SpaceWire-Based
Fault Tolerant Architecture for Redundant Systems

Doug Cornelsen / Space Systems Group / Magellan Winnipeg

MAPLD 2008

Introduction

Magellan Winnipeg has designed a dual redundant C&DH subsystem for use on its MAC-200 SmallSAT bus. The MAC-200 bus was developed as part of the Canadian Space Agency Small Satellite program.

The C&DH is built upon the design developed for Magellans's MAC-100 satellite bus currently being utilized on the SCISAT mission. The MAC-200 C&DH is comprised of a cPCI backplane, power supply module, CPU card and a number of peripheral cards. Configuration and selection of cards is dependent on mission requirements.

The goal of this project was to enhance the design to allow for greater flexibility in the selection of options for reconfiguration. The current redundant C&DH system provides fault monitoring and management to automatically reconfigure the system in the event of a fault. The areas of investigation considered were:

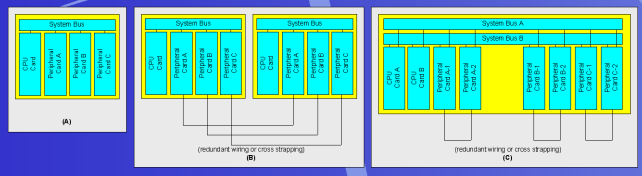
(1) Enhancement of subsystem fault tolerance and reliability

(2) Reduction of the granularity of the system such that an autonomous switch of C&DH units is not necessary in the event of a card fault.

(3) Provision for a higher speed link for increased control and monitoring

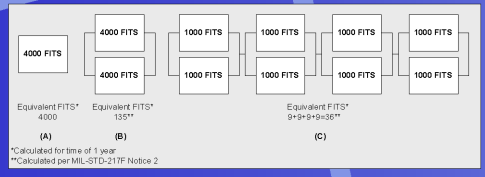
Fault Tolerance and Reliability Background

Three common architectures for C&DH's include single string (A), dual redundant (B) and internally redundant (C). Internally redundant is the most fault tolerant/reliable but most difficult to design to incorporate standards like cPCI. An internally redundant architecture could also utilize switches/routers instead of redundant buses.



Equivalent Failures In Time (FIT) Calculations

Based on results of calculations below architecture (C) provides the greatest reliability. This type of system most likely also has the highest complexity and cost.



Options for Enhancing Architecture (B)

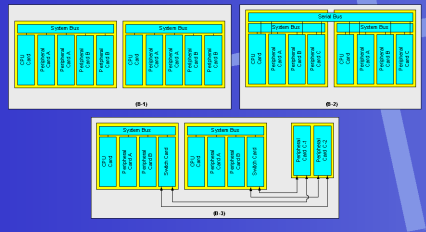
Initially, the choice to implement architecture (B) was made primarily because it provided reliability and development costs inline with the SmallSAT program budgets. Additionally, design of dual redundant cPCI based C&DH system provides for the availability of many "off the shelf" cards.

A few options available to enhance this architecture are:

(1) Add redundant cards inside each C&DH
- -Increased costs and power, utilizes precious backplane slots, but relatively simple

(2) Add redundant link to peripheral cards through alternate protocol (ie SpaceWire, CAN bus, etc) and optionally provide individual card power control
- -May require non standard additions to back plane or additional router/switch components, additional power and cross strapping considerations

(3) Add redundant units outside C&DH unit and connect with standard protocol (ie SpaceWire, CAN bus)



Design Aspects

(B-2) Individual power distribution for each card is the most complex aspect of the system when hot redundancy is not utilized

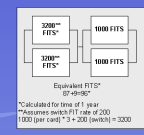
(B-2) Can be done with CAN bus, but maximum data rate 1 Mbps

(B-3) SpaceWire most attractive protocol for this configuration (high speed well defined high layer protocols for register reads and writes)

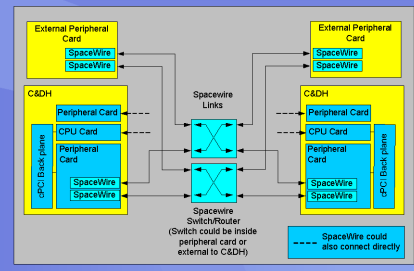
Failure Rate Improvement (B-2)

-Effective FIT rate reduction from 135 to 96 when making one of the cards available to either C&DH through SpaceWire

-This architecture can be used to provide a reliability enhancement while still allowing for the use of standard protocols



Example System



Benefits

-Improved reliability as compared to two fully redundant C&DH units

-Reduced granularity of system allows autonomous fault recovery the ability to recover with less impact in certain situations

-Minimal system modification (cost) as compared to other approaches

-Allows for use of standard cPCI cards (CPU, mass memory, etc)

-Allows for greater scalability of overall system as no longer limited by 8 slot cPCI backplane

System Prototype Architecture

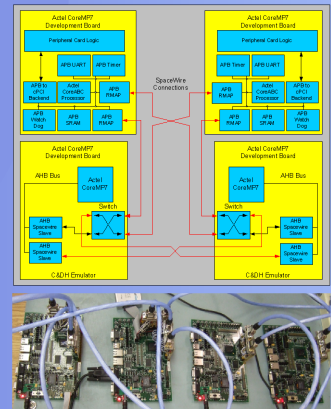
-System prototype was created to emulate operation of fundamental components and demonstrate autonomous system reconfiguration

-Actel CoreMP7 development board was chosen for implementation

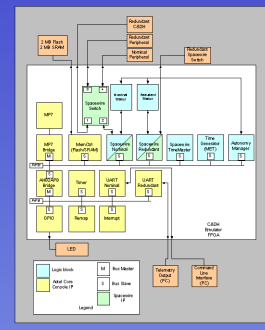
-Desire was to have very small SpaceWire RMAP component to provide register read and write capability

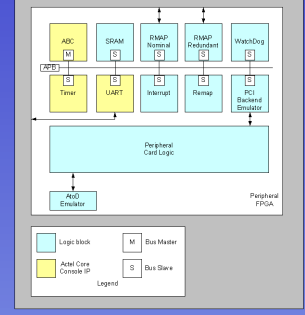
-SpaceWire RMAP interface was created to connect to Actel CoreABC processor

-CoreABC processor was chosen because it can be utilized in RTAX design an provides RMAP interface control in a small logic foot print



Prototype FPGA Designs





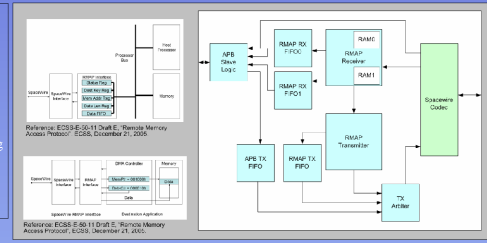
SpaceWire RMAP Options

-Two main options for RMAP interface design

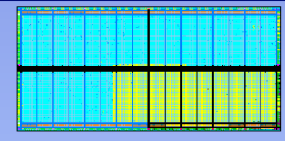
-Implemented RMAP interface with dual data FIFOs instead of DMA

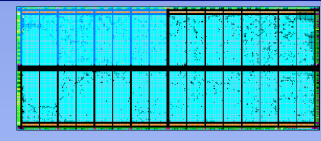
-Primarily because only internal SRAM used for design

-No point in implementing DMA with the small amount of packet buffering available from internal SRAM



Design Layouts





Lessons Learned

(1) When testing the C&DH emulator design it became clear DMA controller would have greatly increased SpaceWire interface performance. Design was implemented with transmit and receive buffers without DMA.

(2) When utilizing a SpaceWire switch in a FPGA a large number clock buffers can be used in the clock recovery blocks. Potential use of local clock buffers for SpaceWire clock recovery should be investigated (ie RTAX).

(3) Debugging of CoreABC design was very effective with Identify AE tool. Debugging considerations should be made for RTAX design.

(4) When considering an CoreABC design source code licensing would be the preferable solution. Additions to processor could then be made.

(5) Link status feedback from switch is extremely important for status monitoring

Conclusions

-Fault recovery capabilities of architecture were demonstrated with prototype

-Applying proposed architecture to current C&DH results in 22% reduction in FITS when two peripheral cards are accessed through the redundant SpaceWire architecture

-Reliability and system flexibility enhancements indicate architecture should be developed further. In particular, power distribution considerations and alternatives should be investigated.

-CoreABC RMAP interface provided an effective control interface for peripheral card. Advantage of this interface is a much smaller logic foot print as compared to other processor based solutions.

-Plan is to pursue this development path for the C&DH subsystem

Contact Information

Doug Cornelsen
Magellan Winnipeg
660 Berry Street, P.O. Box 874
Winnipeg, Manitoba, CANADA
R3C 2S4
204 775-8331 ext 3174
doug.cornelsen@magellan.aero