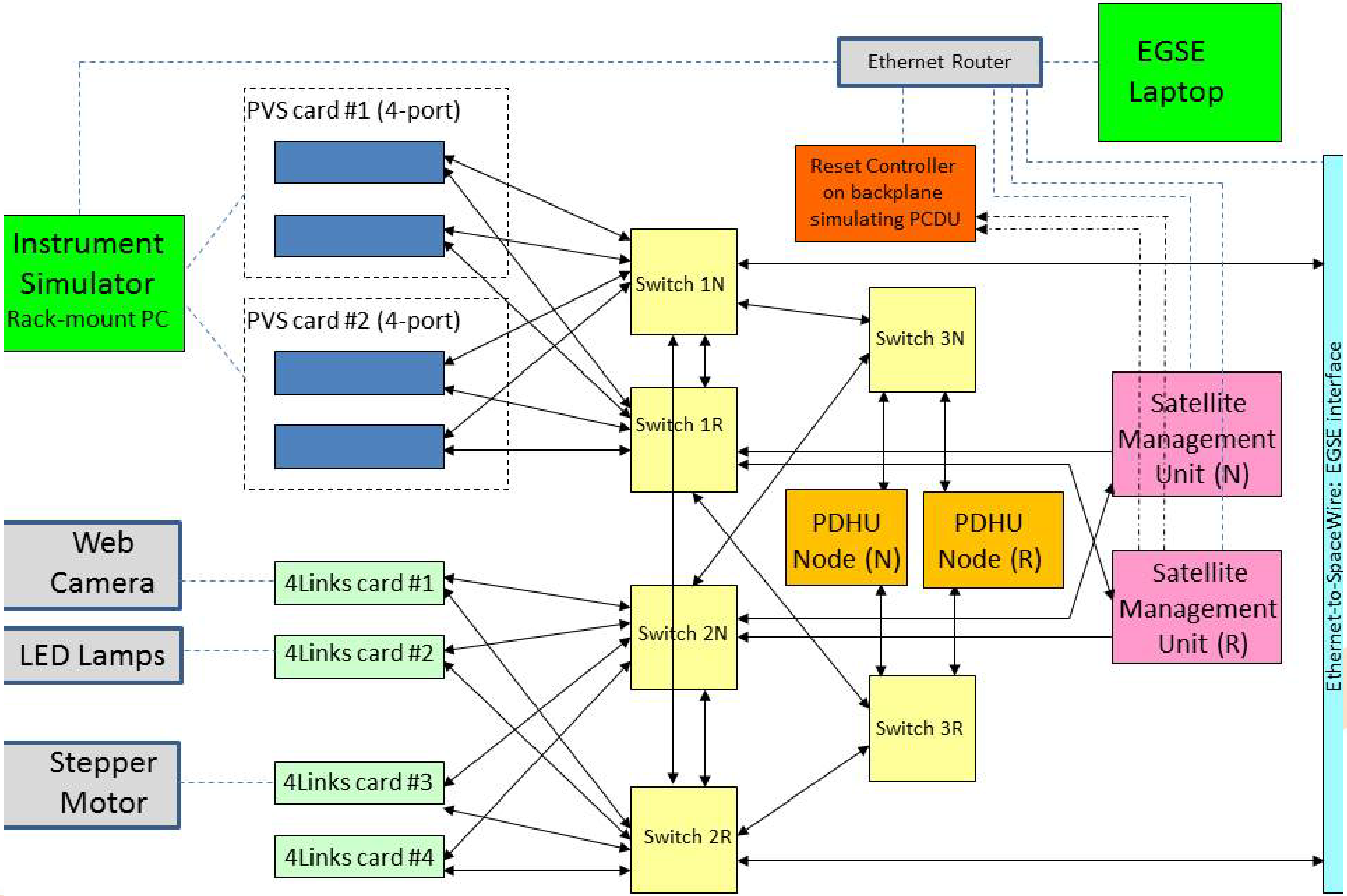




Network Isolation in Switch

- Additional to & Faster than FDIR Manager software.
- Simplifies system behaviour by preventing faults from spreading
- Link timer prevents babbling-idiot nodes from congesting the network
  - *Packet* time-out disconnects link, timeout value configured per port
  - Prevents impact to network Quality of Service.
  - Kills a misbehaving endless packet, not the stalled victims
- Policing of maximum packet rate
  - Protects OBC from overload
  - Throttles babbling idiot sending *too many* packets, that are individually acceptable
- Recovers blockage from routing loops
  - Link timeout prevents stall by discarding packet tail; leaves circulating packet fragment
  - Discard when 3 packets on the same input port & Logical Address within 1 µs

Demonstrator Architectural Design



All the space you need