FAULT TOLERANT SPACEWIRE ROUTING TOPOLOGY AND PROTOCOL

Session: SpaceWire Networks and Protocols

Short Paper

Muhammad Fayyaz and Tanya Vladimirova

Surrey Space Centre, Department of Electronic Engineering, University of Surrey, Guildford, GU2 7XH, UK

E-mail: fayyazrafiq@hotmail.com, t.vladimirova@surrey.ac.uk,

ABSTRACT

This paper is concerned with a fault tolerant routing topology and a protocol for SpaceWire networks on board spacecraft. A fault tolerant routing topology is proposed, which is comprised of cross strapped central SpaceWire router core. The central core is cross strapped in such a way that no single faulty node results in getting down the whole system. In addition, a routing protocol is proposed for the support of dynamic updating of the routing table. The main characteristic of the routing protocol is that any faulty node is immediately isolated from the rest of the system.

1 INTRODUCTION

Space systems require a high degree of reliability, which can be achieved via redundancy. SpaceWire is a full duplex, serial, point to point data communication standard. It is a high speed serial bus with speed limit up to 400Mbp/s and uses low voltage differential signalling (LVDS) for the transmission of data. The SpaceWire standard describes the protocol with respect to physical, signal, character, exchange, packet and network levels [1].

Fault tolerant routing provides redundant paths for routing of packets during the failure of the primary routing node. Group adaptive routing supports link redundancy only, but in case of a failure in any routing node the whole system gets down, which is not acceptable for space missions. In order to enhance the reliability of SpaceWire networks, a fault tolerant routing topology is proposed, which is comprised of cross strapped central SpaceWire router core. The central core is cross strapped in such a way that no single faulty node results in getting down the whole system. In addition, a routing protocol is proposed, which supports dynamic updating of the routing table. The main feature of the routing protocol is that any faulty node is immediately isolated from the rest of the system.

2 FAULT TOLERANT ROUTING TOPOLOGY

A fault tolerant topology scheme using SpaceWire is presented in Figure 1, where each node is considered as dual redundant, i.e. primary and redundant. Table 1 shows the failure mode effects analysis (FMEA) for the fault tolerant routing topology.

Table 1. Failure Mode Effects Analysis of the Fault Tolerant Routing Topology

S. No.	Possible Failure	Effect on the System	Remedy
1	Node to router Link Failure	Loss of Primary Link	Switch to similar node redundant link
2	Node Failure	Loss of Primary Node	Switch to redundant node
3	Router to Router Link Failure	Loss of Primary Link	Switch to redundant link
4	Router Failure	Loss of Primary Router	Switch to redundant router

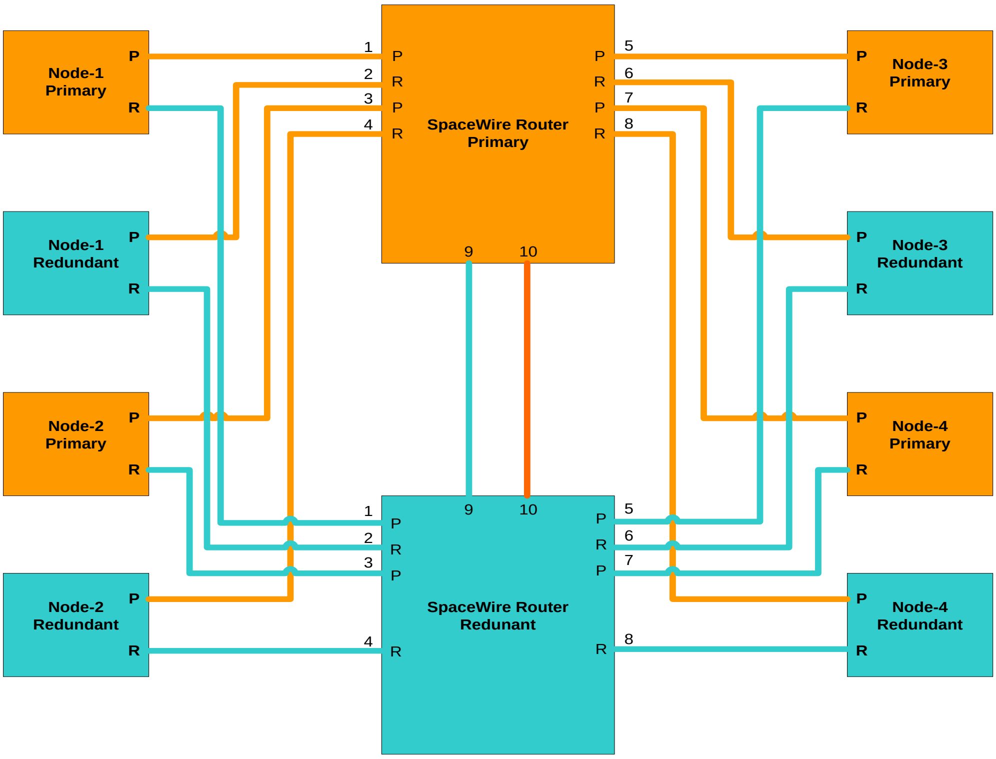

Figure 1. Fault Tolerant Routing Topology

The nodes can be hot redundant or cold redundant. Failure of any hot or cold redundant nodes will not affect the overall system performance. In Figure 2, if a link from node-1 primary to the SpaceWire router primary fails, it will switch to the node-1 redundant link and will route the packets via the redundant router. Similarly if node-1 primary fails, then it will switch to redundant node-1 and will route the packets via the primary router. If the link between the routers fails it will switch to a redundant link. In case of router failure the links between routers and node to router can be used for the exchange of routing information or for the transfer of data packets.

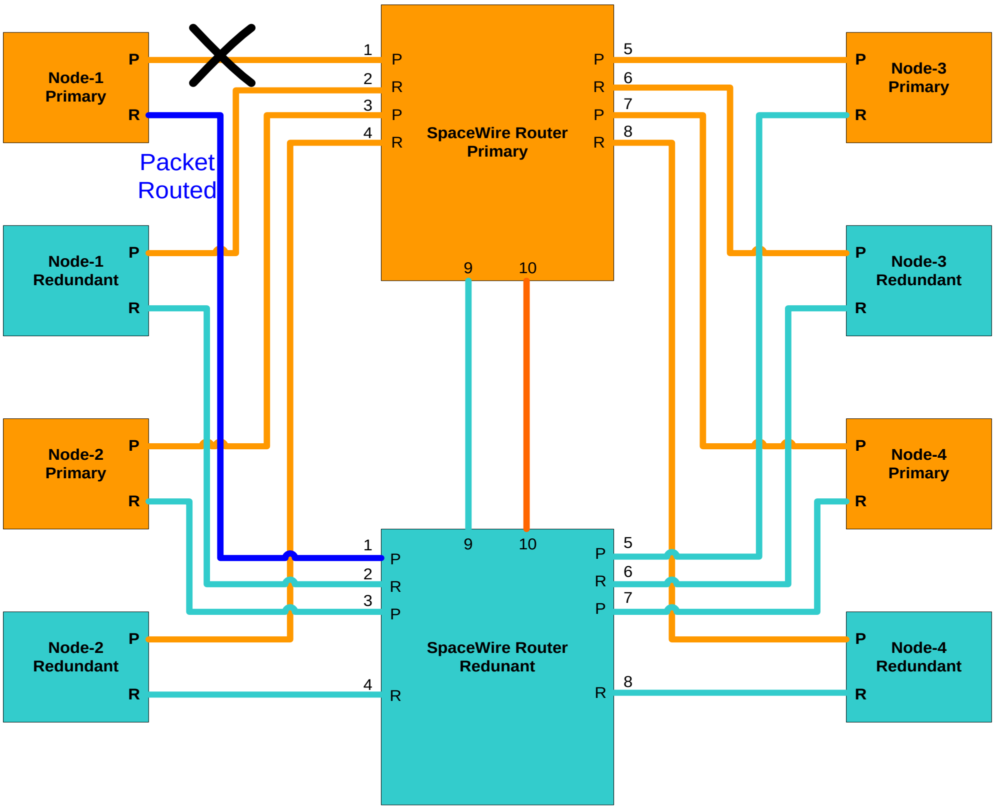

Figure 2. Failure of a Node Link

3 FAULT TOLERANT ROUTING PROTOCOL

In order to support the fault tolerant routing topology presented in the previous section, a fault tolerant routing protocol is required. Table 2 shows the additional message exchange for the fault tolerant routing topology.

Table 2. Fault Tolerant Routing Protocol Keep Alive Messages

Node/Router	Node-1 (P)	Node-1 (R)	Router (P)	Router (R)
Node-1 (P)	No Msg Exchange	No Msg Exchange	Node-1(P) says to Router(P): I am active	Node-1(P) says to Router(P): I am active
Node-1 (R)	No Msg Exchange	No Msg Exchange	Node-1(R) says to Router(R): I am active	Node-1(R) says to Router(R): I am active
Router (P)	Router (P) says to Node-1(P): I am active, Not Busy, Node-1(R) active, Router(R) active.	Router (P) says to Node-1(R): I am active, Not Busy, Node-1(P) active, Router(R) active.	No Msg Exchange	Router (P) says to Router(R): I am active, following links available or busy or faulty.
Router (R)	Router (R) says to Node-1(P): I am active, Not Busy, Node-1(R) active, Router (P) active.	Router (R) says to Node-1(R): I am active, Not Busy, Node-1(P) active, Router (P) active.	Router (R) says to Router (P): I am active, following links available or busy or faulty.	No Msg Exchange

There are mainly three types of messages: node to router, router to node (reply message) and router to router. The formats of these messages are designed in such a way that there is no additional overhead on the network performance. For the support of these packets at network layer, a source logical address is used. Table 2 presents the partial routing table of the primary router. In case of a link failure between the primary router and the primary node-1 no keep-alive messages are exchanged between them and the router considers this node as a dead node. It also informs the redundant node with logical address 10 that the primary node is dead. Now the redundant node starts sending packets to others nodes via the primary router. If the primary node-1 is up again, then the router updates the entry status from down to active and restores the communication with the primary node-1.

Table 3. Partial Routing Table for the Primary Router

Source Logical Address	Destination Logical Address	Out port	Priority	Status
5	15	3,9,10	High	Down
10			Low	Active
5	20	4,9.10	High	Down
10			Low	Active
5	25	5,9,10	High	Down
10			Low	Active
5	30	6,9,10	High	Down
10			Low	Active
5	35	7,9,10	High	Down
10			Low	Active
5	40	8,9,10	High	Down
10			Low	Active

4 Conclusions

The presented fault tolerant routing topology and its protocol fulfil the requirement of space systems. The fault tolerant architecture considered here is for two routers and eight nodes but it can be extended for any numbers of nodes. Future work will involve the implementation of this conceptual design.

5 References

1. European Corporation for Space Standardization, “Space Engineering SpaceWire-Links, nodes, routers and networks”, 31 July 2008.