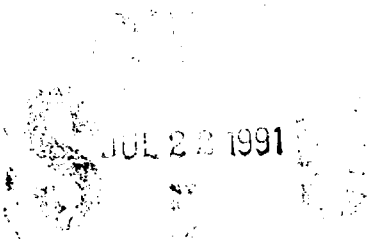
TECHNICAL REPORT BRL-TR-3240

BRL

DESCRIPTION OF A COMPUTER FAULT DETECTOR AND NET ISOLATOR

MARK D. KREGEL



JUNE 1991

U.S. ARMY LABORATORY COMMAND

BALLISTIC RESEARCH LABORATORY
ABERDEEN PROVING GROUND, MARYLAND

NOTICES

Destroy this report when it is no longer needed. DO NOT return it to the originator.

Additional copies of this report may be obtained from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.

The findings of this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

The use of trade names or manufacturers' names in this report does not constitute indorsement of any commercial product.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1991	Final, 4–29 Mar 91

4. TITLE AND SUBTITLE

Description of a Computer Fault Detector and Net Isolator

5. FUNDING NUMBERS

44592-102-51-4233
cc: 443300

6. AUTHOR(S)

Mark D. Kregel

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Ballistic Research Laboratory
ATTN: SLCBR-DD-T
Aberdeen Proving Ground, MD 21005-5066

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

BRL-TR-3240

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The reliability of a simple network can be improved by the use of highly reliable devices that monitor all sending elements attached to it. Such devices block network access if special electrical "keys" are not present before network communications are initiated. Such devices can also lock out network access for messages that exceed preset time limits. This report describes the construction of a simple device that serves these functions, termed a computer fault detector and net isolator, and describes the philosophy of its operation. The use of monitors of this type prevents the possible failure of a single sending element or node from disrupting the operation of an entire network.

14 SUBJECT TERMS

Computer Networks, Monitoring, Fault Detection, Network Isolators.

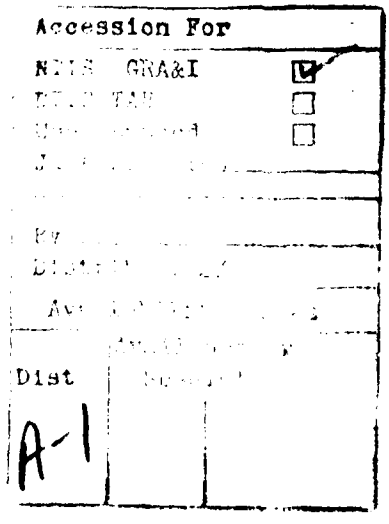
15. NUMBER OF PAGES
10

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

INTENTIONALLY LEFT BLANK.

TABLE OF CONTENTS



INTENTIONALLY LEFT BLANK.

1. INTRODUCTION

In the design of weapons systems, communications between various subsystem elements are normally required. Often, point-to-point wiring techniques are utilized with one wire or wire pair used for each circuit. This may result in a complex and heavy wiring harness requiring many connectors. For many systems, simple networks can be used to replace many of these wires, resulting in the possibility of reduced weight, improved maintainability, more reliable operations, better performance or capabilities, reduced vulnerability, less cost, and easier installation.

For systems where failure would not result in the loss of life and where highly parallel and redundant communications elements are not required, a net utilizing a single processing element at each node is sufficient. For example, in the servicing of a laboratory demonstration or in the construction of a prototype, a simple computer at each node gives the ability to do data acquisition and conversion remotely at each node, as well as allows high baud rate communications between the various nodes with low software overhead and reduced complexity.

A single net, be it an optical fiber or a differential line pair, can be "latched" up by the failure of a single node. For example, consider a net composed of a single conductor that is held "high" by a suitable pull-up resistor connected to a voltage source. Information is passed on the net by the various nodes "pulling" the conductor "low," forming serial characters by the resulting highs and lows. If one of the nodes were to fail and inadvertently hold the conductor low, then modulation of the net by any of the other nodes would be prevented. Thus, a means has to be found to protect the net to preclude a failure of a node from latching the net. If the net were to latch, all the operating nodes would be unable to communicate between themselves. This would preclude even degraded operations over the net and would prevent those operating nodes from determining the faulty node.

For maximum network reliability, the computer at each node, should be isolated from the net by a far more reliable analog circuit that can detect a number of possible computer failures and disable the computer's link to the net if a failure is detected. The analog circuit must be able to detect as many computer failure modes as possible quickly and reliably. In addition, the analog circuit must not place a high computational burden on the computer in order to assure its proper operation.

Fault detectors and net isolators have been used for years in many different networks, each optimized for its particular application. This report provides general insights into the problem of fault detection and net isolation and describes an elementary fault detector and net isolator suitable for use with low cost process control computers. The unit described can be easily constructed by an electronics technician and can be embodied into a simple net with minimal software overhead and programming complexity, making this capability conveniently available to even the simplest networks.

2. THE USE OF PROCESS CONTROL COMPUTERS AS SYSTEM SUBELEMENTS

Since the advent of the microcomputer, technological developments have allowed increased microcomputer performance and speed and, at the same time, at reduced size and cost. As a consequence, in large systems, more and more functions are being distributed to discrete processing elements which are linked by the use of high-speed data links or networks. Such distribution systems allow the partitioning of the various functions or operations of the system to discrete elements. Such elements can support the operation by utilizing higher level (more concentrated) information formats. Such a configuration also allows the partitioning of software into more easily debugged segments that cannot only be used in the original system, but in other systems where identical or similar functions need to be supported.

In addition, process control computers have shrunk in size to the point where an entire computer now resides on a single integrated circuit (IC). Because of improvements in the packaging of such ICs, their use becomes even simpler and with reduced costs. Such simple process control computers can support nets at baud rates approaching one million bits per second.

3. THE USE OF FAULT DETECTORS AND NET ISOLATORS

Simple data links or networks can now be fashioned out of a single conductor that, for example, is held "high" by a pull-up resistor connected to a supply voltage. Each node is connected directly to this conductor. If a node wishes to communicate through the net then it can place information on the net by "shorting" the net at such times as to form a serial message consisting of "highs" and "lows." Normally, net information is in the form of "characters" with each

character assigned a preset number of data bits, normally seven or eight. By using, in the most simple scheme, a "start bit," "data bits," a "parity bit," and one or more "stop bits," various characters can be sent asynchronously. In a more complex scheme, data bits can be sent in a much longer stream with logic transitions being used for synchronization. Sometimes a "clock" line can be utilized for the synchronization of long bit sequences where the same clock signal is available to both the sender as well as the receiver.

Regardless of the form of the information to be transmitted over a data link or a network, the link or network must be modulated. In the simple case of a single wire conductor which is normally held high, the modulation is in the form of "lows" or shorts produced by a sending element. If a sending element were to hold the conductor low continuously then other elements could no longer communicate. Such a "locked" condition does not normally happen. When an element or node has completed transmitting a message, it allows the conductor to return to its normally high state.

If an element were to fail, it could hold the conductor in a low state condition. Since the most complex element of a node (and the one most likely to fail) is the computer, it is felt that a highly reliable analog circuit could be used to "safeguard" the data link or network that would improve the overall reliability of the link or network. That is, considering the reliability of a computer as opposed to the reliability of a small analog circuit, it is felt that the analog circuit would "catch" more failures than it would itself generate.

This is even more true if the computer's software were written with the thought of enhancing the probability of the analog circuit's finding the computer's failures. One such technique is to program all the unused program memory space in the computer with the "halt" instruction.

4. THEORY OF OPERATION OF A FAULT DETECTOR AND NET ISOLATOR

For a fault detector and net isolator to do its job most effectively, it must be able to detect various common computer failures reliably and quickly. One such failure is when the computer simply stops functioning. Another is when the computer is caught in some sort of loop. Many of these failures arise from instruction fetch errors or errors writing to or reading from its random access memory. On the other hand, a fault detector and net isolator must be highly reliable,

certainly more reliable than the associated computer it is assigned to monitor. Thus, the use of a second computer is ruled out. If one wanted to go to a computer based fault detector, then the best strategy may be to use multiple computer based fault detectors that can arbitrate among themselves in case one failed. The cost and complexity, though, becomes considerably higher than the simple scheme proposed here.

In the construction of the fault detector and net isolator, it is assumed that discrete transistors are considered to be most reliable, since they can be tested under conditions more severe than those encountered in usage. For example, the process control computer might have ten-thousand or more transistors in it. Various gate and logic devices are also considered to be less reliable than a single transistor since they may be composed of dozens of transistors. Capacitors are subject to deterioration and change of performance and are also considered less reliable than a single discrete transistor on a long-term basis. To improve the reliability of all these circuit elements, it is essential to reduce electrical noise on power supplies and to prevent temperature extremes, both leading causes of failure of circuit elements. For our needs, complimentary metal oxide semiconductor (CMOS) circuitry may be preferred over transistor to transistor logic (TTL) digital circuits since CMOS draws less power and is more forgiving of supply voltage fluctuations.

Assuming a reliable analog fault detector and net isolator, the first function it must perform is to determine the message length and to break the net connection if any message exceeds a preset length. In addition, one simple strategy is to require the associated computer to transmit a key after each transmission to unlock the fault detector to allow additional transmissions. This key could be as simple as a short logic level transition. Certainly, more complex keys could be used, but, that would entail a more complex fault detector which, in turn, reduces its reliability.

Consider how a computer might fail. One thing it might do is to "lose" its instruction pointer and attempt to execute code across instruction boundaries. This might send the computer "looping" someplace in memory and would probably leave its outputs to the fault detector static, all being either high or low. Here a series of single byte (or word) instructions just before the net driver portion of the software might be sufficient to "resync" the instruction counter. This is especially true if the number of one byte (or word) instructions is greater than the number of bytes (words) required for the longest instruction. One might also expect that the outputs to the fault

detector might become "locked" in some unusual state. On the other hand, the outputs might toggle rapidly if the line driver portion of the software was part of an uncontrolled loop.

5. DESCRIPTION OF A SIMPLE FAULT DETECTOR AND NET ISOLATOR

The simple fault detector and net isolator described here is to be used in cases where human life is not at risk in case of net failure. It should not be used for the control of a lethal weapon or the control of a moving vehicle such as a truck or tank where more redundant methods of control could be used. It is designed for applications dealing with such things as prototypes, where occasional failures would pose no problem. A diagram of the fault detector and net isolator is shown in Figure 1.

One way to understand the operation of the fault detector is to pose a number of fault conditions on the circuit and observe its behavior. As an example, one might assume its inputs are frozen in a number of different logic states. As shown in Figure 1, inputs to the detector are a1 and a2, with a2 being the "lock" input. Normally, a1 and a2 are low. At power-up, the outputs of uB and uD may be uncertain. As long as a2 is low, a1 cannot modulate the net. To place the system in a known state, a short, positive going pulse is input at a2 by the control computer. The desired state for Ud is for it to be high. When Ud is high, the transistor will conduct and will bring the inverting input of uC low, making the output of uC high. Since uA is normally high, uE must be low. In this state, a1 is completely disconnected from the net by the actions of uF and uG. If uD is already high, then a pulse at a1 will have no effect. If uD is low, on the other hand, a positive going pulse at a1 will make uB positive. If uD is low, the transistor will not be conducting, allowing the inverting input to uC to become high. In 0.125 seconds, uC, a voltage comparator, will go low when the voltage on its inverting input exceeds the voltage on its non-inverting input. As uC goes low, uD becomes high. Once uD becomes high it is held there by uE, regardless of any additional voltage changes at a1. Only a positive going voltage at a2, when a1 is low, can now cause uD to become low, enabling uF. The circuit is now "armed" and will allow a1 to modulate the net for a period of no longer than 0.125 seconds. After 0.125 seconds, a1 must be brought low, as well as a2.

A low to high transition at a1 normally causes the output of uB to go high. The triggering of uB causes the output of uC to go low. This, in turn, causes the output of uD to go high, causing

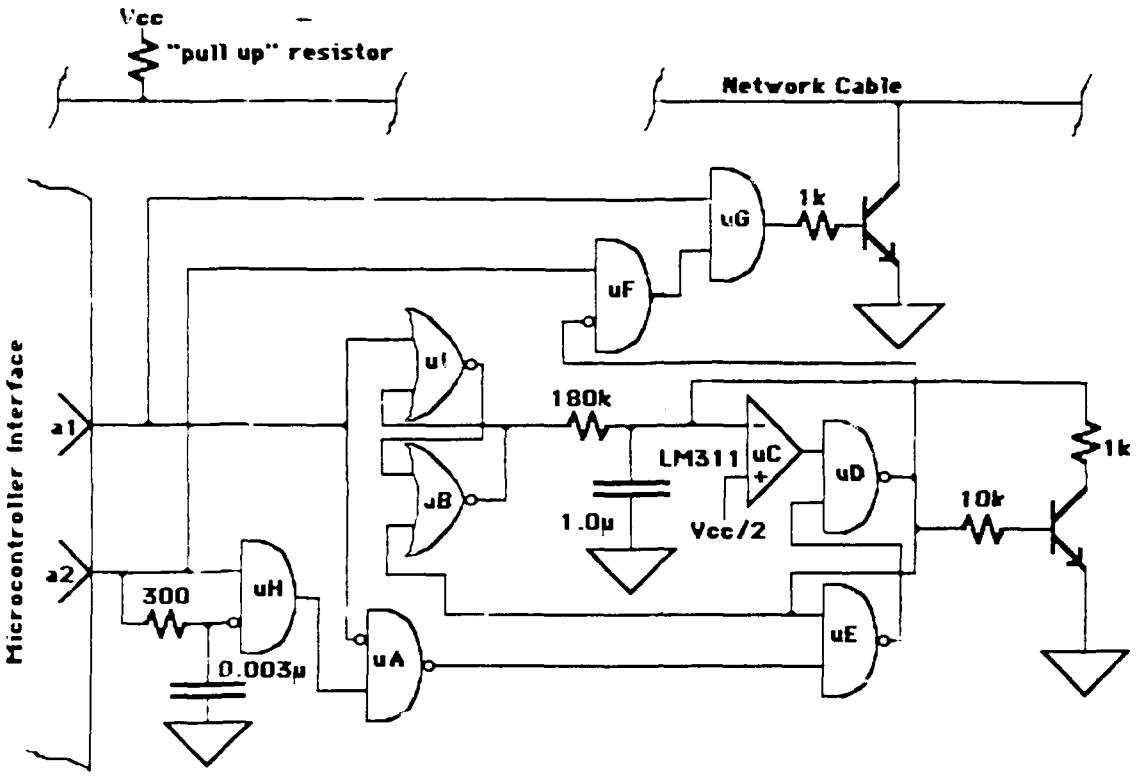


Figure 1. Schematic Diagram of a Simple Two-Input Fault Detector and Net Isolator.*

uF to go high, which, in turn, enables uG, allowing a1 to modulate the net. If uB times out by the action of the RC time constant, then uG is disabled through the same circuit elements. This time though, uD remains high to disable uG and, in effect, provides net isolation. The net remains isolated until a low going "key" strobe is received from uA. But uA cannot generate a strobe if it is disabled by a high from a1.

Because of the use of uH, a steady low or a steady high from a2 cannot prevent the net from being cut by the action of uC upon uD. A high to low transition of a2 is also protected against by uF as well as uH. A low to high transition while a1 is low will enable the net connection and is the normal way the circuit is used. The only way a1 can modulate the net is for a2 to become positive and remain positive while a1 is low. After this occurs, a2 can then modulate the net by

* Included in the diagram is a representation of a single conductor net held in the high level logic state (i.e., at a voltage level near Vcc) by a pull up resistor connected to a suitable voltage source. The net control transistor normally is in a high impedance state (non conducting) but is brought low when the output of uG goes high. Net receivers are not shown but always represent a high impedance state. Input a1 denote the serial input and a2 the "key control" or "lock" input. The time constant, defined by the 1.0u capacitor and the 180k resistor, is designed for a message length no greater than 0.1 second.

becoming high, but only for 0.125 seconds. Thus, after a transmission in which the net is modulated by a1, the only way for net access to be reestablished is for a1 to be brought low (which frees the net), a2 to be brought low (which locks out a1 from the net), a2 to be brought high (which enables the net link), and for a1 to be brought high (for the purpose of modulating the net). The net will remain open only 0.125 seconds after the first transition of a1 from low to high, regardless of what else a1 does. Regardless, a2 can cut the net at any time by going low. Once a2 has cut the net, a1 cannot continue to transmit, even if it is within the 0.125 second window.

6. CONCLUSION

Obviously, a fault detector and net isolator such as the simple circuit shown here can be defeated by a fault that mimics the normal operations of the node's computer and its software. The fault detector shown here, though, can detect and defeat all "locked" states due to failures within the CPU and can defeat some states where one or the other of the two inputs is rapidly changing. As an example, the fault detector and net isolator can defeat all four of the static states where a1 and a2 are not changing in time. It can also defeat the state where a1 is changing rapidly in time for periods longer than 0.125 seconds. The key of course is a2 going high while a1 is low and a2 staying high while a1 goes high. This condition, though, can only "open" the net for the 0.125 second period of time. After this period this key must be reapplied.

The fault detector and net isolator is a valuable product and can significantly aid in the diagnosing of net failures due to a computer failure at one of its nodes by locking out defective nodes. Because some nodes can continue in operation after other nodes fail, software diagnostics can be employed by one or more of the operating nodes that will indicate those nodes that are not responding to "pings," that is, that will indicate those nodes that have failed. This will make diagnostics far easier and allows the operation of the net servicing the remaining nodes.

INTENTIONALLY LEFT BLANK.

No. of Copies	Organization
2	Administrator Defense Technical Info Center ATTN: DTIC-DDA Cameron Station Alexandria, VA 22304-6145
1	Commander U.S. Army Materiel Command ATTN: AMCDRA-ST 5001 Eisenhower Avenue Alexandria, VA 22333-0001
1	Commander U.S. Army Laboratory Command ATTN: AMSLC-DL 2800 Powder Mill Road Adelphi, MD 20783-1145
2	Commander U.S. Army Armament Research, Development, and Engineering Center ATTN: SMCAR-IMI-I Picatinny Arsenal, NJ 07806-5000
2	Commander U.S. Army Armament Research, Development, and Engineering Center ATTN: SMCAR-TDC Picatinny Arsenal, NJ 07806-5000
1	Director Benet Weapons Laboratory U.S. Army Armament Research, Development, and Engineering Center ATTN: SMCAR-CCB-TL Watervliet, NY 12189-4050
(Unclass. only)1	Commander U.S. Army Armament, Munitions and Chemical Command ATTN: AMSMC-IMF-L Rock Island, IL 61299-5000
1	Director U.S. Army Aviation Research and Technology Activity ATTN: SAVRT-R (Library) M/S 219-3 Ames Research Center Moffett Field, CA 94035-1000

No. of Copies	Organization
1	Commander U.S. Army Missile Command ATTN: AMSMI-RD-CS-R (DOC) Redstone Arsenal, AL 35898-5010
1	Commander U.S. Army Tank-Automotive Command ATTN: ASQNC-TAC-DIT (Technical Information Center) Warren, MI 48397-5000
1	Director U.S. Army TRADOC Analysis Command ATTN: ATRC-WSR White Sands Missile Range, NM 88002-5502
1	Commandant U.S. Army Field Artillery School ATTN: ATSF-CSI Ft. Sill, OK 73503-5000
(Class. only)1	Commandant U.S. Army Infantry School ATTN: ATSH-CD (Security Mgr.) Fort Benning, GA 31905-5660
(Unclass. only)1	Commandant U.S. Army Infantry School ATTN: ATSH-CD-CSO-OR Fort Benning, GA 31905-5660
1	Air Force Armament Laboratory ATTN: WL/MNOI Eglin AFB, FL 32542-5000
	Aberdeen Proving Ground
2	Dir, USAMSAA ATTN: AMXSY-D AMXSY-MP, H. Cohen
1	Cdr, USATECOM ATTN: AMSTE-TD
3	Cdr, CRDEC, AMCCOM ATTN: SMCCR-RSP-A SMCCR-MU SMCCR-MSI
1	Dir, VLAMO ATTN: AMSLC-VL-D
10	Dir, BRL ATTN: SLCBR-DD-T

No. of Copies	Organization
1	Director U.S. Army Electronic Technology and Devices Laboratory ATTN: SLCET-SD Fort Monmouth, NJ 07703

USER EVALUATION SHEET/CHANGE OF ADDRESS

This laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers below will aid us in our efforts.

1. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) _____

2. How, specifically, is the report being used? (Information source, design data, procedure, source of ideas, etc.) _____

3. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. _____

4. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) _____

BRL Report Number BRL-TR-3240 Division Symbol _____

Check here if desire to be removed from distribution list. ____

Check here for address change. ____

Current address: Organization _____
Address _____

DEPARTMENT OF THE ARMY
Director
U.S. Army Ballistic Research Laboratory
ATTN: SLCBR-DD-T
Aberdeen Proving Ground, MD 21005-5066

OFFICIAL BUSINESS

BUSINESS REPLY MAIL
FIRST CLASS PERMIT No 0001, APG, MD

Postage will be paid by addressee

Director
U.S. Army Ballistic Research Laboratory
ATTN: SLCBR-DD-T
Aberdeen Proving Ground, MD 21005-5066

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES