Safety of Vital Control and Communication Systems in Guided Ground Transportation

Analysis of Railroad Signaling System: Microprocessor Interlocking

Office of Research
and Development
Washington, D.C. 20590

DOT/FRA/ORD-93/08
DOT-VNTSC-FRA-93-5

Final Report
May 1993

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. PB93-217339

2. REPORT DATE
May 1993

3. REPORT TYPE AND DATES COVERED
Final Report
November 1991 - December 1992

4. TITLE AND SUBTITLE
Safety of Vital Control and Communication Systems in Guided Ground Transportation, Analysis of Railroad Signaling System: Microprocessor Interlocking

5. FUNDING NUMBERS
RR393/R3016
DTRS-57-8D9D0009
Task #VA1038

6. AUTHOR(S)
Simon Reich and Thomas Bessoir

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Thomas K. Dyer, Inc.*
250 West 34th Street
New York, NY 10001

Foster-Miller, Inc.
350 Second Avenue
Waltham, MA 02254

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-FRA-93-5

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Railroad Administration
Office of Research and Development
400 7th Street, S.W.
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT/FRA/ORD-93/08

11. SUPPLEMENTARY NOTES
*under contract to:
U.S. Department of Transportation
Research and Special Programs Administration
Volpe National Transportation Systems Center
Cambridge, MA 02142

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the National Technical Information Service, Springfield, VA 22161

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This study has been conducted with the goal of gaining an insight into the issues of maintaining vital signal systems implemented with microprocessor chips and of making field changes to the application of such systems. To relate these abstract topics to concrete issues, two actual commercial systems were investigated, namely the General Railway Signal Company VPI(R) Vital Processor Interlocking and the GRS GENRAKODE™ microprocessor-based coded track circuit system.

One of the purposes of this study is to determine what actions should be taken by railroads to maintain signal-system safety when microprocessor-based signal systems receive maintenance to correct a failure and when such signal systems are modified after installation because of application changes such as a revision to the track plan or the signal aspects.

A second purpose of this study is to determine whether revisions are required to the Rules, Standards and Instructions Governing the Installation, Inspection, Maintenance and Repair of Signal and Train Control Systems, Devices, and Appliances (RS&I) due to the introduction of microprocessor-based signal systems and to suggest such revisions if they are indicated. These revisions, if any, would be based on the recommendations for maintenance and field-change procedures identified in the first part of the study.

14. SUBJECT TERMS
Microprocessor-based systems, interlocking system, central processing unit, integrated circuits

15. NUMBER OF PAGES
56

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	

PREFACE

This report is concerned with the safety issues associated with the application of microprocessor-based track control systems to railroad operations in the United States. Microprocessor-controlled interlockings and microprocessor-based coded track circuits are relatively recent developments in the field of railroad signalling. These new systems differ from their predecessors in two ways: the elements that perform the safety functions are not inherently safe (the underlying basis for system safety is not some physical characteristic of the element); and, the application logic for enforcing safety is in the form of a stored computer program rather than a physical characteristic of the system (such as wiring).

This study has two goals. The first is to determine what actions should be taken to maintain safety when microprocessor-based systems receive maintenance in the field or are modified to accommodate application changes. Secondly, this report presents recommendations for modifications to 49 CFR Part 236, *Rules, Standards and Instructions Governing the Installation, Inspection, Maintenance, and Repair of Signal and Train Control Systems, Devices, and Appliances* (RS&I).

Specifically, this report represents the analysis of the General Railway Signal Company's (GRS) VPI® (Vital Processor Interlocking) and the GRS GENRAKODE™ microprocessor-based coded track circuit system.

The report was prepared for the Volpe National Transportation Systems Center (VNTSC) in support of the United States Department of Transportation, Federal Railroad Administration, Office of Research and Development by Thomas K. Dyer, Inc., under subcontract to Foster-Miller, Inc.

The authors and the Volpe Center wish to thank the General Railway Signal Company for its cooperation and input during the preparation and review of this document.

METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC

LENGTH (APPROXIMATE)

1 inch (in) = 2.5 centimeters (cm)
1 foot (ft) = 30 centimeters (cm)
1 yard (yd) = 0.9 meter (m)
1 mile (mi) = 1.6 kilometers (km)

AREA (APPROXIMATE)

1 square inch (sq in, in^2) = 6.5 square centimeters (cm^2)
1 square foot (sq ft, ft^2) = 0.09 square meter (m_2)
1 square yard (sq yd, yd^2) = 0.8 square meter (m^2)
1 square mile (sq mi, mi^2) = 2.6 square kilometers (km^2)
1 acre = 0.4 hectares (he) = 4,000 square meters (m^2)

MASS - WEIGHT (APPROXIMATE)

1 ounce (oz) = 28 grams (gr)
1 pound (lb) = .45 kilogram (kg)
1 short ton = 2,000 pounds (lb) = 0.9 tonne (t)

VOLUME (APPROXIMATE)

1 teaspoon (tsp) = 5 milliliters (ml)
1 tablespoon (tbsp) = 15 milliliters (ml)
1 fluid ounce (fl oz) = 30 milliliters (ml)
1 cup (c) = 0.24 liter (l)
1 pint (pt) = 0.47 liter (l)
1 quart (qt) = 0.96 liter (l)
1 gallon (gal) = 3.8 liters (l)
1 cubic foot (cu ft, ft^3) = 0.03 cubic meter (m^3)
1 cubic yard (cu yd, yd^3) = 0.76 cubic meter (m^3)

TEMPERATURE (EXACT)

[(x-32)(5/9)] ^oF = y ^oC

METRIC TO ENGLISH

LENGTH (APPROXIMATE)

1 millimeter (mm) = 0.04 inch (in)
1 centimeter (cm) = 0.4 inch (in)
1 meter (m) = 3.3 feet (ft)
1 meter (m) = 1.1 yards (yd)
1 kilometer (km) = 0.6 mile (mi)

AREA (APPROXIMATE)

1 square centimeter (cm^2) = 0.16 square inch (sq in, in^2)
1 square meter (m^2) = 1.2 square yeards (sq yd, yd^2)
1 square kilometer (km^2) = 0.4 square mile (sq mi, mi^2)
1 hectare (he) = 10,000 square meters (m^2) = 2.5 acres

MASS - WEIGHT (APPROXIMATE)

1 gram (gr) = 0.036 ounce (oz)
1 kilogram (kg) = 2.2 pounds (lb)
1 tonne (t) = 1,000 kilograms (kg) = 1.1 short tons

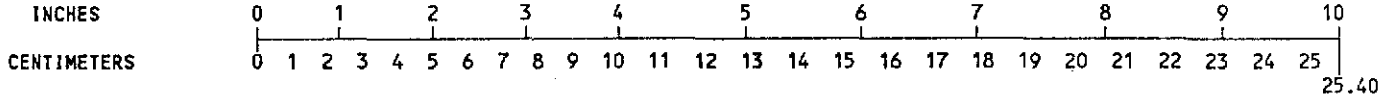
VOLUME (APPROXIMATE)

1 milliliters (ml) = 0.03 fluid ounce (fl oz)
1 liter (l) = 2.1 pints (pt)
1 liter (l) = 1.06 quarts (qt)
1 liter (l) = 0.26 gallon (gal)
1 cubic meter (m^3) = 36 cubic feet (cu ft, ft^3)
1 cubic meter (m^3) = 1.3 cubic yards (cu yd, yd^3)

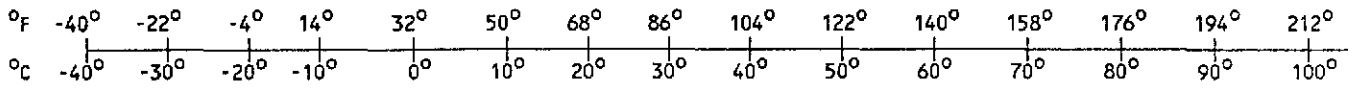
TEMPERATURE (EXACT)

[(9/5) y + 32] ^oC = x ^oF

QUICK INCH-CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT-CELSIUS TEMPERATURE CONVERSION



For more exact and or other conversion factors, see NBS Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50. SD Catalog No. C13 10286.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

EXECUTIVE SUMMARY

This study has been conducted with the goal of gaining an insight into the issues of maintaining vital signal systems implemented with microprocessor chips and of making field changes to the application of such systems. To relate these abstract topics to concrete issues, two actual commercial systems were investigated, namely the General Railway Signal Company VPI® Vital Processor Interlocking and the GRS GENRAKODE™ microprocessor-based coded track circuit system.

The document establishing the minimum level of acceptable safety for design, maintenance, and field changes of railroad signaling safety systems is The Code of Federal Regulations, Title 49, Subtitle B, Chapter II, Part 236, ***Rules, Standards, and Instructions Governing the Installation, Inspection, Maintenance, and Repair of Signal and Train Control Systems, Devices, and Appliances,*** commonly known as the RS&I. This document, which applies to common-carrier railroads, was originally prepared when most interlockings were mechanical and when relay-based signal systems were at the cutting edge of technology. Through the years, the RS&I has been revised as newer signal systems were installed.

Microprocessor-controlled interlockings and microprocessor-based coded track circuits are relatively recent developments in the field of railroad signaling. Safety signal systems using microprocessors are fundamentally different from predecessor signal systems, such as mechanical-locking-based systems and relay-based systems in two principal ways, namely:

1. The elements that perform the safety functions are not inherently safe, that is, some physical characteristic of the element, such as the use of gravity or the use of electrical contacts made out of nonweldable material, is not the underlying basis for building a safe system.

2. The applications logic, that is, the location-unique logic for enforcing safety is in the form of a computer program rather than being a physical characteristic of the system such as the wiring of an all-relay system or the shape and location of locking dogs of a mechanical-interlocking system.

These two factors introduce an element of uneasiness in or even distrust by traditional signal engineers in microprocessor-based systems because the safety of the system cannot be easily verified by visual inspection or by simple tests, like performing insulation tests on a cable.

Because safety can no longer be assured by resorting to simple visual inspections of microprocessor-based signal system, it may

be necessary to develop new methods and minimum standards to provide confidence that proper steps are being taken to ensure an acceptable level of safety in the application, maintenance, and revision of microprocessor-based signal systems.

Thus, one of the purposes of this study is to determine what actions should be taken by railroads to maintain signal-system safety when microprocessor-based signal systems receive maintenance to correct a failure and when such signal systems are modified after installation because of application changes such as a revision to the track plan or the signal aspects.

A second purpose of this study is to determine whether revisions are required to the RS&I due to the introduction of microprocessor-based signal systems and to suggest such revisions if they are indicated. These revisions, if any, would be based on the recommendations for maintenance and field-change procedures identified in the first part of the study.

The main study effort has been divided into three tasks. They are:

Task 1 - A review of the literature describing the GRS VPI® and GENRAKODE™ systems which will concentrate on the underlying principles of operation of these systems, on the methods of the systems' application, as well as the mechanical and electrical details of the systems' interconnection with field apparatus such as signals, switch machines, and line circuits.

Task 2 - Identification of failure scenarios during maintenance or the implementation of field revisions of VPI® and GENRAKODE™ systems from which it will be determined what procedural or other steps should be taken to minimize the safety exposure of the systems during such activities.

Task 3 - Recommend revisions and additions, if any, to the RS&I to codify the recommended procedures developed during the Task 2 effort so that their enforcement can be uniformly implemented.

This series of tasks also provides a logical sequence for presenting the results of the study. Thus, this report will be structured, for each of the two systems studied, as follows:

- Description of the **organization of the system** indicating the division of functions and safety between hardware and software.
- Description of the **hardware elements of the system** including identification of hardware-enforced safety and identification of those safety-related hardware elements that are affected by maintenance and field revisions.

- Description of the means for obtaining safety using **software** including identification of the means of ensuring that the software has been properly compiled and installed in the system.

- Categorizing **maintenance tasks** into those which are safety related and those which are not and identifying, for the safety-related maintenance tasks, those portions of the tasks that potentially affect safety and how.

- Description of **maintenance scenarios** which could result in unsafe conditions and discussion of procedures, techniques, or system changes to minimize exposure to unsafe conditions.

- Description of the scenario for making **field changes to application logic**, such as changing the track layout or revising signal aspects, identification of potential safety-related steps in the procedure, and discussion of means for minimizing exposure to unsafe conditions.

- Identification of the **RS&I sections** that apply to microprocessor-based signal systems of the types studied and discussion of potential interpretation and enforcement of those sections.

- Suggestions for **revisions to or additions to the RS&I** to accommodate microprocessor-based systems to permit uniform application and enforcement of safety requirements to these systems.

What this study will **not** do is make a judgement of the adequacy of the safety-related design of the two systems being studied. Such a determination has already been done by the manufacturer and others and is beyond the scope of this small effort.

Frequently, in the following report, parallels will be drawn with existing mechanical and all-relay systems. This will be done to clarify and illustrate points, to permit extension of existing, time-proven principles to this new technology, and to permit those not familiar with computer jargon to understand and gain confidence in the new systems.

1.0 VPI® VITAL PROCESSOR INTERLOCKING SYSTEM

1.1 INTRODUCTION

The General Railway Signal Company VPI® Vital Processor Interlocking System is a microprocessor-based control system that performs the same functions as a traditional all-relay interlocking, including both the vital (safety-related) and nonvital functions. Vital functions that are performed include:

- Route locking
- Time locking
- Approach locking
- Detector locking
- Switch locking
- Switch control
- Switch indications
- Signal control
- Line circuit control
- Indication locking
- Loss-of-shunt protection
- Traffic locking
- APB control

Nonvital functions that are performed include:

- Code-system controls
- Code-system indications
- Local-control panel operations

Since this report is a safety analysis, only the vital portion of the VPI® system will be described and discussed. Little detail will be given concerning the nonvital portion of the system.

1.2 ORGANIZATION OF THE SYSTEM

Unlike traditional all-relay signal systems which consist of only hardware, the VPI® system is divided into two major interdependent components, namely hardware and software.

Hardware can be thought of as those elements which are produced in a factory. Examples of hardware elements are printed circuit boards, transistors, integrated circuits, microprocessor computer chips, memory chips, capacitors, resistors, transformers, relays, etc.

By themselves, most traditional signaling hardware elements, like relays, resistors, transformers, transistors, etc., perform no useful function from a signaling-system point of view. However, the hardware elements can be assembled into functioning systems by interconnecting the elements using wire!

The introduction of new types of hardware elements, namely microprocessor computer chips, into railway signaling includes the requirement to do more than wire the hardware elements together. **Software** must be added to direct the performance of the microprocessor-based hardware. Thus the software of a microprocessor-based system is analogous to the interconnecting wires of a relay-based system.

The safety-related functions of the GRS VPI® system are divided between the hardware elements of the system and the software.

The safety of the interconnection of the computing elements that perform the signal-logic functions to the actual signal apparatus, such as signals and switch machines, mainly uses hardware techniques. These are the so-called input-output interconnections. In this case, the physical design of the hardware elements and their interconnection with each other prevents shorted or open components, such as transistors, from falsely clearing a signal, throwing a switch, or indicating a switch position.

On the other hand, safely performing the logic functions, such as locking a switch while a signal is clear or clearing a signal only if the route is aligned and locked, is the responsibility of software. Not only does this software make the system operational, but it is also the design of this software that assures that a failure of the computer hardware (which executes the software and which is inherently nonvital in nature) will prevent a switch from throwing under a train or a signal from clearing improperly.

Thus, in a microprocessor-based system such as VPI®, the software is analogous to the wiring of a relay-based system in the sense that the software governs the performance of the system for a specific application. On the other hand, while most relay-based systems use vital relays which are inherently failsafe, since the computing and memory elements of a microprocessor-based system are not inherently failsafe, the software must also be designed to check the operation of the computing elements and prevent permissive outputs if a safety problem is detected in the hardware.

The following sections will describe the hardware and software elements of the VPI® system and give further information on safety enforcement in those elements.

1.3 HARDWARE ELEMENTS

The foundation of the VPI® system hardware is a module with a mother board, slots to accommodate 21 plug-in printed circuit boards (PCBs), and a rear panel with plug couplers. Connections between the VPI® system and other signal apparatus are through the plug couplers located on the rear panel of the VPI® module or may be made directly from the printed circuit board edge connector receptacles.

Each module contains one Central Processing Unit (CPU) board, one Polynomial Divider (PD) board, one Vital Relay Driver (VRD) board, and at least one I/O Bus Interface board. The type and quantity of other PCBs are supplied to meet the requirements of a particular application. The rear of each PCB has three edge connectors. The center edge connector of each PCB plugs into a socket on the mother board for power and bus interconnections. Standard cables connect the appropriate edge connectors on the rear of the PCBs to the plug couplers on the rear panel while other standard cables are used to interconnect PCBs to each other. A computer design program, known as the Computer Aided Application (CAA) program, generates a list of the required cables for the particular installation. This CAA program is described later in this report.

1.3.1 Mother Board

The mother board provides operating power and signal distribution to all of the PCBs in the module through the center edge connector on the rear of each PCB. Wire wrapping certain terminals to common energy on the mother board center edge connector also permits programming information into the system using hardware.

For the CPU board this information consists of the Software Revision Signature whose binary equivalent is encoded by wire wrapping the appropriate pins in the CPU-board slot to 5 volt common. The Software Revision Signature is a number from 1 through 62 which corresponds to a revision number for the application software which should be installed on the CPU PCB.

For each input and output board, this information is a board address which is the binary equivalent of the address by which the CPU will address a particular board of these types. Board addresses are encoded by wire wrapping the appropriate mother board pins in the board slot to 5 volt common. During the design of the system, the CAA program assigns board addresses and generates a list of the wire wrap connections required for each board slot.

1.3.2 Central Processing Unit (CPU) PCB

The purpose of the CPU board is to provide the controlling functions of the VPI® system.

The CPU board contains a 16-bit microprocessor, related program and data memory, and the logic necessary to execute timing and data handling functions. All control and monitoring functions go through the CPU board.

The program memory is divided into two segments so that separate memory elements store the system software and the application software. System software is the program instructions for the CPU which are not unique to a particular application or location. Application software is the program instructions for the CPU which are unique to a particular application or location.

Both system software and application software are stored on integrated-circuit memory chips. These chips are of the Erasable Programmable Read Only Memory (EPROM) type. That means that the information (programs) stored on the chip can be erased and reprogrammed in a suitable fixture off line (away from the VPI® system).

While other integrated circuits and electronic components are soldered directly on the CPU PCB, memory chips are not. They are installed in sockets so that they can be changed in the field. Four sockets are used for system-software EPROMs and six sockets are reserved for application-software EPROMs. The CPU board has an on-board switch which is used to allocate memory for the application software. The application-software EPROMs contain the Software Revision Signature which must match the hardware signature on the wire wrap pins of the mother board to assure that the correct application software is installed (analogous to registration on vital relays).

The main CPU bus is connected to the lower edge connector on the rear of the PCB. This bus is also connected to the lower edge connector of the Vital Relay Driver PCB, the Polynomial Divider PCB, the Extended Code System Emulator PCB, and the Vital Serial Controller PCB and allows communications among those PCBs.

1.3.3 Polynomial Divider (PD) PCB

The main purpose of the PD board is to evaluate the Boolean expressions which form the application logic for the system.

The PD board consists mainly of a 32-bit linear-feedback shift register. This polynomial divider is used to verify the properties of the codes selected for use in the software. The PD board evaluates the Boolean expressions through the combination of the words representing whether an input or output is true or false or whether an intermediate relay equivalent is true or false, aids in the creation of system check words, and tests the words to verify that they have not been corrupted due to a malfunction of the system.

The main CPU bus is connected to the lower edge connector on the rear of the PCB. There are no application-dependent components on the PD board.

1.3.4 Vital Relay Driver (VRD) PCB

The purpose of the VRD board is to energize a vital check relay so long as the internal self-checking functions of the VPI® system indicate that the system is functioning normally. Energy which breaks over front contacts of this vital relay is used to energize all vital outputs so that if a system malfunction is detected and the vital check relay drops, all vital outputs will be deenergized which is, of course, their safe state.

Every one second the main processing system creates a set of data called "main check words" and delivers them to the VRD board. The VRD board processes these check words and converts them into 20 "tokens." Every 50 ms the main processing system creates a set of data called "recheck check words" and delivers them to the VRD board. The VRD uses one token and the recheck check words to create an output signal for 50 ms.

If all of the check words are correct, the VRD board produces an output signal which is a 10-kHz square wave modulated at 500 Hz. This signal passes through a 10-kHz filter to demodulate the carrier, through a 500-Hz filter to verify the modulation frequency, and is rectified. The rectified signal is used to energize the 100-ohm vital check relay which supplies power to the vital outputs. If any of the check words are incorrect or not delivered on time this relay will not be energized.

The main CPU bus is connected to the lower edge connector on the rear of the PCB. The PCB's upper edge connector is connected with a standard cable to a plug coupler on the rear panel. It is through this plug coupler that the VRD board is connected to the external vital check relay.

There are no application-dependent components on the VRD board.

1.3.5 I/O Bus Interface PCB

The I/O Bus Interface board serves as a buffer between the system processing boards and the vital input and output boards. The I/O Bus Interface board also serves as a buffer between the main system module and any expansion modules. Expansion modules are additional PCB housings required because more boards are required than can fit in one housing.

To permit a large number of input and output boards to be associated with a single CPU board as part of one VPI® system, the input and output boards are arranged in groups with each group serviced by an I/O Bus Interface board. Logic on each I/O Bus Interface board compares the main system bus address produced by the CPU board with the address encoded on the mother board for the slot where this board resides. If the bus and slot addresses agree, this interface board and its associated vital input and output boards are enabled. If the addresses do not agree, a control signal is generated to allows an I/O Bus Interface board in an expansion module to be enabled.

Each I/O Bus Interface board also includes logic for the continuous verification of the output states and provides a storage medium for test data obtained during vital input and output port checks.

Each I/O Bus Interface board contains a Signature Header which is used for routing vital input test data to the proper shift register on the board. These test data are the words used to read the inputs during normal system operation, as described in following

sections. When the system is configured, the CAA program assigns one of the 16 varieties of Signature Headers (Signatures A through P) to be installed on this board. The scrambling of the vital input test data is used as a means of verifying the correct vital input addressing. This is analogous to providing registration devices on plug-in relays in that it verifies that the proper boards are correctly installed in the proper slots.

The main CPU bus is connected to the lower edge connector on the rear of the PCB. The upper edge connector is used to connect to an expansion module when one is used.

The plug-in Signature Header, which is of the size and shape of an integrated circuit (IC), is an application-dependent component on this type of board.

1.3.6 Direct Input PCBs

The purpose of each Direct Input board is to provide the means for allowing 16 vital DC inputs to the VPI® system.

Each Direct Input board contains 16 optically-isolated ports. Each port requires two connections to the field, plus and minus for the input point being monitored. Connections to the field are through plug couplers on the rear of the VPI® module which are connected to the Direct Input board's rear edge connectors with standard cables.

The arrangement of hardware for each input is key to providing safety. An optical switch, which is composed of a light-emitting diode and a photosensitive transistor, is used to isolate each vital DC input from the VPI® system. The input energizes the light-emitting diode (LED) so that it is illuminated producing an output from the photosensitive transistor when the input is present. The LED is shunted by a transistor switch which is turned on and off by a data bit stream (the test words referred to in a previous section) which is generated by the VPI® and has unique information for each input point. Thus, when the data bit stream and the vital input are both present, the photosensitive transistor will see the complement (the complement of 'on' is 'off' and the complement of 'off' is 'on') of the data stream and will produce that as the input to the VPI® system. If the vital input is not present, the LED will be dark and no data bit stream will be transmitted to the photosensitive transistor. Failure modes will produce steady energy, no energy, or the data bit stream instead of its complement, to the VPI® system.

All 16 inputs on a board are read at once by sending a unique bit stream to all inputs simultaneously. As each bit of the bit stream is sent to each input, if there is a current between the terminals of an input, the resulting bit at the phototransistor is the complement of the input bit. The resulting bit pattern at the phototransistor is called a word and represents the "true" or "on" status of that input. If this word is not present, it is assumed that the input is "off" and so a different word representing the

"false" or "off" status of that input is introduced by the system instead. Thus, while the "false" word (relay back-contact equivalent) and the complement of the "true" word assigned to each input point are stored in the system, the actual "true" word (relay front-contact equivalent) is not stored and can only be generated on the input board when an input is actually present!

The resulting input words (either "true" or "false") are routed through the Signature Header on the Direct Input board to scramble the words and provide a check on the input addressing which uses nonvital electronic gates and wire wrap board addresses. The scrambled input words are then sent to the I/O Bus Interface board where they are routed through its Signature Header and stored in shift registers to be read by the CPU.

The plug-in Signature Header, which is of the size and shape of an integrated circuit, is an application-dependent component on this type of board.

1.3.7 Vital Output PCBs

The purpose of the Vital Output PCBs is to energize field signal hardware such as signals, line circuits, relays, or switch machines.

There are four types of Vital Output boards, namely single-break, double-break, lamp-driver, and AC. Each board contains eight optically-isolated output ports. Since the system data bus is 16 bits wide two output boards can be addressed simultaneously. Connections to the field apparatus are through plug couplers on the rear of the VPI® module which, in turn, are connected to two of the Vital Output board's rear edge connectors with standard cables.

Safety for vital outputs is achieved by the configuration of hardware as well as by software. There are two key hardware techniques that are used to assure safety. The first is to optically isolate each output from the remaining VPI® system and then to break the energy which actually feeds the field signal hardware over a front contact of the vital check relay previously described. Thus, if a fault is detected in the operation of the VPI® system, the vital relay will drop opening up the energy feed to all the vital outputs.

The second hardware technique used, known as an Absence-of-Current Detector (AOCD), monitors current flowing in each output using a three-winding saturable transformer. The output is routed through one winding of the transformer. A bit stream is fed into the second winding of the transformer while the third winding of the transformer is used to monitor the second winding's bit stream. When no output current is flowing (the output is turned off), the bit stream from the second winding is induced into the third winding. When output current is flowing, either due to a desired output or due to a fault like a shorted output transistor, the transformer core is saturated and the bit stream from the second

winding is not induced into the third winding. System logic examines the output of the third winding and determines that output exists only when it should. If there is output when no output current should be flowing, the system generates corrupted check words which, in turn, prevent the vital check relay from being energized. For the VPI® system, a maximum of 140 ms can elapse between detecting a potentially unsafe failure and removing power to outputs.

Each Vital Output board contains a unique Signature EPROM. When the system is configured, the CAA Compiler program assigns one of the 40 varieties of Signature EPROMs (Signatures 1 through 40) to be installed on each board. Signature EPROM data is used by board addressing to prove that there are no address failures, that is, that a board has responded to the wrong address due to some electronic fault. Improper board addressing will use incorrect signature EPROM data causing incorrect recheck checkwords to be generated and the removal of vital power. The Signature EPROM also contains the output check data for the board which is the information that forms the bit stream which is circulated through the second winding of the transformer core, described above. The VPI® system will not operate with missing or wrong output board EPROMs.

The main processing system controls the status of each output by writing data to the output boards. The status of each output is monitored with circuitry referred to as an Absence-Of-Current-Detector (AOCD), as described above. Data from the Signature EPROM is continuously circulated through the AOCD and the output of the AOCD is processed and stored. This data is reported to the processor every 50 ms and covers 45 of the last 50 ms. The main system processor uses this data to create the recheck check words which are required to energize the vital check relay.

The plug-in Signature EPROMs, which are integrated circuits, are application-dependent components on this type of board.

1.3.8 Field Settable Vital Timer (FSVT) PCB

The purpose of the Field Settable Vital Timer PCB is to provide a field-settable time element which can be introduced into the application logic for such functions as time locking. By making the time element field settable, it can be changed at will due to field-dictated changes, such as changes in train speed limits, without reprogramming the system.

The Field Settable Vital Timer board contains 8 timers each of which can be individually set for a time interval of 0 to 59 minutes, 59 seconds by using four jumpers per timer. All four jumpers must be in place, or the time interval for that timer will never expire. After the jumpers are installed the time selection matrix is enclosed in a sealable cover.

Each FSVT board has unique data for each of the eight timers which is stored in an EPROM on the board. If more than one FSVT board is

used they must have different group numbers to maintain the uniqueness of this data.

The I/O Bus Interface board detects the jumper setting and verifies the setting of that timer. Unique data is stored in a shift register based on the timing constant and the number of the timer. This data is used in evaluating vital timer expressions within the application logic.

1.3.9 Vital Serial Controller (VSC) PCB

The Vital Serial Controller board provides a means of communicating the states of 200 functions between interlockings in a vital manner. This is necessary if an interlocking is so large that more than one VPI® system is required or if two adjacent interlockings communicate over a vital data link.

The block of data to be transmitted is assembled into a message packet and converted into two components, an image field (the data) and a check field. The image field is based on the states of the parameters being transmitted over the link. These parameters might include input data (for instance, the position of switches), output data (for instance, controls for switches and signals), or the solution of intermediate calculations (for instance, the state of route locking or approach locking). The check field contains check words created by the above process. The two fields are transmitted to the other VPI® system. The receiving VPI® system recreates check words from the check field and parameters from the image field. The check words verify the transmission path and the operation of the VSC and CPU software. If the check words are correct, the parameters are used for expression evaluation at the receiving VPI® system. If any of the check words are incorrect all parameters are assumed to be in their restrictive state. Parameters are the terms of the Boolean expressions which comprise the application logic.

The VSC board contains two sets of DIP switches and EPROMs with software dependent on the system controlling the other interlocking and the parameters being transferred. The main CPU bus is connected to the lower edge connector on the rear of the PCB. The upper edge connector is wired to the serial I/O plug coupler with a standard cable.

The plug-in system and application EPROMs, which are integrated circuits, are application-unique components on this type of board.

1.3.10 Extended Code System Emulator (CSEX) PCB

The Extended Code System Emulator board provides a means of nonvital communication to external devices, such as other CSEX boards, modems, and data loggers.

The CSEX board contains an application program dependent on the external devices with which it is communicating. Two sockets on the CSEX board are provided for application program memory. Jumper straps are used to select the size of the application program memory.

The main CPU bus is connected to the lower edge connector on the rear of the PCB. The upper edge connector is connected with a standard cable to a plug coupler on the rear panel. It is through this plug coupler that the CSEX board is connected to the external communication lines.

The CSEX board uses system and application EPROMs and switch settings which are unique to each application, however, these elements do not affect the safety of the system.

1.3.11 Nonvital Input (NVIN) PCB

Each Nonvital Input PCB contains 32 optically isolated, nonvital inputs whose states are read once every 20 ms. The CSEX board with the nonvital application software communicates with the NVIN board through the mother board.

There are no application dependent components on the NVIN board.

1.3.12 Nonvital Output (NVO) PCB

Each Nonvital Output PCB contains 32 optically isolated, nonvital outputs whose states are updated once per second. The CSEX board with the nonvital application software communicates with the NVO board through the mother board to control the state of the outputs.

There are no application-dependent components on the NVIN board.

1.4 SOFTWARE

Several design approaches have been used by different manufacturers to make a microprocessor-based interlocking system failsafe. One approach that has been taken by European manufacturers is to use two or more sets of hardware in a redundant configuration with the results obtained by one set of hardware checked against the results obtained by another before field action is taken. In some examples, the software executed by each set of hardware is the same while in other examples the software in each set of hardware is prepared by different designers and hence is different.

The design approach that has been used for the VPI® system is to use a single main microprocessor chip and to provide redundancy in the software design. Each input is read and processed twice to obtain an output. The input and output words for a given input point and given output point will differ for each of the redundant

cycles. Safety is further augmented by assigning a multibit word for the true value and a different multibit word for the false value of each input and output and for each intermediate step rather than assigning a single bit for each variable (actually, all that is required to perform the required logic) so that errors in the operation of the system, such as stuck, open, or shorted electronic devices, can be more easily detected. By using these software techniques the probability that a false proceed is produced by the system can be mathematically calculated to be at an acceptable level comparable to a traditional signal system.

The VPI® system is designed using two types of software, namely system software and application software. The system software is the software required to make **any** VPI® application work and includes the Safety Assurance Logic™ which verifies that the system is functioning as intended. The application software is the site-specific logic which is the equivalent of the logic circuits of an all-relay interlocking.

Using track plans, locking tables, and aspect charts, the signal engineer writes a set of Boolean expressions which are equivalent to the relay logic circuits for the interlocking. The GRS Computer Aided Applications (CAA) software package is used to compile these equations into the application logic in the form of EPROM code.

The system software can be thought of as performing a three-step cycle, namely obtain inputs, evaluate expressions and perform checks, and control outputs. Once each second, all of the inputs are read, all of the Boolean equations are evaluated, and all of the outputs are updated. Each piece of data corresponding to the state of an input, the state of an output, or the result of an equation is referred to as a parameter. The software uses two different representations for each parameter. These representations are referred to as Channel 1 and Channel 2 and comprise the redundancy of the system to ensure safety.

1.4.1 Input Functions

The software receives inputs from four types of PCBs, namely Direct Input PCBs (vital input points), Vital Serial Controller PCBs (vital inputs from other VPI® systems), Nonvital Input PCBs (nonvital inputs such as from a control panel) and the Extended Code System Emulator PCBs (nonvital inputs from a code system). These inputs are used to assign TRUE and FALSE parameter values to each parameters in the CPU memory once per second.

On a Direct Input PCB, the main processing system sends a different 32-bit test word to each input. These words form the bit stream used to read the input point as described in the hardware section. If the input is present, then a complement of the test word is sent from the input PCB to the CPU memory and is stored as a TRUE value for the input with which it is associated. Otherwise, a FALSE word is stored for the value of the input. Only the inputs that are sensing current will generate result words that are the complement

of the test words. The correct 32-bit complement is the TRUE parameter value; any other word is interpreted as the FALSE value for that parameter. The process is repeated using different test words for the other channel. The input scanning process uses varying times between input reads to protect against AC coupling.

On a Vital Serial Controller PCB, a received message is reconstructed into parameter values resembling those at the transmitting interlocking. Check words are also reconstructed from the received message and combined with the check words generated by this VSC board. If the path is correct and all of the check words are correct, then those parameters which the transmitting end assigned a TRUE state are allowed to assume the correct TRUE parameter value in both channels in the receiving end CPU. If the path or any check word is incorrect, then all of the reconstructed parameter values are assigned FALSE values.

Inputs obtained from a Nonvital Input PCBs are communicated to the Extended Code System Emulator PCB. These nonvital inputs along with those obtained from modems and other CSEX boards directly assign parameter values in both channels in the CPU without any further checking.

1.4.2 Evaluate Boolean Expressions

Parameter values for the inputs to and results of previous Boolean expressions are stored as two different 32 bit words in system memory on the CPU board. The Boolean expressions for the interlocking are stored in the application software EPROMs on the CPU board. Each Boolean expression is evaluated twice per second, once using the parameter values represented in Channel 1 and again using those represented in Channel 2.

The Boolean expressions are evaluated by a polynomial division algorithm. This technique uses the 32-bit, parallel-load shift register on the Polynomial Divider board to combine parameter values into another 32 bit word that is the result of the Boolean expression. The expression results are stored in system memory on the CPU board.

The system software takes precautions to ensure that no equations are skipped and that the equations are evaluated in order.

1.4.3 Perform Safety Checks

The system software generates check words as the result of executing various processes. There are two classifications of check words, main check words and recheck check words.

Main check words are created once per second and verify that the processes carried out by the system software are executed properly. Some of the processes that generate main check words are verifying that old data is erased, verifying that only data current for that

particular cycle is used to evaluate expressions, verifying that system and application software is uncorrupted, and verifying that the timing cycles are accurate.

Recheck check words are created once every 50 milliseconds and verify the state of each vital output. The AOCD that is a part of the vital output circuitry is used for this purpose. A unique pattern of bits is repeatedly applied to each AOCD for 45 of the 50 milliseconds. The bit patterns pass through the AOCD only when the vital output is off. The data passing through the AOCD is compressed in a shift register and a unique numerical value is created for each output. This value has the correct result for the output being off only if there was no current at the output for the entire 45 milliseconds. The processor uses these values and the value of the expressions for the outputs to create the recheck check words.

1.4.4 Output Functions

The software delivers outputs to one or more of eight different types of output PCBs, namely Vital Relay Driver PCB, Single-Break Vital Output PCB, Double-Break Vital Output PCB, Lamp Driver Vital Output PCB, AC Vital Output PCB, Vital Serial Controller PCB, Nonvital Output PCB, and the Extended Code System Emulator PCB.

The main processing system delivers the set of main check words to the VRD board once per second. The VRD board processes these main check words and converts them into 20 "tokens." Every 50 milliseconds the main processing system delivers the recheck check words to the VRD board. The VRD uses one token and the recheck check words to create an output signal for 50 milliseconds if the main and recheck check words were correct. If any of the check words are incorrect or not delivered on time the output signal is not present.

The output signal from the VRD board energizes a 100-ohm vital relay. Contacts on this relay or its repeaters are used to supply power to vital outputs on the Single-Break Vital Output PCB, Double-Break Vital Output PCB, Lamp Driver Vital Output PCB, and AC Vital Output PCB. Thus if any of the check words are incorrect, power is disconnected from all of the vital outputs.

The Vital Serial Controller PCB converts parameter values into a message packet that is transmitted to a VSC board at another interlocking. The message packet incorporates check words to indicate that the VSC is performing its functions correctly.

Since the Nonvital Output PCB and the Extended Code System Emulator PCB have nonvital outputs, they do not incorporate check words to provide safety.

1.4.5 Computer Aided Application (CAA) Package

The application programming of the VPI® system is accomplished by using the GRS Computer Aided Applications (CAA) software package which runs on a personal computer. While the system software is identical for all VPI® systems, the application software must be customized for each location. Using track plans, locking tables, and aspect charts the signal engineer writes a set of Boolean expressions which are equivalent to the relay logic circuits for the interlocking.

The CAA package has the ability to:

1. Compile the Boolean expressions into PROM code.

2. Simulate the operation of the interlocking.

3. Produce reports of the hardware to aid in manufacturing, installation, and testing.

4. Burn the PROM code into an EPROM for installation on the CPU board.

5. Independently verify data burned into the EPROM by reconstructing the hardware configuration and Boolean expression list.

6. Compare two sets of PROM codes for differences to aid in checking revisions.

To carry out these functions, the CAA package contains a Compiler Program, a Simulator Program, and an Application Data Verifier Program.

1.5 SAFETY-RELATED FIELD WORK

Safety-related field work on an in-service VPI® system falls into two categories, namely maintenance and modifications. Modifications are changes to the interlocking logic. Examples of modifications are changes in the track layout, revisions of the signal aspects, and corrections of the original application design. Modifications will require changing the application software EPROMs and may require additional PCB changes depending on the new design. Maintenance consists of tracing a system fault to the board level and replacing the failed PCB. The failed PCB may or may not be part of the vital portion of the processor system.

1.6 MAINTENANCE TASKS

Safety-related maintenance tasks would involve replacing one or more of the following boards:

1. Central Processing Unit PCB
2. Polynomial Divider PCB
3. Vital Relay Driver PCB
4. I/O Bus Interface PCB
5. Direct Input PCB
6. Vital Output PCBs (Single-Break, Double-Break, Lamp-Driver, AC)
7. Field Settable Vital Timer PCB
8. Vital Serial Controller PCB

Some of the above safety-related boards contain configuration data that must remain unchanged when the board is replaced. The necessary precautions for replacing the various boards are described below.

1.6.1 Central Processing Unit (CPU) PCB

The CPU board contains the application software stored on EPROMs. DIP switch SW2, which is used to allocate memory for the application software, must be set on the replacement board to match the failed CPU board.

A revision number for the application software is burned into the EPROM and is referred to as the Software Revision Signature. When the CPU board is replaced, the replacement CPU board must contain EPROMs with the current application software. This can be accomplished by removing the EPROMs from the failed board and installing them on the replacement board. Replacement of EPROMs should be performed at a static-safe work station using the proper IC removal and insertion tools to eliminate the introduction of static discharge into the device and to prevent the bending of device leads. As an alternative the CPU board may be replaced by a spare CPU board with the proper application software EPROMs already installed. To ensure the replacement CPU board has the correct application software installed, the binary equivalent of the Software Revision Signature was encoded on the mother board at the time the system was originally installed by wire wrapping the appropriate pins of the CPU-board slot to 5-volt common. A mismatch between this wiring configuration and the Software Revision Signature on the EPROMs causes the system to not operate.

1.6.2 Polynomial Divider (PD) PCB

The PD board may simply be replaced by a spare since there are no application-dependent components on the PD board.

1.6.3 Vital Relay Driver (VRD) PCB

The VRD board contains SW1, a 16-position rotary switch. When replacing the VRD board, SW1 on the replacement board must be set to position "F." This switch position allows the system to attempt to restart if the VRD relay becomes deenergized. With SW1 in any other position, the system makes no attempt to restart.

1.6.4 I/O Bus Interface PCB

The I/O Bus Interface board contains a 36-pin Signature Header IC which is used for routing vital input test data to the proper shift register on the board. When the I/O Bus Interface board is replaced, the replacement board must contain the correct Signature Header. This can be accomplished by removing the Signature Header IC from the failed board and installing it on the replacement board. Replacement of the Signature Header IC should be performed at a static-safe work station using the proper IC removal and insertion tools to eliminate the introduction of static discharge into the device and to prevent the bending of device leads. As an alternative the I/O Bus Interface board may be replaced by a spare I/O Bus Interface board with the proper Signature Header IC already installed.

1.6.5 Direct Input PCBs

Each Direct Input PCB contains a 36-pin Signature Header IC which is used for routing vital input test data to the proper shift register on the I/O Bus Interface board. When a Direct Input board is replaced, the replacement board must contain the correct Signature Header. This can be accomplished by removing the Signature Header IC from the failed board and installing it on the replacement board. Replacement of the Signature Header IC should be performed at a static-safe work station using the proper IC removal and insertion tools to eliminate the introduction of static discharge into the device and prevent the bending of device leads. As an alternative the Direct Input board may be replaced by a spare Direct Input board with the proper Signature Header IC already installed.

1.6.6 Vital Output PCBs

Each Vital Output PCB contains a Signature PROM which contains a unique set of data for each of the outputs on that board. When a Vital Output board is replaced, the replacement board must contain the correct Signature PROM. This can be accomplished by removing the Signature PROM from the failed board and installing it on the replacement board. Replacement of the Signature PROM should be performed at a static-safe work station using the proper IC removal and insertion tools to eliminate the introduction of static discharge into the device and to prevent the bending of device leads. As an alternative the Vital Output board may be replaced by

a spare Vital Output board with the proper Signature PROM already installed. The VPI® system will not operate with missing or wrong Vital Output board Signature EPROMs.

1.6.7 Field Settable Vital Timer (FSVT) PCB

The Field Settable Vital Timer board contains 8 timers that can be set from 0 to 59 minutes, 59 seconds using four jumpers per timer. The time setting for each timer that is used is normally calculated and specified to be the minimum value for the safety in the particular application for that timer. Thus, when a Field Settable Vital Timer board is replaced, each timer used on the replacement board must be set with the specified time setting to maintain the safety of the application. Using a separate time reference (e.g. a stop watch) each time interval on the replacement board should be verified.

1.6.8 Vital Serial Controller (VSC) PCB

The Vital Serial Controller board contains two sets of DIP switches, SW1 and SW4, and application software stored on EPROMs. DIP switches SW1 and SW4, must be set on the replacement board to match the failed VSC board. When the Vital Serial Controller board is replaced, the replacement Vital Serial Controller board must contain EPROMs with the current application software. This can be accomplished by removing the EPROMs from the failed board and installing them on the replacement board. Replacement of EPROMs should be performed at a static-safe work station using the proper IC removal and insertion tools to eliminate the introduction of static discharge into the device and to prevent the bending of device leads. As an alternative the Vital Serial Controller board may be replaced by a spare Vital Serial Controller board with the proper application software EPROMs already installed.

2.0 FAILURE SCENARIOS DURING MAINTENANCE

2.1 MAINTENANCE PROCEDURES

Maintenance and troubleshooting of the VPI® system requires the connection of an external display terminal. This display terminal may be either a personal computer running the GRS Tracker™ Remote Diagnostic Analyzer software or a GRS Hand-Held Terminal (HHT). When the VPI® system is interrogated, a message is displayed on the terminal indicating the probable cause of the problem. The message is looked up in the troubleshooting chart included in the VPI® system's Pamphlet 2086B, Volume I, ***Operation and Maintenance*** to get corrective action instructions.

The troubleshooting procedure may determine that the corrective action required is the replacement of one or more of the safety-related boards described in the previous section of this report. Replacement of a safety-related board is accomplished by performing the following steps:

1. Turn off system power.

2. Unplug the failed board from the mother board.

3. Remove the Signature Header IC, Signature PROM, or system-software and application-software EPROMs from the failed board and install them on the replacement board. As an alternate, install a new board which already has the proper PROMs and EPROMs in place.

4. Set application-dependent switches or jumpers on the replacement board to match the positions on the failed board. Record this information on the board tag, as appropriate.

5. Install the replacement board in the same slot in the mother board as the failed board was removed from.

6. Turn on system power.

7. Observe the external display terminal for error messages.

8. Observe that the external VRD relay becomes energized.

9. Perform operational tests.

10. Verify configuration information.

11. Update the Service Log.

12. Return the system to service.

A review of this board-replacement procedure was conducted. Possible failure scenarios are based on not properly performing Steps 4, 5, 6, or 7. The general categories of potential problems include:

- Failure to install a PROM or EPROM
- Installation of an incorrect PROM or EPROM
- Failure to set applications switches on boards correctly
- Failure to properly install a board

These failure scenarios are examined in detail below.

2.1.1 Missing or Incorrect Signature Header ICs

A Signature Header IC is installed in a socket on each of the I/O Bus Interface boards and Direct Input boards. Signature Header ICs are used for routing vital input test data from one data line on the bus on which it is received to a different data line on the same bus for return to the point of origin. Thus, a Signature Header takes as an input information that originates on each of the 16 data-bus lines and swaps it for return on a different data-bus line.

Vital input test data is originated on the CPU board, is routed via the data bus to the Direct Input Board where it is circulated to test all of the inputs. The results of the input tests is then routed through a Signature Header on the Direct Input board to return the test data on different lines of the same data bus to the I/O Bus Interface board, where it is similarly routed through a Signature Header on the I/O Bus Interface board and delivered to a shift register on the I/O Bus Interface board. This scrambling of the data bus lines when reading vital input test data prevents address failures of the nonvital logic elements from compromising system safety.

One possible failure scenario is that the Signature Header will be missing from a replacement I/O Bus Interface or Direct Input board. This will not compromise safety because the vital input test data will never be delivered to the shift registers and the inputs will be interpreted as being OFF.

Another possible failure scenario is that an incorrect Signature Header will be installed on one or more I/O Bus Interface or Direct Input replacement boards. An incorrect Signature Header will cause

vital input test data to be routed to the wrong shift register. The misrouted data will not be the correct TRUE word for the vital input corresponding to the shift register. This will not compromise safety because the vital input will be interpreted as being OFF.

2.1.2 Missing or Incorrect Signature PROMs

A Signature PROM is installed in a socket on each of the Vital Output boards. A Signature PROM contains a unique set of data words for each of the eight outputs on that board. This output check data is circulated through the AOCD associated with each output.

One possible failure scenario is that the Signature PROM will be missing from a replacement Vital Output board. When the system tries to read the data words on the Signature PROM, it will not detect the missing PROM but the data will be all zeroes. When these words are circulated through an AOCD, it will appear to the monitoring circuitry as if current is flowing in an output when the output is turned off. The system will fail to generate a proper recheck check word and the VRD relay will not become energized.

Another possible failure scenario is that the incorrect Signature PROM will be installed on a replacement Vital Output board. The incorrect Signature PROM will circulate the wrong output check data through the AOCD and an incorrect result will be processed and stored. The recheck check word based on this result will be invalid and the VRD relay will not become energized.

2.1.3 Missing or Incorrect System-software EPROMs

System-software EPROMs are installed in sockets on the CPU board and the VSC board. The system software is the software required to make any VPI® application work and includes the Safety Assurance Logic which verifies that the system is functioning as intended. Four system-software EPROMs are installed on a CPU board and one system-software EPROM is installed on a VSC board.

One possible failure scenario is that one or more of the system-software EPROMs will be missing from a replacement CPU board. Another possible failure scenario is that an incorrect system-software EPROM will be installed on the CPU replacement boards. This could occur if a system-software EPROM for a VSC board were installed on a replacement CPU board. In either case, without all of the correct system-software EPROMs installed on the CPU board, the VPI® system will be completely inoperative and the VRD relay will not become energized.

Another class of possible failure scenarios involves the system-software EPROM on a VSC board. The system-software EPROM could be missing from a replacement VSC board or a system-software EPROM for a CPU board could be installed on a replacement VSC board.

Although the system will not detect that the system-software EPROM on the replacement VSC board is missing or incorrect, the VSC board will not function without the correct system-software EPROM and so no controls will be transmitted and no indications will be received over the serial data link.

2.1.4 Missing or Incorrect Application-software EPROMs

Application-software EPROMs are installed in sockets on the CPU board and the VSC board. The application software is the software which is unique to a particular application or location. One application-software EPROM is used on a VSC board and six sockets are reserved for application-software EPROMs on a CPU board. Four of the six sockets on a CPU board are used for Application-software EPROMs and the remaining two sockets are used for optional Shadow Application-software EPROMs. CPU board DIP switch SW2 is used to select using the optional 32K of Shadow Application-software EPROMs.

One possible failure scenario is that the application-software EPROM will be missing from a replacement VSC board. This failure scenario is similar to having a replacement VSC board with a missing or incorrect system-software EPROM. Although the system will not detect that the application-software EPROM on the replacement VSC board is missing, the VSC board will not function without this EPROM and so no controls will be transmitted and no indications will be received over the serial data link.

Another possible failure scenario is that an incorrect application-software EPROM will be installed on a replacement VSC board. If the application-software EPROM has incorrect link numbers, message lengths, block numbers, source data, or destination data an incorrect check field will be generated. In this case no controls will be successfully transmitted and no indications will be successfully received over the serial data link.

Another possible failure scenario is that an incorrect application-software EPROM that has the correct link numbers, message lengths, block numbers, source data, and destination data will be installed on a replacement VSC board. This could occur if the list of parameters being transmitted had the position of two parameters interchanged. A checkword generated from the list of parameters is transmitted as part of the message. This incorrect checkword from the transmitting VPI would not match the checkword expected at the receiving VPI and the image field would not be interpreted as having true parameter values.

Another possible failure scenario is that one or more application-software EPROMs will be missing from a replacement CPU board. If one of the four normal application-software EPROMs were missing, the system will fail to generate a proper main check word and the VRD relay will not become energized. Similarly if DIP switch SW2 is set for using the optional 32K of memory and one of the Shadow Application-software EPROMs were missing, the system will fail to

generate a proper main check word and the VRD relay will not become energized.

Another failure scenario is that one or both of the Shadow Application-software EPROMs were missing and DIP switch SW2 was incorrectly set to not use the additional 32K of memory. In this case the system would produce an incorrect memory checksum. The system will then fail to generate a proper main check word and the VRD relay will not become energized.

Yet another possible failure scenario is that an incorrect application-software EPROM will be installed on a replacement CPU board. If the Software Revision Signature contained on any of the application-software EPROMs does not match the hardware signature on the wire wrap pins of the Mother board, the VRD relay will not become energized.

The designer is responsible for maintaining unique Software Revision Signatures for each CPU on the system. Since the number of Software Revision Signatures is limited, this may not be possible, and a set of application-software EPROMs for another location may have the same Software Revision Signature as this location. A possible failure scenario is that a set of application-software EPROMs for another location with the same Software Revision Signature as this location are installed on the replacement CPU board. Since the Software Revision Signature matches the hardware signature on the wire wrap pins of the mother board at this location this failure may not be detected. A variation of this scenario is that a complete set of VPI® boards for a location is replaced with a complete set of boards from a different but similar location. Unsafe conditions might occur if the field equipment for the two locations are similarly wired to the VPI® system but there is a subtle difference between the locations like the track speed of the turnout involved.

It is also possible to have an incorrect application-software EPROM which has the correct Software Revision Signature. For example, suppose the CPU board should have four application-software EPROMs which we will refer to as numbers 1, 2, 3, and 4. It is possible to substitute an incorrect EPROM and thus have a duplicate of another EPROM in its socket (e.g. 1, 2, 2, and 4). This would result in some of the Boolean equations (i.e. those on EPROM 3) not being evaluated. In this case the system would produce an incorrect memory checksum. The system will then fail to generate a proper main check word and the VRD relay will not become energized.

2.1.5 Incorrectly Set On-board Switches

Application-dependent, on-board switches are located on the CPU, VRD, and VSC boards. The CPU board contains DIP switch SW2, which is used to allocate memory for the application software. The VRD board contains a 16-position rotary switch SW1, which is used to allow the VPI® system to attempt to restart if the VRD relay

becomes deenergized. The VSC board contains two sets of DIP switches, SW1 and SW4. SW1 is used to configure handshake signals to the Serial Communications Controller. SW4 is used designate memory sizes and reset functions.

One possible failure scenario is that CPU board DIP switch SW2 may be set for using the additional 32K of memory when no Shadow Application-software EPROMs are installed. Conversely, SW2 may be set to use only the standard application-software EPROMs when in fact Shadow Application-software EPROMs are installed. In either case the system will fail to generate a proper main check word and the VRD relay will not become energized.

Another possible failure scenario is that VRD board switch SW1 may not be set to position "F." This will not cause an unsafe condition since with switch SW1 in any other position, the system makes no attempt to automatically restart.

Another possible failure scenario is that VSC board DIP switch SW1 is incorrectly set. In this case the handshake signals will be incorrect so no controls will be successfully transmitted and no indications will be successfully received over the serial data link.

Another possible failure scenario is that VSC board DIP switch SW4 is incorrectly set. In this case the size of the EPROMs will be incorrectly designated. If the switch designates 16K of memory when a 32K EPROM is installed, portions of the application software will not be accessed. Under these conditions, the system will fail to access the additional memory and the memory checksum will be incorrect. This will result in the VRD relay not being energized.

2.1.6 Missing or Incorrect Time Setting Jumpers

Application dependent time setting jumpers are installed on the FSVT boards. Four jumpers are used to determine the time setting for each of the eight timers on the board. When a FSVT board is replaced, the replacement board must contain the correct time setting jumpers.

One possible failure scenario is that one or more jumpers will be missing from the replacement FSVT board, however, the failure to install all four jumpers for a timer setting results in a timing cycle that never expires. Thus, a missing jumper would not result in an unsafe condition.

Another possible failure scenario is that a time interval will be set incorrectly. If the set time interval is shorter than intended an unsafe condition will arise. All of the time intervals associated with the replaced FSVT board must be verified to function correctly using a separate time reference such as a stop watch.

2.1.7 Main CPU Bus Ribbon Cable Improperly Connected

The main CPU bus ribbon cable is connected to the lower edge connectors of the CPU, VRD, Polynomial Divider, CSEX, and VSC boards. A possible failure scenario is that the main CPU bus ribbon cable will not be properly connected to a replacement board. This will cause the VPI® system to be either completely inoperative or to fail to generate the correct main check words. Neither of these alternatives will compromise system safety because the VRD relay will not become energized.

2.1.8 Expansion Module Cable Improperly Connected

The expansion module cable is connected to the upper edge connectors of the I/O Bus Interface boards in the main system module and any expansion modules. A possible failure scenario is that the expansion module cable will not be properly connected to the I/O Bus Interface replacement board. This scenario will result in the system being unable to read any inputs from the expansion module and being unable to energize any outputs in that module. This is not an unsafe condition.

2.1.9 VRD Relay Cable Improperly Connected

The VRD relay cable is connected to the upper edge connector on the rear of the VRD board. The other end of the cable connects to the external VRD relay through a plug coupler on the rear panel. A possible failure scenario is that this cable will not be properly connected to the replacement VRD board. This will not compromise system safety because the VRD relay will not become energized.

2.1.10 Direct Input Cables Improperly Connected

Standard cables are used to connect the upper and lower edge connectors on the rear of the Direct Input board to field apparatus through plug couplers on the rear panel. One possible failure scenario is that this cable will not be properly connected to the replacement Direct Input board. Failure to properly reconnect these cables will result in the VPI® system being unable to read the inputs associated with the replaced Direct Input board. This is not an unsafe condition.

2.1.11 Vital Output Cables Improperly Connected

Standard cables are used to connect the upper and lower edge connectors on the rear of the Vital Output boards to field apparatus through plug couplers on the rear panel. One possible failure scenario is that this cable will not be properly connected to a replacement Vital Output board. Failure to properly reconnect this cable will result in the VPI® system being unable to energize

the outputs associated with the replaced Vital Output board. This is not an unsafe condition.

2.1.12 VSC Cable Improperly Connected

A standard cable is used to connect the upper edge connector on the rear of the VSC board to field apparatus through a plug coupler on the rear panel.

One possible failure scenario is that this cable will not be properly connected to a replacement VSC board. In this case no controls will be successfully transmitted and no indications will be successfully received over the serial data link. This is not an unsafe condition.

2.1.13 Incorrect Installation of a Replacement Board

A replacement board should be installed in the same slot as the defective board was removed from. Installation of the replacement board in the wrong slot or improper installation of the replacement board in the correct slot will cause one of the following:

1. The system will be completely inoperative.

2. The system will not detect that the board is in the wrong slot and the system will function normally.

3. The system will detect that the board is in the wrong slot or improperly installed and the VRD relay will remain deenergized.

None of these alternatives will compromise system safety.

2.1.14 Incorrect Group Number for a FSVT Board

Replacement FSVT boards must have the same group number as the failed board. Each FSVT board has unique data for each of the eight timers which is stored in an EPROM on the board. If more than one FSVT board is used, they must have different Group Numbers to maintain the uniqueness of this data.

A possible failure scenario is that a replacement FSVT board may have a Group Number which duplicates that of another FSVT board in the module. In this case, none of the time intervals associated with the board with the incorrect Group Number will ever expire.

2.2 FAILURE SCENARIOS DURING FIELD REVISION

Unlike maintenance activity which returns the system to the condition it was in before the activity began, making field

revisions leaves the VPI® system in a condition different than when the activity began.

Revisions to the track layout, the signal aspects, the methods of operation, and the type of link used in the data transmission system are some of the common reasons for making field revisions. Another common reason is to correct errors made during the initial system design. Some of these errors are quite subtle and are not detected during the testing when the system is first placed in service. Other of these 'errors' result from changes in the Transportation Department's requirements for train operation or misunderstandings of what was originally required.

Field revisions fall into the following categories:

1. Revising the CPU application software and possibly reconfiguring the system.

2. Revising the field settable time elements.

3. Revising the VSC application software.

The failure scenarios while making field revisions are described below.

2.2.1 Revising the CPU Application Software

Revisions to the track layout, revisions to the signal aspects, and the correction of errors made during the initial system design will require revisions to the Boolean equations which represent the applications logic (circuits) of the interlocking. These revisions, in turn, will require revision to the application software on some or all plug-in EPROMs on the CPU board. Revisions might also require reconfiguring the system because the quantity of inputs, outputs, or equations is greater than the capacity of the hardware already present. New boards, expansion modules, or both might be required.

To perform these revisions, the designer prepares a new design or revisions to the old design (depending on how extensive the revisions are) in the form of circuit sketches and develops Boolean equations from these sketches. The designer also prepares equipment specifications and then uses the CAA compiler program to prepare the revised coding for the application-software EPROMs and the other system elements.

As part of this design effort, the designer specifies a Software Revision Signature as part of the Compiler Input file for the CAA Compiler Program. The Software Revision Signature corresponds to a revision number (1 through 62) for the new application software for a specific location. Any time the application software is modified, the revision number should be changed.

The binary equivalent of the Software Revision Signature is encoded on the Mother board by revising the wire wrap arrangement of the appropriate pins for the CPU-board slot to 5-volt common. The CAA Compiler program creates a list of these wire wrap assignments and burns the Software Revision Signature onto the application-software EPROMs on the CPU board. A mismatch between this wiring configuration and the Software Revision Signature on the EPROMs causes the system to not operate and thus assures, in the future, that the proper applications program is installed.

Within the limitations of the quantity of signatures available, each location on the system as well as each revision of the software should have a unique Software Revision Signature to guarantee that the correct application-software EPROMs are installed in each VPI® system module. The designer is responsible for revising the Software Revision Signature for each new application and maintaining unique Software Revision Signatures for each CPU on the system.

Some of the possible failure scenarios when revising the CPU application software are similar to those for replacing a defective CPU board. These include:

1. Missing or incorrect system-software EPROMs
2. Missing or incorrect application-software EPROMs
3. Incorrectly set on-board switches
4. Main CPU bus ribbon cable improperly connected
5. Incorrect installation of a replacement CPU board

The consequences of these failures were treated in the previous section.

Another possible failure scenario when revising the CPU application software is that the Boolean equations were designed or encoded incorrectly.

Yet another possible failure scenario when revising the application software is that a change made in one area of the logic unexpectedly affects another area of the logic.

These two scenarios would be equivalent to circuit design or circuit drafting errors.

Still another possible failure scenario when revising the application software is that hardware specification lists or communications links will have errors. These would be equivalent to detailing errors.

There are no inherent characteristics of the VPI® system that will permit detection of these three failure scenarios any more than such failures could be detected in an all-relay or mechanical system.

2.2.2 Revising the Field Settable Time Elements

By making a time element field settable, it can be changed at will due to field-dictated changes, such as revision of train speed limits, without reprogramming the system. The field settable time elements are contained on the FSVT boards.

Some of the possible failure scenarios when revising the field settable time elements are similar to those for replacing a defective FSVT board. These include:

1. Missing or incorrect time-setting jumpers
2. Incorrect installation of a replacement board
3. Incorrect Group Number for a FSVT board

The consequences of these failures were treated in the previous section.

2.2.3 Revising the VSC Application Software

Revisions to the type of link used in the data transmission system or the correction of errors made during the initial system design will require revisions to the application software on some or all plug-in EPROMs on the VSC board.

Some of the possible failure scenarios when revising the VSC application software are similar to those for replacing a defective CPU board. These include:

1. Missing or incorrect system-software EPROMs
2. Missing or incorrect application-software EPROMs
3. Incorrectly set on-board switches
4. VSC cable improperly connected
5. Incorrect installation of a replacement VSC board

The consequences of these failures were treated in the previous section.

Another possible failure scenario is that the VSC application software was designed incorrectly, that is, the communications links and parameter lists have errors. This scenario would be equivalent to detailing errors.

There is no inherent characteristic of the VPI® system that would detect such errors.

3.0 RECOMMENDATIONS FOR REVISIONS AND ADDITIONS TO THE RS&I

3.1 IDENTIFICATION OF APPLICABLE RS&I SECTIONS

The ultimate goal of this study is to determine whether revisions are required to the RS&I due to the introduction of microprocessor-based signal systems and to suggest such revisions if they are indicated. As the next step towards reaching this goal, a survey was conducted of the RS&I to identify those sections that apply to microprocessor-based signal systems of the types studied.

Sections not applicable to microprocessor-based signal systems fell into two categories:

1. Sections that state general requirements.

2. Sections that apply to other systems, devices, or appliances.

Sections in these categories were eliminated from further consideration.

Table 3-1 shows the sections that are applicable to one or both of the microprocessor-based signal systems and whether the section may require revision. For definitions, only those definitions that require revision are cited.

The following paragraphs state the reasoning used to prepare this table.

Sections 236.2, 236.4, 236.11 are general rules and instructions applying to all systems, including microprocessor-based systems. The wording of these sections, as presently written, can be applied to microprocessor-based systems and so there is no need to revise these sections to accommodate such systems.

Section 236.5 establishes the basic design criteria for failsafe electrical and electronic systems and devices. Because closed-circuit principles are not the only principles required to make microprocessor-based systems failsafe, this section should be amplified to include the minimum design requirements for microprocessor-based systems.

Section 236.8 establishes maintenance requirements for signal apparatus which affect the safety of train operation. Such requirements also apply to microprocessor-based systems and so the wording of this rule should be extended to apply to these systems, as well.

Table 3-1. RS&I Sections Applicable to Microprocessor-based Signal Systems

Section Number	VPI® Applies	VPI® Requires Revision	GENRAKODE™ Applies	GENRAKODE™ Requires Revision
236.2	X		X	
236.4	X		X	
236.5	X	X	X	X
236.8	X	X	X	X
236.11	X		X	
236.51			X	
236.56			X	
236.101	X	X	X	X
236.106	X	X	X	X
236.109	X	X	X	X
236.110	X		X	
236.303	X	X		
236.304	X	X		
236.305	X			
236.307	X			
236.308	X			
236.309	X	X		
236.311	X	X		
236.377	X			
236.378	X			
236.379	X			
236.380	X			
236.381	X			
236.410	X	X	X	X
236.717	X	X	X	X
236.737			X	X
236.750	X	X		
236.761	X	X		
236.813a	X	X		

Sections 236.51 and 236.56 are general rules and instructions applying to all track-circuit systems, including microprocessor-based systems. The wording of these sections, as presently written, can be applied to microprocessor-based systems and so there is no need to revise these sections to accommodate such systems.

Section 236.101 defines the general requirements for inspection and tests applying to all systems. The wording of this section needs revision to extend the requirements to microprocessor-based systems.

Section 236.106 defines the inspection and test requirements for relays, the principal component of most conventional signal systems. This section should be amplified to deal with the components of microprocessor-based systems.

Section 236.109 defines the requirement for testing time releases, timing relays, and timing devices. Although microprocessors used in solid-state timers are regarded as timing devices, a microprocessor controlling an interlocking or a track circuit is not normally thought of as a timing device. Therefore, this section should be revised to specifically require testing of time intervals controlled by microprocessor-based systems.

Section 236.110 defines the general requirements for dealing with the results of inspection and tests applying to all systems. The wording of this section, as it is presently written, can be applied to microprocessor-based systems and so there is no need to revise it to accommodate such systems.

Sections 236.303 and 236.304 are general design standards for control circuits at interlockings. The wording of these sections is based on relay circuits. These sections should be revised to allow the same protection to be provided by means of microprocessor-based systems.

Sections 236.305, 236.307, and 236.308 are also general design standards for control circuits at interlockings, however, the wording of these sections is general enough to be applied to microprocessor-based systems as well as to conventional systems. Therefore, the wording of these sections need not be revised to accommodate microprocessor-based systems.

Sections 236.309 and 236.311 are interlocking design standards for providing loss-of-shunt protection and for routing signal control over switch selection. While the principles embodied in these sections should apply to microprocessor-based systems, the actual wording of these sections now specifically applies only to relay-based systems. Therefore, the wording of these sections needs revision to extend the sections' application to microprocessor-based systems.

Sections 236.377, 236.378, 236.379, 236.380, and 236.381 are requirements for testing various types of electric locking. All five sections require that the locking "shall be tested when placed in service and thereafter when modified, disarranged, or at least once every two years, whichever shall occur first." Various railroads apply different interpretations to the word "disarranged." Some railroads consider the locking to be disarranged when a plug-in relay is replaced, while others do not. Not withstanding the Federal Railroad Administration's January 3, 1985 letter to the Association of American Railroads, variations in interpretation of these sections by both railroads and FRA inspectors, all of whom may have serious interest in meeting both the spirit and the letter of the FRA RS&I, has continued. The interpretation of these sections, and the precedent set by their

interpretation for relay-based systems, will also be critical when determining the testing requirements following replacement of a printed-circuit board or an integrated-circuit chip that is part of a microprocessor-based signal systems. Therefore, it appears that rather than set specific requirements for relay-based systems, microprocessor-based systems, and potentially, other systems in these five sections, a more prudent approach might be to deal with the word "disarranged" in Subpart G-Definitions of Part 236. Thus, no changes are recommended for the wording of these sections but an additional definition in Subpart G is suggested, as discussed in the next section of this report.

Section 236.410 defines design requirements for hand-operated switches in traffic control systems. These same requirements should apply to microprocessor-based systems, however, the wording of the section is now only relevant to relay-based systems. This section should be revised so that the wording is applicable to both relay systems and to microprocessor-based systems.

Definitions displayed in **Sections 236.717, 236.737, 236.750, 236.761, and 236.813a** should apply to microprocessor-based systems as well as to conventional systems. The wording of these definitions, though, presently applies to conventional systems only. Therefore, revisions are suggested to extend the meaning of these definitions to microprocessor-based systems.

3.2 DISCUSSION OF REVISIONS AND ADDITIONS TO THE RS&I

It is the purpose of this study to make suggestions for revisions and additions to the RS&I to accommodate microprocessor-based systems so that the application and enforcement of these safety requirements can be made uniformly to these systems. These suggestions are based on the maintenance and field-change procedures identified in the earlier parts of this study.

In these recommendations for rewording the requirements of the RS&I to accommodate microprocessor-based systems, the words "software-controlled" are used instead of "microprocessor-based." Earlier sections of this report established that the main characteristic of systems such as VPI® and Genrakode™ that differentiate these systems from conventional signal systems is that their operation is controlled by stored computer programs, or software, rather than by hardware characteristics, such as wiring or mechanical locking. Microprocessors are only one potential embodiment of such systems. There is no reason, other than economics, why such systems could not be built using minicomputers or even main-frame computers. Furthermore, future technological developments may result in still other embodiments. Thus, to make the recommended revisions to the RS&I as general as possible, the phrase "software-controlled systems" has been adopted.

There are three principal areas to be considered during revision of the RS&I to accommodate software-controlled systems. They are:

1. Adding requirements and sections that recognize the unique nature of software-controlled systems.

2. Adjusting the wording of rules written specifically for relays and relay circuits so that the principles of the rules are extended to software-controlled systems.

3. Addressing the requirements for testing software-controlled systems after servicing due to a failure which requires the replacement of a system component such as a printed circuit board or a plug-in integrated circuit.

In addressing the first of these areas, it is noted that the RS&I presently does not contain any rules, standards, or instructions that directly address software-controlled signal systems. New sections or portions of sections should be added to the RS&I to govern these systems. These additions will perform a similar function as existing sections do for mechanical and relay-based signal systems. In some cases the existing sections will be expanded to include software-controlled systems.

Previous sections of this report have developed that the safety of software-controlled systems is derived from a continuous check of the system's operation. This self-checking feature for obtaining safety from software-controlled systems is directly comparable to the closed-circuit principles used in American signaling technology for obtaining safety from hardware systems such as all-relay interlockings. Therefore, requirements for this principle have been added to the general design criteria and sections defining software-controlled systems and self-checking principles have been added to the definitions of the RS&I.

Section 236.106 defines requirements for testing relays and states how often relays of each type should be tested. Periodic testing of relays is required because there are mechanical and electrical wear mechanisms at work in these devices which might result in the relay developing a failure mode which would affect the safety of train operation. Experience has taught industry the time period that should be specified between such tests. Software-controlled systems do not have known failure mechanisms of this type. Therefore, the requirement for periodic testing of software-controlled systems' components, assemblies, and subassemblies cannot be logically justified. However, units should be tested before being placed in service to assure that their operation meets the requirements of the system. Therefore, an addition to the relay testing section is suggested to require the testing of the component parts of a software-controlled signal system before it is placed in service. **On the other hand, no relaxation of the periodic testing of locking implemented by software-controlled systems can be justified because such testing includes components**

external to the software-controlled system that would not otherwise be tested in compliance with the RS&I.

It is a relatively straightforward matter to address the second of these areas. The RS&I has be reviewed to identify each of the sections that are applicable to software-controlled systems. For sections identified as being applicable, the wording was examined to be sure that it was neutral with respect to the embodiment addressed. Embodiment-neutral sections discussed principles of operation rather than detailed implementation requirements. For those sections that were not embodiment neutral, revised wording was developed which would include software-controlled systems without changing the requirements for conventional systems.

Addressing the third of these areas was more difficult because the RS&I is not clear as to the requirements for conventional systems during maintenance and there is disagreement among well-intentioned signal engineers about what is required by the RS&I and what is reasonably needed to maintain the integrity of the signal system.

The GRS Genrakode™ Track Circuit and Communication System is a relatively simple system. Therefore conducting a complete operational test after performing maintenance or modifications would not be time consuming. Thus, retesting a Genrakode™ installation was not really an issue when considering revising the RS&I.

Retesting an interlocking implemented with a software-controlled system is another issue, though. While it can be argued that the RS&I requires retesting only the affected locking if a single relay of an all-relay interlocking were replaced during maintenance, and that retest would not be disruptive, replacing a single plug-in printed-circuit board of software-controlled system could affect virtually all the locking of the interlocking because of the concentration of functions onto a small number of components. Such a retest following maintenance would be time consuming and thus disruptive. This is especially true because software-controlled systems are particularly advantageous when applied to larger interlockings which, in turn, would result in a greater penalty should retesting be required. For this reason, an alternate approach will be examined.

It should be clearly understood, though, that this alternate approach, which is discussed below, is meant to apply when components are replaced in kind during maintenance. There is no supportable reason to revise the retest requirement following revisions to the design of either a conventional or a software-controlled system because experience has taught that revisions to one logical function frequently affect the operation of another, nominally unrelated function because of sometimes-subtle coupling of logic between the functions.

As mentioned earlier in this report, the requirement for retesting following maintenance is established by Sections 236.377 through 236.381. In these sections, the key word is "disarranged." While

the word "disarranged" is not defined in the RS&I, an FRA response of January 3, 1985 to an earlier AAR letter interpreted the meaning of this expression. This response stated, among other factors, that "Electric locking is considered to be disarranged when (i) a relay is replaced with another..." Since printed-circuit-board modules of a software-controlled system are the functional equivalents of relays in an system employing traditional electric locking, extension of this principle would mean that software-controlled systems would require retesting following most maintenance activities on those systems.

The cited FRA letter justifies this approach on very reasonable grounds, namely "Major sources of false proceed failures for more than five years have been errors in connection and errors in design." Clearly, when system design is modified, there is the possibility that the design modifications, no matter how minor they may seem, might introduce subtle changes in the operation of a system which might render the system less safe than desirable. Therefore, system retesting, no matter whether the system is relay-based or software-controlled, seems imperative. That leaves the matter of errors in connection for further consideration.

The interpretation of the rules cited in the FRA letter makes no distinction among the various types of safety relays that are used at interlockings. Four types commonly used are shelf-mounted relays, with and without plug couplers, and plug-in relays, with and without registration. There can be no argument that connection errors can be made while replacing one shelf relay without a plug coupler with another. There also can be no argument that replacing one plug-coupled shelf relay with another or replacing a nonregistered plug-in relay with another might result in an incorrect substitution which, in turn, might compromise safety if the relay replaced has the wrong contact complement or wrong operating characteristics. Only testing, following the relay replacement, can assure that the work had been done properly. However, it is more difficult to envisage replacing one registered relay with another tested, registered relay and, in the process, compromising safety.

With this in mind, a new definition is suggested herein for inclusion in the RS&I. This definition would define "disarranged" as interpreted in the cited FRA letter but would establish an exemption for replacing one registered, plug-in relay with another tested, registered, plug-in relay. This revision would provide a basis for uniform application of the RS&I to all-relay systems and would also establish a basis for considering the conditions under which maintenance on software-based systems might be exempt from the locking tests required by the RS&I following maintenance. If this premise for exempting the replacement of registered relays is unacceptable, there does not appear to be any logical rationale for exempting software-controlled systems from complete retest following any maintenance.

The first part of this study established that the GRS VPI® system used two general classes of printed circuit boards, namely,

1. Those containing no adjustments and no plug-in memory chips; and

2. Those containing adjustments, plug-in memory chips, or both.

This arrangement would probably be true for any manufacturer's system.

Boards of the first type would be interchangeable between location and could thus be used, without modification, at any location. Since there normally would be boards of various types that fit into this category, these boards could be mechanically registered, electrically registered, or both, to assure that only the correct type of board could be plugged into a socket and have the system operate at all.

Boards of the second type would contain applications software or other adjustments which would make them unique for a particular application, unique for a particular interlocking or unique for a particular system at an interlocking when an interlocking is so large that more than one system is required. To assure that only the correct type of board, and then only with the correct software or adjustment is used, "unique registration" would be required of these boards to permit replacement without a complete retest. "Unique Registration," in this case, means that a plug-in board would work with only one mother board or system module, namely the one of the particular interlocking under consideration. This arrangement would establish the requirement for thousands of potential registrations which would not be difficult to realize using other than mechanical means.

The acceptance of the sanctity of registration for modules comprising a software-controlled system would permit adopting an exemption for testing following maintenance under the disarranged locking rule. This would not be a great leap in faith because registration is already used in signaling, as well as in other areas, to enforce the use of correct replacement parts in safety-critical systems.

The remainder of this section justifies, in detail, the reasonableness of this approach using the analysis of the GRS system.

The first part of this study examined failure scenarios during maintenance. The general categories of potential problems include:

1. Failure to install a PROM or EPROM.

2. Installation of an incorrect PROM or EPROM.

3. Failure to set applications switches on boards correctly.

4. Failure to properly install a board.

Failures in category one may result in the inputs for the replacement board being interpreted as being OFF, the VRD relay not being energized, the vital serial data link being inoperative, or the entire system being inoperative. None of these failures result in an unsafe condition so no special precautions are required.

Failures in category two may result in the inputs for the replacement board being interpreted as being OFF, the outputs for the replacement board failing to be energized, the VRD relay not being energized, the vital serial data link being inoperative, the entire system being inoperative, or the system functioning incorrectly. The last case could result from the application-software EPROMs for a similar location with the same Software Revision Signature being installed. This case would only be detected by a complete operational test being performed after the maintenance was completed.

Failures in category three may result in the VRD relay not being energized, the vital serial data link being inoperative, or the system functioning incorrectly. This last case could result from incorrect time-setting jumpers. If the set-time interval is shorter than intended, an unsafe condition will arise. This case would only be detected by verifying that all of the time intervals associated with a replaced FSVT board function correctly using a separate time reference.

Failures in category four may result in the inputs for the replacement board being interpreted as being OFF, the outputs for the replacement board failing to be energized, the VRD relay not being energized, the vital serial data link being inoperative, the entire system being inoperative, or time intervals not expiring. None of these failures result in an unsafe condition so no special precautions are required.

Failure scenarios while making field revisions were also examined in the first part of this study. Field revisions fall into the following categories:

1. Revising the CPU application software and possibly reconfiguring the system.

2. Revising the field-settable time elements.

3. Revising the VSC application software.

It was determined that when revising the CPU application software, the settable time elements, or the VSC application software, failure scenarios could occur which are equivalent to circuit design, circuit drafting, or detailing errors in an all-relay or a mechanical system. There are no inherent characteristics of the VPI® system that will permit detection of these failure scenarios any more than such failures could be detected in an all-relay or mechanical system without performing operational testing. Thus, it

is recommended that revision to any application logic warrants a complete operational test of the interlocking or interlockings affected.

3.3 REVISIONS AND ADDITIONS TO THE RS&I

In light of the above discussion, the following revisions and additions to the RS&I are recommended. Additions and revisions are highlighted by appearing with a shaded background.

§ 236.5 Design of control circuits on closed-circuit principle; design of software-controlled systems on self-checking principle.

All control circuits whose functioning affects safety of train operation shall be designed on the closed-circuit principle except for roadway equipment of intermittent automatic train-stop system. All software-controlled systems whose functioning affects safety of train operation shall be designed using self-checking principles.

§ 236.8 Operating characteristics of electromagnetic, electronic, electrical, or software-controlled apparatus.

Signal apparatus, the functioning of which affects the safety of train operation, shall be maintained in accordance with the limits within which the device is designed to operate.

§ 236.101 Purpose of inspection and tests; removal from service of relay, device, or system failing to meet test requirements.

The following inspections and test shall be made in accordance with specifications of the carrier, subject to approval of the FRA, to determine if the apparatus and/or equipment is maintained in condition to perform its intended function. Software-controlled system, electronic device, relay, or other electromagnetic device which fails to meet the requirements of specified tests shall be removed from service and shall not be restored to service until its operating characteristics are in accordance with the limits within which such system, device or relay is designed to operate.

§ 236.106 Relays and components of software-controlled systems.

(a) Each relay whose function affects the safety of train operations shall be tested at least once ever four years except:

(1) Alternating-current centrifugal-type relay shall be tested at least once ever 12 months;

(2) Alternating-current vane-type relay and direct-current polar-type relay shall be tested at least once every 2 years; and

(3) Relay with soft iron magnetic structure shall be tested at least once ever 2 years.

(b) Each replaceable assembly and subassembly of a software-controlled system whose function affects the safety of train operations shall be tested before being placed in service.

§ 236.109 Time releases, timing relays and timing devices.

Time releases, timing relays, and timing devices, including software-controlled systems, shall be tested at least once every twelve months. The timing shall be maintained at not less than 90 percent of the predetermined time interval, which shall be shown on the plans or marked on the time release, timing relay, timing device, or software-controlled system.

§ 236.303 Control circuits for signals, selection through circuit controller operated by switch points or by switch locking mechanism.

The control circuit for each aspect with indication more favorable than "proceed at restricted speed" of power operated signal governing movements over switches, movable-point frogs, and derails shall be selected through circuit controller operated directly by switch points or by switch locking mechanism or through relay controlled by such circuit controller, or shall be energized by software-controlled system controlled by such circuit controller, for each switch, moveable-point frog and derail in the routes governed by such signal. Circuits shall be arranged so that such signal can display an aspect more favorable than "proceed at restricted speed," only when each switch, moveable-point frog, and derail in the route is in proper position.

§ 236.304 Mechanical locking or same protection effected by circuits or a software-controlled system.

Mechanical locking, or the same protection effected by means of circuits or a software-controlled system, shall be provided.

§ 236.309 Loss-of-shunt protection; where required.

(a) A loss of shunt of 5 seconds or less shall not permit an established route to be changed at an automatic interlocking.

(b) A loss of shunt of 5 seconds or less shall not permit the release of route locking of each power-operated switch hereafter installed.

§ 236.311 Signal control circuits, selection through track relays or devices functioning as track relays and through signal mechanism contacts and time releases at automatic interlocking.

(a) The control circuits for aspects with indications more favorable than "proceed at restricted speed" shall be selected through track relays or through devices that function as track relays, or shall be energized by software-controlled system with such selection, for all track circuits in the route governed.

(b) At automatic interlocking, signal control circuits shall be selected (1) through track relays, or devices that function as track relays, for all track circuits in the route governed and in all conflicting routes within the interlocking; (2) through signal mechanism contacts or relay contacts closed when signals for such conflicting routes display "stop" aspects; and (3) through normal contacts of time releases, time-element relays, or timing devices for such conflicting route, or contacts of relays repeating the normal position or normal state of such time releases, time-element relays, or timing devices; or shall be energized by software-controlled system which has these selections.

§ 236.410 Locking, hand-operated switch; requirements.

(a) Each hand-operated switch in main track shall be locked either electrically or mechanically in normal position, except:

(1) Where train speeds over the switch do not exceed 20 miles per hour;

(2) Where trains are not permitted to clear the main track;

(3) Where a signal is provided to govern train movements from the auxiliary track to the signaled track; or

(4) On a signaled siding without intermediate signals where the maximum authorized speed on the siding does not exceed 30 miles per hour.

(b) Approach or time locking shall be provided and locking may be released either automatically or by the control operator, but only after the control circuits of signals governing movement in either direction over the switch and which display aspects with indications more favorable than "proceed at restricted speed" have been deenergized or by shunting of track circuit.

(c) Where a signal is used in lieu of electric or mechanical lock to govern movements from auxiliary track to signaled track, the signal shall not display an aspect to proceed until after the control circuits of signals governing movement on main track in either direction over the switch have been deenergized, and either the approach locking track circuits to the switch are unoccupied or a predetermined time interval has expired.

§ 236.717 Characteristics, operating.

The measure of electrical values at which electrical or electronic apparatus, or software-controlled systems, operate (e.g. drop-away, pick-up, maximum and minimum current, and working value).

§ 236.737 Cut-section, relayed.

A cut-section where the energy for one track circuit is controlled by the condition of the adjoining track circuit.

§ 236.7XX Disarranged.

As applied to locking implemented by electric or electronic circuits or by software-controlled systems, removing any relay, assembly, or more than one wire end at a time. Locking shall not be considered to be disarranged when (1) a registered, plug-in relay, other than an adjustable time-element relay, is replaced by another tested, registered, plug-in relay; (2) a registered, plug-in assembly of a software-controlled system which does not contain software-storage elements and does not have adjustments is replaced by an identical, tested, registered, plug-in assembly; or (3) a uniquely registered, plug-in assembly of a software-controlled system containing software-storage elements and which does not have adjustments is replaced by a uniquely registered, tested, identical, plug-in assembly.

§ 236.750 Interlocking, automatic.

An arrangement of signals, with or without other signal appliances, which functions through the exercise of inherent powers, as distinguished from those whose functions are controlled manually, and which are so interconnected by means of electric circuits or a software-controlled system that their movements must

succeed each other in proper sequence with train movements over all routes being governed by signal indication.

§ 236.761 Locking, electric.

The combination of one or more electric locks, controlling circuits, and software-controlled systems by means of which levers of an interlocking machine, or switches or other units operated in connection with signaling and interlocking, are secured against operation under certain conditions.

§ 236.7XX Principle, Self-Checking.

The principle of the design of a software-controlled system where the system's hardware, software, and operation is continuously checked so that any failure of hardware, software, or operation that may affect the safety of train operation will cause the controlled function or functions affected by the failure to assume their most restrictive condition.

§ 236.813a State, most restrictive.

The mode of an electric or electronic device, or the state of a software-controlled system, that is equivalent to a track relay in its deenergized position.

§ 236.8XX System, Software-controlled.

A system whose logical functioning is controlled by computer programs stored within the system. Locking enforced by software-controlled system shall be considered to be "electric locking."

*U.S. G.P.O.:1993-343-273:80013