

DUAL REDUNDANT FAULT TOLERANT ELECTRONIC SYSTEM AND METHOD

FIELD OF INVENTION

- 5 Embodiments of the present invention relate to the field of fault tolerant electronic components for use in various applications, particularly in avionics systems.

BACKGROUND

- 10 In various applications, computer systems are required to function over a wide range of conditions. In some systems, fault tolerance may be provided so that a failure in a single component will not result in a failure of the entire system. For example, in avionics applications, system reliability is critical for survivability and operational success.
- 15 One method of achieving fault tolerance in such systems is to provide a dual redundant system. The conventional approach in implementing a dual redundant architecture provides two identical avionics equipment packages in the system. For example, two separate components capable of performing identical functions can be used to provide fault tolerance. If the first component fails, the second component can automatically
- 20 take over the requisite functions. Modern day avionics equipment packages can perform many functions, have a faster processor speed, and provide higher throughput and/or bandwidth capabilities. In these systems, each piece of equipment must be designed to handle maximum power requirements, although at any one time, one of the redundant packages is operating at full capacity, whereas the other is on standby. Unfortunately,
- 25 such systems have some drawbacks and limitations.

- First, particularly with respect to avionics equipment, space within the cabin of the aircraft may be extremely limited. Providing dual components uses a great deal of the space available in the aircraft. Additionally, each of these components must be
- 30 connected to the overall system. These connections require large amounts of cabling, which further reduce available space.

Additionally, all of the redundant components, as well as the cables required to connect them, increase the ground weight of the aircraft. This increased weight directly correlates to increased fuel usage when operating the aircraft.

- 5 Finally, providing redundant systems greatly increases the costs associated with creating such systems. Each individual component must be purchased in duplicate. Similarly, all of the required connections and cabling must be purchased in duplicate.

10 It would therefore be a great advantage in the art if a system and/or method could be developed to overcome one or more of the above-mentioned problems.

SUMMARY

15 One aspect of the present invention provides a fault tolerant system for electronic components, the system comprising: a first Versa Module Eurocard (VME) module located within a housing; and a second Versa Module Eurocard (VME) module located within said housing; wherein said first and second VME modules are electrically isolated from each other and are capable of providing identical VME functionality.

20

In alternate embodiments, each of said first and second modules may be located on a single backplane. Each of the first and second modules may further include: a plurality of card slots; a CPU card in one of said plurality of card slots; and an input/output (I/O) card in one of said card slots. Each of the modules may also
25 include at least one input/output (I/O) channel providing an external connection to said system, said I/O channel being electrically connected to a plurality of user defined I/O connections on each of said VME modules.

30 In some embodiments, a fault in said first VME module may be automatically detected, and, when said fault is detected, control of said system may be automatically switched to said second VME module via a control command provided on one of said I/O connections.

In alternate embodiments, the input/output channel may be provided via a single connector on said housing. The user defined input/output connections may be selected from a group consisting of a transistor to transistor logic (TTL) discrete in Master ID, a TTL discrete in System Handover in, a TTL discrete out system handover out, and a communications link between said first and second backplanes.

In further embodiments, the electronic component may be part of an avionics system. The system may also include an electromagnetic interference filter electrically connected to said I/O channel. Each of said first and second VME modules may conform to a 64 bit bus VMEbus standard.

An alternate aspect of the present invention provides a method for providing fault tolerance for electronic components, the method comprising the steps of: providing a first Versa Module Eurocard (VME) module located within a housing; and providing a second Versa Module Eurocard (VME) module located within said housing; wherein said first and second VME modules are electrically isolated from each other and are capable of providing identical VME functionality.

In alternate embodiments, each of the first and second modules may be located on a single backplane. Each of said first and second modules may further include: a plurality of card slots; a CPU card in one of said plurality of card slots; and an input/output (I/O) card in one of said card slots.

In other embodiments, each of said modules may further include at least one input/output (I/O) channel that is electrically connected to a plurality of user defined I/O connections on each of said VME modules; and said method further comprises providing an external connection to said system over said channel.

In further embodiments, the method may also include the steps of: detecting a fault in said first VME module and, when said fault is detected; automatically switching control of said system to said second VME module via a control command provided on one of said I/O connections.

Alternate embodiments of the method may also include the steps of selecting said user defined input/output connections from a group consisting of a transistor to transistor logic (TTL) discrete in Master ID, a TTL discrete in System Handover in, a TTL discrete out system handover out, and a communications link between said first
5 and second backplanes.

BRIEF DESCRIPTION OF THE DRAWINGS

10 Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Figure 1 illustrates a schematic view of one embodiment of a fault tolerant system
15 according to the present invention;

Figure 2 is a flow chart illustrating one method of implementing fault tolerance in the system of Figure 1;

20 Figure 3 is a flow chart illustrating additional steps in the flow chart of Figure 2; and

Figure 4 is a flow chart illustrating further additional steps in the flow chart of Figure 2.

25

DETAILED DESCRIPTION

Figure 1 illustrates a schematic view of one embodiment of a fault tolerant system, designated generally as reference numeral 100, according to the present invention.
30 In one embodiment, the system 100 may be implemented using, by way of example and not limitation, a Versa Module Eurocard bus (VMEbus) architecture. In a preferred embodiment, the system 100 may be implemented using a VME64x bus architecture. However, it is understood that the embodiments of the present

invention may be implemented using other bus architectures and other bus widths, and that the discussion of VMEbus systems is provided by way of example only.

In general terms, a bus is a subsystem that transfers data between computer components inside a computer or between computers. The VMEbus standard outlines the specific configuration of the cards/pins that provide the input/output functions to the card. By way of example and not limitation, the VME bus standard may comply with ANSI/IEEE Std. 1014-1987, ANSI/VITA 1-1994, or other standards known to those of skill in the art. As stated above, other standards may also be used.

The system 100 includes a first VMEbus module 110 and a second VMEbus module 150. Each of the VMEbus modules 110, 150 may contain one or more VME card slots (not shown) used to connect one or more interface cards to each of the backplanes 110, 150. In the embodiment illustrated in Figure 1, VMEbus module 110 may include a central processing unit (CPU) card 115, a video card 120, and an input/output (I/O) interface card 125. Similarly, VMEbus module 150 may include a central processing unit (CPU) card 155, a video card 160, and an input/output (I/O) interface card 165. It is understood that a larger or smaller number of cards, each having a corresponding slot on the modules 110, 150, may be used as desired.

In the system 100, VMEbus module 110 may be considered the primary module, while VMEbus module 150 may be considered the secondary module. It is understood that the reverse may also be true. In a preferred embodiment, each of the modules 110, 150 will have an identical configuration of VME card slots and interface cards to provide a dual redundant fault tolerant system 100.

In another preferred embodiment, each of the VMEbus modules 110, 150 may form part of a single backplane 102. However, it is understood that two separate VME modules 110, 150 may also be provided in a single enclosure or chassis as desired to implement the embodiments of the system 100.

In one embodiment, the system 100 may also include an electro-magnetic filter (EMI) board 130. The EMI filter board 130 may include one or more external connectors 132 that provide various electrical and/or data signals to the system 100.

For example, when using a VMEbus system 100, circular or other types of connectors having two sets of wires may be used to connect the system 100 to other components. While the embodiment of the system 100 shown in Figure 1 illustrates the external connectors 132 being associated with the EMI filter board 130, it is understood that alternate connection methods may also be used.

Data may be routed to/from each of the modules 110, 150 through the external connector(s) 132 along data path 134. In order to provide for fault tolerance for the system 100, data path 134 may be split into data paths 134a and 134b. Data path 134a may be routed through an electromagnetic interference (EMI) data filter 136 to the first module 110, and consequently to one or more of the cards 115, 120, 125. Similarly, data path 134b may be routed through an electromagnetic interference (EMI) data filter 137 to the second module 150, and consequently to one or more of the cards 155, 160, 165. This will be discussed in more detail below with reference to Figures 2-4. The external connectors 132 may include any type of signal connection that may be useful in transferring data to/from the modules 110, 150. By way of example and not limitation, the connectors may include any type of circular or rectangular connector, and the signal connections may include graphics signals, analogue signals, digital signals, etc.

Each of the modules 110, 150 may also contain internal circuitry (not shown) providing connections between the modules 110, 150 and the various cards 115, 120, 125, 155, 160, 165 respectively. These connections are illustrated in system 100 as connection 140 for module 110, and connection 170 for module 150. The specific design of the modules 110, 150 will be dependent on the application of the system 100. In the present embodiment, the modules 110, 150 may conform to the VMEbus64x specification.

System 100 may also include a power input 180. Power input 180 may be split into input lines 180a and 180b. Each of the input lines 180a, 180b may have a power filter 181, 182 respectively. Filtered power from lines 180a, 180b, may be directed into a dual output power supply 184. Power supply 184 may then be used to independently power module 110 using power line 186, and module 150 using power line 188. In some embodiments, as the power supply to the modules 110, 150 is usually of high reliability,

the power supply functions may not need to be dual redundant. In this embodiment, a mechanism may be required such that, in the event a failure occurs, for example a short circuit occurs on the supply output 186 to one module 110, this does not impact the other module 150, which still remains functional. For example, this may be accomplished by using a current-limiting device in each of the power supply outputs 186, 188. An overcurrent or short-circuit circuit fault condition on one output would then be contained by the current-limiting device, and therefore would not cause a disturbance to the other output.

10 In the embodiment of system 100 illustrated in Figure 1, the power supply 184 may be a single module with dual outputs 186, 188. Each output 186, 188 may have a protection current limiting feature such that a fault on one output would not affect the other. Each module 110, 150 may also have an electrical ground 189a, 189b, respectively. In alternate embodiments of the system 100, two different power sources may also be used.

To address the space problems discussed above, the system 100 may provide a dual redundant VME Embedded System that includes a first and second VMEbus module 110, 150 on a monolithic backplane 102, or as dual modules 110, 150, in a single enclosure or chassis. In this embodiment of the system 100, the various VMEbus signals; namely the data transfer bus, arbitration bus, priority bus and the utility bus of each system are electrically isolated from each other. This system 100 provides redundancy and fault tolerance such that a fault on VMEbus module 110 will not affect the VMEbus module 150, and vice-versa.

25 The VMEbus standard provides for dedicated user input/output pins on the control bus. These pins allow embodiments of the present invention, using appropriate software commands, to effect a seamless transition from, for example, the VMEbus module 110 to the VMEbus module 150 when a fault condition is detected in VMEbus module 110.

30 One example of the commands that may be generated is shown in Table 1, and discussed with reference to Figures 2-4 below.

S/N	Hardware Interface/Signal Name	Function
1	TTL Discrete In / Master ID	To determine if the System is a Master or Slave. This discrete is an input to the CPU card.
2	TTL Discrete In / System Handover In	Read by the System Slave CPU card to determine if the System Master is ready to handover the control.
3	TTL Discrete Out / System Handover Out	Output from the System Master to indicate that it is ready to handover the control to the System Slave.
4	Ethernet or RS422 I/O / Comms1 and Comms 2	Used to pass data from System Master to System Slave.

TABLE 1

- 5 Figure 2 is a flow chart illustrating one method, designated generally as reference numeral 200, of implementing fault tolerance in the system 100 of Figure 1. Figure 3 is a flow chart illustrating additional steps in the flow chart of Figure 2. Figure 4 is a flow chart illustrating further additional steps in the flow chart of Figure 2. The method 200 provides a foundation for a computer algorithm that may be
- 10 programmed, by way of example and not limitation, into the CPUs 115, 155 to implement the control features that are discussed below. In alternate embodiments, the algorithm may be programmed into an external device. This will be discussed in more detail below.
- 15 With continuing reference to Figures 1-4, and Table 1 above, the method 200 begins with the hardware and kernel installation as shown with reference numeral 202. Next, a power on test is performed as shown with reference numeral 204. The first CPU card 115 on the first module 110 then checks the Master ID signal to determine the default Master/Slave status for the card 115, as shown with reference numeral
- 20 206. As shown in Table 1, the system ID signal, identified as the Transistor-Transistor Logic (TTL) Discrete In / Master ID may be sent on line 1, To determine if the CPU 115 is currently identified as a Master or Slave. This discrete is an input to the CPU card. In one embodiment, this input is provided from the backplane. Alternately, the input may be provided by an external apparatus in, for example, a larger avionics
- 25 system.

The CPU card 115 then establishes communication with the CPU card 155 on the other module 150 to determine its current Master/Slave status, as shown with reference numeral 208. This communication may also be effected using line 1 on the CPU card 155. Based on the data received and the default status, the first CPU
5 card 115 then makes a determination as to its required status, as shown with reference numeral 210.

If the required status of the CPU 115 is determined to be that of Master, as shown with reference numeral 212, the next step is to determine if the CPU card 155 on
10 module 150 is in control, as shown with reference numeral 214. If the CPU card 155 is not in control, CPU 115 will then set its status to master, as shown with reference numeral 216. If the CPU 155 is in control, the next step is to take control, as shown with reference numeral 218, then set the status of CPU 115 to Master (step 216).

15 If the required status of the CPU 115 is determined to be that of Slave, as shown with reference numeral 212, the next step is to determine if the CPU card 155 on module 150 is in control, as shown with reference numeral 220. If the CPU card 155 is in control, the next step is to set the status of CPU card 115 to slave, as shown with reference numeral 222. If the CPU card 155 is not in control, the next step is to
20 take control, and set the status of CPU 155 to master, as shown with reference numeral 224.

Figures 3 and 4 provide a flow chart indicating one embodiment of a method by which the designation and/or the handover of the CPU cards 115, 155 as Master
25 and Slave may be accomplished. Figure 3 illustrates a flow chart of one method, designated generally as reference numeral 240, for the current Master CPU to hand over control to the current slave CPU. Similarly, Figure 4 illustrates a flow chart of one method, designated generally as reference numeral 250, for the current Slave CPU to accept control from the current Master CPU.

30

Whichever CPU 115, 155 is currently the Master sends a handover command to the slave, as shown with reference numeral 242. The current Slave receives and acknowledges the handover command, as shown with reference numeral 252.

The current Master CPU then provides an output signal to indicate that it is ready to hand over control to the Slave, as shown with reference numeral 244. This may be accomplished, for example, using I/O line 3, TTL Discrete Out / System Handover Out, which provides Output from the System Master to indicate that it is ready to handover the control to the System Slave. This signal may then be read by the current slave CPU, as shown with reference numeral 254. In this embodiment, the output signal from I/O line 3 on the current Master is sent as an input signal on I/O line 2, TTL Discrete In/ System Handover In, of the current Slave, as shown in Table 1. The current Master CPU then sets its status as slave, as shown with reference numeral 246. Similarly, the current Slave CPU then sets its status to Master, as shown with reference numeral 256.

In the embodiment of the present invention illustrated in Figures 2-4, Figure 2 shows one method for determining the Master/Slave arrangement during the power-on sequence. In the event that the default allocated master is unable to take control, the default allocated slave will take control instead. Figures 3 and 4 show the case where both cards are operating initially and then there is a handover. In this embodiment, the master is initially in control, and the handoff may be executed as described. It is understood that various methods may be used to determine which CPU card 115, 155 is the Master, and which is the Slave. By way of example and not limitation, the current Master may detect that it has a problem, and then initiate the control commands, informing the slave to take control. Alternately, the current Slave may detect a problem with the current Master, and initiate the control commands, instructing the Master to relinquish control. In other embodiments, external equipment, such as may be associated with a larger avionics systems package, may detect that the Master has a problem and initiate instructions to the Master and/or Slave to perform the handover sequence.

In some embodiments, the fault detection capabilities discussed above may be performed by external hardware or software modules by way of the signal lines 134, 134a, and 134b. In alternate embodiments, fault detection may be accomplished using, for example, built-in test (BIT) circuitry located on the VME modules 110, 150. The BIT circuitry may be provided as part of one or more of the VME specifications discussed above. The BIT circuitry may be capable of monitoring various functions of the VME

modules 110, 150, as well as functions associated with the various interface cards 115, 120, 125, 155, 160, and/or 165. By way of example and not limitation, the BIT circuitry may be capable of monitoring and detecting a fault status for both processing and I/O functions of the modules and associated cards. In one example implementation, an RS422 receiver can be provided to monitor an RS422 transmitter output by means of a technique called "signal wraparound". It is understood that other fault detection systems and methods may be employed for use in embodiments of the system 100.

Additional communication between the CPU 115 and CPU 155 may be accomplished using I/O line 4. In embodiments of the present invention, I/O line 4 may use, by way of example and not limitation, Ethernet channels, RS422 I/O channels, MIL-STD-1553 channels, Comms 1 and Comms 2, or other communications interfaces associated with the respective modules 110, 150. For data synchronization, each of the two modules 110, 150 may have serial high-speed busses interconnected between them to ensure that both modules maintain current data. Using this system, when a handover/takeover is executed, it may be seamless and transparent to the overall system user. For example, in avionics applications, embodiments of the system 100, as implemented using the method 200 of Figures 2-4, provide continuous system functionality for the avionics systems of the aircraft should a fault occur.

User I/O pins are allocated (but not defined) by the various VME bus specifications discussed above. In some embodiments, the user I/O pins may be connected to the various interface cards 115, 120, 125, 155, 160, 165 located on the VME modules 110, 150, without being directly connected to the VME bus signals. For example, the user I/O pins may be connected from the VME modules 110, 150, via the backplane 102, to either the external connectors 134, or to other modules. The I/O pins may be used to transmit and receive analogue, digital, video or any other signal type. It is understood that the specific configuration for the I/O signal channels shown in Table 1 and discussed above is provided by way of example only. The I/O lines may be defined by the user depending on the specific interface required for any particular application.

As discussed above, the User I/O signal interfaces 1-4 are designed to operate in a dual redundant mode with a blocking mechanism, whereby a fault on the Main I/O does not affect the Backup I/O signal. By way of example and not limitation, this blocking

mechanism may be achieved using driver devices that are capable of being disabled through software control. When disabled, such a driver is effectively in a high-impedance state that does not affect the operation of another driver (similar but enabled) that is connected to the same output line. By enabling the Master card's output drivers and disabling the Slave's, the Slave's drivers will not affect operation of the system 100, or other avionics components to which the system 100 is connected. In alternate embodiments, when using output drivers that do not have this enable/disable capability, additional circuitry can be added to the modules 110, 150 or cards 115, 120, 125, 155, 160, 165 to achieve a similar functionality.

In a preferred embodiment using VMEbus backplanes 110, 150, the system 100 provides not only fault tolerance related to VME functions, it also provides redundancy for the User IO lines, in order to maintain full system functionality at all times. The particular design of the User defined Input/Output circuitry, and the way that these signals are combined for external functionality in, for example, a larger avionics system of which the system 100 is one component, allows full functionality at the larger system level to be maintained even when there is a fault on one of the VME modules. In this embodiment, the I/O signals from the Master and Slave cards may be combined by direct connection. Alternately, filter components may be used to provide electromagnetic compatibility within the system 100. The enable/disable aspect of the module design (discussed above) allows the direct connection of output signals which would otherwise require external selector switches. This direct connection reduces the number of external signal pins required.

Embodiments of the system 100 provide several advantages over the prior art. First, using embodiments of the system 100 allows an avionics equipment manufacturer or operator to reduce the size of the required avionics components in the aircraft. As outlined in the background, in a conventional dual redundant system, 2 identical avionics equipment packages would be put onto the aircraft. With dual redundancy housed in one avionics equipment package, there can be space savings derived from a smaller mechanical enclosure, the use of a single power supply with dual outputs, and fewer or smaller connectors.

Additionally, with the Main and Backup VMEbus modules designed in a single enclosure, the total power required, and the thermal management considerations associated with power usage, need only take into account the Main system operating at full capacity and the Backup system on standby. In contrast, each of the two identical avionics equipment
5 packages provided in the prior art must be designed to operate at maximum power. Since the interconnection signals may be routed on the monolithic backplane in the chassis, and the dual redundant I/O signal uses a single connector pin, this enables a smaller connector or fewer connectors to be designed on the mechanical enclosure. This provides for additional space savings using the system 100.

10

The reduced size associated with the embodiments of the present system also provides weight savings for the overall package. Similarly, the elimination of interconnecting cables required for the 2 identical avionics systems of the prior art provides further weight savings. In addition, the interconnections between the 2 modules may be
15 hardwired on a single backplane. Common signals such as Power and Ground need only be routed to a single system. This reduces the amount of cables installed in the aircraft, which reduces the weight. The use of fewer connector pins or smaller connectors also helps to reduce the weight.

20

Embodiments of the present invention also provide for cost savings, as only one chassis containing both VMEbus modules is required. In addition, since the handover and serial communication signals between the 2 modules reside in the same chassis, there will be cost savings associated with a reduction in the number of connector pins and aircraft wiring, since these additional components are not required. Furthermore, production
25 testing, such as, but not limited to an Environmental Stress Screening, may be performed once on the single system instead of twice on 2 identical avionics equipment packages.

30

A further advantage of the embodiments of the present system is that power consumption from the aircraft generator is reduced. With a single power supply and prudent choice of components, the embodiments of the present system will consume less power.

It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to
5 be illustrative and not restrictive.

CLAIMS

1. A fault tolerant system for electronic components, the system comprising:
 - a first Versa Module Eurocard (VME) module located within a housing; and
 - a second Versa Module Eurocard (VME) module located within said housing;
 - wherein said first and second VME modules are electrically isolated from each other and are capable of providing identical VME functionality.
2. The system of claim 1, wherein each of said first and second modules is located on a single backplane.
3. The system of claims 1 or 2 wherein each of said first and second modules further comprises:
 - a plurality of card slots;
 - a CPU card in one of said plurality of card slots; and
 - an input/output (I/O) card in one of said card slots.
4. The system of claim 3, wherein each of said modules further comprises at least one input/output (I/O) channel providing an external connection to said system, said I/O channel being electrically connected to a plurality of user defined I/O connections on each of said VME modules.
5. The system of claim 4, wherein a fault in said first VME module can be automatically detected, and, when said fault is detected, control of said system can be automatically switched to said second VME module via a control command provided on one of said I/O connections.
6. The system of any one of claims 4 or 5, wherein said input/output channel is provided via a single connector on said housing.

7. The system of any one of claims 4 to 6, wherein said user defined input/output connections are selected from a group consisting of a transistor to transistor logic (TTL) discrete in Master ID, a TTL discrete in System Handover in, a TTL discrete out system handover out, and a communications link between said first and second backplanes.
8. The system of any one of the preceding claims, wherein said electronic component is part of an avionics system.
9. The system of any one of the preceding claims, further comprising an electromagnetic interference filter electrically connected to said I/O channel.
10. The system of any one of the preceding claims, wherein each of said first and second VME modules conform to a 64 bit bus VMEbus standard.
11. A method for providing fault tolerance for electronic components, the method comprising the steps of:
- providing a first Versa Module Eurocard (VME) module located within a housing; and
 - providing a second Versa Module Eurocard (VME) module located within said housing;
 - wherein said first and second VME modules are electrically isolated from each other and are capable of providing identical VME functionality.
12. The method of claim 11, wherein each of said first and second modules is located on a single backplane.
13. The method of claims 11 or 12, wherein each of said first and second modules further comprises:
- a plurality of card slots;
 - a CPU card in one of said plurality of card slots; and
 - an input/output (I/O) card in one of said card slots.

14. The method of claim 13, wherein:

each of said modules further comprises at least one input/output (I/O) channel that is electrically connected to a plurality of user defined I/O connections on each of said VME modules; and

said method further comprises providing an external connection to said system over said channel.

15. The method of claim 14, further comprising:

detecting a fault in said first VME module and, when said fault is detected;

automatically switching control of said system to said second VME module via a control command provided on one of said I/O connections.

16. The method of claims 14 or 15, further comprising selecting said user defined input/output connections from a group consisting of a transistor to transistor logic (TTL) discrete in Master ID, a TTL discrete in System Handover in, a TTL discrete out system handover out, and a communications link between said first and second backplanes.