

FAILSAFE DISPLAY SYSTEM

Richard M. Fullalove, B.Sc(Eng)

Post-Graduate Student
Department of Electrical Engineering
University of Cape Town

A half-dissertation submitted to the Faculty of Engineering, University of Cape Town,
in partial fulfilment of the requirements for the degree of Master of Science in Electrical
Engineering.

Cape Town, 1994.

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

Declaration

I declare that the work contained in this dissertation is my own. All sources of reference material referred to in whatever form for use in this research have been acknowledged. This dissertation has not been submitted for graduation purposes at any other educational institution.

Signed by candidate

(Signature of Candidate)

3rd Day of June 1994

Acknowledgements

The author wishes to thank the following persons and organizations for the generous support and assistance given:

Professor Michael Inggs of the University of Cape Town, who acted as project supervisor and provided guidance on how to approach the project from a systems engineering aspect.

Mr. Michael Schröner of Spoornet, who provided substantial technical input throughout the development period. Mr. Schröner was responsible for the development of the related Failsafe Data Transmission System, and was able to provide relevant advice to the project.

Mr. Graham Paverd, who acted as liaison at Spoornet, and who helped to define the user requirement and ensure that these requirements were adhered to. He also provided relevant documentation from Spoornet.

Mr. Ben van der Merwe and Mr. Hennie van der Venter, of Spoornet (Signals), who were instrumental in authorizing this project, and provided the opportunity to obtain a Masters Degree.

Mr. Louis Beukes and Mr. Chris Bester of Spoornet, who provided advice and guidance, as well as relevant reference material from the Proceedings of the Institution of Railway Signal Engineers.

Mr. André Goodisen of Kopp Electronics, for his assistance in acquiring the necessary, but sometimes difficult to obtain reliability data on LED displays.

Mr. Paul Daniels for making the prototype printed circuit boards.

Terms of Reference

The investigation into the philosophy of failsafe displays, and the subsequent design and development of a failsafe display system, was proposed by Spoornet. Mr.G.B.Paverd and Mr.H.van der Venter of Spoornet approached the University of Cape Town to undertake the supervision of the research and provide the research infrastructure. Professor M.R.Inggs was appointed as the research supervisor. It was decided that the scope of this research would fulfil the requirements of a half-thesis for the degree of Master of Science in Engineering.

The development of hardware and software may be undertaken for demonstrating concepts. It is envisioned that the design, development and manufacture of a failsafe display system for the purpose of locomotive cab signalling will result from this research. A proposal has already been submitted to the Chief Engineer (Signals) in Johannesburg, and a tentative user requirement compiled.

The initial literature search and feasibility study began on 1 March 1992, followed by the main body of research. It is expected that once this conceptual research is completed, a detailed hardware and software development phase will commence. This will be followed by an extensive testing phase, final safety evaluation, industrialisation phase, and commissioning.

Abstract

A requirement exists to reduce signalling costs on branch lines throughout the South African rail network, by replacing expensive track side signalling with a Radio Token System. The Radio Token System uses a non-failsafe radio data link and non-failsafe printer in the cab. Spoornet intend to replace the printer with a *failsafe display* in order to eliminate lengthy verbal message protocols and increase safety. This thesis investigates the various concepts of failsafe display, and the means to achieve them. It also investigates the wide range of display technologies available and their suitability for use in a failsafe display. The LED, together with monitoring circuitry, emerges as the most suitable for the application.

Glossary of Terms and Abbreviations

Aspect:	The state of a signal that is displayed to a train driver (red, amber, or green, for example)
BIST:	Built In Self Test.
Composite Safety:	A concept where at least two unrelated failures are necessary before a wrong-side condition could result, and the occurrence of any one failure is detected and negated rapidly compared to its expected incidence.
CTR:	Current Transfer Ratio; the ratio between the input (LED) current and output (collector) current for an optocoupler.
EMC:	Electromagnetic Compatibility.
Error:	That part of the system state which is liable to lead to failure, i.e., to the delivery of a service not complying with the specified service. The cause of an error is a fault.
Failsafe:	A design quality of signalling equipment and of the system within which it is used, that under failure conditions will provide safety for traffic. A failsafe system is one that either continues to function safely or lapses into a predefined condition known to be safe (see Vital).
Failure:	This occurs when the delivered service deviates from the specified service. The failure occurred because the system was erroneous.
Fault Latency:	The time between the occurrence of a physical fault and the subsequent corruption of data causing an error.
FMECA:	Failure Modes, Effects and Criticality Analysis.

FSDS:	Fail Safe Display System.
FSDTS:	Fail Safe Data Transmission System.
Inherent Safety:	A concept where one failure would lead to a wrong-side condition, and the incidence of that failure is extremely rare.
Latency time:	The time during which a failure goes undetected.
Life Critical:	See Failsafe, Vital.
Markov model:	A model of a random process where the next state of the process depends only on the present state, and not on any past states.
MTBF:	Mean Time Between Failures; a measure of reliability of a component or system. In its simplest form, expressed as the reciprocal of the failure rate, λ (assuming constant failure rate).
MTBUF:	The Mean Time Between Unsafe Failures, a probabilistic specification of the level of safety for a microcomputer-based system.
MTBWSF:	Mean Time Between Wrong Side Failures; a measure of the Fail-safety of a component or system. Proportional to the MTBF and inversely proportional to the square of the latency time.
MTTR:	Mean Time To Repair; a measure of the maintainability of a component or system.
Right-side failure:	A failure that could result in an unsafe condition for traffic, and which is detected by the signalling system.
RCM:	Reliability Centred Maintenance.

RTC:	Real Time Clock.
Safety:	Freedom from unplanned adverse effects in using, operating, and maintaining a system.
SSI:	Solid State Interlocking.
Stay-as-last-set:	A mode that a system reverts to under failure conditions, whereby it retains its last state before the failure occurred.
TMR:	Triple Modular Redundancy.
Validation:	A method for providing proof of correctness by looking for illogical conditions in software. The process of evaluating a system at the end of its development to ensure compliance with requirements.
Verification:	The process of determining whether the products of a given phase of development fulfil the requirements established in the previous phase.
Vital:	Railway safety equipment that reverts to a safe state if it can no longer perform its function (see Failsafe).
Wrong-side failure:	A failure that could result in an unsafe condition for traffic, and which remains undetected by the signalling system.

List of Illustrations

<u>FIGURE</u>	<u>DESCRIPTION</u>	<u>PAGE</u>
1	Locomotive Token Unit	p.1
2	Failsafe Radio Token System	p.2
3	Non-Electronic causes of Accidents	p.3
4	Lamp Display	p.5
5	7-Segment Font	p.6
6	16-Segment Font	p.6
7	Dot-Matrix Font	p.7
8	Graphic Display	p.7
9	Alphanumeric Display	p.10
10	LED Failure Modes	p.15
11	Proving with Photodiodes	p.27
12	Proving with a CCD Camera	p.28
13	Window Detector	p.29
14	Conflicting Characters	p.30
15	Display Ghosting	p.31
16	Coupling Strategies	p.36
17	2-out-of-2 Comparative System	p.37
18	System Architecture	p.38
19	System Block Diagram	p.41
20	Segment Module	p.43
21	Segment Circuit	p.43
22	Digit Module	p.46
23	Digit Circuit	p.46
24	Power Module	p.49
25	Soft Start Circuit	p.50
26	Control Module	p.51
27	System Flowchart	p.53
28	Aims of Signalling	p.150

Table of Contents

Title Page	i
Declaration	ii
Acknowledgements	iii
Terms of Reference	iv
Abstract	v
Glossary	vi
List of Illustrations	ix
Table of Contents	x

CHAPTER 1: INTRODUCTION p.1

1.1	USER REQUIREMENT	p.2
1.1.1)	Scope	p.2
1.1.2)	Signalling Philosophy and Technology	p.2
1.1.3)	Human Factors	p.3
1.1.4)	General Purpose Capabilities	p.3
1.1.5)	Display Format	p.3
1.1.6)	Display Appearance	p.4
1.1.7)	Environment	p.8
1.1.8)	Reliability	p.8
1.1.9)	Safety	p.8
1.1.10)	Maintainability	p.8
1.1.11)	Availability	p.9
1.1.12)	Cost	p.9
1.1.13)	System Integration	p.9
1.2	REQUIREMENTS REVIEW	p.9
1.2.1)	Display format	p.9
1.2.2)	Display Appearance	p.10
1.3	PROJECT PLAN	p.11

CHAPTER 2:	DISPLAY TECHNOLOGY TRADE-OFF STUDY	p.14
2.1	SCOPE	p.14
2.2	DISPLAY ELEMENT PROVING	p.15
2.3	VIEWABILITY	p.19
2.4	RELIABILITY	p.19
2.5	RUGGEDNESS	p.20
2.6	ELECTROMAGNETIC COMPATIBILITY	p.21
2.7	TEMPERATURE RANGE	p.21
2.8	COST EFFECTIVENESS	p.22
2.9	AVAILABILITY	p.22
2.10	SIZE	p.23
2.11	WEIGHT	p.24
2.12	POWER CONSUMPTION	p.24
2.13	DISPLAY TECHNOLOGY CHOICE	p.24
CHAPTER 3:	FAILSAFE DISPLAY CONCEPTS	p.26
3.1	DISPLAY CORRESPONDENCE	p.26
3.2	DISPLAY ELEMENT PROVING	p.26
3.2.1)	Integrated Photo-Detectors	p.27
3.2.2)	Image Processing with Feedback	p.28
3.2.3)	Window Detector	p.29
3.2.4)	Conclusion	p.30
3.3	DISPLAY CONFLICT	p.30
3.4	DISPLAY GHOSTING	p.31
CHAPTER 4:	SYSTEM CONFIGURATION PROPOSAL	p.32
4.1	SCOPE	p.32
4.2	SELF-TEST FEATURE	p.33
4.3	KNOWN-GOOD TEST FEATURE	p.34
4.4	FEEDBACK FEATURE	p.34

4.5	2-OUT-OF-2 COMPARISON FEATURE	p.34
4.6	POST-FAILURE SYSTEM STATUS	p.35
4.7	COUPLING STRATEGY	p.35
4.8	CONCLUSION	p.37

CHAPTER 5: SYSTEM HARDWARE p.38

5.1	SYSTEM ARCHITECTURE AND PHILOSOPHY	p.38
5.2	DISPLAY MODULE	p.42
	5.2.1) Display Circuit	p.42
5.3	SEGMENT MODULE	p.43
	5.3.1) Segment Driver	p.44
	5.3.2) Segment Detector	p.45
5.4	DIGIT MODULE	p.46
	5.4.1) Digit Driver	p.47
	5.4.2) Digit Detector	p.47
5.5	POWER MODULE	p.49
	5.5.1) Power Supplies	p.49
	5.5.2) Soft Start Circuit	p.49
5.6	CONTROL MODULE	p.51

CHAPTER 6: SYSTEM SOFTWARE p.53

6.1	INTRODUCTION	p.53
6.2	SUBSYSTEM INITIALIZATION	p.54
6.3	DATA RECEIVER POLLING	p.54
6.4	DISPLAY UPDATING	p.55
6.5	SUBSYSTEM SELF-TEST	p.56
6.6	SUBSYSTEM DATA EXCHANGE	p.57
6.7	SOFTWARE SAFETY	p.57

CHAPTER 7:	RELIABILITY AND FMECA	p.59
7.1	RELIABILITY AND SAFETY	p.59
7.2	FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS . .	p.59
CHAPTER 8:	CONSTRUCTION AND TESTING	p.62
CHAPTER 9:	CONCLUSIONS	p.65
REFERENCES		p.67
APPENDIX A:	Schematic Diagrams	p.71
APPENDIX B:	Failure Modes, Effects and Criticality Analysis	p.86
APPENDIX C:	PCB Artworks	p.97
APPENDIX D:	Component Lists	p.116
APPENDIX E:	Correspondence & Data Sheets	p.123
APPENDIX F:	Component Calculations	p.142
APPENDIX G:	Failsafe Signalling System Design	p.148
APPENDIX H:	Reliability Calculations	p.154
APPENDIX I:	Test Results	p.159

Chapter 1: Introduction

Railway systems in South Africa use a number of signalling techniques to indicate the state of the railway track ahead of the driver and authorize the driver to proceed safely into a defined section of track. Track side signalling is expensive and should only be used on lines where a high traffic density is expected. These signals are tightly interlocked with points and track circuits to provide failsafe signalling.

On branch lines where the traffic density is relatively low, *Radio Token Block* [1],[2] can be used. This technique eliminates costly track side signalling and the accompanying cost of maintenance. The locomotive token unit for a radio token system is shown in Figure 1:

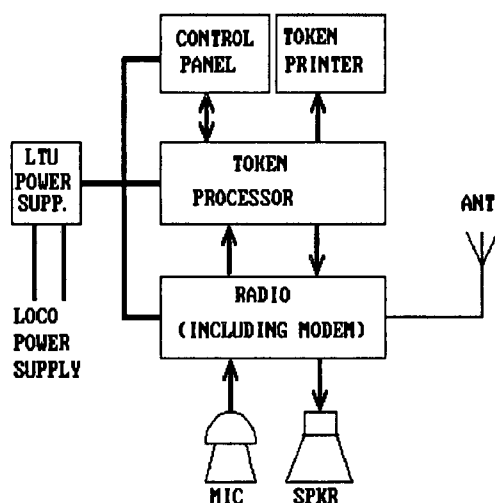


Figure 1. Locomotive Token Unit

The Radio Token Block uses a non life-critical radio data link between the remote interlocking and the locomotive cab, together with a non life-critical printer in the cab.

The safety of the Radio Token System can be increased by replacing the non life-critical printer with a *Failsafe Display System* to display the token in the cab. Once this has been achieved, the probability of errors will be reduced. The execution of orders will be speeded up, resulting in higher traffic throughput. The replacement of the non life-critical radio data link with a Failsafe Data Transmission System is being addressed elsewhere [11].

1.1 USER REQUIREMENT

1.1.1) Scope

Implementation of the proposed Failsafe Display System is shown in Figure 2:

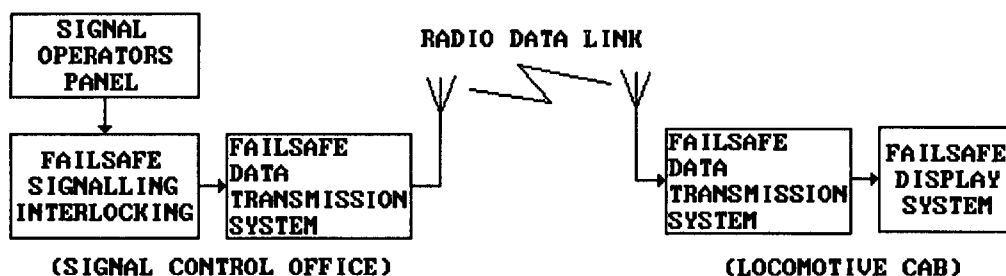


Figure 2:Failsafe Radio Token System

Included in the scope of this project is research into the concepts and philosophies of failsafe displays. Safe reception of token data over the radio data link is beyond the scope of this project [11]. Proving the token validity (i.e. station names, token type, train number, etc...) is beyond the scope of this research. It has been proposed that this research into the philosophy of designing a failsafe display be carried out in conjunction with the University of Cape Town. Prototype hardware and software may be produced to test and demonstrate concepts.

1.1.2) Signalling Philosophy and Technology

The philosophies for the design of failsafe track side signals shall be applied to a cab-mounted display system. However, the technologies suitable for track side signals may not necessarily be suitable for mounting in a locomotive cab. The controlling of a signal is carried out in track side signals by means of relays. Safety relays are very expensive in relation to the number of functions they support. They consume power, are bulky, and are prone to vibration in the locomotive cab environment. For this reason, *solid-state logic* is the preferred solution. However, solid-state devices are not inherently failsafe [7], since they have many failure modes, giving them unpredictable failure outcomes.

1.1.3) Human Factors

Human factors also influence the safety of the system [8],[9]. Possible factors include *driver fatigue, optical interference, stress, malicious intent, inadequate training, and deviation from regulations* (Figure 3), and shall be addressed by operating staff where possible. It is possible for a driver to pass a red signal due to the above factors, since it is not operating policy to implement Automatic Train Control [10]. The design of the display must consider all optical problems such as glare, reflection, glint, brightness, contrast, character size, viewing distance, viewing angle, and display placement, as found in a locomotive cab.

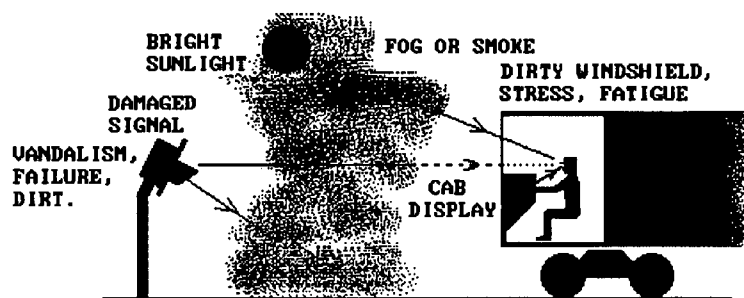


Figure 3. Non-electronic causes of Accidents

1.1.4) General Purpose Capabilities

Apart from the specific requirement to display radio tokens, the system shall also be capable of displaying *general purpose messages* in a failsafe manner. It is preferred that the display use alphanumeric characters, although symbols or indicators may also be used, if practical.

1.1.5) Display Format

Character dimensions will affect the overall display dimensions. It is important to select a size that is readable from up to 2 metres, without resulting in a cumbersome display. This is the maximum foreseeable distance that the locomotive driver could be from the display while the locomotive is in motion. This decision is influenced by what is available in the market. Manufacturers have preferred sizes, limiting the range of choices available.

Displays are often manufactured with the multiplexing and memory integrated into the display. Therefore, they conform to the required dimensions, but do not provide access to the display elements. This is unacceptable, since display element proving is essential for fail-

safety. Compromises have to be made to limit display size, such as reducing the number of characters per line or the number of display lines. A few options have been considered:

- The *single line* display, in which messages are restricted in length to exactly fit on the line. Station names and token type would be displayed in mnemonic form.
- The *single line scrolled* display, in which messages longer than the display line length are scrolled from right to left in a continuous moving display. This is cost-effective, since the number of characters required to display a message can be limited. The user requirement is that the entire message be visible at any moment in time.
- The *multiple line* display shows related portions of a lengthy message simultaneously. It displays the message in relevant blocks. It allows the operator to view more of the message at one time, but is less cost-effective to implement as a failsafe design.
- The *full page* display provides enough lines to display a long message in its entirety. This is the least cost-effective, since it requires the most display hardware. It consumes the most power and would be less reliable. It is also desirable to keep messages as short and as simple as possible.

1.1.6) Display Appearance

The requirement here is to evaluate and select the display type and configuration that best satisfies the user requirement for general purpose messages. Six display types have been selected for evaluation and are listed below:

- *Status Indicators*

Status indicators are merely an extension of the conventional track side colour light signals used to convey signalling information in a failsafe manner to the driver. Status indicators are thus an acceptable means of conveying information. An example is shown in Figure 4:



Figure 5:7-Segment Font

- 16-Segment Font

This font is also known as the *Starburst* font, and is only recommended for displaying upper case alphanumeric characters, as shown in Figure 6:

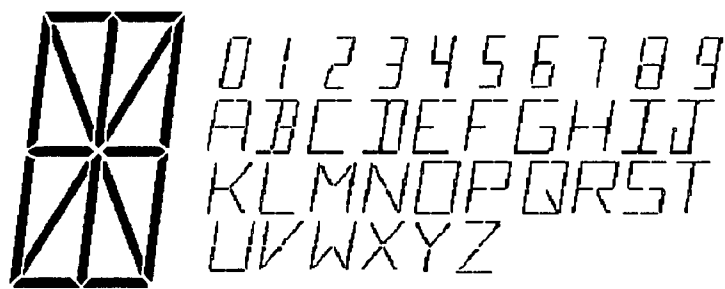


Figure 6:16-Segment Font

Special ASCII characters and lower case characters may appear confusing [28],[29]. This is not considered to be a problem, since only upper case alphanumeric characters are required for displaying tokens. 16-Segment displays have the advantage of simple multiplexing circuitry, being extensions of 7-segment displays. This increases reliability, maintainability, availability, and cost-effectiveness. A variant of the 16-segment font is the 14-segment font, which is also capable of displaying all upper case alphanumeric characters. If possible, this font should be selected, since it reduces the driver hardware without affecting display readability.

- Dot-Matrix Font

This font is capable of representing the entire ASCII character set clearly and unambiguously. The most available format is the 5x7 matrix shown in Figure 7. Due to the wider variety of displays available in this font, compared to the Starburst font, it is a popular choice. However, driver circuits are more complex, especially for

multi-character displays. It requires long shift registers and latches to load the column data for each row before enabling the row.

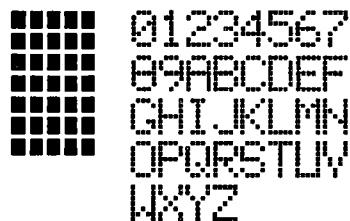


Figure 7:Dot-matrix Font

Since the prime user requirement is to display tokens, requiring upper-case characters, this font does not make a significant improvement over the 16-segment font.

- *Bit-mapped Graphic Display*

An advanced display system could employ a *bit-mapped graphics* display (CRT or LCD flat-panel monitor). Graphical symbols or *icons* representing different commands or conditions could be displayed, as shown in Figure 8:

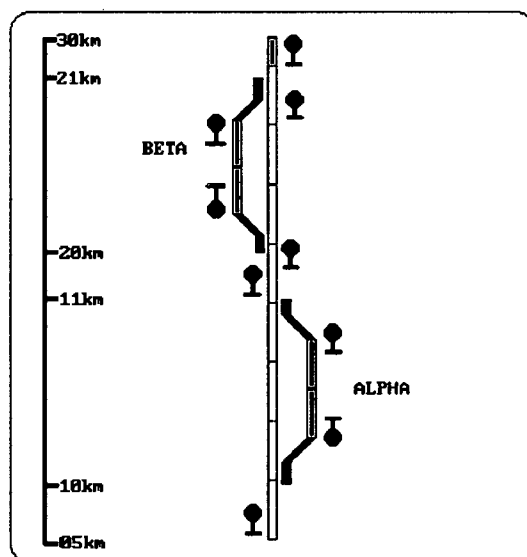


Figure 8:Graphic Display

The advantages of a graphic display are a *geographic* representation of all track and signal conditions presented to the driver, giving him a visual and immediate picture of his surroundings. Since the display of graphics was not part of the user requirement, these displays will not be considered. The complexity required to prove correct operation of a graphic display is also a negative point.

- *Vector Graphic Display*

As with the bit-mapped graphics displays, these displays do not offer any advantage over dedicated alphanumeric displays, and are extremely costly. They are restricted to CRT technology, which is not considered reliable enough. They are also unsuitable for implementation of display proving logic.

1.1.7) Environment

Typical conditions found at the in the locomotive cab at any point within the South African railway network, at any time of the year. These include vibration, dust, temperature extremes, lightning induced transients, humidity, and electromagnetic compatibility with other electronic equipment and power equipment.

1.1.8) Reliability

A Mean Time Between Failure (MTBF) of 10 years has been tentatively set by the user. This figure may turn out to be less, as long as it does not affect the system safety level, and availability is still higher than existing signalling systems.

1.1.9) Safety

The system Mean Time Between Wrong Side Failure (MTBWSF) shall be 10^7 years, with a *fault detection time* of less than 1 second. The display shall be a read-only system, with no possibility of data entry or interference with the displayed message by the cab driver. The system shall revert to a predictable, safe state that is *irreversible*.

1.1.10) Maintainability

The system shall have a Mean Time To Repair (MTTR) of 30 minutes by Spoornet technicians. The system shall meet the maintenance and logistic requirements of the South African railway authority. The system shall use elements of the Failsafe Data Transmission System [11] in order to ensure system integration and parts commonality.

1.1.11) Availability

The Failsafe Display System shall have an availability at least as high as existing track-side signals. In the event of system failure in remote regions, the driver shall revert to Radio Train Order methods of authorization until technical help is available.

1.1.12) Cost

The system shall be at least as cost-effective as existing signalling techniques. Unit costs may be higher than existing trackside signal units, but overall operating and maintenance costs are expected to be lower, due to the lack of long cables in the system.

1.1.13) System Integration

The system shall be capable of interfacing directly to the Failsafe Data Transmission System under development [11]. The system shall derive its power from the locally available electrical supplies in the locomotive cab. The system shall be of such dimensions as are practical for mounting within the confines of a locomotive cab without restricting the movement or visibility of the driver.

1.2 REQUIREMENTS REVIEW

The Requirements Review will only cover those topics in the User Requirement (section 1.1) that required evaluation of alternative proposals. All other requirements remain fixed as defined in section 1.1.

1.2.1) Display Format

Referring to the User Requirement, section 1.1.4, a *single line display* using 16-segment LED displays shall be used for the purposes of prototype development and demonstration of principles. This is in line with similar systems developed elsewhere [2]. A display line length of *16 characters* has been selected. It is recommended that this format be adopted in production models of the system, with a possible slight increase in display line length.

1.2.2) Display Appearance

Referring to the User Requirement, section 1.1.5, *status indicators* are acceptable for displaying non-varying messages in certain limited cases, and may be implemented.

The *Starburst font* is recommended due to the relative simplicity of the driver and failsafe circuitry required. The *alphanumeric* display format appears to exhibit the best trade-off of safety-testability, simplicity, message redundancy, cost, and reliability. It is the preferred method of fail-safe display for this particular application.

A suggested configuration for an *alphanumeric display* to convey textual signalling information is shown in Figure 9:

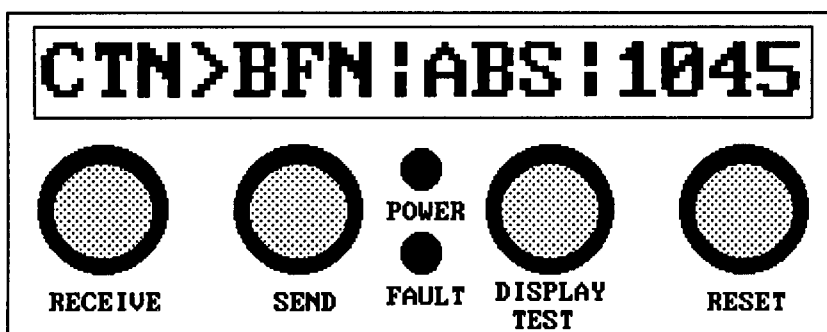


Figure 9: Alphanumeric Display

The proposed format of the 16 character message is in mnemonic form, and is recommended in order to keep display size and resulting complexity to a minimum. Three character mnemonic notation is commonly used for station names within the South African rail network, and is recommended. The first field indicates the station of departure mnemonic (e.g. Cape Town Station), followed by a ">" character to indicate the permitted direction of travel. The second field indicates the destination station mnemonic (e.g. Bloemfontein Station). A "|" character separates the third field which contains the token type mnemonic (e.g. Absolute Token). A further "|" character separates the fourth and final field which contains the train number (e.g. Train Number 1045).

The failure modes of the alphanumeric display would be more complex to analyze than a simple status lamp display. However, it would be more flexible in the message types displayed. The inherent redundancy in textual messages will, in the event of wrong-side

failures, increase the probability of the driver detecting message errors, reducing the *criticality* of wrong-side failures. He could shut down the display manually and revert to radio train orders (verbal). A typical example of a wrong-side failure in the display would be if a desired station name such as '*Johannesburg*' was displayed with a single symbol error as '*Johannfsburg*'.

Although from a strictly technical point of view this is an unsafe, wrong-side failure if undetected by the failsafe system, there is a higher likelihood that the driver, who is familiar with his daily route, will still understand this message. Therefore, the *criticality* of certain wrong-side failures may be lower than others. For conservative design, every effort is made to eliminate *all* possible wrong-side failures.

1.3 PROJECT PLAN

The concept of *Radio Token Block* railway signalling has been introduced. Non-failsafe aspects of data transmission and message display associated with this approach were highlighted. A *user requirement* and *requirements review* were compiled. The type of display desired is addressed (status indicators, alphanumeric or graphics), as well as the amount of information that can practically be displayed within reasonable cost constraints.

A *trade-off study* of various display technologies is then conducted in chapter 2 to find the technology most suitable to the user requirement. The selection criteria used range from very important (proving, viewability and reliability) to less important (size, weight and power).

Failsafe display concepts are introduced and explained in chapter 3. Firstly, safe conversion of received codes to displayed characters is addressed, followed by display element proving. This involves proving that the display elements are visible when activated electrically. The prevention of conflicting characters is addressed. The issue of ghost characters and preventative measures are discussed.

The failsafe *system configuration proposal* that may satisfy the safety and reliability requirement is discussed in chapter 4. The proposal includes features from systems with a Built In Self Test program, known-good tests, feedback, and 2-out-of-2 comparative systems.

Once the system configuration has been selected, the design of the *hardware* at the subsystem and modular level is addressed in chapter 5. It is at this stage that the failsafe concepts and philosophies identified are implemented. The system is broken down into modules which are then developed at the component level. Schematic diagrams of the basic circuits to perform the various module tasks are shown. The issue of statistical independence of failure events in the system is identified as crucial to the development of a failsafe system.

No *system software* is to be written at this stage. However, the tasks to be performed by the system software are identified and classified into software modules in chapter 6. This will ease the coding task at a later stage.

Writing failsafe software is time consuming and care must be exercised in verifying and validating the code. It should be noted that software is not a physical entity and therefore it cannot fail. It cannot be analyzed by traditional reliability techniques. It can however be invalid (not suited to the task at hand) or erroneous (filled with programming errors). It is vitally important therefore that software validation and verification be carried out before commissioning of a failsafe system.

A *reliability* analysis of the system is undertaken in chapter 7 using reliability data for generic electronic components where manufacturers data is not available. An analysis of all possible failures and their outcomes is carried out in the form of a Failure Modes, Effects and Criticality Analysis. Once the system reliability has been estimated, the Mean Time Between Wrong Side Failure is calculated.

The *construction* of the hardware is then discussed in chapter 8. Complete circuit schematics are generated for each system module. Printed Circuit Boards are generated and populated. Decisions taken with regard to placing and selection of components for cost-effectiveness, manufacturability and maintainability are addressed. Since it is not intended to generate system software at this stage, the processor module will not be built. A test card to emulate the outputs of the processor module will instead be built for the purpose of static tests.

Full functional *testing* of the system under operational conditions is not possible, since no software is to be written at this stage. The system is tested rather under static conditions to

ensure correct functional connectivity between modules. Serious design flaws that may arise during printed circuit board generation, such as short circuits, bridges and open circuits, are checked for.

Conclusions are drawn in Chapter 9, and future plans for the further development and industrialisation of the system are discussed.

Chapter 2: Display Technology Trade-Off Study

2.1 SCOPE

The following display technologies [12],[13],[14],[15],[19],[20],[21] have been identified as possible candidates for a failsafe display system:

- Light Emitting Diodes (*LED*).
- Liquid Crystal Displays (*LCD*).
- Cathode Ray Tubes (*CRT*).
- Vacuum Fluorescent Displays (*VFD*).
- Thin Film Electroluminescent (*TFEL*).
- Neon Plasma Displays (*NPD*).
- Electromechanical Displays (*EMD*).
- Incandescent Lamp Displays (*ILD*).

Each display technology will be evaluated on a comparative basis according to the following key criteria, in order of priority, and a weighted table of merit compiled for comparison and selection of the most suitable display technology:

- *Display element proving capabilities.*
- *Viewability under predicted ambient light conditions.*
- *Reliability (Mean Time Between Failure).*
- *Ruggedness.*
- *Electromagnetic Compatibility (EMC).*
- *Temperature range.*
- *Cost effectiveness.*
- *Availability (of display as well as support electronics).*
- *Size.*
- *Weight.*
- *Power consumption.*

2.2 DISPLAY ELEMENT PROVING

This is by far the most important criterion for evaluating candidate technologies for a failsafe display. A thorough understanding of the failure modes of the particular technology is essential. The technology must also have well defined operational characteristics.

LEDs, just like normal diodes, have a predictable threshold voltage of 1.5V to 2V in their forward biased mode. At this point they begin to pass current while simultaneously emitting light, and are thus well suited to lamp proving. The current through the LED is also within a predictable range, and can be used for lamp proving. The following failure modes in LEDs [32] will be investigated, as shown in Figure 10:

- Permanent short circuit.
- Permanent open circuit.
- Intermittent open circuit.
- Leakage current increase (prior to a short).
- Dynamic resistance increase (prior to break).
- Light output decrease.

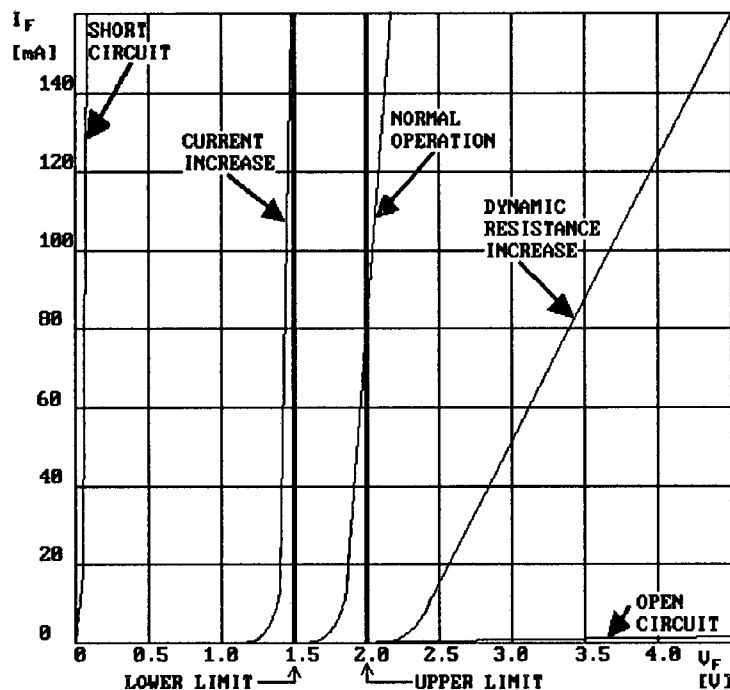


Figure 10:LED Failure Modes

Note that a failure is defined as any part or event that causes the system to fail to operate correctly, or to display erroneous information. The first 5 failures can be directly tested by making use of the shape of the LED electrical characteristic curve. It has a distinct "elbow" that lies between 1.5V and 2V when biased at currents between 0mA and 60mA, as shown in Figure 10. A window detector can be built that has an upper limit reference of 2V and a lower limit reference of 1.5V. If the LED forward voltage remains within these limits, then the window detector output is TRUE. The abovementioned LED failure modes will be discussed in detail with reference to the shape of the characteristic curve in Figure 10, and resulting window detector response:

- *Permanent Short Circuit*

It can be seen from Figure 10 that a short in the LED effectively shifts the forward voltage down to 0V, well below the lower limit of the window detector. The output of the window detector will therefore be False (low). Correspondence with the display manufacturer has revealed that the short circuit failure mode has never occurred in their LEDs. However, since the E.R.R.I. (European Rail Research Institute) regards a short as a possible failure mode [32],[34], the window detector will be retained.

- *Permanent Open Circuit*

An open circuit in the LED effectively changes the forward characteristic to that of a high resistance, since no current flows through the LED. The voltage across the LED jumps up to the supply voltage, well above the upper limit of the window detector. The output of the window detector will therefore be False (low) in the presence of an open circuit.

- *Intermittent Failures*

In multiplexed LED display system, the time frame for measuring the electrical characteristic of the LED has already been made sufficiently short. It can detect intermittent open circuits of duration longer than the refresh period. The output of the window detector will be False (low) in the presence of an intermittent break.

- *Leakage Current Increase*

This failure is a deviation from the specified characteristic that occurs in a *reverse-biased* diode. In this application, the LED is never reverse biased, and therefore reverse leakage current is irrelevant. However, a slight increase in forward current may occur due to a drop in forward resistance caused by a *rise in temperature*. This is due to the negative temperature coefficient of forward voltage, quoted as $-2\text{mV}/^{\circ}\text{C}$ by the manufacturer.

If the typical forward voltage is $1.6\text{V} @ 30\text{mA} @ 27^{\circ}\text{C}$, then $V_{F\text{max}}$ will be $1.674\text{V} @ -10^{\circ}\text{C}$, and $V_{F\text{min}}$ will be $1.554\text{V} @ 50^{\circ}\text{C}$. This is a relatively small change. Referring to the data sheets [30], the relative luminous efficiency varies from $85\% @ 10\text{mA}$ peak, to $115\% @ 200\text{mA}$ peak, well beyond the expected current excursions expected for this display. Note that a 50% drop in relative luminous efficiency is barely detectable by the human eye. Therefore, fairly large temperature excursions will not affect light output. However, in the event of V_F decreasing excessively due to a rise in temperature, the window detector will be False (low).

- *Dynamic Resistance Increase*

This failure is a deviation from the specified characteristic caused by a *drop in temperature*, due to the negative temperature coefficient of the forward voltage. The same calculations apply here as for the case of forward current increase. The LED forward voltage shifts toward the supply voltage and the slope becomes gentler. The light output will not be affected by wide temperature excursions, due to the guaranteed operating temperature ranges specified. If V_F did rise above the upper limit reference, the window detector output will be False (low).

- *Light Output Decrease*

For all the above failures, a decrease (whether noticeable or not) in the light output of the LED is expected, except for increasing forward current, where output may increase with increasing current. However, it has been documented [12],[32] that a

LED experiences a gradual degradation in light output over its lifetime. Typically it can drop to 50% of its original intensity after 100 000 hours. This is barely detectable by the human eye [35].

Any LED whose light output degrades by more than 50% is considered a failure. This is believed to be caused by a growth in crystal dislocations, an unavoidable ageing process arising from temperature cycling, current flow stresses, and shock.

How close this failure mode correlates with changes in the electrical characteristics mentioned above is not clear. However, it can be assumed that crystal dislocations resist current flow, resulting in increased forward resistance. This would lead to V_F rising and being detected by the window detector.

This failure is regarded more as an ageing process than as a catastrophic failure. It can be combatted by adopting a Reliability Centred Maintenance (RCM) program. It must be ensured that the LEDs are replaced after 80% of the MTBF has elapsed to avoid the LED becoming too dim.

Consulting the reliability figures for the HDSP-6508 display [30], it is very likely that the display lifetime will exceed the system operational lifetime. A means of addressing this problem has been postponed, pending decisions on the expected operational lifetime of the equipment. It is expected that the useful light output will be available from the display for a period exceeding the operational lifetime of the system, based on reliability figures presented by the manufacturer.

LCDs rely on an electric field rather than an electric current to re-align their crystals. The resulting current flow is too small to measure practically, typically 10nA. Their "on" threshold voltage is less well defined over wide temperature ranges. They also need to be energized by an AC field, compounding the complexity of lamp proving.

TFEL, VFD, NPD, and CRT displays all operate at voltages of 100 Volts or higher, making their drive electronics as well as any lamp proving electronics more complex. The higher the operating voltage, the higher the noise voltage, for a fixed signal to noise ratio. The

reliability of the lamp proving electronics at these voltages would be questionable.

EMD displays can be proved by means of electrical contacts or optocouplers mounted next to each display element. However, this becomes extremely expensive to implement in large displays. Mechanical signals were the original method of conveying signalling information to drivers at the turn of the century. ILD displays can use the same principles as for conventional colour-light signals by using current relays in series with each filament to prove an open circuit. This is the dominant failure mode of incandescent signalling lamps.

2.3 VIEWABILITY

A contrast ratio of at least 10:1 is preferred [13]. Contrast of multiplexed LED displays is relatively low under bright light. It can be considerably enhanced by the use of louvred filters combined with display shading. LCD displays have a high contrast ratio in bright sunlight at the optimum angle of 0° from the normal. However, this decreases rapidly as the viewing angle increases beyond 40° from the normal. LCDs are dependent on external light sources in order to be visible (passive displays).

ILD displays, just like LED displays, have a relatively low contrast ratio and require filters to enhance their contrast ratio under bright light. EMD displays, just like LCDs, are not emissive displays, but have a good contrast ratio (only when viewed under bright light). However, this contrast ratio does not decrease as the viewing angle increases.

A typical TFEL display has a high contrast ratio of 60:1 under a wide range of viewing angles. A typical NPD display has an even higher contrast ratio of 100:1. CRTs have a relatively low contrast ratio in bright sunlight, and are not acceptable.

2.4 RELIABILITY

LED displays, operating under reasonable conditions, have a MTBF of 100 000 hours, and are thus very reliable. A single LED can have a MTBF of 1 000 000 hours [26]. LCDs, due to their low power consumption, have proven to be reliable displays if operated within reasonable temperature ranges.

TFEL and NPD displays are expected to exceed the user requirement for a MTBF of 10 years, since they are used extensively in the military environment. However, their driver circuits have to operate at high voltages with subsequent reduction in operating lifetime or increased cost. VFD displays also have to operate at elevated voltages, resulting in reduced lifetimes for driver circuitry. CRTs have a relatively low MTBF of less than 20 000 hours, thus excluding them due to the user requirement of $MTBF = 10$ years.

Due to their mechanical nature, EMD displays do not have a high MTBF. ILD displays, due to their high filament temperatures, do not have a long life, typically $< 10\,000$ hours. Miniature 5V bi-pin lamps are available that have a MTBF of 10 000 hours under laboratory conditions, (no vibration, 27°C, AC operation).

2.5 RUGGEDNESS

LED displays are light and encapsulated in epoxy-plastic, making them rugged and capable of withstanding a rough environment. LCD displays have relatively thin glass substrates in comparison to electroluminescent and plasma displays. However, due to their exceptionally light weight, they are considered to be rugged enough for this application.

Colour CRTs have a shadow mask, which is a large, relatively unsupported area, and an electron gun. These are susceptible to shock and vibration, requiring extensive shock-proofing. VFD displays have a grid electrode that is susceptible to excessive shock and vibration, although this has been remedied lately. They are increasingly being used in automobiles.

The NPD is the type most frequently used for military and other harsh environmental applications. Its glass substrate is the thickest of any flat-panel display and the envelope is hermetically sealed. TFEL displays are also used extensively in military displays, and have the simplest construction of all. They consist of thin-film layers deposited on glass, giving excellent shock and vibration characteristics.

EMD displays are not considered suitable for environments where mechanical shocks are

expected. This is due to the presence of moving mechanical components making up the display elements. ILD displays rely to a large extent on bayonet or screw-in plugs, as well as having a delicate high-temperature filament. They are less suitable for vibration-ridden environments. Miniature 5V bi-pin lamps, due to their low mass, may be rugged enough.

2.6 ELECTROMAGNETIC COMPATIBILITY

Due to their relatively low forward operating voltage and current, LED displays radiate relatively low level Electromagnetic fields as compared to CRTs, EMDs, ILDs, NPDs and TFEL displays. Since they do not rely on ionized gases and electric fields to emit light, they are immune to stray light emission caused by strong ambient electromagnetic fields or ionizing radiation. Due to their reliance on an electric field to activate them, LCDs can be activated, (and even damaged) by electrostatic discharge, unless well protected.

TFEL, VFD, CRTs, and NPD displays all rely on supply voltages of 100 Volts or more to operate, and thus are likely radiators of electromagnetic interference. Plasma displays are gas filled, and are susceptible to false activation if exposed to ionizing radiation. The electron beam of a CRT can be distorted by powerful DC and 50Hz electromagnetic fields. VFDs operate on similar principles to CRTs, and are therefore also susceptible to EM fields, although to a lesser extent.

ILD displays, just like their colour-light signal counterparts, are relatively immune to electromagnetic fields. They can operate at voltages as low as 3 Volts. EMD displays could vibrate due to strong 50Hz electromagnetic fields found in the track side environment. They would have to be "AC-immunized", as has been done with certain track-side relays.

2.7 TEMPERATURE RANGE

LED displays have wide operating temperatures ranging from -20° to +85°C for commercial grades. LCDs are more sensitive to temperature than their emissive display counterparts. Rise and decay time increases as temperature decreases. Viewing angle and the electro-optical transfer characteristic decrease as temperature increases. The plastic polarizers become unstable at temperatures exceeding 85°C.

NPD and TFEL displays are temperature limited mainly by driver component ratings, but have a very wide temperature range, justifying their use in military equipment. CRTs can operate over a reasonable range of temperatures (higher than LCDs, but lower than TFEL, plasma, LEDs and incandescent lamps). The light output of VFDs decreases as temperature increases as a result of phosphor quenching, as with CRTs.

EMD and ILD displays can operate in a wide range of temperatures, although electromechanical displays are limited in operation at the lower temperatures. This is due to the risk of freezing-up of moving parts.

2.8 COST EFFECTIVENESS

There is a high availability of dedicated alphanumeric displays with 16-segment and 5x7 dot matrix fonts. Graphic displays are more cost-effective when many characters are to be displayed. Therefore, cost effectiveness is measured per alphanumeric character rather than per display as a whole. Due to the widespread use of LED displays over the last three decades, the price is low per character, if few characters are required in the display. LCD displays are the most cost-effective alphanumeric displays, and are very common.

EMD displays and ILD displays are less cost-effective per character than the other displays. Typically, electromechanical dot matrix displays will cost up to R500 per 5x7 character for large font sizes. Incandescent displays could be built using miniature bi-pin lamps placed behind segmented legends at reasonable cost.

As far as graphics displays are concerned, LCDs and CRTs are the most cost-effective. They are followed by TFEL displays, VFD displays, NPD displays, and finally ILD and EMD matrix displays.

2.9 AVAILABILITY

The criterion used here is for alphanumeric displays, and not simple binary indicators or technologies capable of displaying graphics. Most types of LED alphanumeric displays are available, whether segmented or in the 5x7 font. LCDs offer the greatest variety of matrices

(and alphanumeric displays), followed by NPD, TFEL, and VFD in that order. CRTs, because of their long history as display devices, are well established in industry and readily available from numerous sources.

EMD displays, such as those used in airport flight schedule panels, are the least common technology. They are being slowly replaced by solid-state displays or large-screen CRTs. They are mainly used for electronic scoreboards and advertising. ILD displays generally use back-lit legends to indicate a single condition, and can thus be custom-built by the designer. Seven-segment miniature filament displays do exist, but not in 16-segment or dot-matrix fonts. An alphanumeric display could be built using miniature bi-pin lamps mounted on a PCB behind a 16-segment legend.

2.10 SIZE

For small alphanumeric displays of 16 characters, which is the approximate length of the message to be displayed, LED displays are compact enough. LED displays come in various sizes and formats, although no graphics displays (as with LCDs) have been built. LEDs are used to display alphanumeric (5x7 dot matrix or 16-segment), hexadecimal (9-segment), or decimal (7-segment) characters. In these formats, character heights vary from 2.5mm to 58mm. When large amounts of text or graphics are to be displayed, graphic displays (LCD, CRT, TFEL, NPD) are more compact for the number of characters they can display. LCD displays come in the same sizes and formats as the LED displays. They also include custom-built symbolic displays (watches, portable games, etc.) and graphics displays in various sizes for use in notebook computers.

CRTs are bulky displays, requiring considerable depth to house the electron gun, power supply, drivers and decoding circuits. VFDs are available in a wide variety of sizes, and are used in the home entertainment, automobile, and retail industry. TFEL and NPD displays are generally available as graphic displays only, either in half-page or full-page sizes.

EMD and ILD displays are not available in small sizes, especially when a large amount of text/graphics needs to be displayed, and are thus not acceptable. Reasonably small ILD displays can be built using discrete miniature bi-pin lamps.

2.11 WEIGHT

Being solid-state and composed of plastic and epoxy, LED displays are reasonably light per character, for displays of about 20 characters. An LED display will be relatively heavy when an attempt is made to display as many characters as graphic displays (LCD, TFEL, plasma). Of the flat-panel matrix displays, LCDs are the lightest, followed by TFEL, VFD and NPD.

CRTs and EMD displays are heavy displays, and are not acceptable for the locomotive cab. Lightweight ILD displays are possible if miniature lamps are used and the number of digits is low, although the power supply will be heavier than for LEDs, LCDs, VFDs and NPDs.

2.12 POWER CONSUMPTION

Power consumption of LED displays is fairly high per character element compared to other technologies. However, when used in a multiplexed display, it is lower than in CRTs, NPDs, TFEL and ILD displays for alphanumeric displays of less than 40 characters.

LCD displays consume the least power of all the graphic displays, since they are not emissive, followed by TFEL displays, then VFD, NPD, and finally CRT displays. However, when operating at maximum power, (all pixels energized), TFEL and plasma displays can exceed CRTs in power consumption.

EMD displays require a large amount of power to move and hold each display element by means of miniature solenoids. ILD displays that have to display a large amount of information, such as matrices, consist of many incandescent lamps. Each consumes power of the order of Watts, making them the greatest consumers of power per display element.

2.13 DISPLAY TECHNOLOGY CHOICE

The table indicated below displays the binary weighted judging criteria in the left column in order of priority. Proving, viewability and reliability are regarded as being of extreme importance to safety, and therefore have been given the highest weights. This avoids arriving at close scores for any two technologies judged over the entire range of criteria.

The device relative performance rating is linear, from 1 for worst, to 8 for best out of 8 possible display technologies , and is multiplied by the appropriate criterion weighting. Thus, each entry in the relative performance table shown below is the product of the relative rating (1 to 8) of the specific display technology and the binary weighting for that particular judging criterion. This gives a better perspective of the relative merits of the different technologies in relation to the various criteria. The technologies that score on the most important issue, lamp proving, will automatically attain much higher total scores.

CRITERION	WEIGHTING	ILD	EMD	CRT	NPD	VFD	TFEL	LCD	LED
Proving	1024	8192	7168	2048	3072	5120	4096	1024	6144
Viewability	512	2048	1024	512	4096	3072	3584	1536	2560
Reliability	256	256	512	768	1792	1024	1536	1280	2048
Ruggedness	128	128	256	384	896	512	768	640	1024
EMC	64	448	128	64	192	320	256	384	512
Temperature	32	160	128	96	224	64	192	32	256
Cost	16	32	16	112	48	64	80	128	96
Availability	8	16	8	48	40	24	32	56	64
Size	4	8	4	12	16	24	20	32	28
Weight	2	4	2	6	8	10	12	16	14
Power	1	1	2	3	4	6	5	8	7
TOTALS		11293	9248	4053	10388	10240	10581	5136	12753

It can be deduced that the *LED display is the prime candidate* for research in this case. The results of this trade-off study do not suggest that other technologies, such as ILDs and EMDs, are not suitable for failsafe information display. In fact, due to the existence of miniature 5V bi-pin incandescent lamps, ILDs could be considered as an alternative option to the LED. Despite the reduced reliability, incandescent lamps have a well defined failure mode (open circuit) that is simple to detect.

Similarly, mechanical signals and incandescent lamps in colour-light signals have been used for the last 100 years in track side signalling. They have thus been proved to be capable of fulfilling the failsafe signalling function. However, their use is not appropriate to a portable cab-mounted alphanumeric display due to their bulkiness and power consumption.

Chapter 3: Failsafe Display Concepts

3.1 DISPLAY CORRESPONDENCE

Alphanumeric messages have to be displayed to the driver such that they correlate directly to the codes being received by the display over the communications channel. The display system must convert the *valid codes* at its input into the corresponding *alphanumeric message*. The appropriate display elements must illuminate in a failsafe manner. This corresponds to *aspect proving or correspondence checking* used in conventional railway signals, where relay logic is used to confirm that the aspect shown correlates with the control signal sent.

Since solid-state logic (which is not inherently failsafe) is to be used, certain techniques have to be employed when designing the logic circuitry to detect correct display operation. Periodic checking of the ROM look-up table or display decoder chip that converts the received code into display data is one example. Other solutions are message confirmation, display feedback and comparison, and redundant display driver subsystems.

3.2 DISPLAY ELEMENT PROVING

The display elements must be proved to be illuminated when the correct signals are sent to them. The frequently-used lamp test is insufficient to meet the safety requirement, since it relies on a human to identify faulty display elements. A human would be unable to sense out of tolerance failures and intermittent failures. The traditional lamp test could be employed as a supplementary test for use by a repair technician. However, if the test is automated [12], and a means developed by which the system can sense failures in the display elements, then the traditional lamp test is unnecessary, and will not be used here.

Note that display correspondence proving differs from display element proving, in that in the former, the correct display element is proved to be selected, whereas in the latter, the display element is proved to be active when selected. Display element proving corresponds to the technique of *lamp proving or filament proving* used on track side colour light signals using incandescent lamps. However, to use incandescent lamps in a cab-mounted alphanumeric display would be impractical and inefficient. This is due to excessive power consumption,

bulkiness, frailty, and the number of lamps needed to construct an alphanumeric display.

For this reason, an alternative display technology is required. It must have electrical characteristics that correlate closely to light output in a predictable manner. It must also meet the requirements of low power consumption, compactness, ruggedness, and reliability. Three basic parameters identify correct display element operation:

- *current* through the display element.
- *voltage* across the display element.
- *light* output: a) *emissivity* (active displays).
b) *reflectivity* (reflective LCD displays).
c) *transmissivity* (backlit LCD displays).

For incandescent lamps, it is possible to correlate directly light output with current flow through the filament, since a bulb with a broken filament does not emit light. However, with other technologies, this is not necessarily the case.

It has been shown in Chapter 2 that LEDs are an acceptable display technology for this application, since their light output correlates closely with their electrical parameters. Means of proving their safe operation are needed, and a few possible solutions are shown below:

3.2.1) Integrated Photo-Detectors

A photo-detector could be placed adjacent to each display element in such a way that ambient light and adjacent display elements did not falsely activate it. It could be built using medium-scale integration of LEDs and photo-diodes onto the same substrate, as shown in Figure 11. Relevant drive and detection electronics could also be integrated onto the substrate, making this an extremely compact and cost-effective solution, if implemented on a large scale.

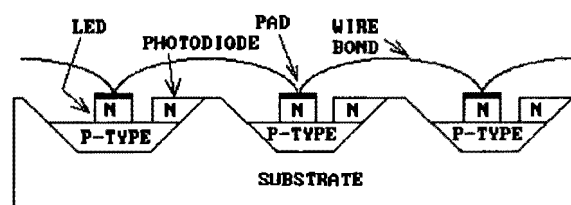


Figure 11: Proving with Photodiodes

This is a possible solution, but can only be implemented by the display manufacturer. In order to avoid false detection of ambient light, each display element would need to be tested with a pseudo random code sequence, using synchronous detection to detect valid light output pulses from the display elements at valid sampling times. Since there is at present no widespread demand for this type of display technology, it would not be cost effective.

3.2.2) Image Processing with Feedback

Another approach would be to place the display under an angled semi-transparent mirror (or triangular beam splitter prism), so that most of the light from the display could be directed to the viewer. A percentage of the light would be directed via suitable optics to a charge-coupled device (CCD) camera. Images received by the camera could be processed by software in order to compare the displayed message with the desired message and detect any discrepancies. An example of this approach is shown in Figure 12:

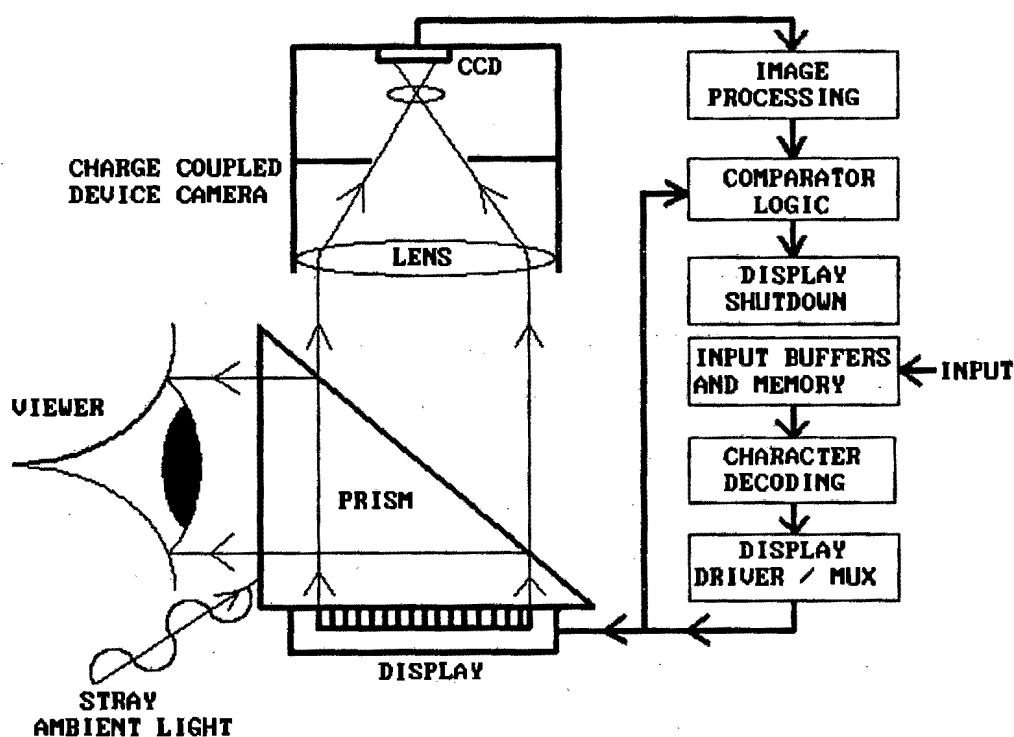


Figure 12: Proving with a CCD Camera

This approach would be complex, unreliable, and not cost-effective. The optics require precise alignment. The system would have to be made vibration proof, and protected from false images generated by ambient light.

3.2.4) Conclusion

To measure directly the light output of a display as a means of proving its safe operation is impractical with available devices. Large numbers of display elements would have to be measured. False activation of optical proving sensors by ambient light could mask a failure in a display element rendering optical techniques suspect. The electrical technique of proving the integrity of the display with window detectors appears to be more practical, and is not prone to ambient optical interference. Note that darkness or fog would be less likely to hamper identification of a faulty cab display by the driver than in the case of a faulty track-side signal. This advantage cannot be relied upon, but does highlight the relative criticality of failures in cab displays in comparison to track-side signals.

3.3 DISPLAY CONFLICT

It has to be ensured that no attempt is made to send more than one character code to a particular digit. This could result in the lighting of spurious pixels or segments in that particular digit within the display, as shown in Figure 14:

COMMAND 1:-----	STOP
COMMAND 2:-----	MOVE
COMMAND 1 OR 2:-----	MOVE

Figure 14:Conflicting Characters

False characters could be displayed which may appear to be meaningful. The result is false information being conveyed to the viewer. This could occur in a multiplexed display, if the multiplexer developed a "stuck-at" fault in its scanning sequence. It would enable the same character more than once per display scan. This type of fault can be detected by means of self-test circuits and feedback from the display. This concept is analogous to the probability of simultaneously displaying a red and a green aspect on a conventional railway signal.

Note that the virtue of an alphanumeric display is the inherent information redundancy that exists in textual information as opposed to simple binary indicators. Therefore, the *criticality* of wrong-side failures may be reduced by using alphanumeric displays. In the event of an

Chapter 4: System Configuration Proposal

4.1 SCOPE

Seven possible failsafe system configurations or features [3],[5],[18],[21],[22],[23] were evaluated in order to decide which one satisfied the criteria specified in the user's requirement. Not all the options were considered to be pertinent to the Failsafe Display System, and will not be discussed in detail. The configurations/features looked at were:

- *System with Self-Test* (accepted)
- *System with Software Diversity* (not accepted)
- *System with Known-Good Test Vectors* (accepted)
- *System with Feedback* (accepted)
- *System with 2-out-of-2 Comparison* (accepted)
- *System with Dual Redundant Displays* (not accepted)
- *System with Triple Modular Redundancy* (not accepted)

Certain features from the accepted options were combined in defining an acceptable system configuration. Once this configuration is defined, a post-failure system state must be defined.

Software diversity was not accepted due to the difficulty experienced in guaranteeing true diversity in software. Generally, diverse software systems have only been implemented on single-processor systems, which do not meet the users safety requirements [11]. Common-mode power supply transients are typically expected to cause problems.

Dual redundant displays were not accepted, since two displays would simply double the cost, while still relying on a human operator to discriminate between them for possible errors. If the error is subtle, then a human operator is more likely to miss the error than dedicated hardware/software. Although this type of error may seem trivial when taken in the context of the displayed message as a whole, it is totally unacceptable in the signalling environment. For example, it is likely that station names may be displayed as three-letter mnemonics, say, "CTN" for "Cape Town". The shorter the mnemonic, the higher the probability that two similar names may be mistaken for one another in the event of a display fault. This

highlights the inherent risks in relying on human judgement to visually discriminate between two adjacent redundant displays. It is more desirable to automate error detection on the display output.

Triple Modular Redundancy (TMR) was rejected as inappropriate to the failsafe requirement, since TMR maintains system availability in the event of failure. TMR is also very costly.

4.2 SELF-TEST FEATURE

In addition to running the system program (the basic function of receiving and displaying a message), the system must run a self-testing program in order to avoid faults remaining in the system beyond the fault detection time.

The *test program*, stored elsewhere in the system memory, cycles through a series of self-test routines. It checks the correct operation of all critical segments of the system [3]. This is often referred to as *BIST (Built In Self-Test)*. The test program performs a signature analysis [18] of the system and a ROM checksum. It verifies outputs to the display elements. In this way the detection of any relevant first faults is ensured. Discrepancies will cause the system to automatically shut down.

Advantages are low hardware cost due to software implementation, a single system program, and the ability to generate a fault report for the technician in the event of a system failure. The ability to detect transient faults (temporary resetting of a memory element) is possible.

Disadvantages are that an extra check (BIST) program has to be written and verified. In order to detect latent faults as soon as possible, the BIST program must be run frequently. The execution of the test program is time consuming. It has to run before the system program processes and outputs data to the display element. Corruption of the check program could lead to an undetected fault occurring in the system, and is avoided by using it in conjunction with the 2-out-of-2 Comparative configuration. Software validation and verification are essential.

processors must operate in an asynchronous manner in order to avoid common-mode clock-related failures.

Advantages are that a single processor type and a single program need to be designed. This system offers good failsafe characteristics due to statistical independence. A hardware data comparator is fast and does not affect system speed, but requires tight subsystem synchronisation. The possibility of common-mode power transients led to the rejection of hardware comparison and the acceptance of software comparison of asynchronous subsystems. Assuming the subsystems output fault-free data, it is possible that the display will be faulty. In this case, the system is allowed to control the faulty device for a specified maximum time, detect the fault through feedback, compare this data with the data sent, and shut the system down if the comparison fails.

Disadvantages are processor hardware duplication, resulting in cost doubling. Extensive electrical isolation techniques are required to achieve statistical independence. Software data comparison may significantly affect the speed of the system, and must be accounted for.

4.6 POST-FAILURE SYSTEM STATUS

The system configuration containing the above-mentioned features can be classified further as a failsafe system in terms of its intended response to a failure. As long as the processors send "system safe" signals to the decision logic, a control output continues. If one processor detects a fault, however, and terminates its "system safe" signal, the logic operates a switch (fuse) to disconnect the system from display element. The system is then forced into a predetermined safe state, which is irreversible. This system is effective when such a state can be defined, i.e. a railway signal reverting to danger.

4.7 COUPLING STRATEGY

The two primary strategies are *loose and tight coupling* of the processors [33]. Within these approaches failsafe functions can be implemented in either hardware or software: *error detection*, *error isolation* and *system recovery*, as shown in Figure 16:

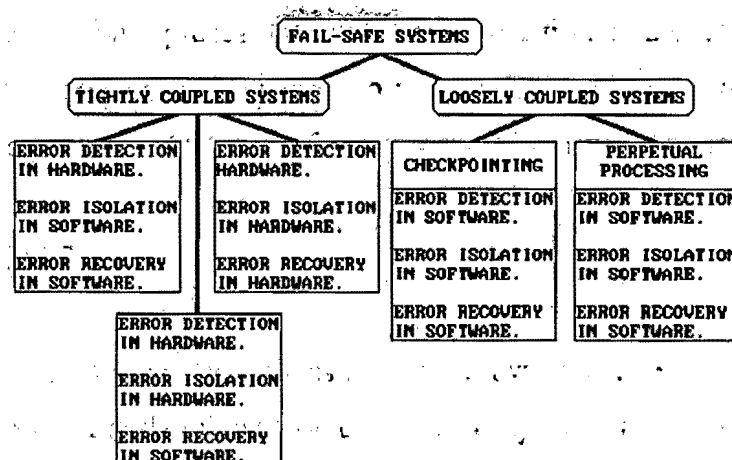


Figure 16: Coupling Strategies

Loosely coupled systems rely primarily on software to implement these functions. The function of error isolation is to disconnect the erroneous processor from the decision-making process to allow the system to revert to a safe state. The function of system recovery is to re-configure the system to operate normally without the disconnected processor. For the 2-out-of-2 comparative system adopted in the Failsafe Display System, the function of system recovery is not necessary and will not be implemented, since system operation after failure is not a user requirement.

In tightly coupled systems, processors have a common clock and frequently a common memory and software as well. Such systems have better processing efficiencies due to the use of hardware for the failsafe functions. However, the nonredundant common memory is a potential point of failure that could affect the whole system. In addition, the shared memory may become a bottleneck if both processors need to use it simultaneously.

Processors in loosely coupled systems are relatively independent of one another; each has its own memory and copy of the software. Loosely coupled systems depend exclusively on software to implement their failsafe functions. This leads to a relatively low level of functional performance.

Two strategies are further identified within loosely coupled systems; *checkpointing* and *perpetual processing*. Perpetual processing requires an additional synchronization processor which adds additional cost and will not be used here. With checkpointing, the software is assigned to both processors. In one processor the program is the *master* process; in the other

higher level of safety can be achieved if one subsystem in the Control Module selects the segment, and the other subsystem selects the digit. This is referred to as *dissimilar control*.

Control Module 1 (actually subsystem 1 of the Control Module in the 2-out-of-2 comparative system) selects the relevant segments for a selected digit via the Segment Module. Subsystem 2 of the Control Module has identical segment drive outputs which are not used, due to the concept of dissimilar control discussed in the previous paragraph. This arrangement is chosen in order to maintain hardware and software similarity between the two subsystems. The segment select outputs of the segment module are directly connected to the segment pins of the display module (the LED anodes in a common-cathode, 16-segment alphanumeric LED display). The segment LED anodes are also connected to the segment detector inputs in the Segment Module for segment detection feedback.

Control Module 2 (subsystem 2 of the Control Module) selects the relevant digit during the multiplexing scan cycle via the Digit Module. Subsystem 1 of the Control Module has identical digit drive outputs to subsystem 2. The Digit outputs of the Digit Module are connected to the common cathodes for each 16-segment digit in the display. The common cathode of each digit is also connected to the digit detector inputs in the Digit Module for digit detection feedback.

In order to make the subsystems of a failsafe system *statistically independent* of one another [5], their inputs and outputs must be electrically isolated from one another. In the event of a fault in one subsystem, the other subsystem will not be affected electrically. This can be achieved by splitting the data input to the Display System, and then using optocouplers to isolate these inputs from the subsystem inputs. Data comparison paths between the two subsystems and the subsystem outputs to the Display Module must be electrically isolated.

Optocouplers contribute significantly to the component count, cost and failure rate. However, they are essential for increasing system safety via statistical independence. This simplifies any reliability and safety analysis. Throughout the design of this system, and especially when performing the FMECA (Failure Modes, Effects and Criticality Analysis), reference has been made to [31] and [32] for possible failure modes and reliability figures of components.

Power supply isolation is needed in order to prevent power supply failures in one subsystem from creating related failures in the other. In the event of serious electrical failure (supply short circuit or open circuit) in one subsystem, the other subsystem must not experience a similar failure. Each subsystem is powered from isolated supplies V_1 & V_2 . A third power supply (V_{SAFE}) provides power to the display circuit itself, which includes sections of the Display Module, Segment Module, and Digit Module. At system power-up, a *soft-start circuit* [11] in the Power Module prevents premature blowing of the fuse until all supply voltages have stabilized and system initialization has been completed.

The *fuse-blow* circuit can be activated from either subsystem in the Control Module, and is optically isolated from both subsystems. When activated, it removes V_{SAFE} from the Display Module. A facility must be provided to momentarily test the fuse-blow circuit and the fuse. The supply is temporarily shorted by the fuse-blow switch for a brief period. Feedback is provided to verify a successful fuse test. Both controllers must not attempt to test the fuse simultaneously. If they did, the sum of the currents drawn by their respective fuse-blow circuits could blow the fuse unnecessarily.

Data input to the system is in *serial format* and fed to both subsystems via optically coupled interfaces. The two controllers operate *asynchronously* in a loosely-coupled system [33] by means of separate clocks. The data receiver is polled periodically at a rate exceeding the expected data input rate. In a safety application, the data input *cannot be interrupt-driven*, since the outcome of interrupts on system software is difficult to evaluate with software verification techniques. As a result, a polling technique is used that consumes vital processor time. A *timing budget* must be calculated to ensure that the system is not slowed down by a significant amount. The data reception software will not be written for the purposes of this research, but will be budgeted for in program memory space and execution time.

Feedback facilitates monitoring of the controlled device (in this case, the display). All possible failures in the display must be detected and fed back to both subsystems in the Control Module for comparison with the intended outputs. It is necessary to duplicate the detection and feedback circuitry in order to avoid undetected failures due to a faulty detection circuit. The feedback is provided by the Segment *and* Digit Modules.

Optically isolated *data communication links* (DATA XCHG) between the subsystems 1 and 2 of the Control Module are needed. Subsystem status data from each subsystem in the Control Module must be *compared* with the other subsystem data in order to meet the system safety requirements. Typical status data would include self-test results, display feedback results, and re-synchronization data. This requires a *bidirectional* transfer of data between the memories of each subsystem.

In order to set up a data exchange protocol, one subsystem must be configured as the *master* and the other as the *slave*. Thus, the master will initiate data exchange, and the slave will respond. This implies some minor software disparities in the two subsystems. Any data discrepancy must result in safe system shutdown. A more detailed block diagram of the complete system is shown in Figure 19:

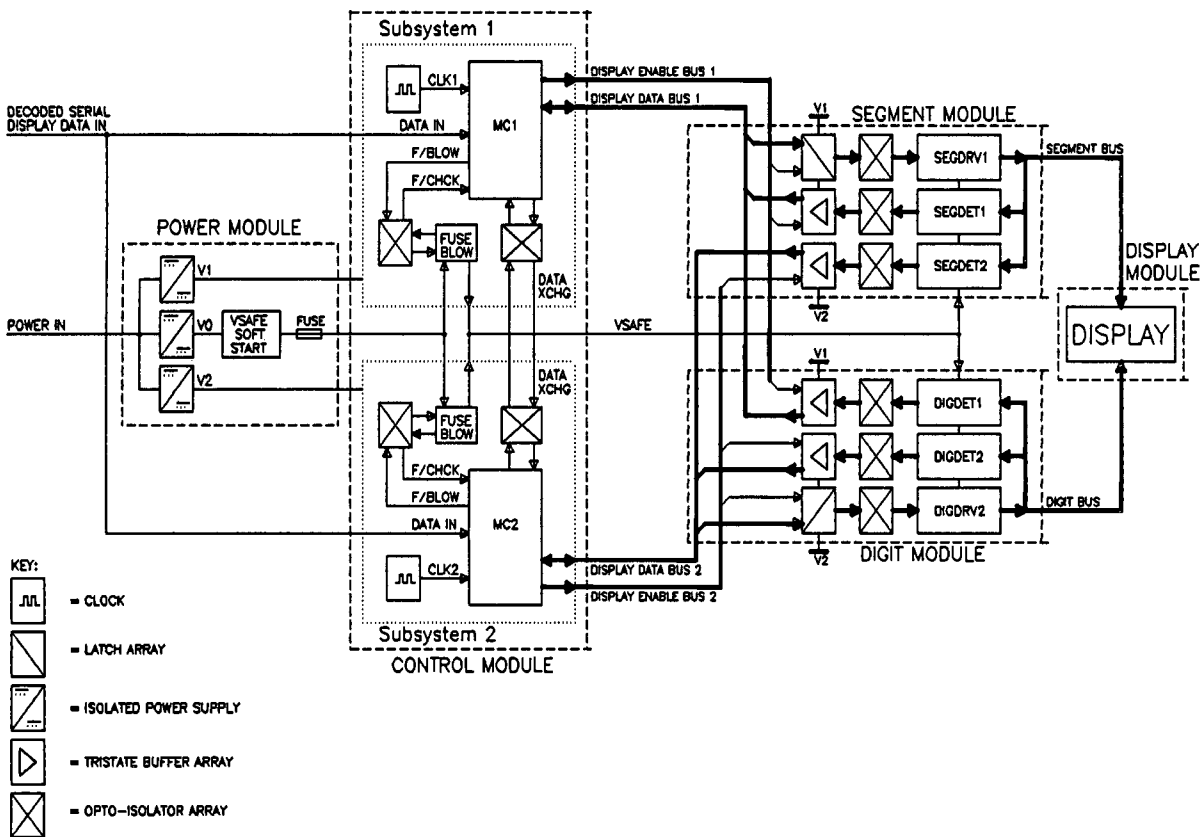


Figure 19. System Block Diagram

A system level Failure Modes, Effects and Criticality Analysis (FMECA) was performed using the block diagram in Figure 19, and is documented in Appendix B. This was necessary in order to verify the robustness of the proposed system configuration before design began at the modular level. A system level reliability figure was calculated, giving a reliability budget for each module. This is documented in Appendix H.

5.2 DISPLAY MODULE

5.2.1) Display Circuit

In order to display 16 digits, 16 digit lines and 16 segment lines are needed. The segments are connected to the SEG lines from the Segment Module. The digits of the Display Module are connected to the DIG lines from the Digit Module. The detailed schematic diagram of the Display Module is shown in Appendix A, Figure 3.

Latent faults in the display window detectors could result in subsequent LED failures going undetected. An LED failure must be simulated at a predictable time in order to verify the correct response of all window detectors to this failure. Dummy *test digit 17* consists of 16 standard silicon diodes to simulate the forward voltages of segment LEDs dropping to a lower threshold of 0.6V. Test digit 17 thus simulates a digit with all 16 segment LEDs approaching a *short circuit*, testing the ability of all window detectors to detect short circuited LEDs.

Dummy *test digit 18* consists of 16 reverse-biased 2.2V zener diodes to simulate the forward voltages of segment LEDs rising to an upper threshold of 2.2V. Test digit 18 thus simulates a digit with all 16 segment LEDs approaching a *open circuit*. This will test the ability of all the window detectors to detect open circuited segment LEDs.

Provided test digits 17 and 18 are selected at least once within the specified fault detection time, no undetected failures will be allowed to persist in the window detectors. Since the segment LED forward voltage is expected to be 1.65V @ a forward current of 50mA under multiplexed conditions, it is expected to lie well within these upper and lower reference limits. When these test digits are selected, all 16 window comparator outputs should go low, indicating a failure condition (a deliberate and predictable false-alarm).

The display comprises two HDSP-6508 8-digit, 16-segment unintelligent alphanumeric LED displays from Hewlett Packard [30]. The 16-segment display was chosen for its relatively simple drive requirements. The HDSP-6508 is tested in accordance with MIL-STD-883, and was electrically over-stressed above the maximum allowed operating conditions of $T_j = 110^{\circ}\text{C}$. The Display Module calculations are shown in Appendix F.

5.3 SEGMENT MODULE

Essential functions for the Segment Module are shown in Figure 20:

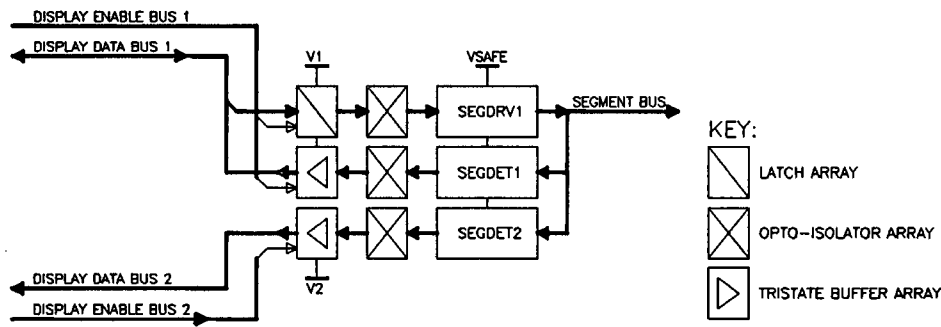


Figure 20:Segment Module

Due to the repeatability and high component count of the circuitry needed to implement the drive and detection functions for all 16 segments, it is not possible to show the complete circuit here. Therefore, a portion of the Segment Module dedicated to segment 1 (i.e., 1/16 of the Segment Module) is shown in Figure 21. Note that the part reference designators used in Figure 21 do not necessarily reflect those used in the actual subsystem schematics and on the PCB. They serve only as references to the text in order to explain operating principles.

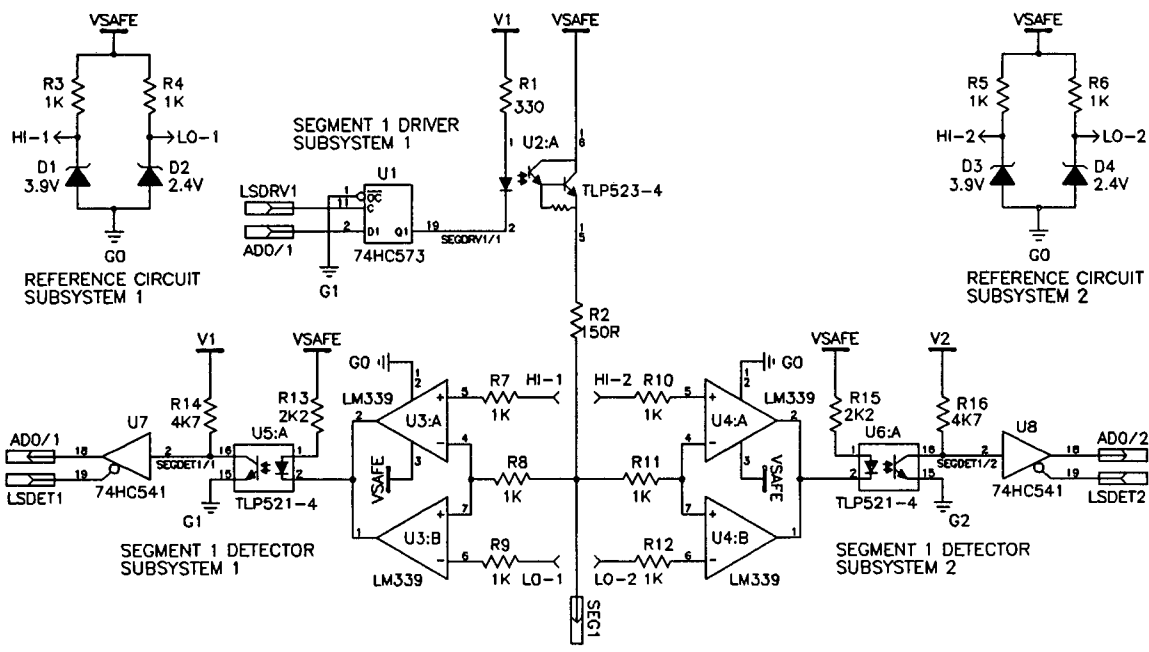


Figure 21:Segment Circuit

For more detailed diagrams of the various sub-modules that comprise the Segment Module, refer to the schematic diagrams in Appendix A, Figures 5→7. These schematics have been subdivided into segment driver and segment detector sub-modules. There are 16 identical

circuits that comprise the Segment Module; one per display segment. There is one reference circuit per subsystem, made up of R3, R4, D1, and D2 for subsystem 1, and R5, R6, D3 and D4 for subsystem 2. Latch U1 and buffers U7, U8 are one of 8 in an octal package, the others being used for 7 other segment circuits.

5.3.1) Segment Driver

What follows is a description of the driver circuitry to activate segment 1. The same description holds for the relevant circuitry of segments 2 to 16.

Control Module 1 (subsystem 1 of the Control Module), selects the appropriate segments to be displayed. Segment 1 is selected by pulling the segment drive line from Control Module 1 to segment 1 low. This is achieved by writing the appropriate segment data byte to Display Data Bus 1 (AD0..7/1). Two segment data bytes have to be written sequentially to the Segment Module to select all 16 segments. This data is then latched into U1 by pulling its enable pin high, using the appropriate line on Display Enable Bus 1 (LSDRV1).

Once the segment data is latched into U1 and the latch enable returns to zero, the data remains latched indefinitely until the latch enable goes high again. This is convenient, since many self-test and feedback tasks need to be executed during a display cycle. The segments will thus remain lit for the maximum duty cycle while other tasks are being performed.

The LED in Darlington optocoupler U2 is then activated by the output of U1. A quad Darlington optocoupler was selected to reduce parts count and size, while increasing reliability and sustaining the high pulsed forward current of 50mA required for the segment LED under multiplexed conditions. U2 also provides statistical independence in the event of a failure in subsystem 1 or in the display circuit. Since only one segment LED is activated by each Darlington optocoupler in U2 at any moment, the current handling capabilities are sufficient for direct connection to the segment line. Resistor R2 provides current limiting for the LED display under multiplexed conditions. The pulsed current will be higher than the steady state current of 10mA normally drawn by a LED.

5.3.2) Segment Detector

The segment LED proving is performed by a window detector consisting of two comparators from LM339 quad comparator U3. Each quad comparator package provides a window detector for two adjacent segments, thus reducing parts count and size, while increasing overall reliability. The circuit has been duplicated in order to provide detection outputs to both channels. In the event of a component failure in the one detector, the other will detect the condition of the display segment.

For subsystem 1, the upper reference voltage of 3.9V is provided by R3 and reference diode D1 to the non-inverting input of comparator U3:A. The lower reference voltage of 2.4V is provided by R4 and reference diode D2 to the inverting input of comparator U3:B.

The outputs of each window detector are optically coupled to their respective Display Data Bus lines. This ensures that failures in the window detectors and the Control Module do not influence one another electrically. The window detector derives its power from the display power supply (between G_0 and V_{SAFE}).

The appropriate segment detector output is selected by pulling the output enable of tri-state buffers U7 and U8 low, using the appropriate select line on Display Enable Bus 1 and 2 (LSDET1, LSDET2). This places the segment detect data on the Display Data Bus, where it is fed back to the Control Module for comparison. Once the data has been read, the appropriate enable line must be pulled high until that segment is selected again.

5.4 DIGIT MODULE

Essential functions of the Digit Module are shown in Figure 22:

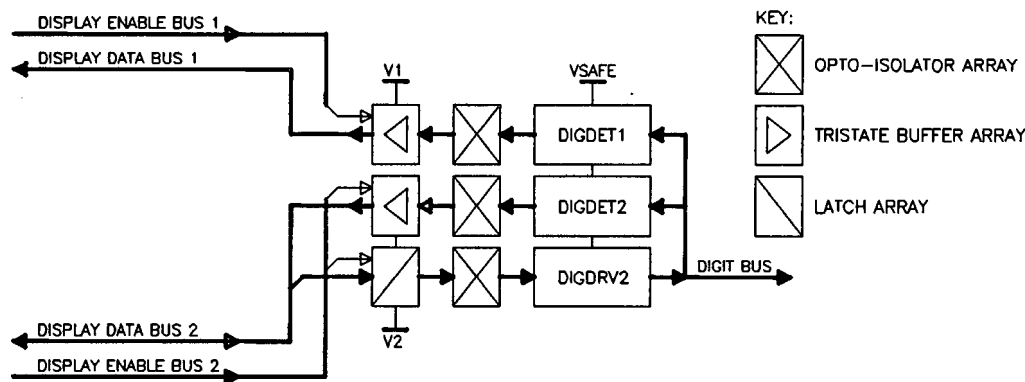


Figure 22:Digit Module

Due to the repeatability and high component count of the circuitry needed to implement the drive and detection functions for all 18 digits, it is not possible to show the complete circuit here. Therefore a portion of the Digit Module dedicated to digit 1 (i.e., 1/18 of the Digit Module) is shown in Figure 23. Note that the reference designators used in Figure 23 do not correspond with those used in the actual subsystem schematics and PCB layout. They serve only as references to the text in order to explain operating principles.

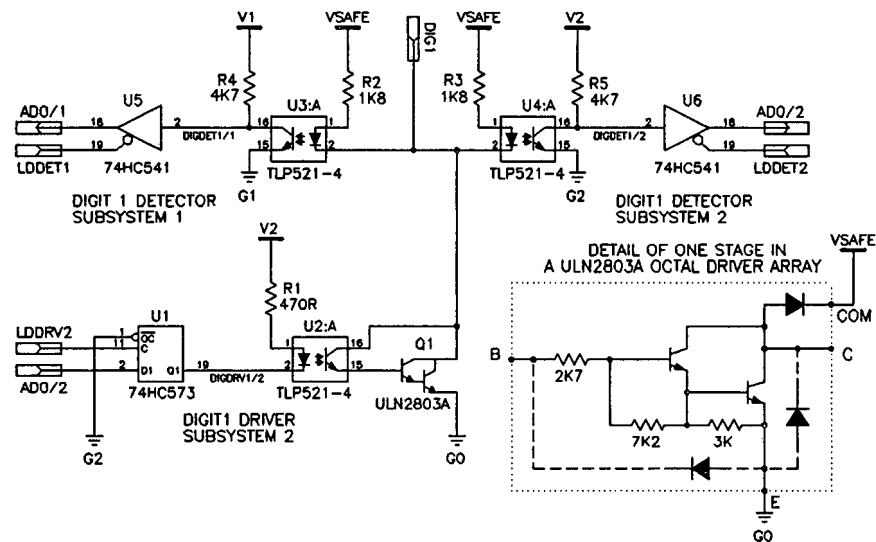


Figure 23:Digit Circuit

For a more detailed description of the various sub-modules that comprise the Digit Module, refer to the schematic diagrams in Appendix A, Figures 9→11. These schematics have been subdivided into digit driver and digit detector sub-modules. The Digit Module comprises 18 identical circuits, including the circuitry for the two test digits.

Latch U1 and buffers U5, U6 are one of 8 in an octal package, the others being used for 7 other digit circuits. A single switch, Q1, is used to select the appropriate digit in the display. This switch is one of eight in a ULN2803A octal Darlington driver array.

5.4.1) Digit Driver

What follows is a description of the driver circuitry and actions performed by the circuitry to select digit 1. The same description holds for the relevant circuitry of digits 2 to 18.

Control Module 2 (subsystem 2 of the Control Module) selects the appropriate digit. Digit 1 is selected by pulling the digit drive line from Control Module 2 to digit 1 high, deactivating U2 and switching Q1 on. This is achieved by writing the appropriate digit data bytes to Display Data Bus 2 (AD0..7/2). Three data bytes have to be written sequentially to the Digit Module in order to select all 18 digits. This data is then latched into U1 by pulling its latch enable high, using the appropriate select line on Display Enable Bus 2 (LDDRV2).

Once the digit data is latched into U1 and the latch enable returns to zero, the data remains latched indefinitely until the latch enable goes high again. This is convenient, since many self-test and feedback tasks need to be executed during a display cycle. The appropriate digit will thus remain selected for the maximum desired duty cycle while other tasks are being performed. The LED in optocoupler U2 is then activated by U1 output. U2 provides statistical independence in the event of a failure in subsystem 2 or in the display circuit.

Q1 must have sufficient power rating to carry the sum of currents from 16 simultaneously lit segments per digit under multiplexed conditions. The device can therefore be rated much lower than the sum of the currents if the duty cycle is low (no multiplexing). On average, 10 segments are simultaneously lit for most alphanumeric characters. However, the worst-case situation of 16 simultaneously lit segments has been assumed.

5.4.2) Digit Detector

The Digit Module has a detector circuit for each subsystem. Their task is to prove that the digit select switch, Q1, is operating correctly. Currents through the LEDs of U3 and U4 are

independent of the number of lit segments. The collector current of Q1 is the sum of the total segment currents and the LED currents of U3 and U4.

The appropriate digit detector output is selected by pulling the Output Enable of tristate buffers U5 and U6 low, using the appropriate select line on Display Enable Bus 1 and 2 (LDDDET1, LDDDET2). This places the digit detect data on the appropriate Display Data Bus, where it is fed back to the Control Module for comparison. The outcome of failures in Q1 as seen by the digit detectors for subsystem 1 only is now explained:

In the event of a *short circuit* in Q1, the LED of U3 will be permanently lit and DIGDET1/1 will be permanently low. During the multiplex cycle when digit 1 is not selected, DIGDET1/1 will remain low, indicating that it has been erroneously selected. A discrepancy in the output of the comparator software in Control Module 1 will result. This comparator logic can be implemented more cost-effectively in software in a micro-controller than with hardware comparators.

In the event of an *open circuit* in Q1, the optocoupler will be permanently inactive, and DIGDET1/1 will be permanently high. When the digit is selected during the multiplex cycle, DIGDET1/1 will remain high, indicating that the digit has been erroneously de-selected. A discrepancy in the output of the comparator software in Control Module 1 will result.

The same explanation holds for subsystem 2. In order to see the operation of the Segment and Digit Module on the Display Module, refer to the display circuit in Appendix A, Figure 12. It shows the appropriate circuitry from the Display Module, Segment Module and Digit Module, to activate Segment 1 of Digit 1, as well as detect its output.

5.5 POWER MODULE

This module contains the isolated power supplies for the two subsystems and the display circuit, and a soft-start circuit. The subsystems for the module are shown in Figure 24:

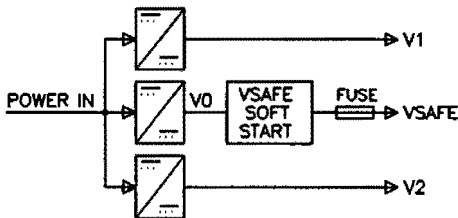


Figure 24:Power Module

5.5.1) Power Supplies

The schematic diagram in Appendix A, Figure 13 indicates the V_{SAFE} power supply, the Soft-Start, and the two identical 5V power supplies for the two subsystems. The Control Module subsystems for the 2-out-of-2 comparative architecture require 5V regulated power supplies. These must be isolated for statistical independence between the subsystems.

The display circuit requires a 5V regulated power supply. It must also be isolated for statistical independence between the display circuit and both controller subsystems. The supply should be trimmable to compensate for the voltage drop across the V_{SAFE} series-pass soft-start switch, Q2. The switched-mode DC-DC converter is the obvious candidate, since it provides input-output isolation and good regulation over wide current ranges. Since switched-mode power modules are readily available in 5V configurations, it was not considered necessary to design them, but rather to purchase off-the-shelf modules.

5.5.2) Soft Start Circuit

The soft-start circuit [11] shown in Figure 25 is situated in the Power Module, and supplies V_{SAFE} to both fuse-blow circuits in the Control Module. The soft-start circuit prevents the fuse-blow circuits from blowing the fuse when the systems starts up, due to unstable voltage levels present at power-up, which could present a false fuse-blow signal. It allows the processors to initialise and perform self-test routines before V_{SAFE} is connected to the display.

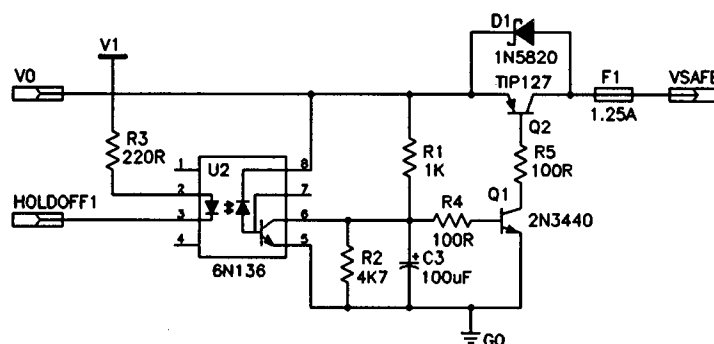


Figure 25. Soft Start Circuit

A *Holdoff* facility is provided in order to inhibit V_0 , and hence V_{SAFE} . In the event of initialization and self-test failures in either processor this line is pulled low by energizing the optocoupler, U2. The collector of U2 goes low switching Q1 off. This causes Q2 to turn off. This prevents the fuse from blowing at start-up.

Capacitor C3 charges up via R1, until Q1 switches on and forward biases series-pass switch Q2. This provides sufficient time for voltage levels in both subsystems of the Control Module to stabilise, and for initialisation to take place. Q2 was selected as a Power BJT, since its forward resistance and collector-emitter voltage is low and relatively constant over a wide range of currents drawn. A Power FET on the other hand, requires at least 8V between gate and source to pass high currents, and has a linear (albeit low) forward resistance, resulting in increasing forward voltage with increasing forward current.

Fuse F1 has been selected to be a 1.25A, fast-blow fuse. This ensures that any fuse-blow pulse of longer duration than a fuse-test pulse will blow the fuse. This also avoids possible damage to the shorting switch, Q1 in the fuse blow circuit. Although the fuse-blow circuit forms an integral part of the system power supply, it is located in each subsystem of the Control Module. It is therefore the function of the Control Module to control the testing or blowing of the V_{SAFE} fuse. This will be discussed later in the Control Module section.

Power for each subsystem in the Control Module is derived from an isolated DC-DC 5V converter in the Power Module. The Control Module either tests or blows the display fuse via the *F/BLOW* (fuse-blow) output, and verifies the fuse-test or fuse-blow via the *F/CHK* (fuse-check) input. The fuse-blow circuitry for providing V_{SAFE} to the display circuitry is included in the Control Module.

A local oscillator provides the clock. Data is received in a serial format via *DATA IN*. The input is polled on a periodic basis for received data. Data input to the system will not be interrupt driven, since it is *difficult to verify the outcome of interrupts* on system software [36]. Interrupts occur asynchronously and at random, and are thus difficult to analyze with software verification techniques.

Data is exchanged on a periodic basis with the other subsystem in the Control Module via *DATA XCHG*. With this data, it is possible to detect discrepancies between, and hence, failures in the hardware of either subsystem. Soft errors, such as spontaneous toggling of RAM contents due to interference, should also be detected.

Chapter 6: System Software

6.1 INTRODUCTION

For the purposes of this thesis, the primary tasks and sub-tasks of the software will be defined, and timing budgets assigned to them. This ensures that when the code is eventually written, it will fit into the system cycle time adequately. A flow chart indicating the major tasks to be performed by the system software is shown in Figure 27:

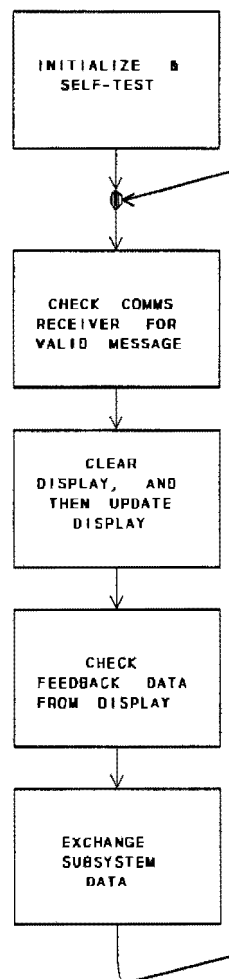


Figure 27:System Flowchart

Requirements and rationales for adopting certain methods and options will be discussed. The writing of system software will not be undertaken at this stage of the project as software safety has to be considered.

6.2 SUBSYSTEM INITIALIZATION

The system must undergo *initialization and self-testing* on start-up to ensure system integrity before a message is received and displayed. Since these tasks are performed once only, they must be thorough, since they will not form part of the display refresh loop. They do not affect system performance in terms of cycle time. All temporary storage dedicated to system configuration, received data, feedback data, self-test data and exchanged data is initialized. All flags used to indicate certain critical states of the system are initialized.

Each subsystem is configured to operate in a 2-out-of-2 comparative system, with data exchange links and feedback from the controlled device. The software differs slightly between the two subsystems to ensure that one is configured as the *master* and the other as the *slave*. This avoids both subsystems attempting to interrogate each other simultaneously.

Once each subsystem has undergone an initial self-test, the master must interrogate the slave in order to exchange test results and achieve loose synchronization. The entire contents of the EPROM in each subsystem is checked by means of a *cyclic redundancy check (CRC)*. All registers, internal and external RAM are cleared and then tested. Finally, both subsystems are synchronized.

Each subsystem must attempt to blow the fuse over a short time duration to ensure that the fuse-blow circuitry will operate when needed. It must be ensured that both subsystems do not attempt to test the fuse-blow circuit simultaneously, since the paralleled shunt currents could blow the fuse inadvertently.

6.3 DATA RECEIVER POLLING

This task will not be implemented in the current system software until a decision is taken as to whether the Communications Module of the FSDTS, or whether the FSDS itself should perform the task. A decision on the format of the received data needs to be finalised, and is beyond the scope of this research. A pre-stored message will be used for initial development purposes. It will be assumed that a message has been received, decoded, and stored in memory as 16-segment data (2 consecutive data bytes per alphanumeric digit). The

message will be permanently stored in a range of consecutive addresses in the EPROMs of both subsystems. A timer loop will be included to simulate the delay required to poll the receiver and receive the valid message.

The data reception hardware must be designed and the relevant software written, such that the data input to the system is periodically confirmed to be valid. This will avoid any invalid messages remaining locked in the display in the event of a data link failure. The data receiver must therefore be *polled* on a regular basis to check for a recurring valid message. Whenever possible, *demand interrupts should be avoided* [36]. The software should be able to determine when and in what order it interfaces with the outside world. This tends to increase the number of instructions required and may limit I/O response to millisecond rather than microsecond resolution. However it leads to more *predictable* operation and is more easily *verified*.

When the data receiver is found to be active (a message is waiting for reception), a Data Reception procedure must be activated until the entire message has been received. The message must then be decoded and stored in RAM for writing to the display.

6.4 DISPLAY UPDATING

Before any segments of a particular digit can be displayed, the first digit must be selected and all segments must be cleared. The relevant digit is then selected, followed by the relevant segments for a desired character to be displayed. The status (faulty/fault-free) of the selected digit and segments is determined by the relevant digit and segment detectors, and must be read and compared with the output digit and segment data.

During the display update routine, the functions of *output, feedback, and comparison* need to be performed on the system output (display). The lowest rate at which a multiplexed display can be refreshed without serious flicker is about 25Hz. A refresh rate of 50Hz has been selected. This translates to 20ms of refresh time, during which all 16 active digits must be lit. This gives a period of 1.1ms per digit displayed. During this time, the relevant digit and segments are selected, segment LED voltage detected, fed back to the Control Module, and compared. This is the maximum time made available for failure detection of digits and

segments, within the speed limits of the controller. However, system self-tests and general housekeeping need only be completed within a time limit that ensures that a second fault does not appear.

It is necessary to ensure that the relevant digit is activated for the maximum percentage of the refresh period, to ensure a high duty cycle. This will result in a lower peak LED current requirement to satisfy display viewability requirements, as well as reducing stress on the display elements. Counters are needed to control the sequential selection and detection of the digits. The software needs to control the latches that select the relevant digit and associated segments. It also needs to read the data fed back from the digit and segment detector buffers.

6.5 SUBSYSTEM SELF-TEST

To ensure continuing system integrity after the initial subsystem self-test a *periodic partial self-test* is executed within the main display loop. This self-test checks critical sections of the subsystems, until a complete system diagnosis is accumulated, whereupon the process repeats itself. This avoids latent faults from creeping into the system and possibly masking a fault that would otherwise manifest itself directly.

All storage elements, permanent or temporary, must be verified for integrity. This involves cyclic redundancy check (CRC) tests on the EPROM, and exchanges of RAM contents and registers. System flags must be checked too.

In addition to the 16 active digits in the display, two 'dummy' test digits are included for periodically testing the integrity of the segment window detectors. The software needs to activate these two digits and read the resultant outputs from their window detectors to ensure the ability of the system to detect shorted or open display segments. However, these two digits need not be selected during every refresh period.

The fuse-blow circuit must be tested from both subsystems in the Control Module and verified to be operational by detecting the drop in display voltage, V_{SAFE} . This task need not be performed during every display refresh period (roughly 1.1ms) but must be performed within

the system failsafe detection time set by the user requirement.

6.6 SUBSYSTEM DATA EXCHANGE

A facility must be provided for data exchange between the two subsystems for the purposes of *data comparison*, *subsystem failure detection*, and *subsystem re-synchronization*. Because the two subsystems run asynchronously, a timing delay will accumulate between them over time. Therefore, *software time-outs* need to be implemented to ensure that adequate time is allocated for the subsystems to respond to one another. The software will differ slightly between the subsystems configured as the master and the slave.

The subsystem configured as the master initiates data exchange with the subsystem configured as the slave. Relevant data for exchanging with the slave subsystem is collected, formatted into a data block, and transmitted to the slave subsystem. The relevant data block from the slave subsystem is then received by the master and compared with the data block sent. Any discrepancies must result in blowing the VSAFE fuse, leading to safe system shutdown. The exchange of data must be sufficiently frequent in order to avoid errors accumulating in the system to the point where one error may mask another error. Typical data exchanged for this purpose would be display counters, flags, CRC test results and feedback from the display.

Since the two subsystems run asynchronously from separate crystal clocks, they will gradually drift out of synchronization. It is therefore necessary to provide synchronization data to periodically re-synchronize the subsystems. Re-synchronization involves temporary storage of exchanged data in buffers, comparison, signalling consensus, and marking of completed intervals [37],[38]. This is accomplished in software using suitable inter-module data links. This avoids the problem of time correlated operation, which is subject to *correlated malfunction* if subjected to common-mode external electromagnetic radiation.

6.7 SOFTWARE SAFETY

The issue of Software Safety [5],[11] is being addressed elsewhere, and is beyond the scope of this research. It is sufficient to say at this stage that techniques are being developed for the correct validation and verification of safe software, and that these techniques will be

applied to any software written for the FSDS project.

Every possible situation must have a predictable outcome. This can be evaluated by constructing a fault tree. Each possible event, or combination of events, must be evaluated with respect to their effects on the software. It is also necessary to consider the position in time when an event occurs. Briefly, every event, in combination with the state of all flags and variables within the software, must have a predictable outcome at a predictable point in time. This justifies the use of polling within the software rather than interrupts. However, it is still necessary to maintain asynchronism of the execution of the code in the two subsystems in order to maintain statistical independence.

Where possible, state diagrams should be compiled in order to evaluate the effect of previous states plus present state events on the next state of the system. Since the system has memory, the state transition tables could be very complex.

Chapter 7: Reliability and FMECA

7.1 RELIABILITY AND SAFETY

The individual device failure rates must be calculated [31] before the system reliability can be calculated. Once the failure rates of all device types used in the system have been evaluated, their failure rates can be multiplied by the number of devices of each type. These cumulative failure rates for each device type are added to give a system failure rate. The reliability, expressed as the Mean Time Between Failure (MTBF) for the system, can then be calculated. The system safety, expressed as Mean Time Between Wrong-Side Failure (MTBWSF), is calculated last.

Reference [31] provides extremely conservative (and often unrealistic) failure rates for electronic devices. Actual manufacturers tests often revealed lower failure rates. For example, Hewlett Packard quote an MTBF of the order of 1 million hours for the HDSP-6508 16-segment LED display [30]. In this case, the manufacturers figure was taken in preference to the prediction in [31]. The Reliability and Safety Calculations are shown in Appendix H.

7.2 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

A module level Failure Modes, Effects and Criticality Analysis (FMECA) was performed for each component type. From this, system safety under failure conditions could be evaluated, and corrective action taken in the design to protect against critical failures. This was an iterative process, repeated until desired system safety was achieved.

The FMECA has been documented in tabular form making use of [31] and [32]. The recording of each failure mode is extensive and is therefore included in Appendix B. The analysis only covers the Segment Module, Digit Module, and Display Module at this stage. The device numbers refer to the Display Circuit diagram in Appendix A, Fig.12, which illustrates the operating principle only. It does not refer to the actual component reference designators used in the detailed schematic diagrams of the modules or the PCB artworks. Since the hardware design is not finalised, hardware changes may take place, necessitating an update of the overall system reliability and safety figures.

A number of failure modes (fault models) have been identified and used for the integrated circuit components [18],[39]. Since there are many components (up to tens of thousands in VLSI chips), it is not possible to identify every failure mode of every device within that chip. The failure analysis can be eased by a "*fault model*", a set of simplifying assumptions about the failure mechanism. A failure mechanism is a physical defect which produces a fault, where the fault is a divergence from the circuits fault-free behaviour.

The fault model is a simplified description of the relation between *failure mechanism* and *fault effect*. An example would be in the case of an LED, where a failure mechanism may be the electro-migration of metal ions from the wafer connections under prolonged DC conditions. This would result in the LED going open circuit (the fault model). The fault effect would be the LED failing to illuminate. In the context of the failsafe display system, the electronics would only be able to identify the fault model (the open circuit), while the operator would only see the fault effect (the unlit LED). The failure mechanism of electro-migration would be transparent to the system as a whole. The fault models identified for use on digital ICs (and quasi-digital voltage comparators) are:

- *Stuck-at fault*: It is based on the assumption that one of the inputs or the output of a gate is stuck-at logic "0" (s-a-0) or stuck-at logic "1" (s-a-1). This model offers good short circuit and open circuit analysis. Faults in MOS circuits cannot necessarily be modelled as s-a-0 or s-a-1 faults.
- *Bridging fault*: This results from accidental connection between two logical signal lines as a wired-AND (positive logic) or wired-OR (negative logic). They are classified either as either *input bridging* or output-input bridging (*feedback bridging*). Feedback bridging can convert combinational logic into a sequential circuit that oscillates.
- *Stuck-open fault*: This is typical of CMOS circuits, and would cause the output to be connected to either the positive or negative supply. This often creates sequential circuits from combinational logic, resulting in oscillations. This increases the difficulty of both testing the circuit and designing a set of test vectors so that a high percentage of fault coverage is achieved.

- *Temporary fault*: System malfunction caused by temporary faults represent the majority of faults, and can represent as much as 90% of total maintenance expenses. They can be grouped into two categories:
 - *Transient faults* are non-recurring temporary faults caused for example by power supply variation or α -particle radiation. Such faults are not repairable because there is no permanent physical damage to the system. The majority of faults found in semiconductor memory systems are of this type. They can be detected by performing periodic checksums or cyclic redundancy checks on the entire memory contents.
 - *Intermittent faults* are recurring faults. They are caused by loose connections, by deterioration or ageing components, by fluctuating environmental conditions (temperature, humidity, etc.) or by poor design. A circuit is poorly designed if components are operated close to their maximum tolerances and thresholds, or when devices are incorrectly biased. Intermittent faults only cause system malfunction when they are active. In this case the circuit is in its *fault active* state otherwise it is in its *fault not-active* state, and is random in nature. "Well behaved" and "signal independent" faults are described by the *two-state Markov model*. Intermittent faults can be detected and overcome by using redundant circuits that are statistically independent, or diverse in nature.

From analysis of preliminary charts, it was found that failures in the window detectors and their associated references in the Segment Module could go undetected, leading to wrong-side failures. As a result of these findings, appropriate redesign was carried out. This involved including two 'dummy' test digits in the Display Module. These test digits consist of 16 zener diodes each. Each zener diode mimics either a display segment short or open circuit, depending on which test digit it belongs to. The purpose of the test digits is for periodically testing the response of the window detectors to simulated short circuits and open circuits in all 16 segments of a display digit. The updated FMECA charts are included in Appendix B. Charts tabulating the probability of failure for each component against failure severity, have been compiled for each module. These serve as a summarised guideline for identifying critical components within the system.

Chapter 8: Construction and Testing

The modular nature of the proposed Failsafe Display System (FSDS), coupled with the need for compatibility with the related Failsafe Data Transmission System (FSDTS) [11], required the use of plug-in cards using the DIN41612 (Eurocard) type connectors. It was decided to use the 64 pin DIN41612C connectors with the middle row of pins removed (A-C type), since these were used in the FSDTS, and since the increased pin spacing enhances safety.

These cards are to be plugged into corresponding sockets on an interconnecting back-plane. Although these cards are not pin compatible with the back-plane of the FSDTS, it is possible that after industrialization they may be made compatible. The Printed Circuit Board (PCB) layouts for each module are located in Appendix C. Each card is represented by its solder layer, component layer, and silkscreen layer to help with component placement. In order to show each PCB on a single A4 page, some of the artworks are actually 80% to scale.

In its present development configuration, the system consists of four main 6U-size cards plugging into Eurocard connectors mounted on an interconnecting back-plane. The four cards are the Segment Module, Digit Module, Control Module, and Power Module. Each card has two 64-pin, A-C type, DIN41612C male connectors for connection to the corresponding sockets on the back-plane. The back-plane thus carries eight 64-pin female Eurocard sockets, as well as a male 40-pin DIN41651 ribbon cable connector to the Display Module.

All boards have been designed for double-sided through-hole plating, although at present solder pins are being used as through-connections during the development phase to contain costs. Once the system is fully tested and the design verified, it will be possible to immediately generate through-hole plated boards with no extra design cost.

The design of a 2-out-of-2 comparative failsafe system is costly. All functions need to be duplicated, resulting in a doubling in system cost. The detection and feedback circuitry required to verify correct operation of the display element provides an additional cost. An essential element for failsafe systems is the requirement for statistical independence between the duplicated subsystems under failure conditions. This statistical independence was achieved by using optocouplers to interconnect all physical connections and isolated power supplies for

each subsystem. These components can result in a further doubling in the system cost. All these factors have a multiplier effect on the cost of the PCBs, due to the resultant increase in size. The cost of the software is higher than that required to implement the basic function of displaying a message. This is due to the presence of two asynchronous controllers that require synchronisation in order to activate a common display. Finally, development costs and times are greater. All these factors contribute to an approximately five-fold increase in the system cost over that required to implement the basic message display function.

To implement a 2-out-of-2 comparative system, the entire system is divided into two identical subsystems. For each module (card) the relevant subsystem circuitry is duplicated and placed side-by-side on the same card. In the Segment Module, there are two subsystems for segment drive, segment detect and for references. Similarly on the Digit Module card there are two subsystems for digit drive and digit detect, and two identical controller subsystems on the Control Module card. For the Power Module, there are three power supplies; one for each subsystem, and one for the display circuit which is common to both subsystems.

A fifth card, the Display Module, is connected to the back-plane card with a ribbon cable connector. This card contains two 8-character, 16-segment alphanumeric LED displays. This module is common to both subsystems. Both subsystems are needed to activate a display element, and both subsystems sense the electrical state of each display element. Display activation and sensing are all carried out between the Segment and Digit Modules and the Display Module via the back-plane connecting path and ribbon cable.

In its present state of development, the system is not installed in a cabinet, although the PCBs have been sized to fit into a standard Eurocard cabinet when industrialization of the system commences. The primary power supply input voltage has not been finalized. However the input voltage range of the selected DC-DC converters on the Power Module PCB extends from 20V to 72V, with a nominal input voltage of 48V.

The design of the Control Module card, which contains the microcontroller circuitry and associated software, will not be undertaken at this stage. This is beyond the scope of this research, and will likely consist of modified version of the Communication Module developed for the FSDTS [11]. As a temporary measure, a Test Module (Schematic Diagram in

Appendix A, Figure 14) was developed to simulate the display control outputs from the Control Module. This Module consists of two banks of 18 toggle switches, one bank per subsystem. There is a toggle switch for each output, which provides a high or low signal to the Segment and Digit Modules. This will facilitate static testing of the display activation, latching and buffering. A PCB artwork (Appendix C) was designed for the Test Module, and a PCB manufactured and populated.

The Segment, Digit and Display Modules were statically tested by toggling the relevant switches on the Test Module in a manner which simulates the display multiplexing control signals from Control Module to Display Module. The resultant effects on the relevant display elements in the Display Module were noted in Appendix I, and compared with expected normal operation. The test results confirmed that the system and module design is sound.

The PCBs were checked for artwork design errors such as missing connections, through-holes, power supply shorts, and breaks in tracks. In this way, the basic electrical integrity of the interconnected boards was verified. The connectivity between each of the boards was checked with a continuity meter and with reference to the circuit schematic diagrams. This ensured that all connections between the modules via the Eurocard connectors and the back-plane were functionally and electrically correct. A number of layout errors were located and rectified.

Chapter 9: Conclusions

The concept of the Radio Token Block System and its desirability were discussed. A User Requirement was compiled from user statements and certain options that became apparent as research progressed. Where there were options to be considered, these were listed under the appropriate requirement, and a decision documented in a Requirements Review.

A trade-off study of display technologies revealed the LED display as the most suitable candidate for the display element. Failure modes of LEDs and their effects on the window detectors were identified. A trade-off between complex graphics displays and single-lamp signalling was made, and the 16-segment display was selected. A single line 16-character display was selected as the display format in order to keep the system as simple as possible.

System concepts unique to a Failsafe Display System were identified and discussed. These included integrity of the data displayed, electrical integrity of the display element itself and related subsystem hardware. The technique of voltage window detection of the display element was introduced and discussed. The window detector circuits are to be checked within a period shorter than the fault detection time in order to ensure their integrity.

A loosely-coupled 2-out-of-2 comparative architecture with feedback from the display element, was selected as the appropriate solution for a Failsafe Display System. The concept of dissimilar control was introduced, where one subsystem selects the appropriate digit and the other selects the segments, in order to activate a display element. The requirement for statistical independence between the subsystems was identified as crucial to failsafe system operation.

An architecture was developed based on the concepts and philosophies developed in the preceding sections. The system hardware was partitioned into a number of modules, each containing two similar subsystems for the purpose of data comparison. These included a Display Module, Segment Module, Digit Module, Power Module, and Control Module. The operation and primary functions of each module were discussed. A system-level FMECA and Reliability Analysis were performed to verify the basic system layout before detailed design commenced.

The software tasks of initialisation, data receiver polling, display updating, self-testing, and subsystem data exchange were discussed. The coding of these tasks into software will be undertaken in subsequent research. The verification of the software to implement these tasks is beyond the scope of this paper, and is currently being investigated in related research [11].

Module-level reliability was evaluated, leading to a figure for the system MTBF. This figure is not final, since the hardware design has not been finalised. However, it serves as the basis for the evaluation of system MTBF. A safety figure (MTBWSF) was calculated which exceeded the user requirement. A module-level Failure Modes Effects and Criticality Analysis was conducted in order to document as accurately as possible, all possible failure modes and their outcomes for each component in the system. As the hardware design is not complete, this will be expanded on.

All circuit boards, excepting the Control Module PCB, were manufactured and statically tested for basic design faults, connectivity and basic functional correctness. Dynamic testing (operational testing) will follow once Control Module hardware is built and software written.

References

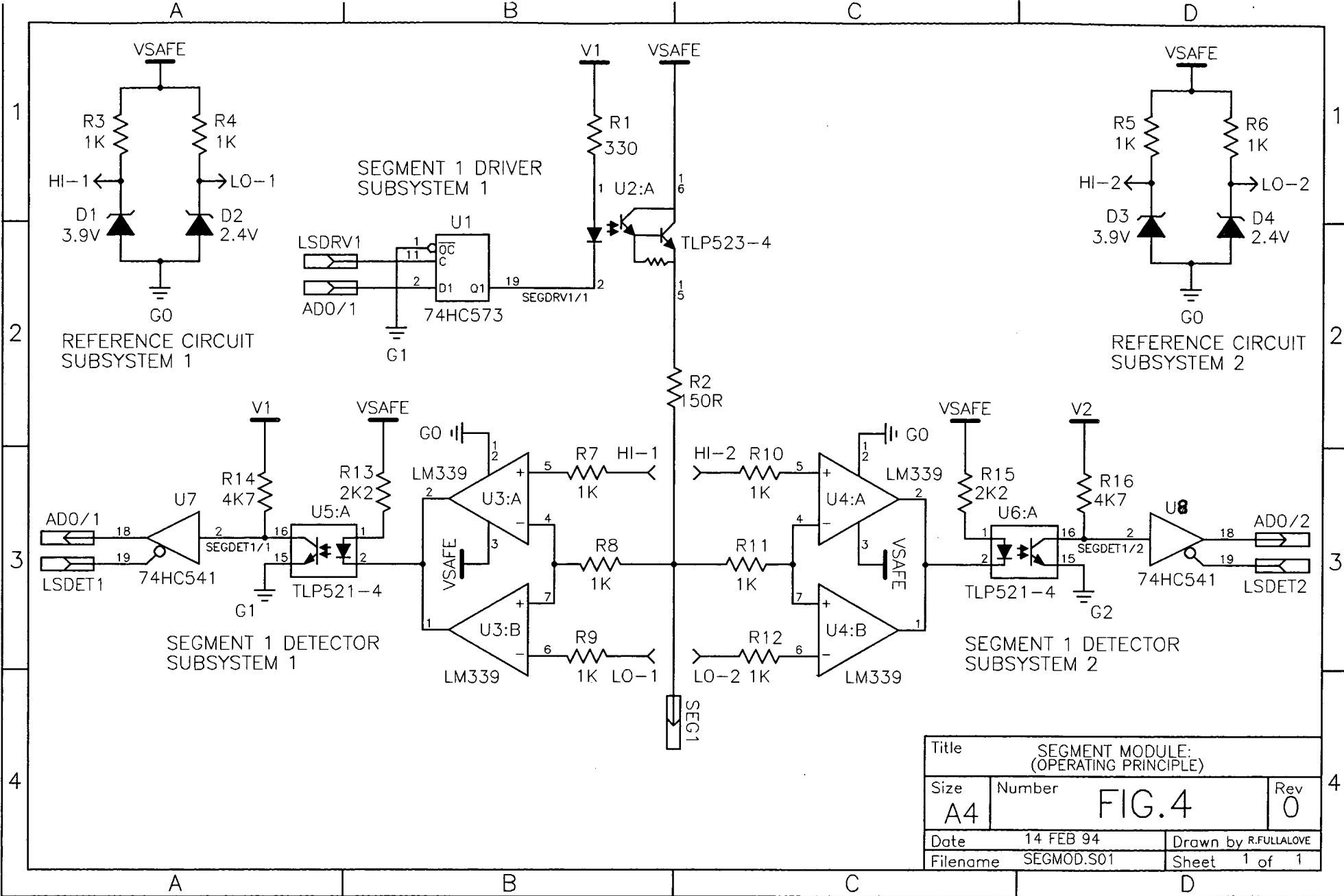
- [1] "SARRAT MK1 Radio Token System"; Woodhead, R.B; Specification No. CSE 630/1, Issue 1XK, Spoornet (Sept. 1991).
- [2] "Low Cost Signalling by Radio"; Birkin, M.S; Proceedings of the Institution of Railway Signal Engineers (I.R.S.E.) (1984/85); pp48-66.
- [3] "Processor Based Safety Systems"; Mills, J.D; Proceedings of the I.R.S.E. (1984/85); pp68-84.
- [4] "Safety Considerations"; South African Transport Services; Trains Working Regulations (May 1984).
- [5] "Electronic Safety"; Paverd, G.B; Chief Signal Engineers Research Laboratories, South African Transport Services; March 1988.
- [6] "Office of Research and Experiments Report A155/RP12"; International Union of Railways; April 1988, pp15-16.
- [7] "Learning to live with Microelectronic Signalling"; Barnard, R.E.B; Proceedings of the I.R.S.E. (1986/87); pp 114-133.
- [8] "Neasden Depot-An Application of Computers to Interlocking"; White, C.R. and J.D.Corrie; Proceedings of the I.R.S.E. (1985/86); pp85-103.
- [9] "Accidents-How do they relate to Signalling and Traffic?"; Allsop, R.E. and M.J.Savage; Proceedings of the I.R.S.E (1984/85); pp132-148.
- [10] "Continuous Automatic Train Control with Microprocessors"; Hollands, R.D. and D.Barton; Proceedings of the I.R.S.E. (1986/87); pp93-113.

-
- [11] "Fail-Safe Data Transmission System"; Schröner, M.B; PhD Thesis (to be published), University of Cape Town, South Africa (1993).
 - [12] "Optoelectronic Designers Handbook"; Gage, Stan; Hewlett Packard; 1978.
 - [13] "How to select a flat-panel display" Silverstein, M.F.; IEEE Spectrum (Sept. 1989); pp41-45.
 - [14] "Manufacturing hurdles challenge large-LCD developers"; Stix, G.; IEEE Spectrum (Sept. 1989); pp36-40.
 - [15] "Perfecting the picture"; Apt, C.M.; IEEE Spectrum (July 1985); pp60-66.
 - [16] "An Experimental Study of Memory Fault Latency"; Chillarege, R. and R.K.Iyer; IEEE Transactions on Computers, Vol.38, No.6, June 1989, pp869-874.
 - [17] "Digital Communications"; Haykin, S; John Wiley & Sons; 1988; pp370-393
 - [18] "VLSI System Design: Systems on Silicon, Vol.2"; Dragffy, G; Lecture Notes, Bristol Polytechnic (1986); pp24.2-24.11, pp36.2-36.11, pp37.14-37.19.
 - [19] "Computer displays: new choices, new tradeoffs"; Perry, T.S. and P.Wallich; IEEE Spectrum (July 1985); pp52-59.
 - [20] "Flat-panel displays displace large, heavy, power-hungry CRTs"; Tannas Jr., L.E.; IEEE Spectrum (Sept. 1989); pp34-35.
 - [21] "A Review of Jointless Track Circuits"; Brown, C; Proceedings of the I.R.S.E. (1984/85); pp111-131.
 - [22] "Designing micro-based systems for fail-safe travel"; Turner, D.B. et.al; IEEE Spectrum (February 1987); pp58-63.

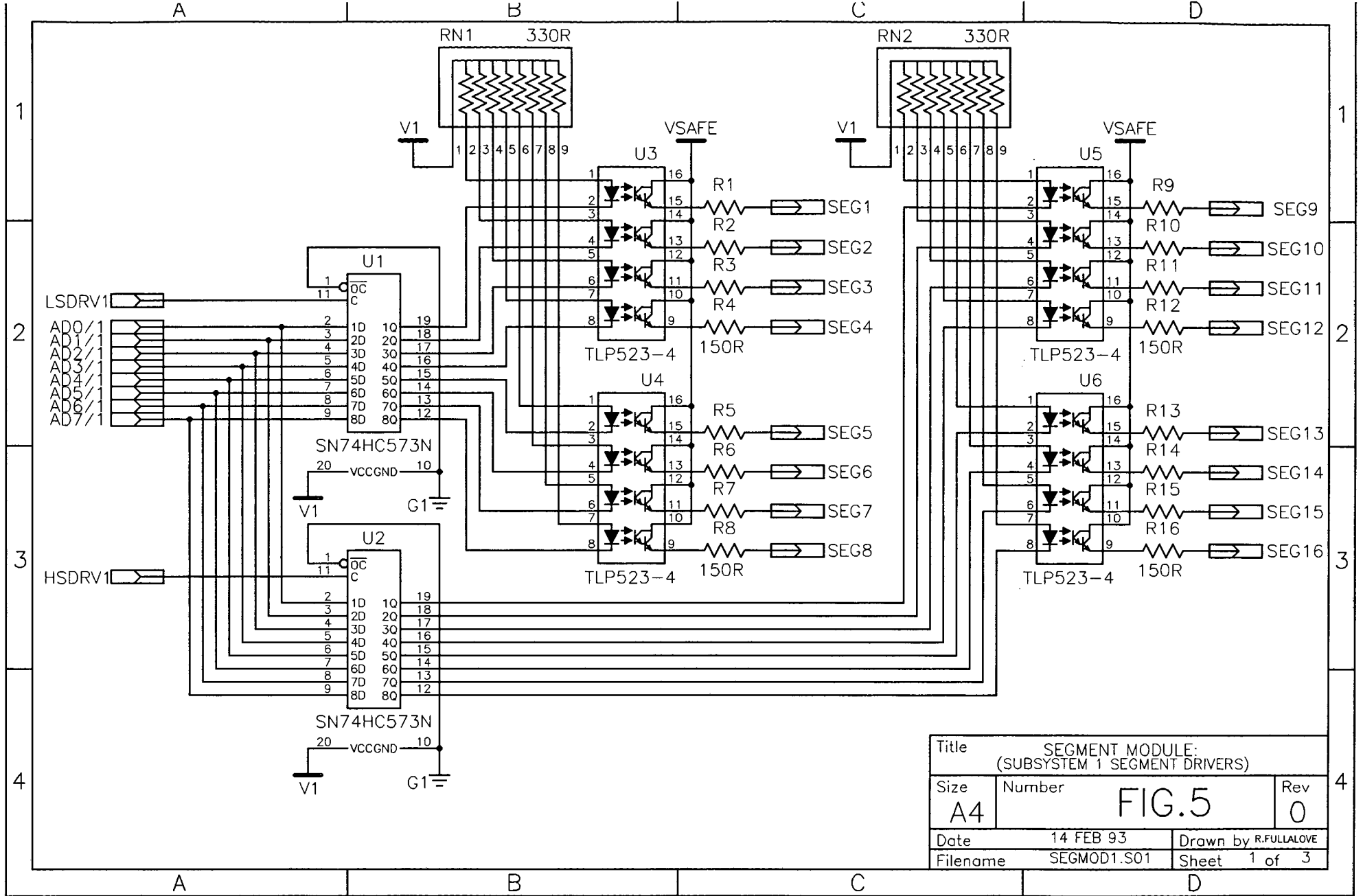
-
- [23] "URTL Circuit System U1 with High Safety and Automatic Fault Diagnosis"; Lohmann, H.-J. et.al; Siemens Review XLII (1975),No.4; pp145-160.
- [24] "Fail-Safe Data Processing in Railway Signalling Systems"; Lohmann, H.-J; Siemens Forsch.-u Entwickl.Bd.7(1978)Nr.6; Springer Verlag 1978; pp374-377.
- [25] "The workhorse CRT: new life"; Baldauf, D.R.; IEEE Spectrum (July 1985); pp67-73.
- [26] "Reliability Data: Plastic Lamps"; Hewlett Packard Optoelectronics Division; February 1992 (see Appendix E).
- [27] "Automatic Train Control for Heavy Mineral Railways"; Knowles, T; Proceedings of the I.R.S.E. (1983/84); pp74-93.
- [28] "Intersil Data Book"; Intersil; 1982; p6-135.
- [29] "General Instrument Optoelectronic Products"; General Instrument/Quality Technologies; 1985; pp359-362.
- [30] "HDSP6508 16-segment display data sheet and reliability data"; Hewlett Packard Optoelectronics Division; February 1981 (see Appendix E).
- [31] "MIL-HDBK-217E: Reliability Prediction of Electronic Equipment"; Department of Defense; 1986.
- [32] "Report 12-Failure Catalogue for Electronic Components"; Office of Research and Experiments, International Union of Railways; April 1988; p68.
- [33] "Computers that are 'never' down"; Zorpette, G.; IEEE Spectrum (April 1985); pp46-54.

-
- [34] Correspondence with the Deputy Director (Technical and Production) of the European Rail Research Institute (Utrecht, Netherlands); Smith, W.R ; November 1992 (see Appendix E).
- [35] Correspondence by Fax with Hewlett Packard application engineers in Germany; Thomas, Uwe; Hewlett Packard Germany; Oct 1992 (see Appendix E).
- [36] "Architectures for Fault-Tolerant Spacecraft Computers"; Rennels, D.A; Proceedings of the IEEE, Vol.66, No.10, October 1978; pp1255-1268.
- [37] "FTMP-A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft"; Hopkins, A.L. et al; Proceedings of the IEEE, Vol.66, No.10, October 1978; pp1221-1225.
- [38] "SIFT:Design and Analysis of a Fault-Tolerant Computer for Aircraft Control"; Wensley, J.H. et al; Proceedings of the IEEE, Vol.66, No.10, October 1978; pp1240-1254.
- [39] "Metals Handbook: Failure Analysis and Prevention - Failure Analysis of Integrated Circuits"; Bailey, C.M. and D.H.Hensler, AT&T Bell Laboratories; American Society for Metals, Vol.11; 9th Edition; pp766-789.

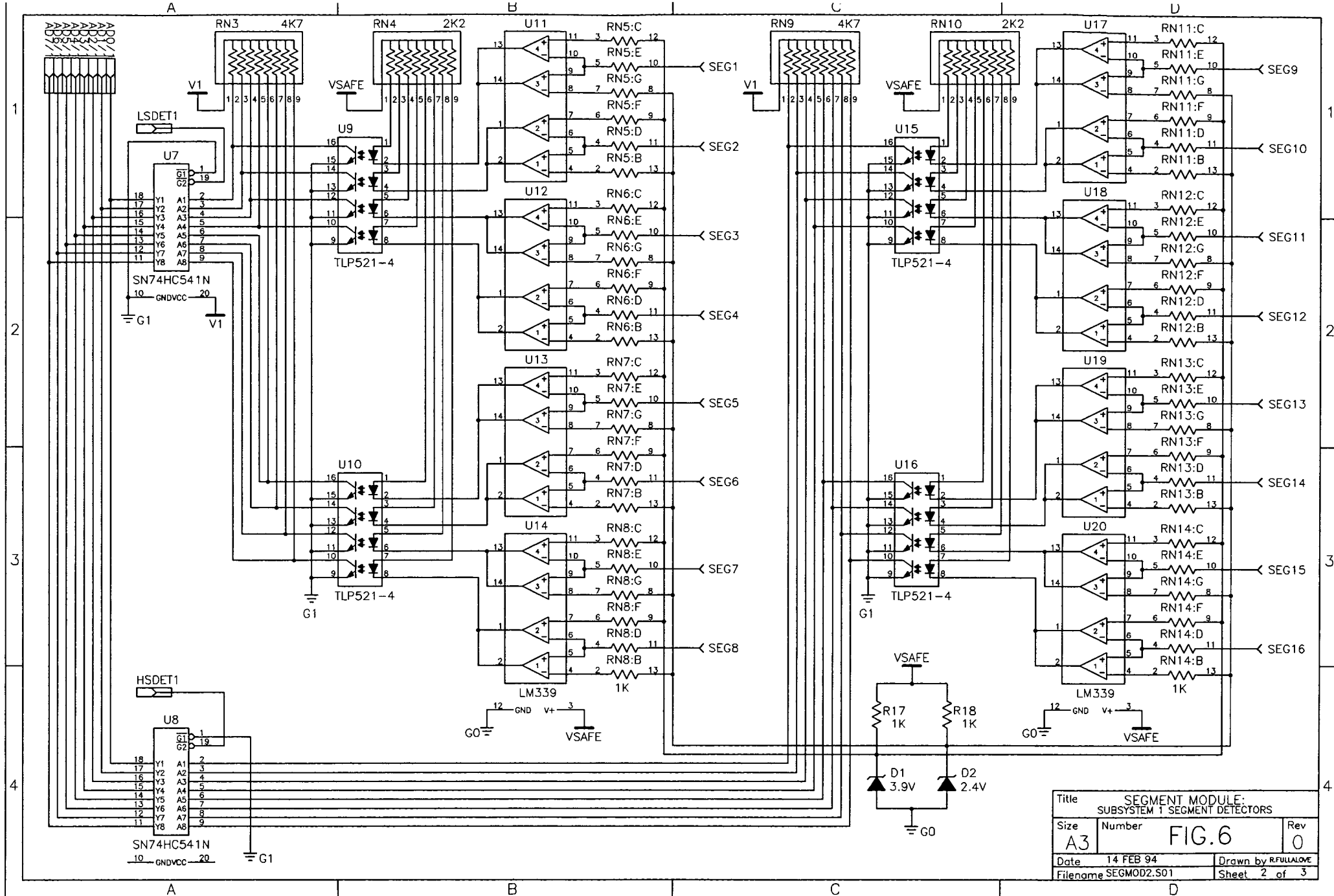
APPENDIX A: Schematic Diagrams



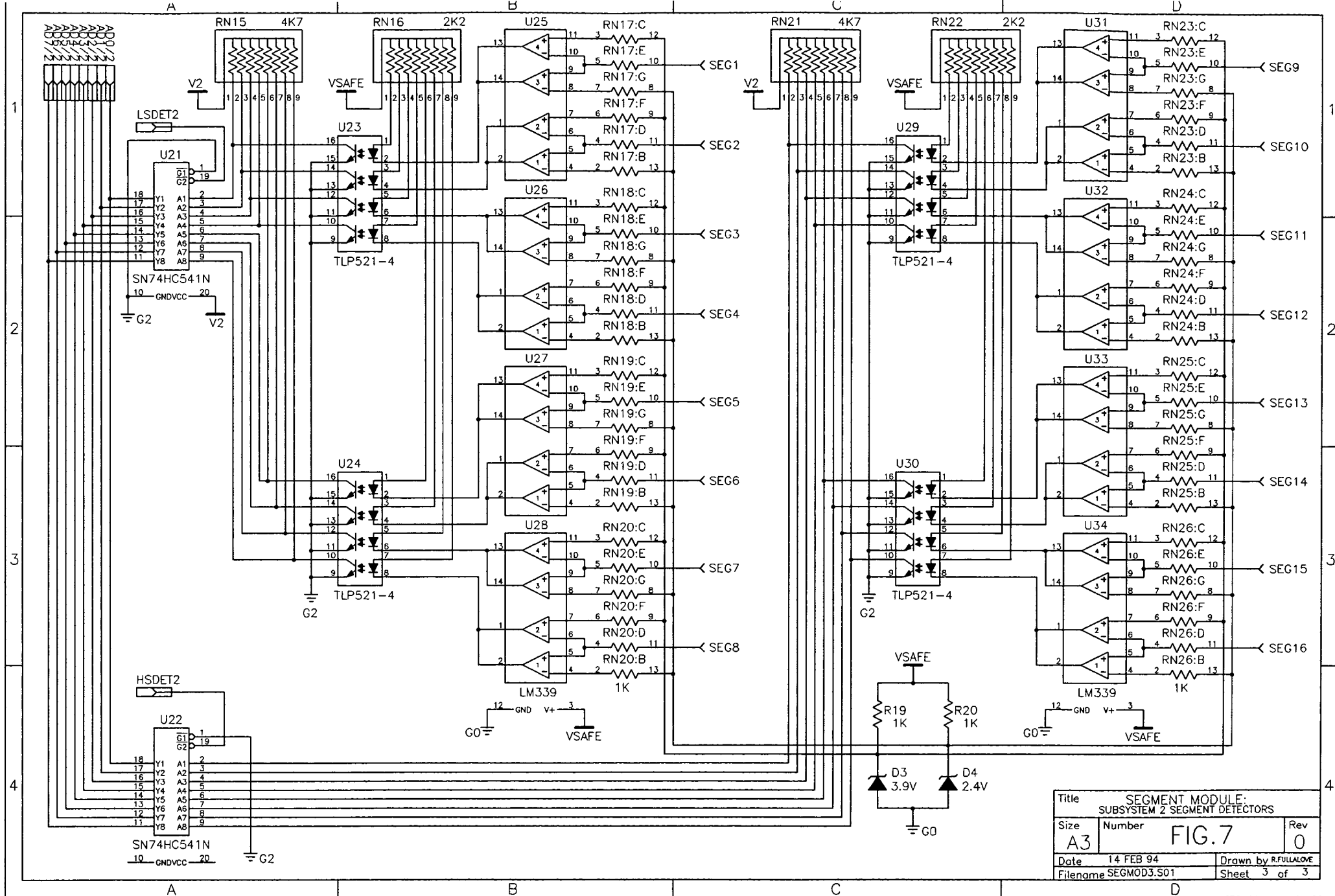
Title			SEGMENT MODULE: (OPERATING PRINCIPLE)	
Size	Number	Rev		
A4	FIG.4	0		
Date	14 FEB 94	Drawn by R.FULLALOVE		
Filename	SEGMOD.S01	Sheet 1 of 1		

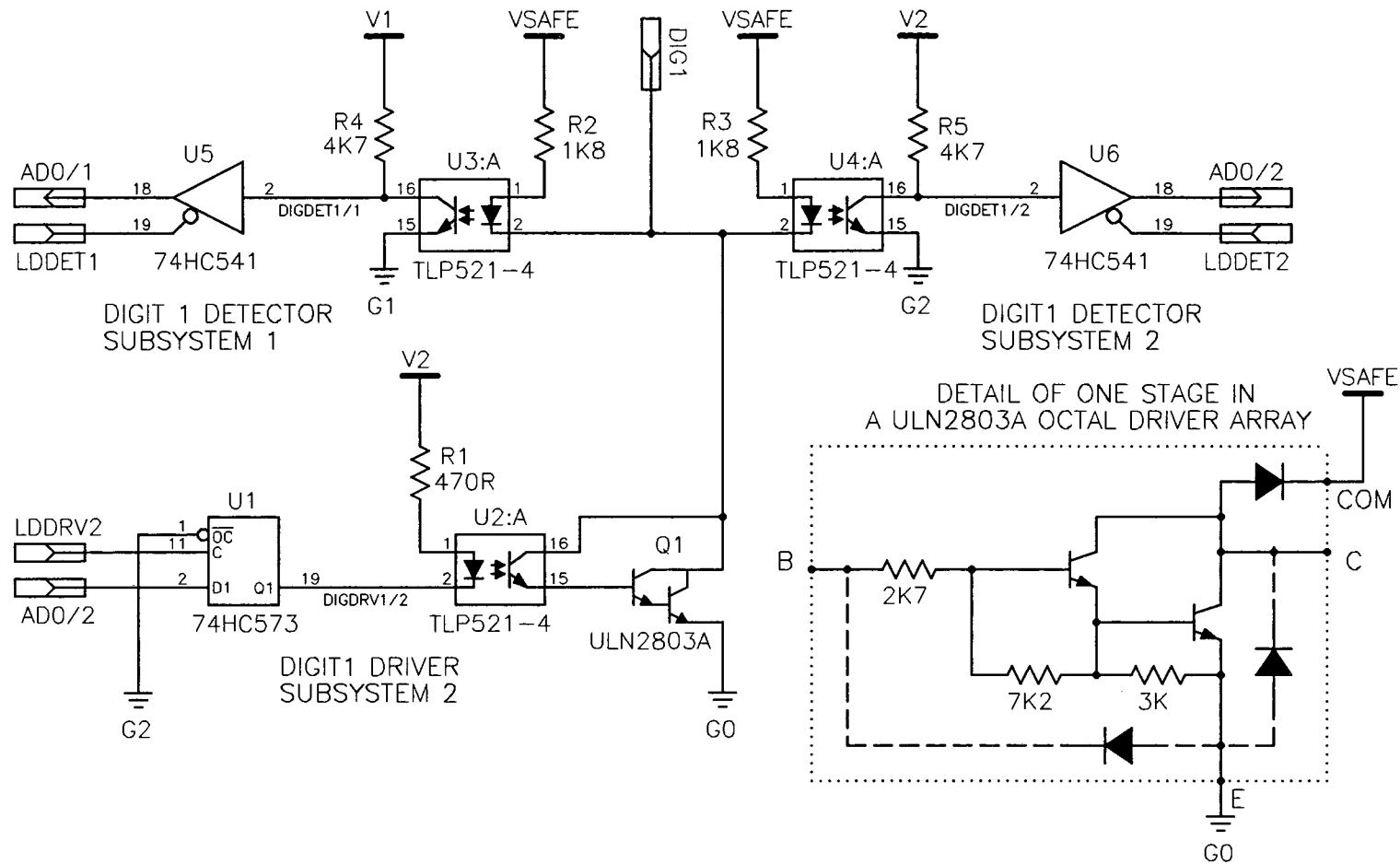


Title			SEGMENT MODULE: (SUBSYSTEM 1 SEGMENT DRIVERS)
Size	Number	Rev	
A4	FIG.5	0	
Date	14 FEB 93	Drawn by R.FULLALOVE	
Filename	SEGMOD1.S01	Sheet 1 of 3	

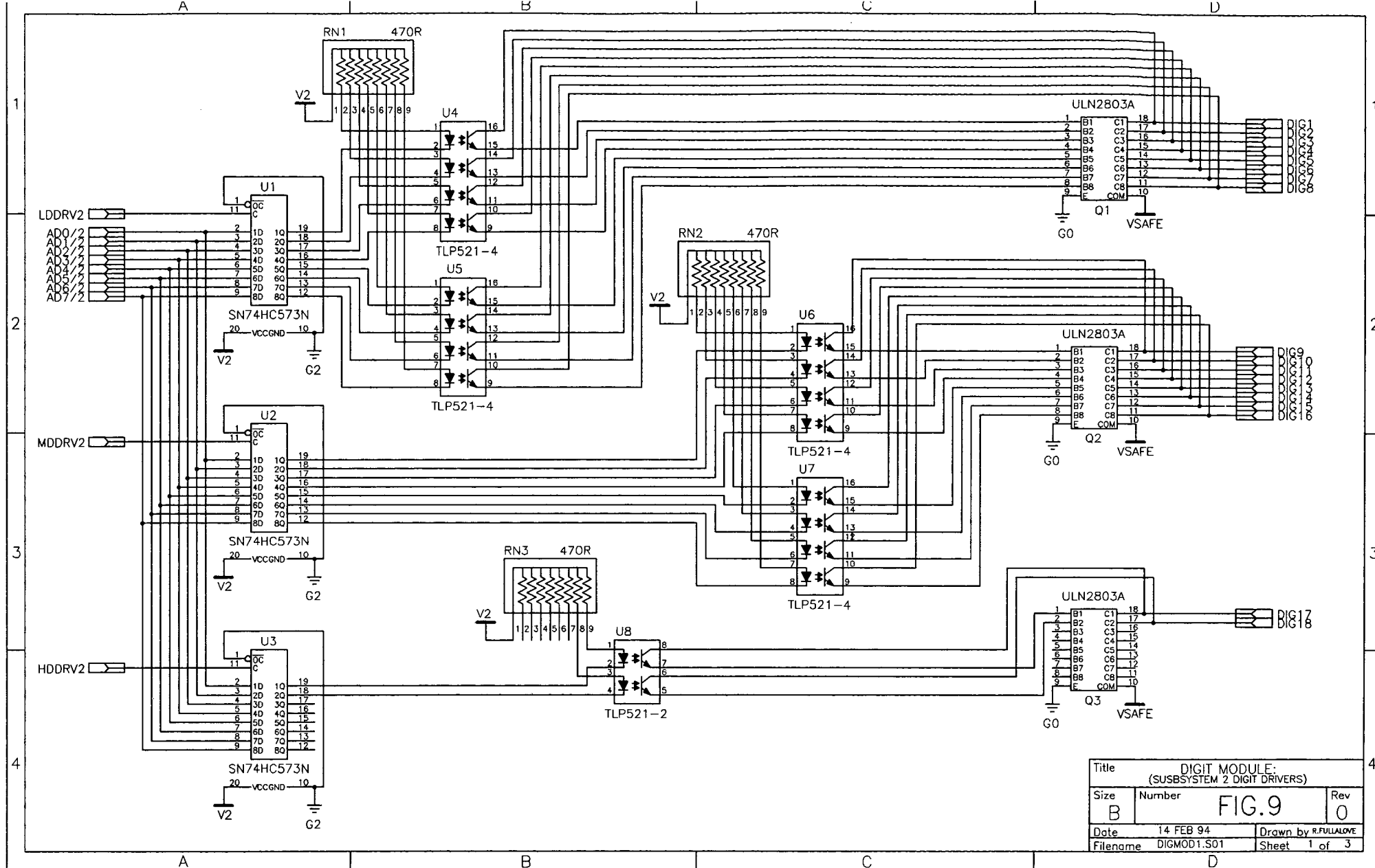


Title			SEGMENT MODULE: SUBSYSTEM 1 SEGMENT DETECTORS
Size	Number	Rev	
A3	FIG.6	0	
Date	14 FEB 94	Drawn by R.FULLOVE	
Filename	SEGMOD2.S01	Sheet 2 of 3	

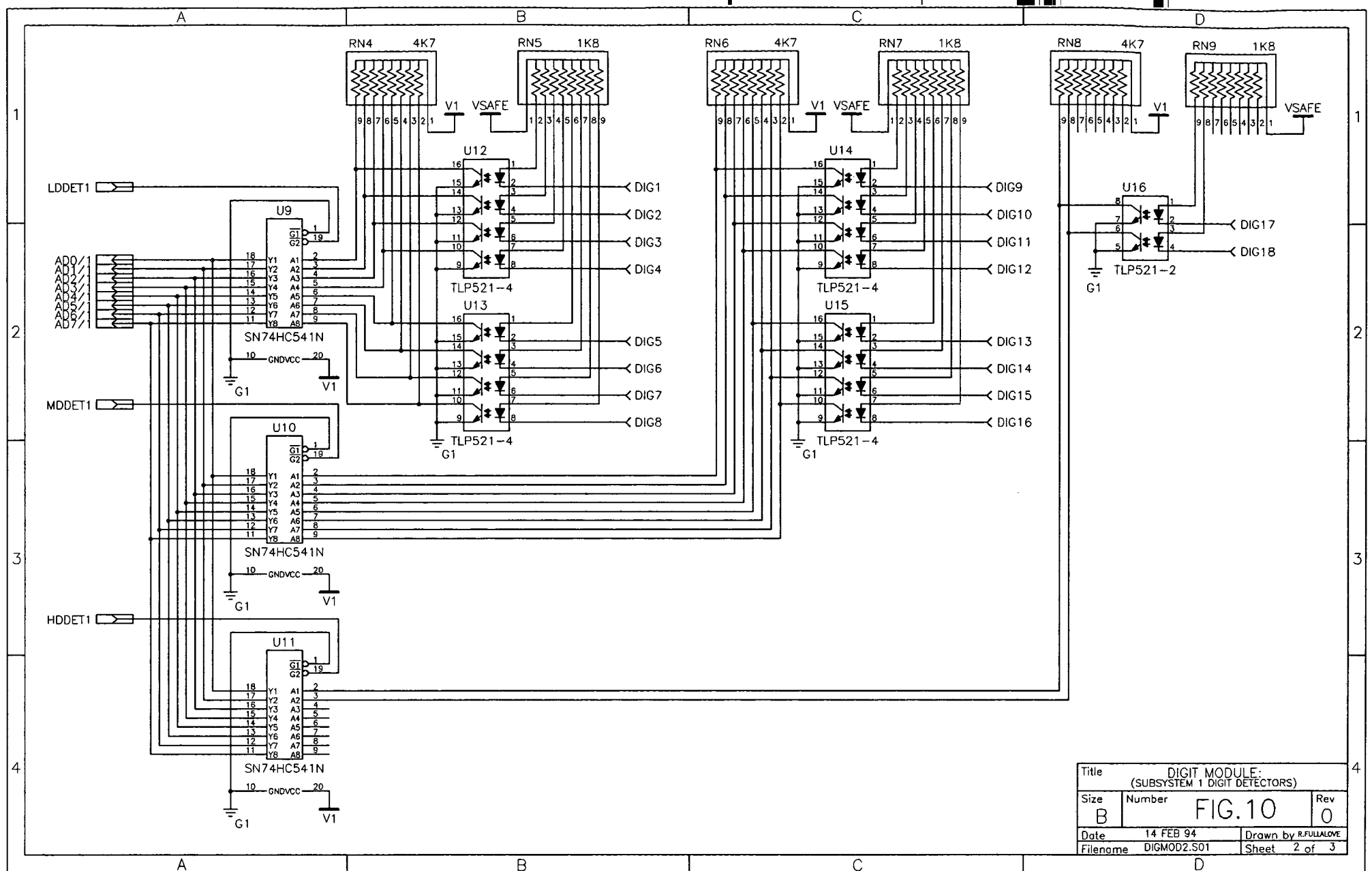




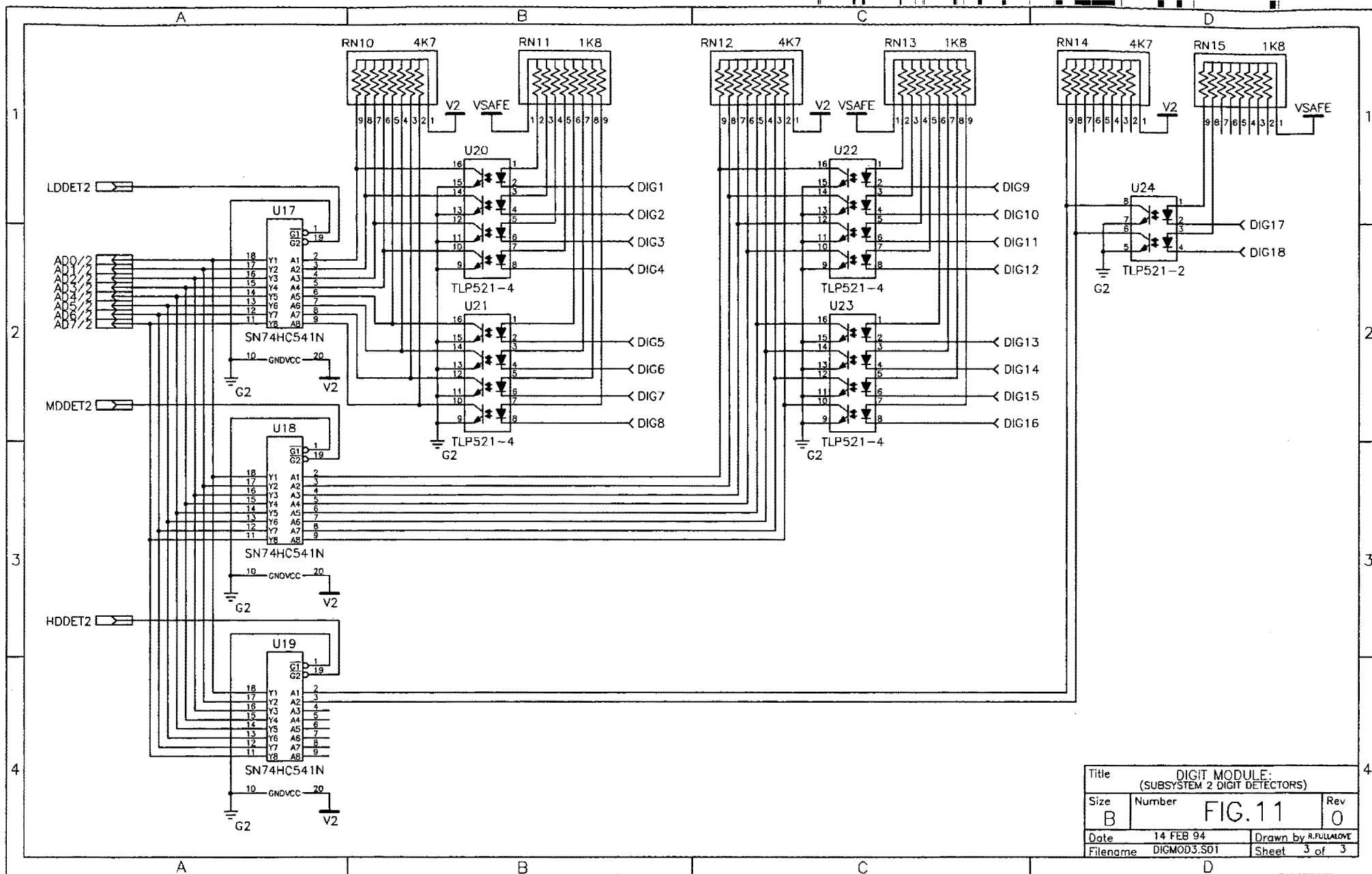
Title DIGIT MODULE: (OPERATING PRINCIPLE)		
Size A4	Number FIG.8	Rev 0
Date 14 FEB 94	Drawn by R.FULLALOVE	
Filename DIGMOD.S01	Sheet 1 of 1	



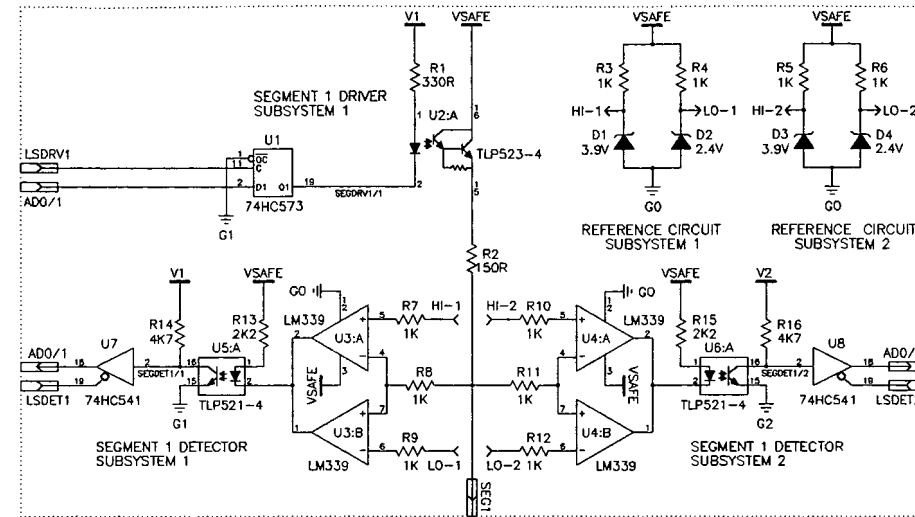
Title			DIGIT MODULE: (SUBSYSTEM 2 DIGIT DRIVERS)	
Size	Number	FIG.9		Rev
B				0
Date	14 FEB 94	Drawn by R.FULLALOVE		
Filename	DIGMOD1.S01	Sheet 1 of 3		



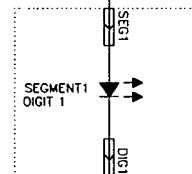
Title			DIGIT MODULE: (SUBSYSTEM 1 DIGIT DETECTORS)	
Size	Number	FIG.10		Rev
B				0
Date	14 FEB 94	Drawn by R.FULLALOVE		
Filename	DIGMOD2.S01	Sheet 2 of 3		



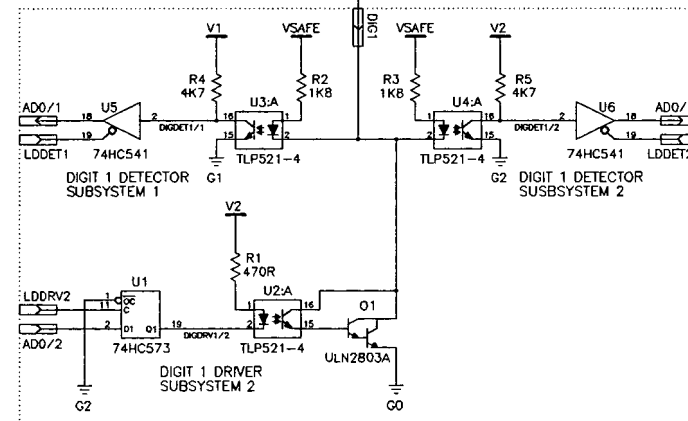
Title			DIGIT MODULE: (SUBSYSTEM 2 DIGIT DETECTORS)
Size	Number	Rev	
B		FIG.11	
Date	14 FEB 94	Drawn by R.FULLALOVE	
Filename	DIGMOD3.S01	Sheet 3 of 3	



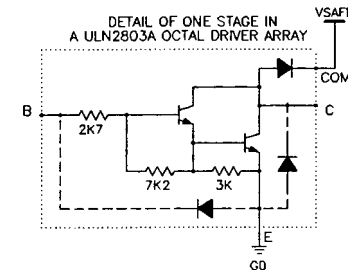
SEGMENT MODULE (SEGMENT 1)



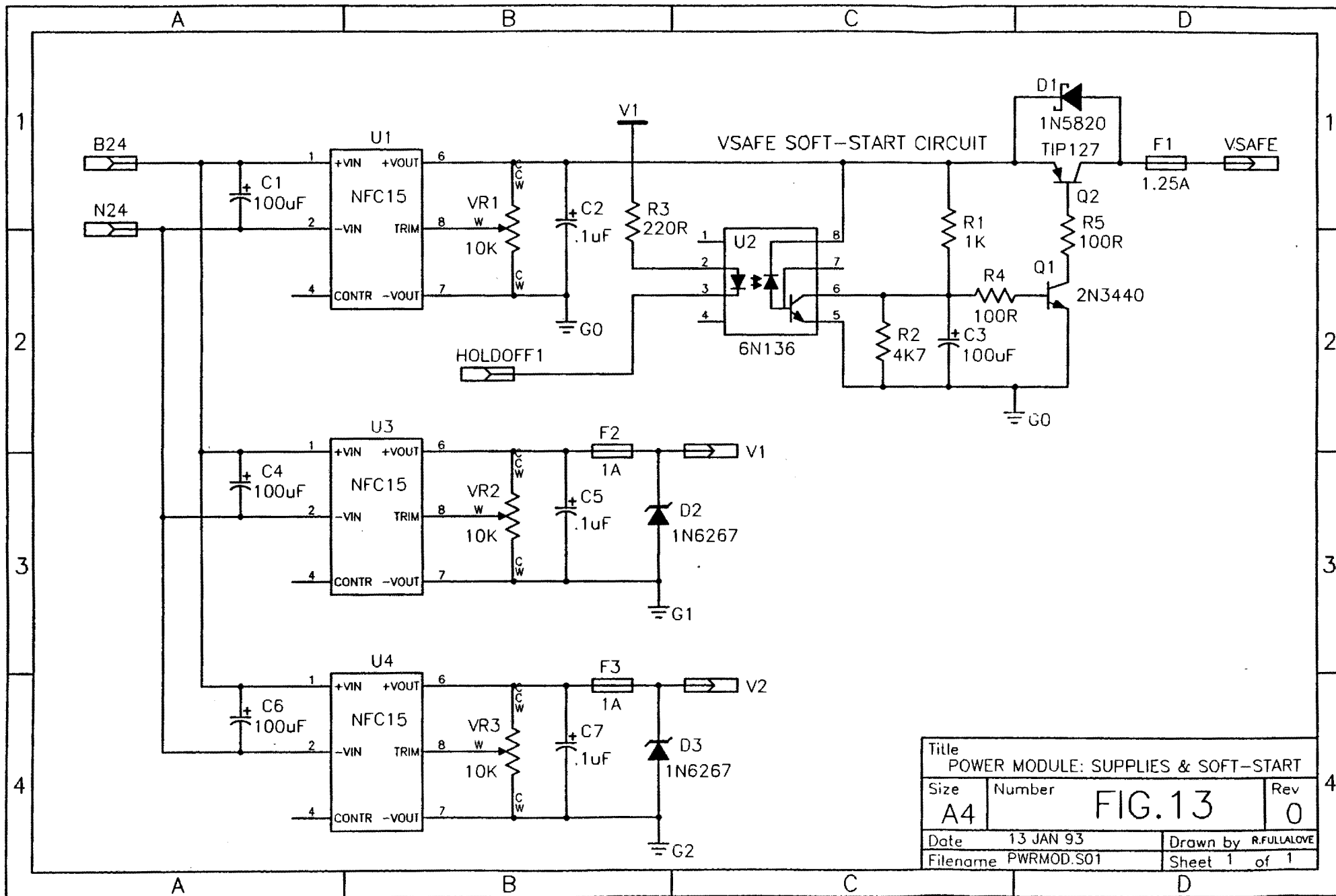
DISPLAY MODULE (SEGMENT 1 OF DIGIT 1)



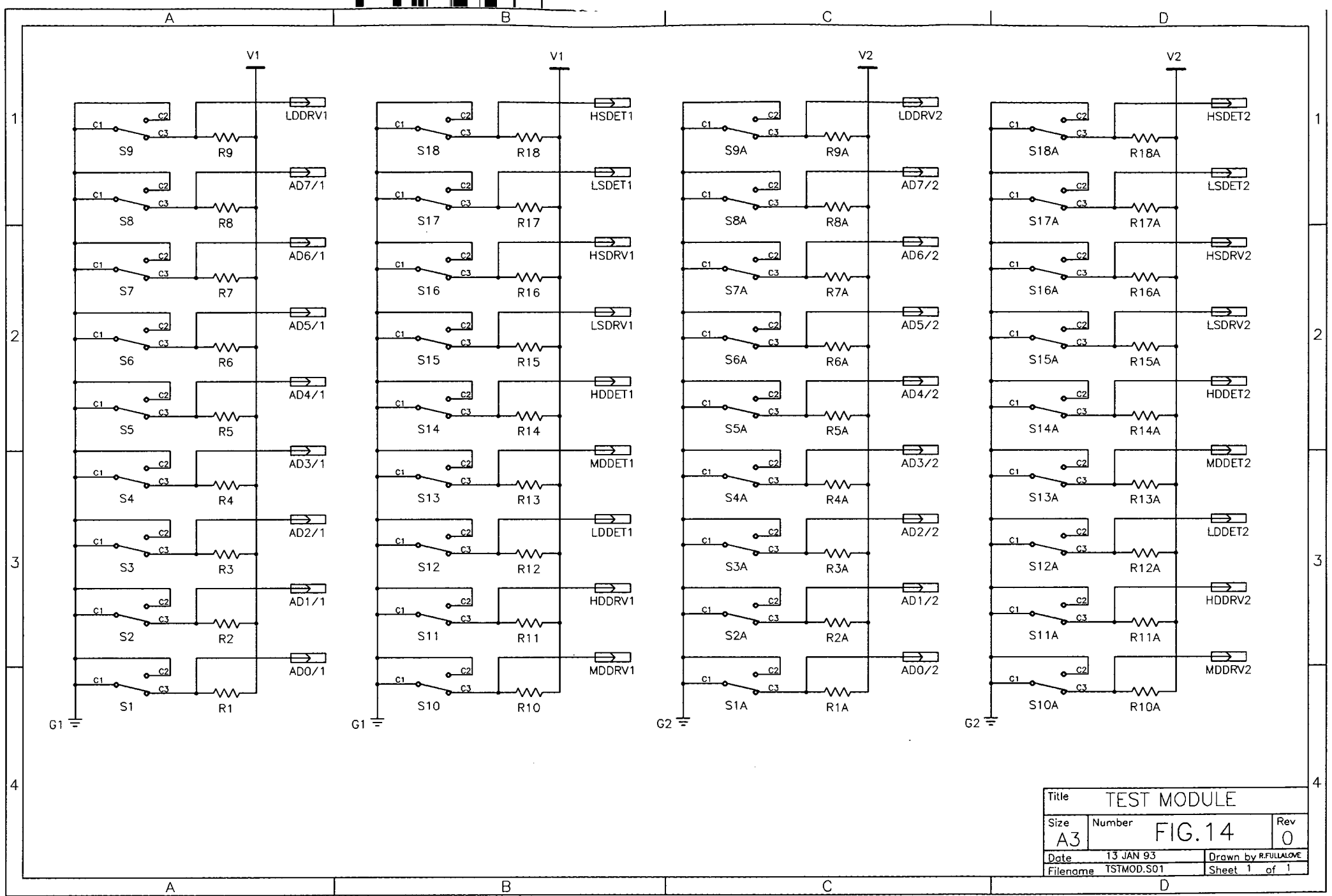
DIGIT MODULE (DIGIT 1)



Title			
DISPLAY CIRCUIT: (OPERATING PRINCIPLE; SEGMENT 1 OF DIGIT 1)			
Size	Number	Rev	
C	FIG.12	0	
Date	14 FEB 94	Drawn by R.FULLALOVE	
Filename	DISPLAY.S01	Sheet 1 of 1	



Title POWER MODULE: SUPPLIES & SOFT-START		
Size A4	Number FIG.13	Rev 0
Date 13 JAN 93	Drawn by R.FULLALOVE	
Filename PWRMOD.S01	Sheet 1 of 1	



Title TEST MODULE		
Size A3	Number FIG.14	Rev 0
Date 13 JAN 93	Drawn by R.FULLALOVE	
Filename TSTM0D.S01	Sheet 1 of 1	

APPENDIX B: Failure Modes, Effects and Criticality Analysis

System-Level Failure Modes, Effects and Criticality Analysis (FMECA)

MODULE:	Power Module
INDENTURE:	Level 1 (System)
REF.DWG:	Appendix A, Fig.2
MISSION:	Provide isolated power to both subsystems and common display circuitry.

DATE: 24 May 1994
SHEET: 2
COMPILED: R.Fullalove

Function	Failure Modes	Mission Phase	System Failure Effects	Failure Detection Method	Compensation Provisions	Severity Class	Remarks
Power supply V1	5 Volt supply lost	Train en route & information stored in display.	Subsystem 1 of the 2-out-of-2 comparative system loses power	Data discrepancy detected by other subsystem.	System shutdown	II	Refer to [11] in the reference list.
Power supply V2	5 Volt supply lost		Subsystem 2 of the 2-out-of-2 comparative system loses power	Data discrepancy detected by other subsystem.	System shutdown	II	
Power supply V0	12 Volt supply lost		Common display circuitry loses power, resulting in blank display. Prior to shutdown, subsystems 1 and 2 are still operational in order to detect this failure, and remain operational after this.	Data discrepancy detected by both subsystems in the Control Module, via feedback paths from Display Module.	System shutdown	II	
Soft-Start Circuit	Disabled/faulty	System start-up	Safety fuse blows prematurely before system initialization is completed.	Fuse-Blow safety circuit operates.	System shutdown	II	
Safety Fuse	Remains intact when fuse-blow attempted	Train en route, token displayed	Ref [11]	Ref [11]	Ref [11]	Ref [11]	

MODULE: Control Module
INDENTURE: Level 1 (System)
REF.DWG: Appendix A, Fig.2
MISSION: Control Display, Receive Feedback

DATE: 24 May 1984
SHEET: 2
COMPILED: R.Fullalove

Function	Failure Modes	Mission Phase	System Failure Effects	Failure Detection Method	Compensation Provisions	Severity Class	Remarks
Display Enable Bus (10 lines per subsystem) Either: a) Latches 8 segments at a time. b) Latches 8 digits at a time. c) Enables 8 segment feedback buffers at a time. d) Enables 8 digit f/b buffers at a time.	Display Enable Bus control line s-a-0.	Train en route & information stored in display	Relevant segment (or digit) drive latch (or feedback buffer) permanently enabled. Either: a) 8 segments retain last state b) 8 digits retain last state. c) 8 segment feedback lines retain last state permanently. d) 8 digit feedback lines retain last state permanently.	Feedback and comparison of data in software.	System shutdown	II	Reference [11] is the FMECA performed by Mr. M.B. Schronen for the Communications Module in the FSDTS designed by him. Since the Control Module of the FSDS will be a slightly modified version of the Comms Module, no detailed FMECA is required here.
	Display Enable bus control line s-a-1.		Relevant segment/digit drive latch/feedback buffer permanently disabled. Either: a) 8 segments follow changing data on Display Data Bus. b) 8 digits follow changing data on Display data Bus. c) 8 segment feedback lines disabled indefinitely. d) 8 digit feedback lines permanently disabled.	Feedback and comparison of data in software.	System shutdown	II	
Display Data Bus (8 lines per subsystem) Either: a) Selects a segment. b) Selects a digit. c) Feeds back segment data. d) Feeds back digit data.	Display Data Bus line s-a-0.		Corresponding segment/digit permanently lit. Either: a) 1 segment (per group of 8 segments per latch), is lit permanently. b) 1 digit (per group of 8 digits per latch), is permanently lit c) 1 segment feedback appears permanently selected. d) 1 digit feedback appears permanently selected	Feedback and comparison of data in software.	System shutdown	II	
	Display Data Bus line s-a-1.		Corresponding segment/digit permanently disabled. Either: a) 1 segment is off permanently b) 1 digit is off permanently. c) 1 segment feedback appears to be permanently selected. d) 1 digit feedback appears to be permanently selected.	Feedback and comparison of data in software.	System shutdown	II	
Subsystem Data Xchg (Exchanges subsystem data for comparison in a 2-out-of-2 comparative architecture).	Reference [11]		Reference [11]	Reference [11]	Reference [11]	II	
Fuse-Blow operation (Blows fuse in the event of any detected system failure).	Reference [11]		Reference [11]	Reference [11]	Reference [11]	II	
Serial Data reception (Receives token data in serial format with error correcting codes, and verifies validity).	Reference [11]		Reference [11]	Reference [11]	Reference [11]	II	

MODULE: Segment Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.4
 MISSION: Segment Select, Detect, & Feedback

F.M.E.C.A.

DATE: 23 December 1992
 SHEET: 1
 COMPILED: R.Fullalove

Id. No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
R1	Resistor Network	Current limit for U2 input LED	Open circuit Intermittent Resistance increase	Train en route, information displayed to driver.	U2 LED off always • sometimes U2 LED dims eventually	Relevant segment off always • sometimes eventually	Incorrect character displayed • sometimes eventually	Redundant F/B circuit for segs. •	System Shutdown •	II II III	Increasing H has no effect on U5, as long as R low enough to ensure pull-up for output of U5, as well as source current to the SEGDET line.
R2	Resistor	Current limit for relevant segment LED	Open circuit Intermittent Resistance increase		No current to relevant segment LED • sometimes Reduced display segment LED current	Relevant segment LED does not light • sometimes Reduced display segment brightness	Erroneous character displayed • sometimes None visible for under 50% reduction	Redundant F/B & comparison of segment LEDs •	• •	II II III	
R3 (R5)	Resistor	Current limit for D1 (D3) Zener	Open circuit Intermittent Resistance increase	Train en route, information displayed to driver.	Zener D1 cathode floats • sometimes eventually	High ref. limit for window detector floats • sometimes eventually	o/cct detection unpredictable • sometimes eventually	Periodic self-test of window detectors, using dummy test digits •	System Shutdown •	II II III	
R4 (R6)	Resistor	Current limit for Zener D2 (D4)	Open circuit Intermittent Resistance increase		Zener D2 cathode floats always • sometimes eventually	Low ref. limit for window detect floats always • sometimes eventually	Unpredictable s/cct detection always • sometimes eventually	• • •	• • •	II II III	Without periodic testing of the window detectors, this failure would go unnoticed, since the redundant sub-system continues to detect segments correctly. Input resistance for comparators is very high, thus not affected much by increasing input resistance
R7 (R10)	Resistor Network	Input resistance to window detect U3 (U4), high limit reference	Open circuit Intermittent Resistance increase		(+)I/p of U3:A floats always • sometimes eventually	High ref. limit floats always • sometimes eventually	Unpredictable o/cct detection • sometimes eventually	• • •	• • •	II II III	
R8 (R11)	Resistor Network	Input resistance to U3 (U4) for segment LED anode voltage	Open circuit Intermittent Resistance increase		Measuring I/p of U3 floats always • sometimes eventually	False triggering of hi/lo limits possible, always • sometimes eventually	System shutdown always • sometimes eventually	• • •	• • •	II II III	
R9 (R12)	Resistor Network	Input resistance to window detect U3 (U4), low limit reference	Open circuit Intermittent Resistance increase	Train en route, information displayed to driver.	(-)input of U3:B floats always • sometimes eventually	Low ref. limit floats always • sometimes eventually	Unpredictable s/cct detection always • sometimes eventually	Periodic self-test of window detectors using dummy test digits •	System Shutdown •	II II III	Input resistance for comparators is very high, thus not affected by increasing input resistance
R13 (R15)	Resistor Network	Current limit for U5 (U6) input LED	Open circuit Intermittent Resistance increase		U5 LED off, always • sometimes eventually	SEGDET line low, always • sometimes eventually	No segment F/B, always • sometimes eventually	• • •	• • •	II II III	
R14 (R16)	Resistor Network	Pull-up resistor for U5 (U6) output SEGDET Line	Open circuit Intermittent Resistance increase		U5 collector floats when U5 is off, always • sometimes None	SEGDET line floats when U5 is off, always • sometimes None	Unpredictable segment F/B always • sometimes None	• • •	• • •	II II IV	

F.M.E.C.A.

MODULE: Segment Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.4
 MISSION: Segment Select, Detect & Feedback

DATE: 23 December 1992
 SHEET: 2
 COMPILED: R.Fullalove

Id. No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
D1 (D3)	Zener Diode	High reference limit for segment voltage	Open circuit	Train en route, information displayed to driver.	Zener D1 cathode goes high (+5V)	hi-ref. limit rises to +5V	Possible masking of display LED o/cct	Periodic test of window detectors	System Shutdown	II	Failure detected in one display refresh cycle
			Intermittent		" sometimes	" sometimes	" sometimes	"	"	II	
			Short circuit		D1 cathode goes low (0V)	hi-ref. limit drops to 0V, below V _{led}	Detected by window detector	"	"	II	Failure detected immediately
			Leakage current rise		D1 cathode volts decreases	hi-ref. limit decreases	"	"	"	II	
			Series resistance rise		D1 cathode volts rise	hi-ref. limit increases	Possible masking of LED voltage increase	"	"	II	
			Zener voltage rise (up to 5%)		"	"	"	"	"	II	
			Zener voltage decrease		D1 cathode volts decreases	hi-ref. limit decreases	Detected by window detector	"	"	II	
D2 (D4)	Zener Diode	Low reference limit for segment voltage	Open circuit	Train en route, information displayed to driver.	Zener D2 cathode goes high (+5V)	lo-ref. limit rises to +5V	Detected by window detector	Failure detected by the window detector itself	System Shutdown	II	Failure detected in one display refresh cycle
			Intermittent		" sometimes	" sometimes	" sometimes	"	"	II	
			Short circuit		D2 cathode goes low (0V)	lo-ref. limit drops to 0V, well below V _{led}	Possible masking of display LED s/cct	Periodic test of window detector	"	II	Failure detected immediately
			Leakage current rise		D2 cathode volts decreases	lo-ref. limit decreases	eventually	"	"	II	
			Series resistance rise		D2 cathode volts increases	lo-ref. limit increases	Detected by window detector eventually	Failure detected by the window detector itself	"	II	
			Zener voltage rise (up to 5%)		" eventually	" eventually	eventually	"	"	II	
			Zener voltage decrease		D2 cathode volts decreases	lo-ref. limit decreases	Possible masking of LED voltage decrease	Periodic test of window detector	"	II	
U1	Octal tri-state latches. (74HC573)	Latches segment data to the display from a common 8-bit bi-directional bus connected to a port on the micro-controller in the Control Module	Data input line stuck at 0 or 1 (D1 to D8)	Train en route, information displayed to driver.	Relevant data output line low or high always	Relevant seg. selected or deselected permanently	Erroneous char. displayed always	Redundant Micro-Controller channel with F/B and comparator S/W.	System Shutdown	II	No undetectable failures apparent
			Data output line stuck at 0 or 1 (Q1 to Q8)		Relevant data output line low or high always	Relevant seg. selected or deselected permanently	" always			II	
			Latch enable pin (G), stuck at 0.		Relevant latch deselected permanently	Relevant 8 segs de-selected permanently	" always			II	
			Latch enable pin (G), stuck at 1.		Relevant latch selected always	Relevant 8 segs selected always	" always			II	
			Tristate output enable, /(OE), stuck at 1		Relevant latch's outputs disabled always	Relevant 8 seg lines in hi-Z state always	" always			II	
			Tristate output enable, /(OE), stuck at 0		Relevant latch's outputs enabled always	Relevant 8 seg lines enabled always	None			IV	

F.M.E.C.A.

MODULE: Segment Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.4
 MISSION: Segment Select, Detect & Feedback

DATE: 23 December 1992
 SHEET: 3
 COMPILED: R.Fullalove

Id. No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
U2	Darlington Opto-coupler	Selects the appropriate seg. LED, while giving electrical isolation between the control channel & display circuit	Open circuit (LED) Intermittent (LED) Short circuit (LED) I-leak increase (LED) R-series rises (LED) Light output falls (LED) Open circuit (BJT) Intermittent (BJT) Short circuit (BJT) I-leak increase (BJT) Energy sensitivity (BJT) decreases	Train en route, information displayed to driver.	U2 inactive, always. • sometimes • always • eventually • eventually • eventually U2 collector high, always • sometimes U2 Vce very low, always • eventually U2 collector high, eventually	Selected segment LED off, always. • sometimes • always • eventually • eventually • always • sometimes Segment selected, always • eventually Segment not selected, eventually.	Incorrect char. displayed, always • sometimes • always • eventually • always • sometimes always • eventually	Redundant F/B & comparator logic.	System Shutdown	II II II III III II II III III	No undetectable failures apparent
U3 (U4)	LM339 Quad Comparator	Implemented as a window detector to check that the voltage across the display LED is within certain limits, thus displaying in a fault-free manner	U3:A (+)input stuck at 0V U3:A (+)input stuck at +5V U3:A (-)input and U3:B (+) input stuck at 0V U3:A (-)input and U3:B (+) input stuck at +5V U3:A (+) and (-) inputs bridged U3:A or U3:B output stuck at 0V. U3:A output stuck at +5V U3:B (-)input stuck at 0V U3:B (-)input stuck at +5V U3:B (+) and (-) inputs bridged U3:B output stuck at +5V	Train en route, information displayed to driver.	(-)I/p > (+)I/p thus, o/p low always (-)I/p < (+)I/p thus, o/p high always (-)I/p < (+)I/p thus, U3:A o/p high; U3:B (+)I/p < (-)I/p, thus U3:B o/p low always. (-)I/p > (+)I/p thus, U3:A o/p low; U3:B (+)I/p > (-)I/p, thus U3:B o/p high always. (+)I/p = (-)I/p thus U3:A o/p low always. Both U3:A and U3:B o/p low permanently. U3:A o/p high provided U3:B o/p not low. (+)I/p > (-)I/p thus, U3:B o/p high always. (-)I/p > (+)I/p thus, U3:B o/p low always. (+)I/p = (-)I/p thus U3:B o/p low always. U3:B o/p high provided U3:A o/p not low.	SEGDET line low always Loss of high window detect ref.limit. SEGDET line low always. SEGDET line low always. SEGDET line low always. SEGDET line low always. Loss of high window detect ref.limit. Loss of low window detect ref.limit. SEGDET line low always. SEGDET line low always. Loss of low window detect ref.limit.	No segment detection & F/B Possible masking of display LED o/cct No segment detection and F/B No segment detection and F/B No segment detection and F/B. No segment detection and F/B. Possible masking of display LED o/cct Possible masking of display LED s/cct No segment detection and F/B. No segment detection and F/B. Possible masking of display LED s/cct	Redundant segment detector using a window detector with F/B Periodic self-test of the window detectors	System Shutdown	II II II II II II II II II II II	Due to its multiple component nature, this device has been evaluated at a functional rather than component level. Only two of the four comparators in the package is evaluated. Easy to detect with redundant circuit, therefore low severity Periodic tests on window detectors prevent masking of display LED failures s/cct is unlikely failure mode in LEDs (Hewlett Packard)

F.M.E.C.A.

MODULE: Segment Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.4
 MISSION: Segment Select, Detect & Feedback

DATE: 23 December 1992
 SHEET: 4
 COMPILED: R.Fullaove

Id. No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
U5 (U8)	Optical Isolator	Detects correct operation of segment. Also provides electric isolation between the display cct. and the control channel	Open circuit (LED)	Train en route, information displayed to driver.	U5 inactive, always.	SEGDET line high, always	No segment F/B, always	Comparator logic in Software compares SEGDRV and SEGDET lines.	System Shutdown	II	No undetectable failures apparent
			Intermittent (LED)		▪ sometimes	▪ sometimes	▪ sometimes			II	
			Short circuit (LED)		▪ always	▪ always	▪ always			II	
			I-leak increase (LED)		▪ eventually	▪ eventually	▪ eventually			III	
			R-series rises (LED)		▪ eventually	▪ eventually	▪ eventually			III	
			Light output falls (LED)		▪ eventually	▪ eventually	▪ eventually			III	
			Open circuit (BJT)		U5 collector high, always	▪ always	▪ always			II	
			Intermittent (BJT)		▪ sometimes	▪ sometimes	▪ sometimes			II	
			Short circuit (BJT)		U5 collector low, always	SEGDET line low, always	No segment F/B, always			II	
			I-leak increase (BJT)		▪ eventually	▪ eventually	▪ eventually			III	
			Energy sensitivity (BJT) decreases		U5 collector high, eventually	SEGDET line stuck high, eventually	▪ eventually			III	
U7 (U8)	Octal tri-state buffers (74HC541)	Routes seg. F/B from the display to a common 8-bit bi-directional bus connected to both subsystems in the Control Module	Data input line stuck at 0 or 1 (A1 to A8)	Train en route, information displayed to driver.	Relevant data output line low or high always	Relevant seg. feedback low or high permanently	Relevant seg. F/B disabled always	2-out-of-2 Control Module with F/B and comparator S/W.	System Shutdown	II	No undetectable failures apparent
			Data output line stuck at 0 or 1 (Y1 to Y8)		Relevant data output line low or high always	Relevant seg. feedback low or high permanently	Relevant seg. F/B disabled always			II	
			Tristate output enable, /(G1), stuck at 1		Relevant buffers outputs disabled always	Relevant 8 seg. F/B lines in hi-Z state always	Relevant 8 seg. F/B lines disabled always			II	
			Tristate output enable, /(G1), stuck at 0		Relevant buffers outputs enabled always	Relevant 8 seg. F/B lines enabled always	Relevant 8 seg. F/B lines enabled always			II	

F.M.E.C.A

MODULE: Digit Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.8
 MISSION: Digit Select, Detect & Feedback

DATE: 23 December 1992
 SHEET: 1
 COMPILED: R.Fullalove

Id. No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
R1	Resistor Network	Current limit for U2 LED	Open circuit Intermittent Resistance increase	Train en route, information displayed to driver.	U2 LED off, always • sometimes • eventually	Relevant digit select off always • sometimes • eventually	Missing digit in display always • sometimes • eventually	Digit F/B & comparison • • •	System Shutdown	II II III	No undetectable failures apparent
R2	Resistor Network	Pull-up resistor for U2 output	Open circuit Intermittent Resistance increase	Train en route, information displayed to driver.	Digit select Q1 off, always • sometimes • eventually	Relevant digit select off always • sometimes • eventually	Missing digit in display always • sometimes • eventually	Digit F/B & comparison • • •	System Shutdown	II II III	No undetectable failures apparent
R3 (R4)	Resistor Network	Current limit for U3 (U4) LED	Open circuit Intermittent Resistance increase		U3 LED off, always • sometimes • eventually	DIGDET line high, always • sometimes • eventually	No digit F/B, always • sometimes • eventually	Digit F/B & comparison		II II III	
R5 (R6)	Resistor Network	Pull-up resistor for U3 (U4) output. (DIGDET Line)	Open circuit Intermittent Resistance increase	Train en route, information displayed to driver.	U3 collector floats when inactive • sometimes • No effect	DIGDET line floats when U3 inactive • sometimes • No effect	Digit F/B unpredictable • sometimes • No effect	Redundant F/B circuit for digits	System Shutdown	II II IV	Increasing R has no effect, as long as R low enough to ensure pull-up for U3 o/p, as well as source current to the DIGDET line.
U1	Octal tri-state latches (74HC573)	Latches digit data to display via a common 8-bit bi-directional data bus from Control Module	Data input line stuck at 0 or 1 (D1 to D8) Data output line stuck at 0 or 1 (Q1 to Q8) Latch enable pin (G), s-a-0. Latch enable pin (G), stuck at 1. Tristate output enable, /!(OE), stuck at 1 Tristate output enable, /!(OE), stuck at 0	Train en route, information displayed to driver.	Relevant data output line low/high always Relevant data output line low/high always Relevant latch deselected permanently Relevant latch selected always Relevant latch's outputs disabled always Relevant latch's outputs enabled always	Relevant digit selected or deselected permanently Relevant digit selected or deselected permanently Relevant 8 digits de-selected permanently Relevant 8 digits selected always Relevant 8 digit lines in hi-Z state always Relevant 8 digit lines enabled always	Relevant digit lit or unlit always Relevant digit lit or unlit always Relevant 8 digits unlit always Relevant 8 digits lit always Relevant 8 digits unlit always None	2-out-of-2 Control Module with F/B and comparator S/W.	System Shutdown	II II II II IV	No undetectable failures apparent
U2	Optical Isolator	Drives Digit Select switch, Q1, while giving electrical isolation between the control channel & display circuit	Open circuit (LED) Intermittent (LED) Short circuit (LED) I-leak increase (LED) R-series rises (LED) Light output falls (LED) Open circuit (BJT) Intermittent (BJT) Short circuit (BJT) I-leak increase (BJT) Energy sensitivity (BJT) decreases	Train en route, information displayed to driver.	U2 inactive, always. • sometimes • always • eventually • eventually • eventually U2 collector high, always • sometimes U2 collector low, always • eventually U2 collector high, eventually	Q1 stuck on, always • sometimes • always • eventually • eventually • always • sometimes Q1 stuck off, always • eventually Q1 stuck on, eventually	Digit selected, always • sometimes • always • eventually • always • sometimes Digit de-selected, always • eventually Digit selected, eventually	Comparison Logic in Software	System Shutdown	II II II III III III II II III III	No undetectable failures apparent

MODULE: Digit Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.8
 MISSION: Digit Select, Detect & Feedback

F.M.E.C.A.

DATE: 23 December 1982
 SHEET: 2
 COMPILED: R.Fullalove

Id. No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
U3 (U4)	Opto-coupler	Detects correct operation of digit select switch, Q1. Provides isolation between the display cct. and the controller sub-system	Open circuit (LED) Intermittent (LED) Short circuit (LED) I-leak increase (LED) R-series rises (LED) Light output falls (LED) Open circuit (BJT) Intermittent (BJT) Short circuit (BJT) I-leak increase (BJT) Energy sensitivity (BJT) decreases	Train en route, information displayed to driver.	U3 inactive, always. " sometimes " always " eventually " eventually " eventually " eventually U3 collector high, always " sometimes U3 collector low, always " eventually U3 collector high, eventually	DIGDET line high, always " sometimes " always " eventually " eventually " eventually " always " sometimes DIGDET line low, always " eventually DIGDET line stuck high, eventually	No digit F/B always " sometimes " always " eventually " eventually " eventually " always " sometimes No digit F/B, always " eventually "	2-out-of-2 Control Module with F/B and comparator S/W.	System Shutdown	II II II III III III II II II III III	No undetectable failures apparent
U5 (U6)	Octal tri-state buffers (74HC541)	Routes digit F/B from the display to a common 8-bit bi-directional bus connected to both subsystems in the Control Module	Data input line stuck at 0 or 1 (A1 to A8) Data output line stuck at 0 or 1 (Y1 to Y8) Tristate output enable, / (G1), stuck at 1 Tristate output enable, / (G1), stuck at 0	Train en route, information displayed to driver.	Relevant data output line low or high always Relevant data output line low or high always Relevant buffers outputs disabled always Relevant buffers outputs enabled always	Relevant digit feedback low or high permanently Relevant digit feedback low or high permanently Relevant 8 digit F/B lines in hi-Z state always Relevant 8 digit F/B lines enabled always	Relevant digit F/B disabled always Relevant digit F/B disabled always Relevant 8 digit F/B lines disabled always Relevant 8 digit F/B lines enabled always	2-out-of-2 Control Module with F/B and comparator S/W.	System Shutdown	II II II II	No undetectable failures apparent
Q1	NPN Darling. Switch	Selects relevant digit from a 16-segment alphanumeric, common-cath. LED display of 16 digits	Base o/cct Collector o/cct Emitter o/cct B intermittent C intermittent E intermittent B-E s/cct B-C s/cct C-E s/cct B-E s/cct, C o/cct B-C s/cct, E o/cct C-E s/cct, B o/cct Gain Increase Gain decrease	Train en route, information displayed to driver.	No collector current, always " always " always " sometimes " sometimes " sometimes Collector current unpredictable Collector stuck at 0.7V always Collector stuck at 0V permanently Collector current=0 Collector current=0 Collector stuck at 0V permanently Collector current rises Collector current falls	No digit selected, always " always " always " sometimes " sometimes " sometimes Q1 on or off status unpredictable Q1 stuck on permanently (Vce=0.7V) Q1 stuck on permanently (Vce=0V) Q1 off permanently Q1 off permanently Q1 stuck on permanently (Vce=0V) Q1 may go s/cct, eventually Q1 may go o/cct eventually	Missing digit in display " always " always " sometimes " sometimes " sometimes Digit could be on or off, always Digit displayed, permanently Digit displayed, permanently Digit not displayed, permanently Digit not displayed, permanently Digit displayed, permanently Digit stuck on eventually Digit may grow dim eventually	Redundant digit detection, feedback, and comparison with controls sent.	System Shutdown	II II II II II II II II II II II III III	No undetectable failures apparent

MODULE: Display Module
 INDENTURE: Level 2 (Modular)
 REF.DWG: Appendix A, Fig.3
 MISSION: Display Message, Test Window Detectors

F.M.E.A.

DATE: 23 December 1992
 SHEET: 1
 COMPILED: R.Fullalove

Id.No.	Part Name	Function	Failure Modes & Causes	Mission Phase / Operational Mode	Failure Effect			Failure Detection Method	Compensation Provisions	Severity Class	Remarks
					Local	Modular	System				
U1, U2	Display LEDs	16-segment alphanumeric, comm. cathode LED display of 16 characters (HDSP-6508)	Open circuit	Train en route, Information displayed to driver.	Segment 1 LED unlit always.	Segment unlit, always	Erroneous character shown always	Redundant segment detector using a window detector with F/B	System Shutdown	II	One segment only is analyzed here.- The same applies for all other segments
			Intermittent		• sometimes	• sometimes	• sometimes			II	
			Short circuit		• always	• always	• always			II	Manufacturers regard a s/cct in a LED as highly unlikely
			I-leak increase		• eventually	• eventually	• eventually			III	
			R-series rises		• eventually	• eventually	• eventually			III	
			Light output falls		Segment 1 LED grows dimmer gradually.	Segment 1 gets dimmer over time	Erroneous character may appear to be shown over a long time period			III	This is a gradual degradation, & will not affect safety if display replaced before 10 years of use

FAILURE SEVERITY vs PROBABILITY

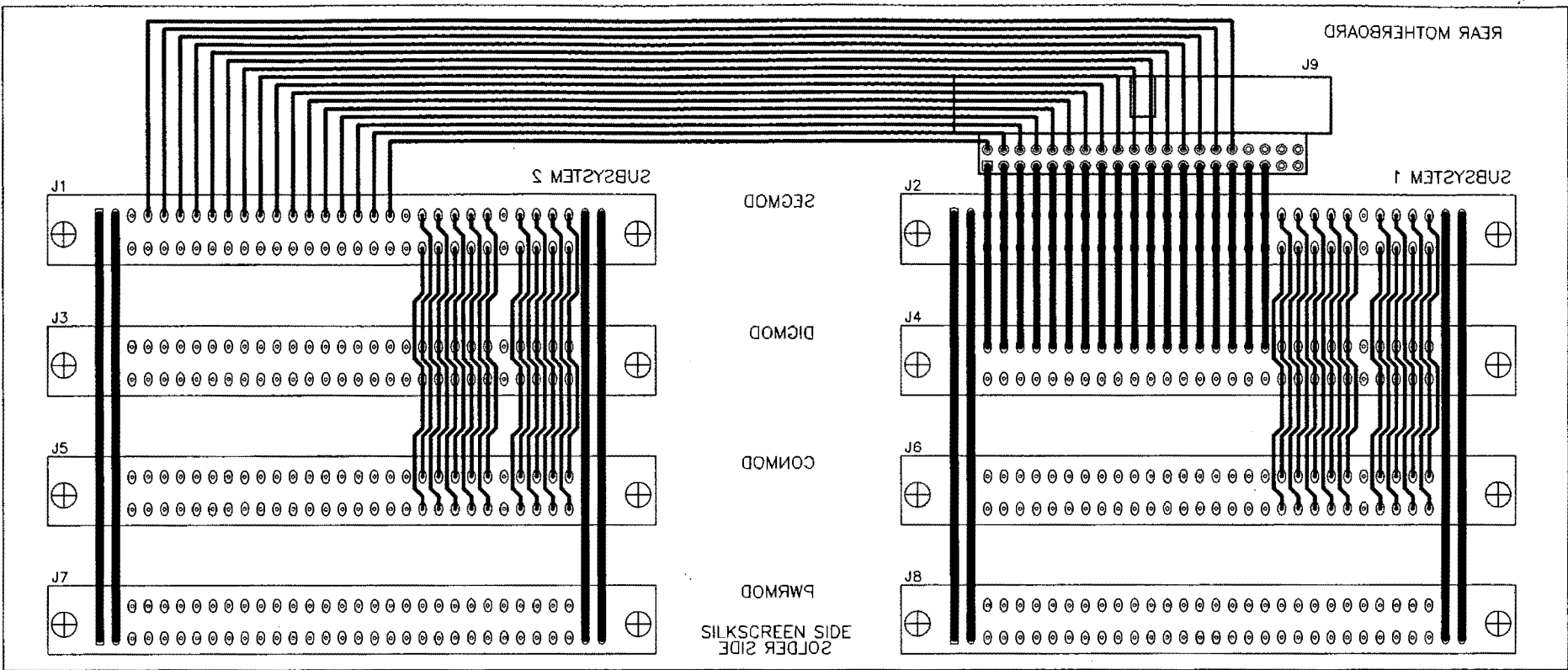
SEGMENT MODULE					
Probability of Failure P(F)	High		U2, U5, U8	U2, U5, U8	
	Medium				
	Low			U3,U4	
	V.Low	R16 U1	R1 - R13, R15	R1 - R16 D1 - D4 U1, U7, U8	
		(IV) No Failure, No Maintenance	(III) No Failure, Maintenance	(II) Failure detected Safe shutdown	(I) Failure masked Unsafe situation
Severity Level					

DISPLAY MODULE					
Probability of Failure P(F)	High				
	Medium				
	Low		U1, U2	U1, U2	
	V.Low				
		(IV) No Failure, No Maintenance	(III) No Failure, Maintenance	(II) Failure detected Safe shutdown	(I) Failure masked Unsafe situation
Severity Level					

SHADING = UNSAFE OPERATION

DIGIT MODULE					
Probability of Failure P(F)	High		U2, U3, U4	U2, U3, U4	
	Medium				
	Low				
	V.Low	R5, R6 U1	R1 - R4, R7 Q1	R1 - R6 Q1 U1, U5, U8	
		(IV) No Failure, No Maintenance	(III) No Failure, Maintenance	(II) Failure detected Safe shutdown	(I) Failure masked Unsafe situation
Severity Level					

APPENDIX C: Printed Circuit Board Artworks



REAR MOTHERBOARD

[illegible]

SEGMOD

DIGMOD

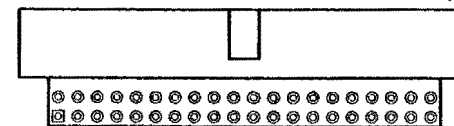
CONMOD

PWRMOD

COMPONENT SIDE

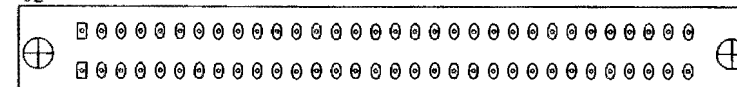
REAR MOTHERBOARD

J9



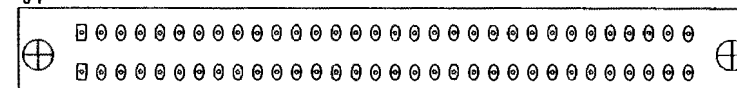
SEGMOD

J2



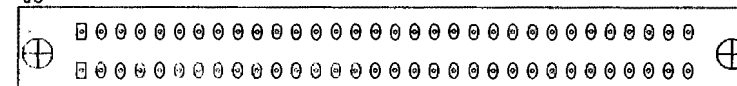
DIGMOD

J4



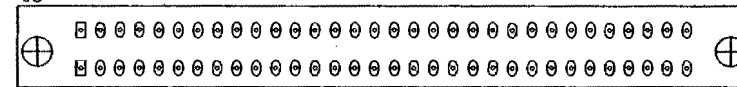
CONMOD

J6



PWRMOD

J8

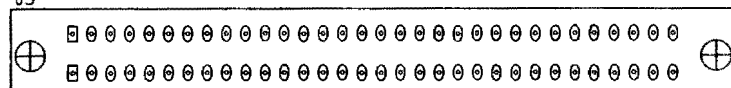


SILKSCREEN SIDE
COMPONENT SIDE

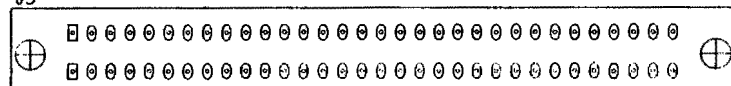
J1



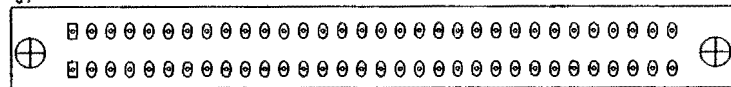
J3

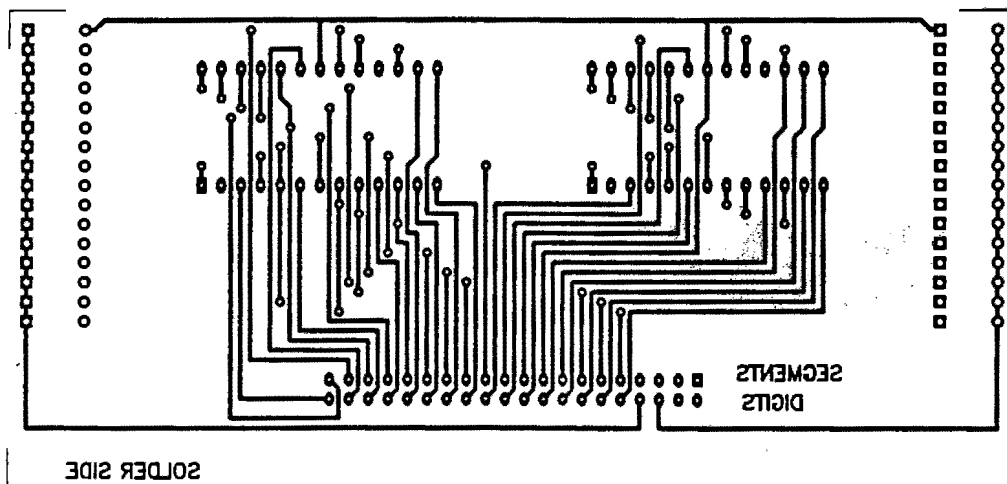


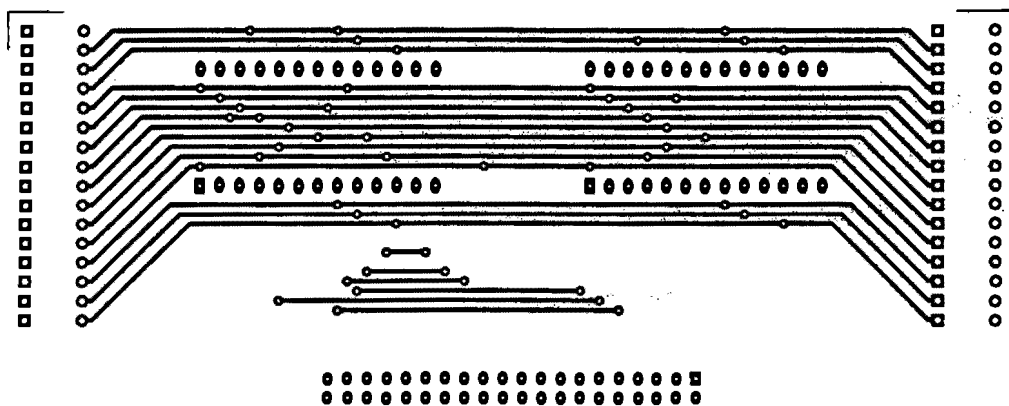
J5



J7

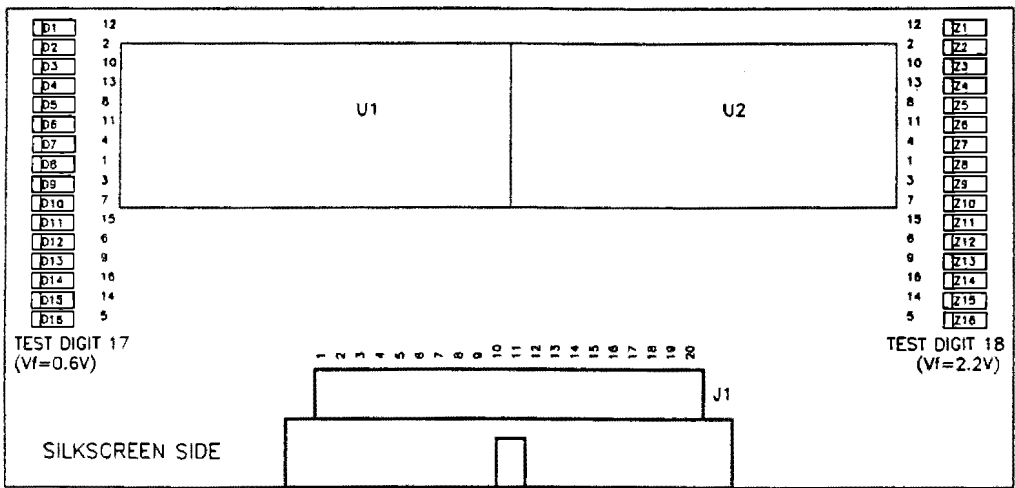


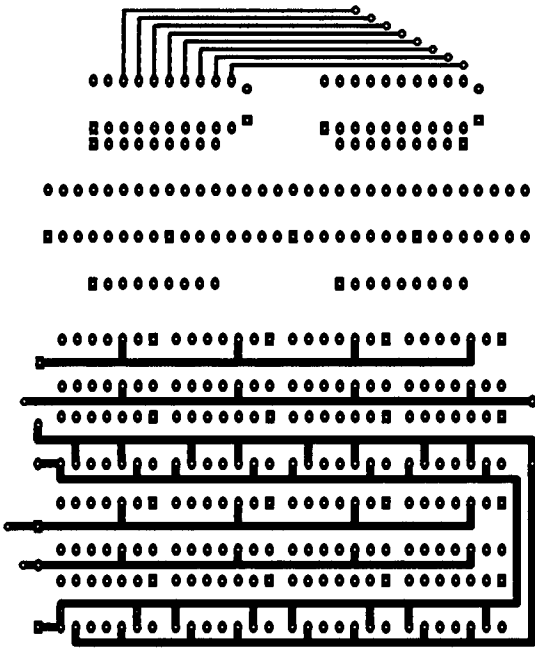
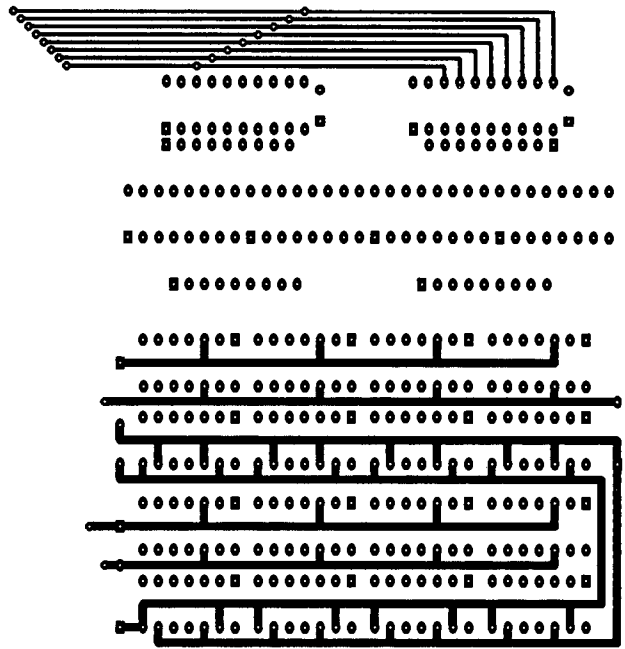
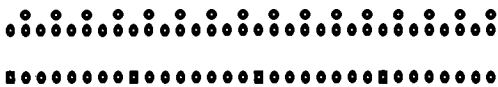
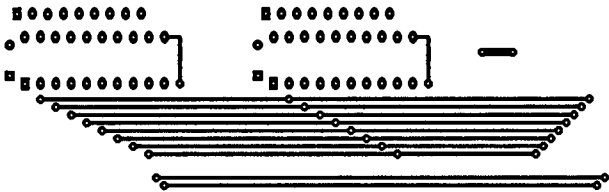
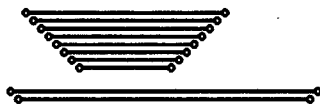
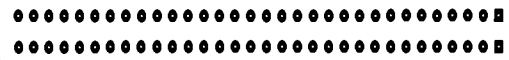




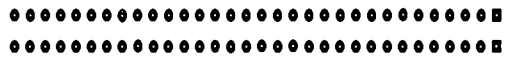
COMPONENT SIDE

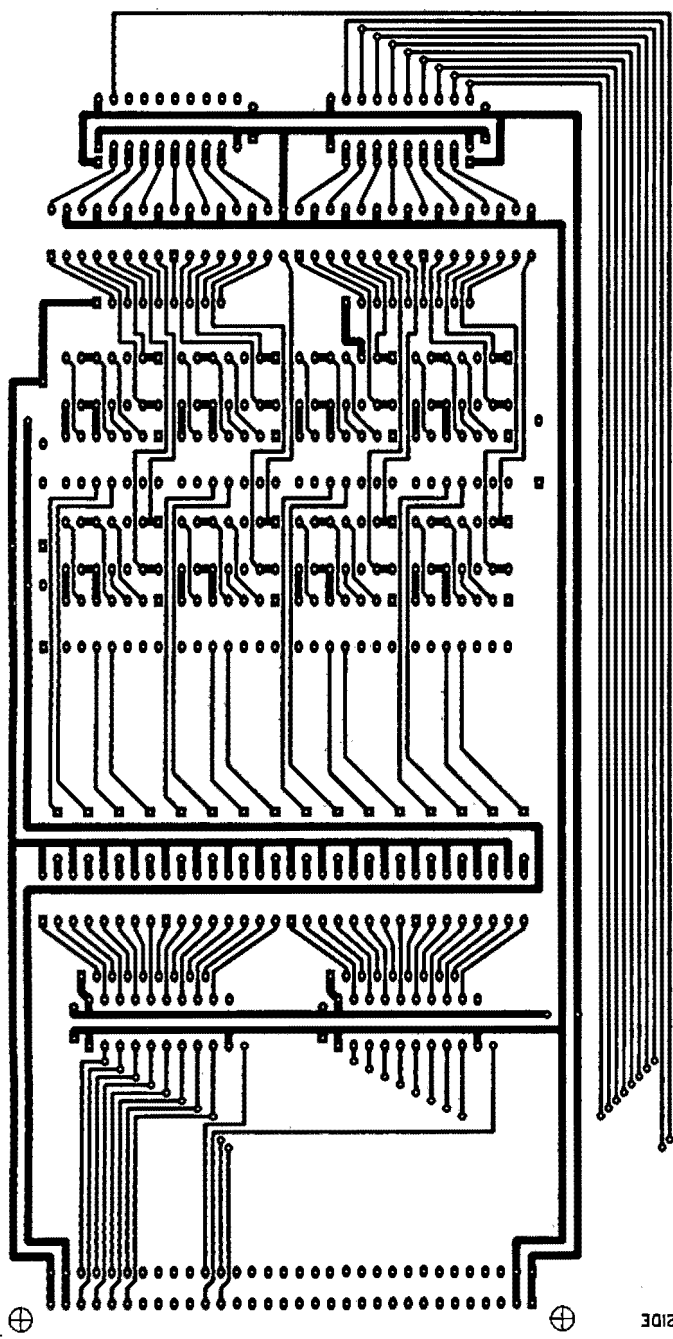
DISPLAY MODULE



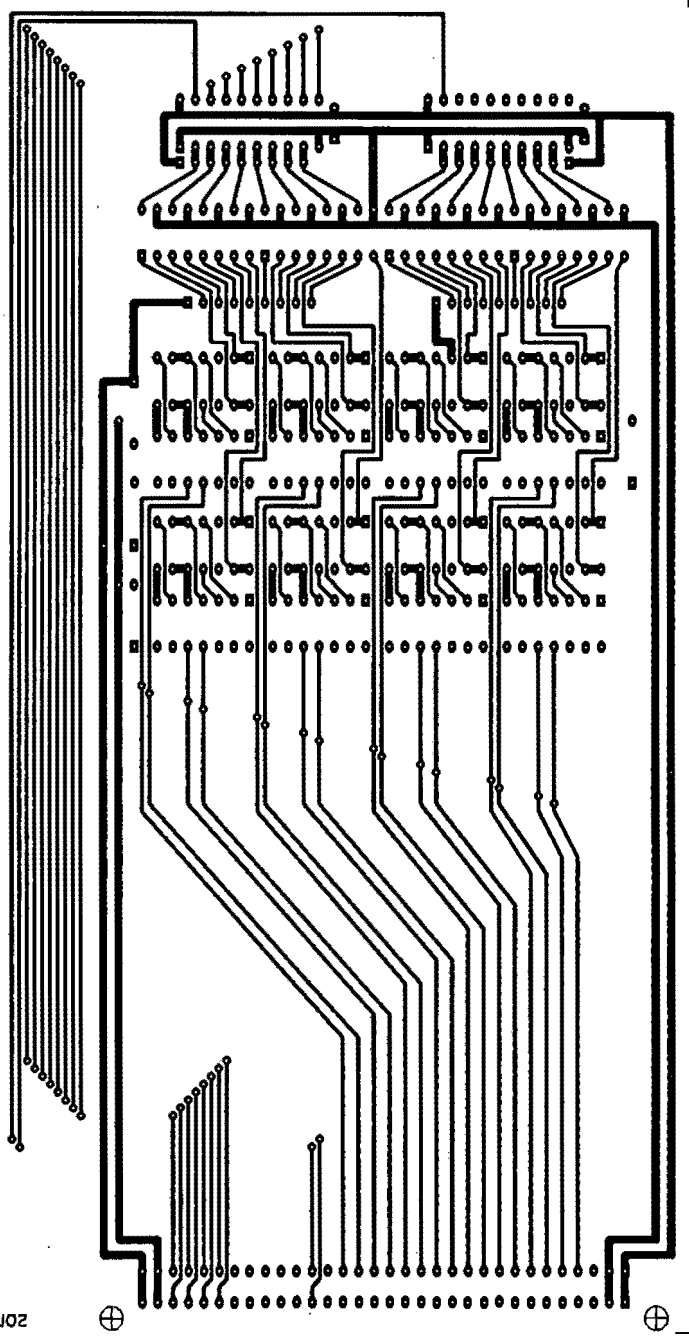


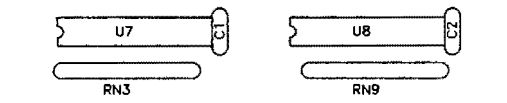
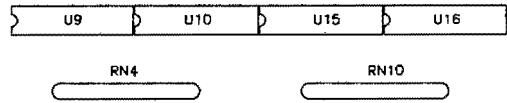
SEGMENT MODULE
COMPONENT SIDE



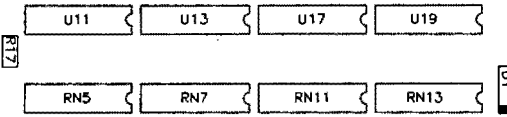
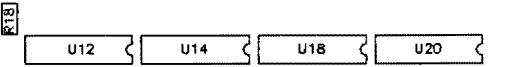
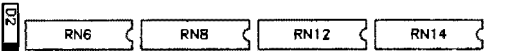


2000R 2102

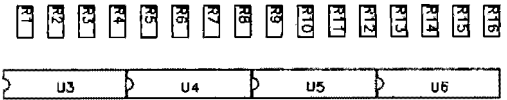
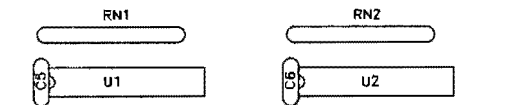
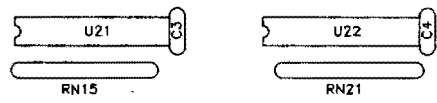
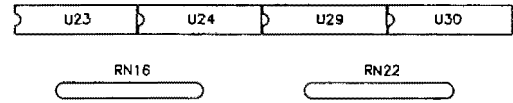




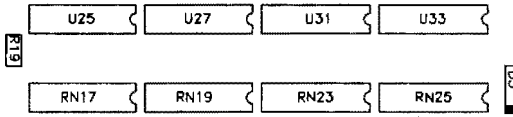
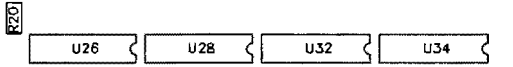
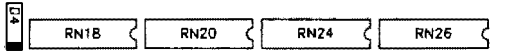
SEGMENT DETECTOR 1



SEGMENT DRIVER 1

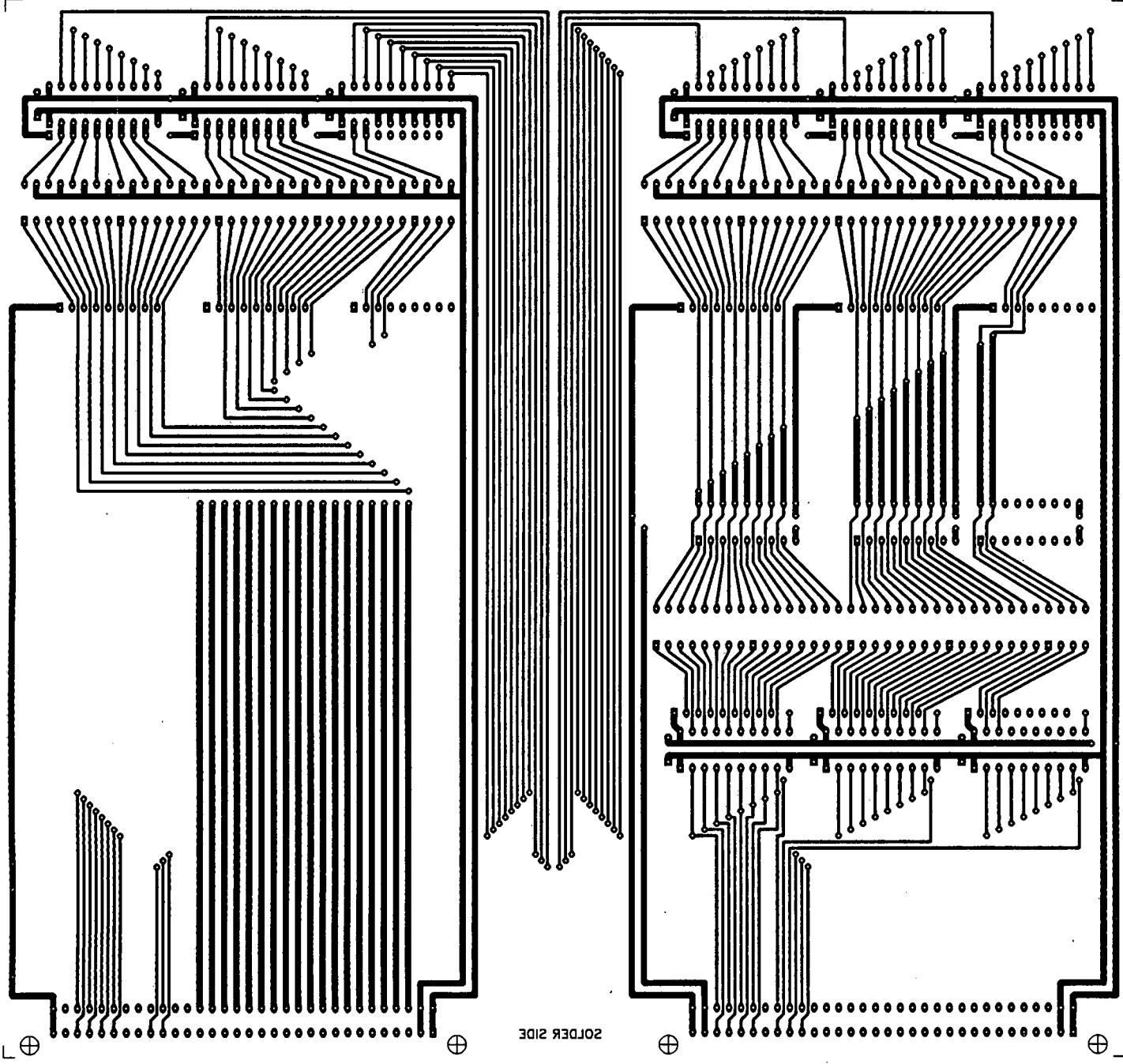


SEGMENT DETECTOR 2

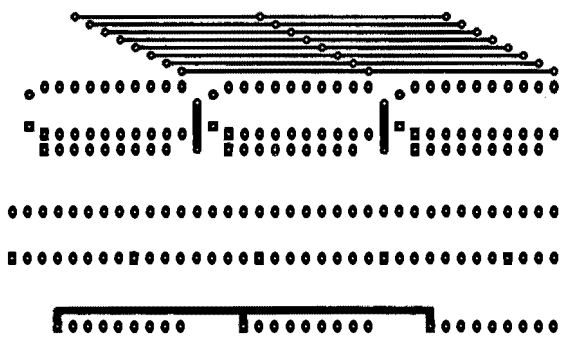
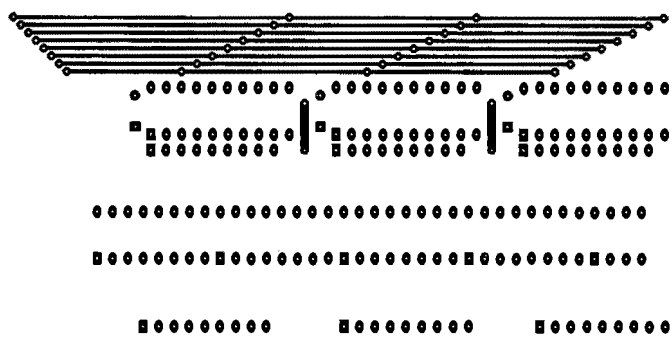
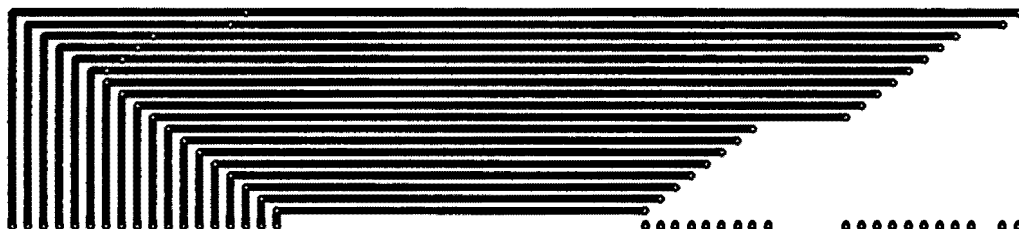
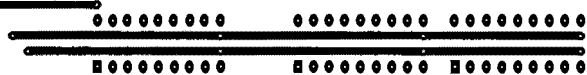
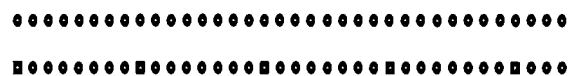
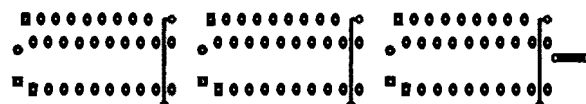
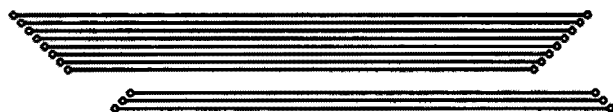
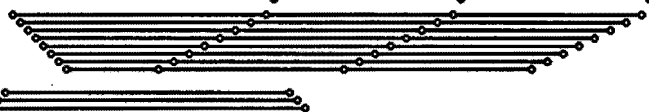
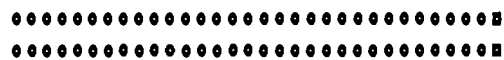


SEGMENT LINES

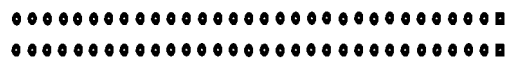


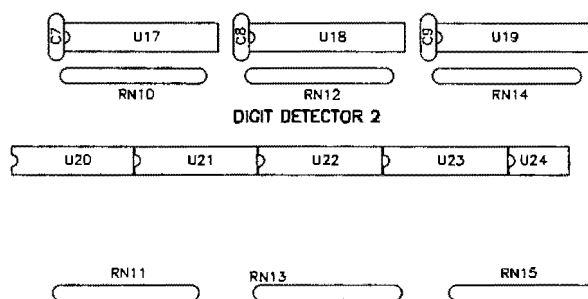
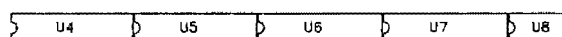
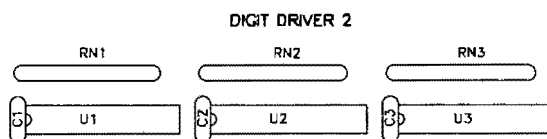
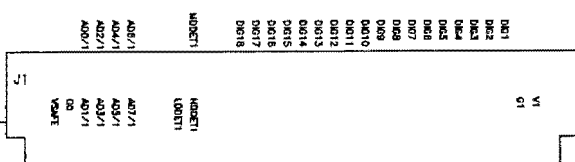
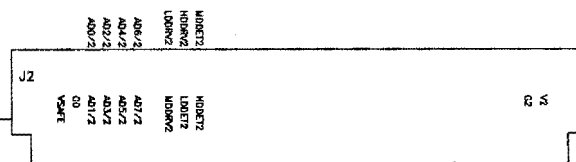


2012 R3D102



DIGIT MODULE
COMPONENT SIDE





└

└

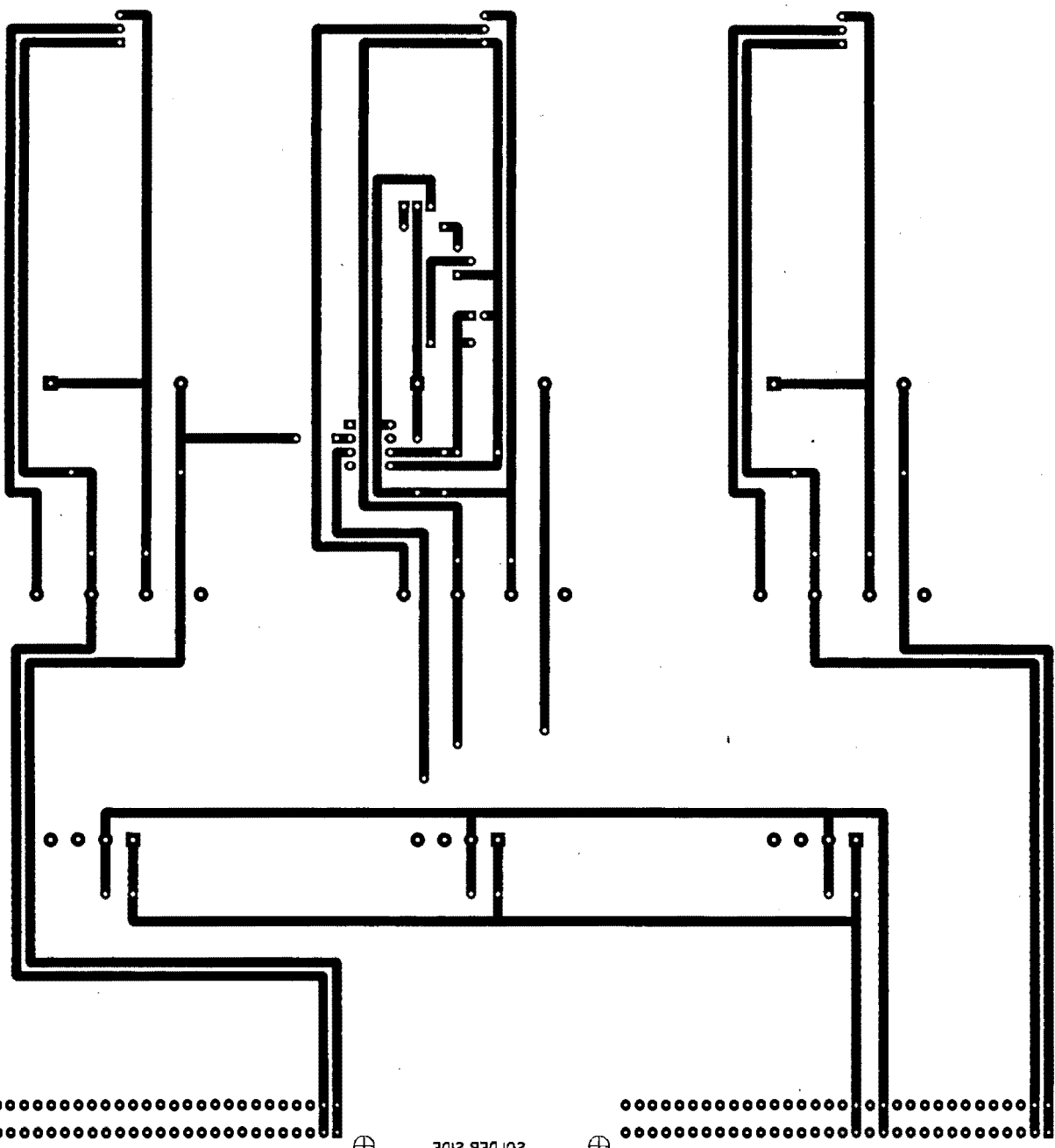
└ ⊕

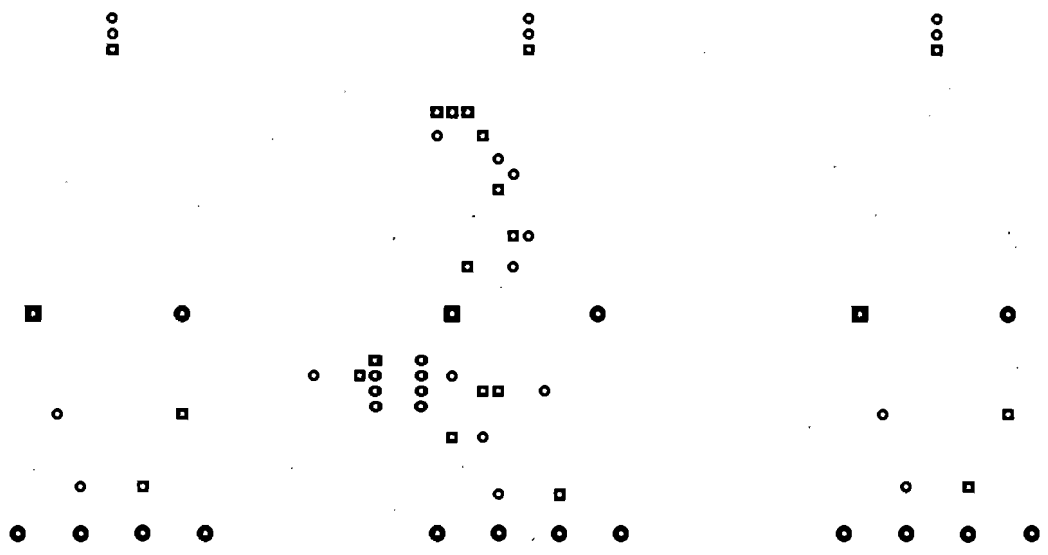
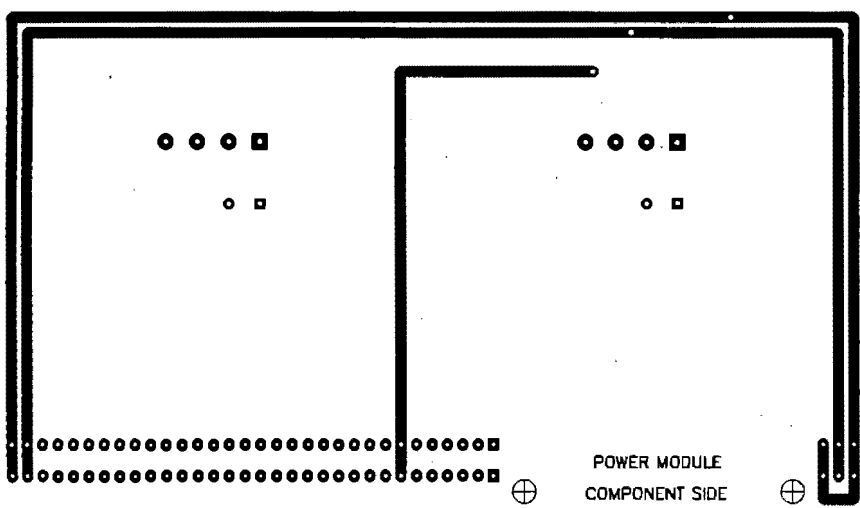
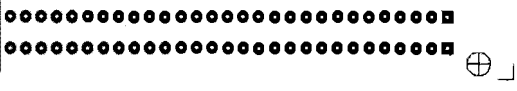
⊕

2012 R21D

⊕

└ ⊕





VR2

VR1

VR3

O2

R5

Q1

C3

R4

F2

F1

F3

D2

R3

U2

D1

R1

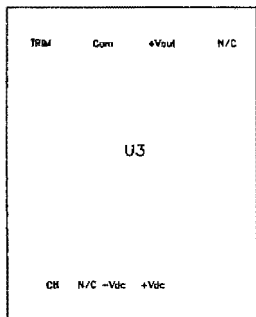
R2

D3

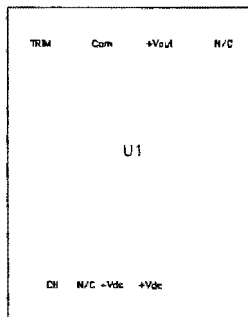
C5

C2

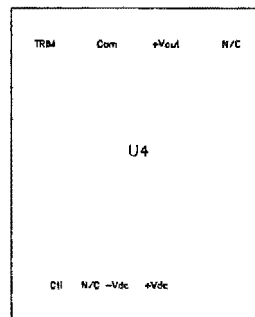
C7



C4 +



C1 +



C6 +

J1

DO
VAVT

HOLDOFF

DI
VI

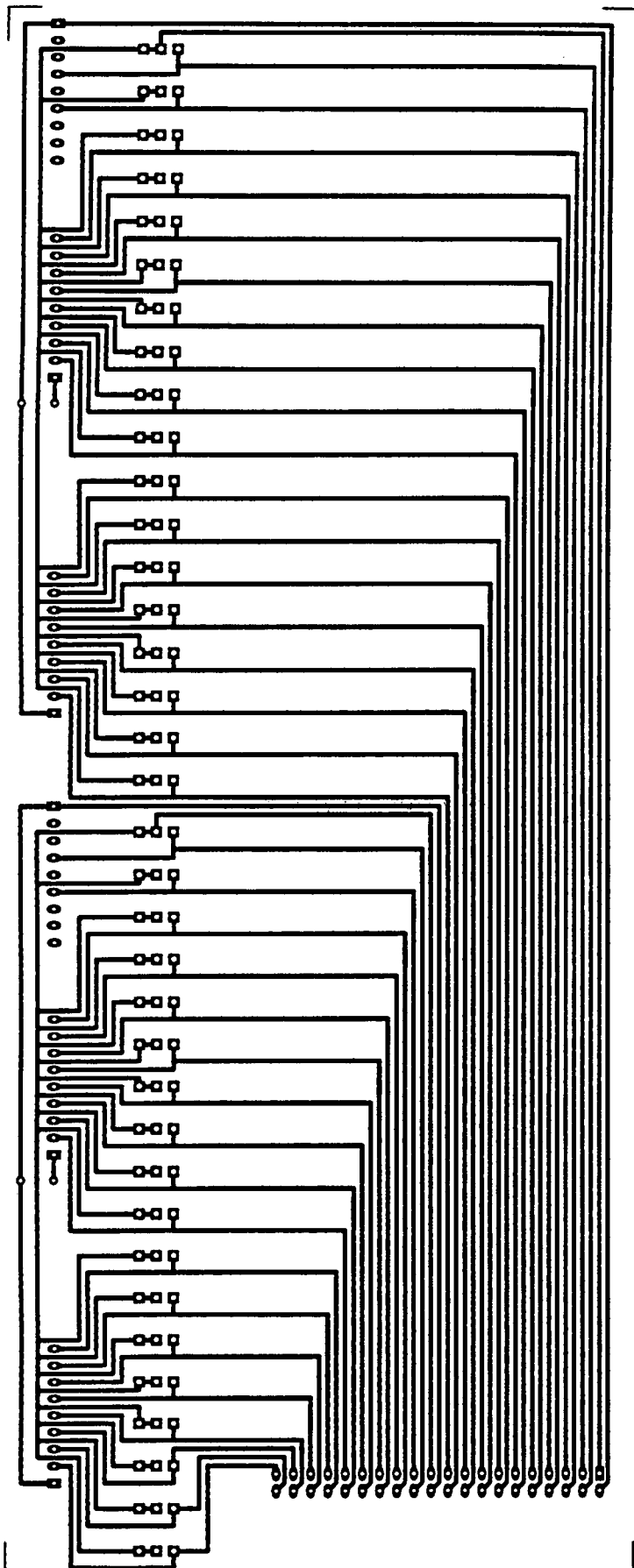
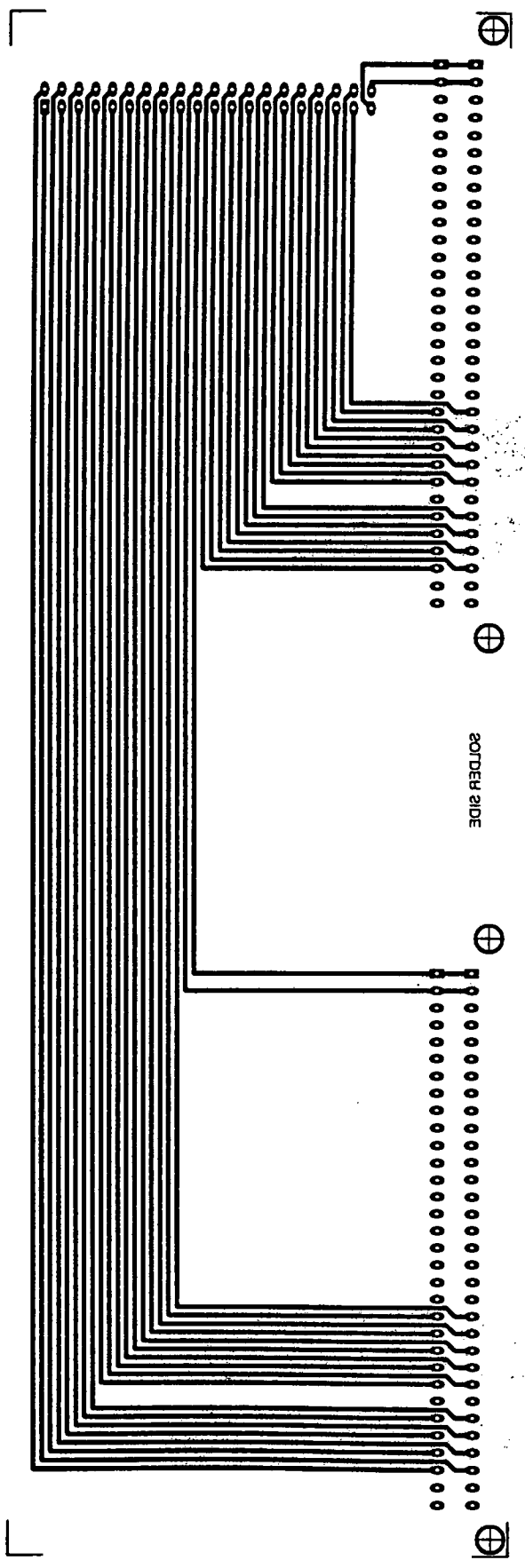
POWER MODULE
SILKSCREEN SIDE

J2

DO
VAVT

+24V
-24V

DI
VI

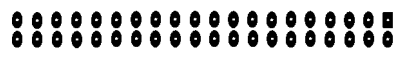


SOLDER SIDE



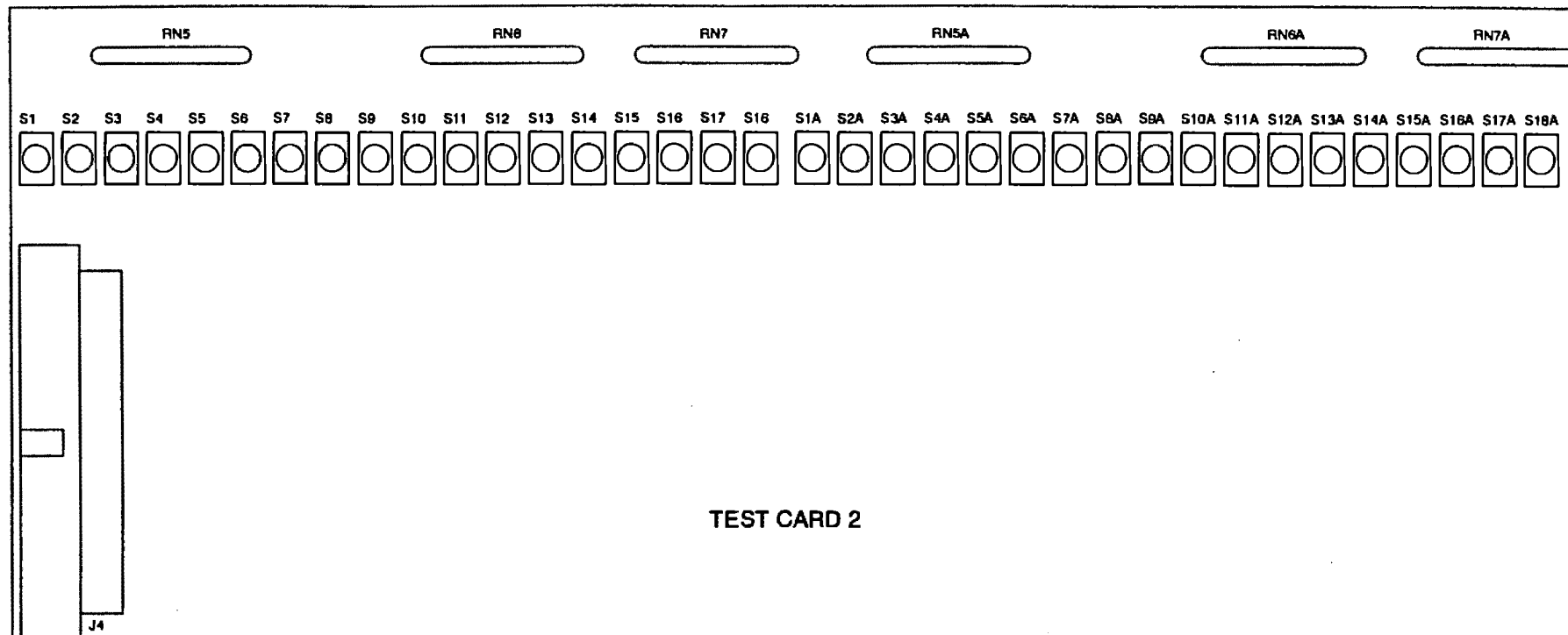
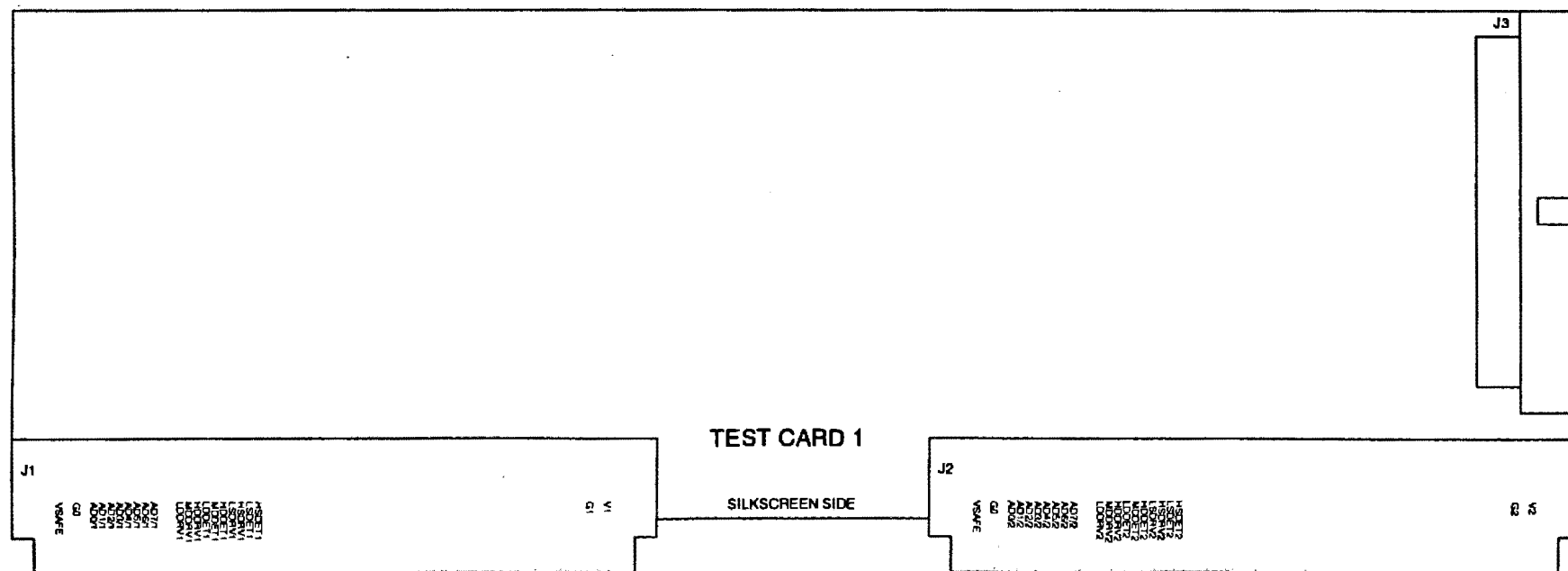
- □ □ HSD2T2
- □ □ LSD2T2
- □ □ HSDRV2
- □ □ LSDRV2
- □ □ HDDET2
- □ □ MDDET2
- □ □ LDDET2
- □ □ HDDRV2
- □ □ MDDRV2
- □ □ LDDRV2
- □ □ AD7/2
- □ □ AD6/2
- □ □ AD5/2
- □ □ AD4/2
- □ □ AD3/2
- □ □ AD2/2
- □ □ AD1/2
- □ □ AD0/2
- □ □ HSD2T1
- □ □ LSD2T1
- □ □ HSDRV1
- □ □ LSDRV1
- □ □ HDDET1
- □ □ MDDET1
- □ □ LDDET1
- □ □ HDDRV1
- □ □ MDDRV1
- □ □ LDDRV1
- □ □ AD7/1
- □ □ AD6/1
- □ □ AD5/1
- □ □ AD4/1
- □ □ AD3/1
- □ □ AD2/1
- □ □ AD1/1
- □ □ AD0/1

UP—LOW
DOWN—HIGH



COMPONENT SIDE





APPENDIX D: Component Lists

MOTHERBOARD

Quantity	Type	Value	Ref Designators
8	DIN41612C-FEMALE	A64-S2-111/LP4	J1,J2,J3,J4,J5,J6,J7,J8
1	DIN41651 HEADER	AWH40A-0202	J9

DISPLAY MODULE

Quantity	Type	Value	Ref Designators
2	16-SEG DISPLAY	HDSP-6508	U1,U2
1	DIN41651 HEADER	AWH40A-0202	J1
16	DIODE	1N4148	D1,D2,D3,D4,D5,D6,D7,D8, D9,D10,D11,D12,D13,D14, D15,D16
16	ZENER DIODE	2.2V	Z1,Z2,Z3,Z4,Z5,Z6,Z7,Z8, Z9,Z10,Z11,Z12,Z13,Z14, Z15,Z16

SEGMENT MODULE

Quantity	Type	Value	Ref Designators
4	3-STATE BUFFERS	74HC541	U7,U8,U21,U22
16	7-RESISTOR NET	899-3-R1K	RN5,RN6,RN7,RN8,RN11,RN12, RN13,RN14,RN17,RN18,RN19, RN20,RN23,RN24,RN25,RN26
4	8-RESISTOR NET	L91S-R2K2	RN4,RN10,RN16,RN22
4	8-RESISTOR NET	L91S-R4K7	RN3,RN9,RN15,RN21
2	8-RESISTOR NET	L91S-R330	RN1,RN2
2	DIN41612C-MALE	A64-S1-111	J1,J2
4	METAL RESISTOR	1K	R17,R18,R19,R20
16	METAL RESISTOR	150R	R1,R2,R3,R4,R5,R6,R7,R8, R9,R10,R11,R12,R13,R14, R15,R16
2	OCTAL D-LATCH	74HC573	U1,U2
6	POLYESTER CAP	.1uF	C1,C2,C3,C4,C5,C6
16	QUAD COMPARATOR	LM339	U11,U12,U13,U14,U17,U18, U19,U20,U25,U26,U27,U28, U31,U32,U33,U34
4	QUAD OPTO-DARL	TLP523-4	U3,U4,U5,U6
8	QUAD OPTOCOUPLER	TLP521-4	U9,U10,U15,U16,U23,U24, U29,U30
2	ZENER	2.4V	D2,D4
2	ZENER	3.9V	D1,D3

DIGIT MODULE

Quantity	Type	Value	Ref Designators
6	3-STATE BUFFERS	74HC541	U9,U10,U11,U17,U18,U19
6	8-RESISTOR NET	L91S-R1K8	RN5,RN7,RN9,RN11,RN13,RN15
6	8-RESISTOR NET	L91S-R4K7	RN4,RN6,RN8,RN10,RN12,RN14
3	8-RESISTOR NET	L91S-R470	RN1,RN2,RN3
2	DIN41612C-MALE	A64-S1-111	J1,J2
3	DUAL OPTOCOUPLER	TLP521-2	U8,U16,U24
3	OCTAL D-LATCH	74HC573	U1,U2,U3
3	OCTAL DARL ARRAY	ULN2803A	Q1,Q2,Q3
9	POLYESTER CAP	.1uF	C1,C2,C3,C4,C5,C6,C7,C8,C9
12	QUAD OPTOCOUPLER	TLP521-4	U4,U5,U6,U7,U12,U13,U14, U15,U20,U21,U22,U23

POWER MODULE

Quantity	Type	Value	Ref Designators
----------	------	-------	-----------------

3	DC-DC CONVERTER	NFC15-48S05	U1,U3,U4
2	DIN41612C-MALE	A64-S1-111	J1,J2
1	ELECTROLYTIC CAP	100uF 16V	C3
3	ELECTROLYTIC CAP	100uF 63V	C1,C4,C6
1	METAL RESISTOR	1K	R1
1	METAL RESISTOR	4K7	R2
2	METAL RESISTOR	100R	R4,R5
1	METAL RESISTOR	220R	R3
1	NPN BJT	2N3440	Q1
1	OPTOCOUPLER	6N136	U2
3	PCB FUSE HOLDER	S19K3F	F1,F2,F3
1	PNP BJT	TIP127	Q2
3	POLYESTER CAP	.1uF	C2,C5,C7
1	SCHOTTKY DIODE	1N5820	D1
2	TRANZORB	1N6267	D2,D3
3	TRIMPOT	67X-R10K	VR1,VR2,VR3

TEST MODULE

Quantity	Type	Value	Ref Designators
6	8-RESISTOR NET	L91S-R10K	RN5,RN5A,RN6,RN6A,RN7,RN7A
2	DIN41612C-MALE	A64-S1-111	J1,J2
2	DIN41651 HEADER	40 PIN	J3,J4
36	PCB SPDT SWITCH	UT1E-1	S1,S1A,S2,S2A,S3,S3A,S4, S4A,S5,S5A,S6,S6A,S7,S7A, S8,S8A,S9,S9A,S10,S10A, S11,S11A,S12,S12A,S13, S13A,S14,S14A,S15,S15A, S16,S16A,S17,S17A,S18,S18A

APPENDIX E: Correspondence and Data Sheets

Hewlett Packard
Components Marketing Operation
Application Lab Europe
Phone: (49) 7031 14-3635
Fax: (49) 7031 14-2216
FAX 49. 7031 14 2216



Urgent Fax

July, 17th 1992

TO: Brian Grainsford
FROM: Uwe Thomas
Applications Engineer

PAGE 1 OF 20

SUBJECT: Outstanding questions

Dear Mr. Grainsford,

I am the application engineer for opto electronic devices in HP. Gilbert Garin has forwarded your questions concerning LED's and displays to me.

1) We have no specific critical analysis report for LED's. When a failed product comes back to our manufacturer facilities we make a failure analysis report. We have made a lot of these reports to improve our manufacturing process.

2) Attached you will find the most important reliability sheets. Basically we have reliability data for every product family. Please come back to me when you need any specific data.

3) Yes we do have a "unintelligent" 16-segment display where you have access to the segments. the part number is HDSP-6504/6508. Attached you will find the data sheet.

↑
R217.37

(4 wks.)

4)

4.1) We have never seen a short with our LED's.

4.2) Open circuits are due to wire bond cutting, die cracking and die lifting.

4.3) We have seen intermittent failures with LED's at different operating temperatures. Imagine the die lifted after soldering due to different expansion of epoxy and leadframe. At lower temperatures the material shrinks again and the die get in contact with the leadframe again. So the LED may illuminate at low temperatures and not at higher temperatures.

4.4) We specify a certain reverse current at a certain reverse voltage in our datasheets. We have no data about forward leakage currents.

4.5) The forward current versus forward voltage curve of a LED varies with temperature. Also the slope of this curve varies with temperature like all semiconductor. Because the slope of this curve is equal to the dynamic resistance, it varies also.

4.6) We have degradation data for different families and under different conditions. Please come back to me if you need any specific data.

4.a) Mean time between these failures is on the attached reliability datasheets.

4.b) see 4.2) and 4.3)

Hope this helps you in the first step. Please feel free to contact me if you need any additional information.

Best regards and have a nice day



**HEWLETT
PACKARD**

16 SEGMENT SOLID STATE ALPHANUMERIC DISPLAY

**HN5P-6504
HDSP-6508**

TECHNICAL DATA FEBRUARY 1981

Features

- **ALPHANUMERIC**
Displays 64 Character ASCII Set and Special Characters
- **16 SEGMENT FONT PLUS CENTERED D.P. AND COLON**
- **3.81mm (0.150") CHARACTER HEIGHT**
- **APPLICATION FLEXIBILITY WITH PACKAGE DESIGN**
4 and 8 Character Dual-In-Line Packages
End Stackable-On Both Ends for 8 Character and On One End for 4 Character
Sturdy Gold-Plated Leads on 2.54mm (0.100") Centers
Environmentally Rugged Package
Common Cathode Configuration
- **LOW POWER**
As Low as 1.0-1.5mA Average
Per Segment Depending on Peak Current Levels
- **EXCELLENT CHARACTER APPEARANCE**
Continuous Segment Font
High On/Off Contrast
6.35mm (0.250") Character Spacing
Excellent Character Alignment
Excellent Readability at 2 Metres
- **SUPPORT ELECTRONICS**
Can Be Driven With ROM Decoders and Drivers
Easy Interfacing With Microprocessors and LSI Circuitry
- **CATEGORIZED FOR LUMINOUS INTENSITY**
Assures Uniformity of Light Output From Unit to Unit Within a Single Category .



Description

The HDSP-6504 and HN5P-6508 are 3.81mm (0.150") sixteen segment GaAsP red alphanumeric displays mounted in 4 character and 8 character dual-in-line package configurations that permit mounting on PC boards or in standard IC sockets. The monolithic light emitting diode character is magnified by the integral lens which increases both character size and luminous intensity, thereby making low power consumption possible. The rugged package construction, enhanced by the back fill design, offers extended environmental capabilities compared to the standard PC board/lens type of display package. Its temperature cycling capability is the result of the air gap which exists between the semiconductor chip/wire bond assembly and the lens. In addition to the sixteen segments, a centered D.P. and colon are included. Character spacing yields 4 characters per inch.

Applications

These alphanumeric displays are attractive for applications such as computer peripherals and terminals, computer base emergency mobile units, automotive instrument panels, desk top calculators, in-plant control equipment, hand-held instruments and other products requiring low power, display compactness and alphanumeric display capability.

Device Selection Guide

W

Characters Per Display	Configuration		Part No. HDSP-
	Device	Package	
4		(Figure 6)	6504
8		(Figure 7)	6508

Absolute Maximum Ratings

Symbol	Parameter	Min.	Max.	Units
I_{PEAK}	Peak Forward Current Per Segment or DP (Duration $\leq 312\mu s$)		200	mA
I_{AVG}	Average Current Per Segment or DP (1)		7	mA
P_D	Average Power Dissipation Per Character (1,2)		138	mW
T_A	Operating Temperature, Ambient	-40	85	$^{\circ}C$
T_s	Storage Temperature	-40	100	$^{\circ}C$
V_R	Reverse Voltage		5	V
	Solder Temperature at 1.59mm (1/16 inch) below seating plane $t \leq 3$ Seconds		260	$^{\circ}C$

NOTES:

- Maximum allowed drive conditions for strobed operation are derived from Figures 1 and 2. See electrical section of operational considerations.
- Derate linearly above $T_A = 50^{\circ}C$ at $2.17mW/^{\circ}C$. P_D Max. ($T_A = 85^{\circ}C$) = 62mW.

Electrical/Optical Characteristics at $T_A = 25^{\circ}C$

Symbol	Parameter	Test Condition	Min.	Typ.	Max.	Units
I_V	Luminous Intensity, Time Average, Character Total with 16 Segments Illuminated (3,4)	$I_{PEAK} = 30mA$ 1/16 Duty Factor	0.40	1.65		mcd
V_F	Forward Voltage Per Segment or DP	$I_F = 30mA$ (One Segment On)		1.6	1.9	V
λ_{PEAK}	Peak Wavelength			655		nm
λ_d	Dominant Wavelength (5)			640		nm
I_R	Reverse Current Per Segment or DP	$V_R = 5V$		10		μA
$\Delta V_F / \Delta^{\circ}C$	Temperature Coefficient of Forward Voltage			-2		mV/ $^{\circ}C$
$R_{\theta J-PIN}$	Thermal Resistance LED Junction-to-Pin			232		$^{\circ}C/W/Seg$

NOTES:

- The luminous intensity ratio between segments within a digit is designed so that each segment will have the same luminous sterance. Thus each segment will appear with equal brightness to the eye.
- Operation at peak currents of less than 7mA is not recommended.
- The dominant wavelength, λ_d , is derived from the C.I.E. chromaticity diagram and represents that single wavelength which defines the color of the device, standard red.

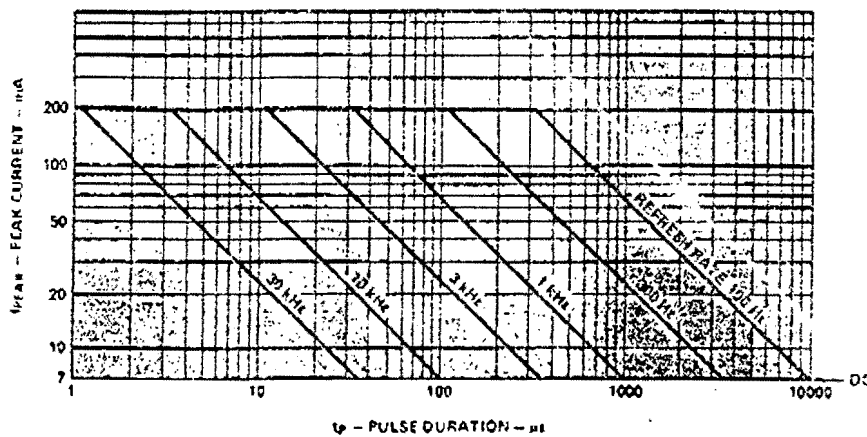


Figure 1. Maximum Allowed Peak Current vs. Pulse Duration, Derate derived operating conditions above $T_A = 50^\circ\text{C}$ using Figure 2.

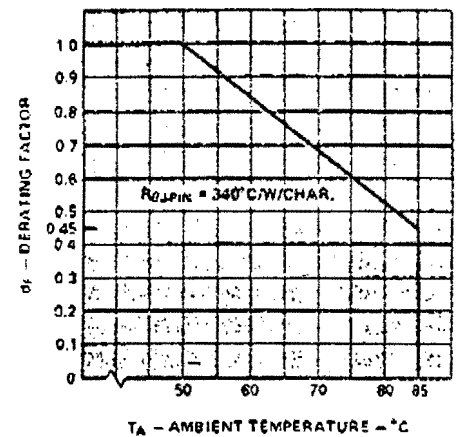


Figure 2. Temperature Derating Factor For Peak Current per Segment vs. Ambient Temperature. $T_{JMAX} = 110^\circ\text{C}$

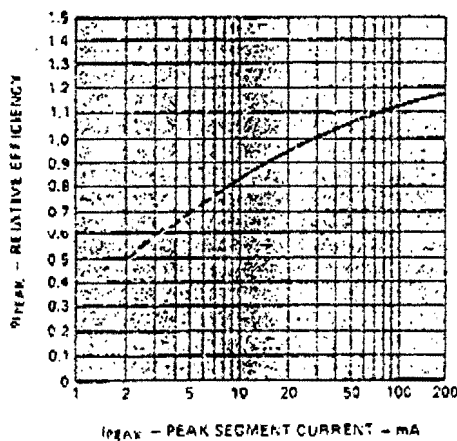


Figure 3. Relative Luminous Efficiency (Luminous Intensity Per Unit Current) vs. Peak Segment Current.

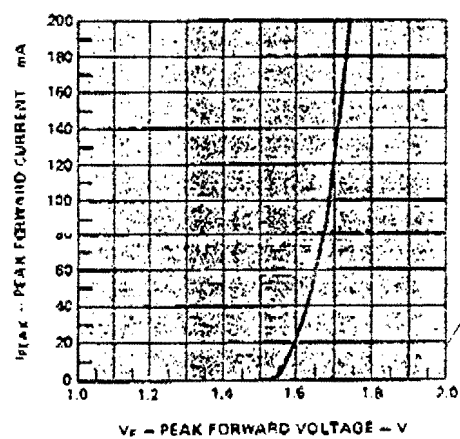


Figure 4. Peak Forward Segment Current vs. Peak Forward Voltage.

For a Detailed Explanation on the Use of Data Sheet Information and Recommended Soldering Procedures, See Application Note 1005, Page 458.

		A ₃	A ₂	A ₁	A ₀														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
A ₅	A ₄	0	0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
	1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
	1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		

Figure 5. Typical 64 Character ASCII Set.

0 1 2 3 4 5 6 7 8 9 √ ÷ Σ
△ □ P V →

Additional Character Font

Package Dimensions

(W)

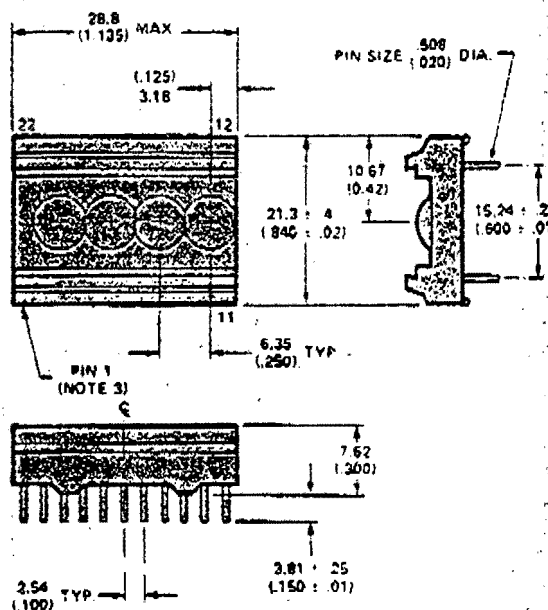


Figure 6. HDSP-6504

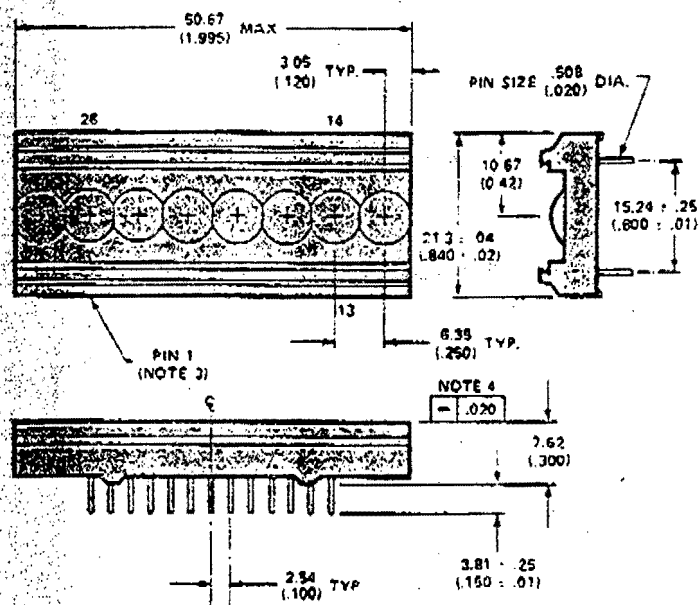


Figure 7. HDSP-6508

NOTES:
 1. ALL DIMENSIONS IN MILLIMETRES AND (INCHES).
 2. ALL UNTOLERANCED DIMENSIONS ARE FOR REFERENCE ONLY.
 3. PIN 1 IDENTIFIED BY INK DOT ADJACENT TO LEAD.

Magnified Character Font Description

DEVICES
 HDSP-6504
 HDSP-6508

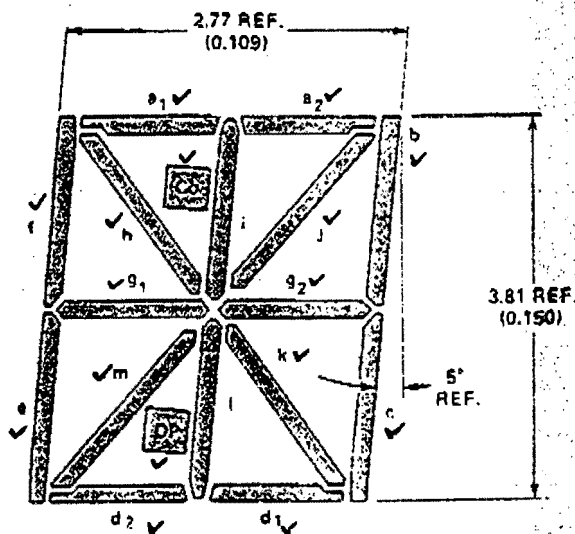


Figure 8.

Device Pin Description

Function			
Pin	HDSP-6504	HDSP-6508	
1	Anode Segment 9	Anode Segment 9	1
2	Anode Segment 8	Anode Segment 8	2
3	Cathode Digit 4	Cathode Digit 4	3
4	Anode Segment 2	Anode Segment 2	4
5	Anode Segment 1	Anode Segment 1	5
6	Cathode Digit 3	Cathode Digit 3	6
7	Anode Segment 7	Anode Segment 7	7
8	Anode Segment 6	Anode Segment 6	8
9	Anode Segment 5	Anode Segment 5	9
10	Cathode Digit 2	Cathode Digit 2	10
11	Anode Segment 4	Anode Segment 4	11
12	Anode Segment 3	Cathode Digit 6	12
13	Anode Segment 0	Cathode Digit 8	13
14	Anode Segment 0	Cathode Digit 7	14
15	Anode Segment 2	Cathode Digit 5	15
16	Anode Segment 1	Anode Segment 0	16
17	Cathode Digit 2	Anode Segment 0	17
18	Anode Segment 7	Anode Segment 0	18
19	Anode Segment 6	Anode Segment 0	19
20	Anode Segment 5	Anode Segment 0	20
21	Anode Segment 4	Cathode Digit 2	21
22	Anode Segment 3	Anode Segment 0	22
23	Anode Segment 2	Anode Segment 0	23
24	Anode Segment 1	Anode Segment 0	24
25	Anode Segment 0	Anode Segment 0	25
26	Anode Segment 0	Anode Segment 0	26

Operational Considerations

ELECTRICAL

The HDSP-6504 and -6508 devices utilize large monolithic 16 segment GaAsP LED chips with centered decimal point and colon. Like segments of each digit are electrically interconnected to form an 18 by N array, where N is the quantity of characters in the display. In the driving scheme the decimal point or colon is treated as a separate character with its own time frame. A detailed discussion of character font capabilities, ASCII code to 18 segment decoding and display drive techniques appear in Application Note 1003.

These displays are designed specifically for strobed (multiplexed) operation, with a minimum recommended time peak forward current per segment of 7mA. Under normal operating situations the maximum number of illuminated segments needed to represent a given character is 10. Therefore, except where noted, the information presented in this data sheet is for a maximum of 10 segments illuminated per character.*

The typical forward voltage values, scaled from Figure 4, should be used for calculating the current limiting resistor values and typical power dissipation. Expected maximum V_F values for the purpose of driver circuit design may be calculated using the following V_F model

$$V_F = 1.85V + I_{PEAK} (1.8\Omega)$$

$$\text{For: } 30mA \leq I_{PEAK} \leq 200mA$$

$$V_F = 1.58V + I_{PEAK} (10.7\Omega)$$

$$\text{For: } 10mA \leq I_{PEAK} \leq 30mA$$

OPTICAL AND CONTRAST ENHANCEMENT

Each large monolithic chip is positioned under a separate element of a plastic aspheric magnifying lens, producing a magnified character height of 3.810mm (.150 inch). The aspheric lens provides wide included viewing angles of typically 75 degrees horizontal and 75 degrees vertical with low off axis distortion. These two features, coupled

*More than 10 segments may be illuminated in a given character, provided the maximum allowed character power dissipation, temperature derated, is not exceeded.



with the very high segment luminous sterance, provide to the user a display with excellent readability in bright ambient light for viewing distances in the range of 2 metres. Effective contrast enhancement can be obtained by employing any of the following optical filter products: Panelgraphic: Ruby Red 60, Dark Red 63 or Purple 90; SGL Homalite H100-1605 Red or H100-1804 Purple; Plexiglas 2423. For very bright ambients, such as indirect sunlight, the 3M Light Control Film is recommended: Red 655, Violet, Purple or Neutral Density.

For those applications requiring only 4 or 8 characters, a secondary barrel magnifier, HP part number HDSP-6505 (four character) and -6509 (eight character), may be inserted into support grooves on the primary magnifier. This secondary magnifier increases the character height to 4.45mm (.175 inch) without loss of horizontal viewing angle (see below)

MECHANICAL

These devices are constructed by LED die attaching and wire bonding to a high temperature PC board substrate. A precision molded plastic lens is attached to the PC board and the resulting assembly is backfilled with a sealing epoxy to form an environmentally sealed unit.

The four character and eight character devices can be end stacked to form a character string which is a multiple of a basic four character grouping. As an example, one -6504 and two -6508 devices will form a 20 character string. These devices may be soldered onto a printed circuit board or inserted into 24 and 28 pin DIP LSI sockets. The socket spacing must allow for device end stacking.

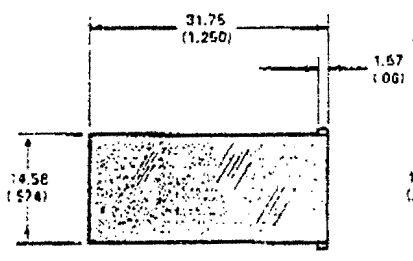
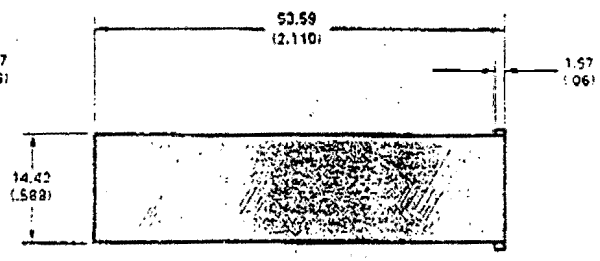
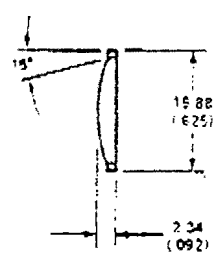
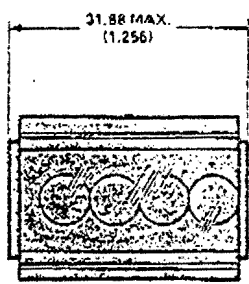
Suitable conditions for wave soldering depend upon the specific kind of equipment and procedure used. For more information, consult the local HP Sales Office or Hewlett-Package Components, Palo Alto, California.

W

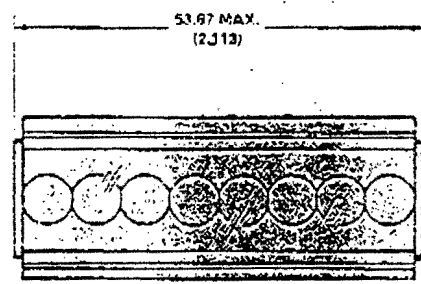
OPTIONAL
4 DIGIT MAGNIFIER
HDSP-6505

OPTIONAL
8 DIGIT MAGNIFIER
HDSP-6509

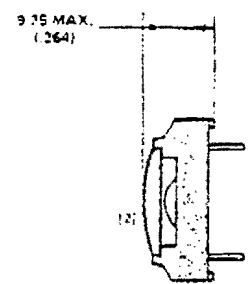
END VIEW
(BOTH)



MOUNTED ON HDSP-6504



MOUNTED ON HDSP-6508



- NOTES:
1. ALL DIMENSIONS IN MILLIMETRES AND (INCHES).
 2. THIS SECONDARY MAGNIFIER INCREASES THE CHARACTER HEIGHT TO 4.45mm (.175 in.)

Figure 9. Design Data for Optional Barrel Magnifier in Single Display Applications.



HEWLETT
PACKARD

RELIABILITY DATA

HDSP-6504/6508

SEPTEMBER 1982

4 and 8 Character Monolithic Alphanumeric Displays

The following cumulative test results have been obtained from testing performed at Hewlett-Packard in accordance with the latest revision of MIL-STD-883.

For the purpose of this reliability data sheet, a failure is any part which causes the user's system to fail to operate correctly or to display erroneous information. Any LED whose light output degrades by more than 50% is considered a failure. ALL FAILURE RATES GIVEN ARE BASED ON AN 8 CHARACTER PACKAGE.

I. LIFE TEST

Test	Test Conditions	Units Tested	Total Hours	Failed	Failure Rate (%/1K Hrs.)
High Temperature Storage	Storage at 100°C	117	100,531	0	<0.990%
High Temperature Operating Life	220 mA peak at 1/32 duty cycle $T_J = 125^\circ\text{C}^{(1)}$	223	297,300	0	<0.340%

Note.

1. These devices were electrically overstressed above the maximum allowed operating conditions of $T_J = 110^\circ\text{C}$.

A. Failure Rate Prediction

The failure rate given above was obtained from drive conditions above the maximum allowable stress conditions. The failure rate at other drive conditions will depend directly on the junction temperature of the device. The estimated life at a lower temperature can be determined using the following table. This table is based on 297,300 device hours at a junction temperature of 125°C . The extrapolated failure rates are based on a typical power dissipation of 59 mW/character (35 mA/character). This corresponds to a junction to ambient temperature rise of 20°C . Estimates were done based on HDBK-217 which specifies an activation energy of 0.43 eV for hybrid products.

8 Character Device Failure Rates

Ambient Temp° C	Junction Temp° C	Point [2]		90% Confidence Level [3]	
		Device MTBF	Failure Rate/ 1K Hrs. Operation	Device MTBF	Failure Rate/ 1K Hrs. Operation
75	95	965,000	0.104%	419,000	0.239%
70	90	1,163,000	0.086%	505,000	0.198%
65	85	1,410,000	0.071%	612,000	0.163%
60	80	1,717,000	0.058%	746,000	0.134%
55	75	2,104,000	0.048%	914,000	0.109%
50	70	2,593,000	0.039%	1,126,000	0.089%
45	65	3,216,000	0.031%	1,397,000	0.072%
→ 40	60	4,014,000	0.025%	1,743,000	0.057%
35	55	5,044,000	0.020%	2,190,000	0.046%
30	50	6,383,000	0.016%	2,772,000	0.036%
25	45	8,128,000	0.012%	3,534,000	0.028%

Notes:

- The point MTBF is simply the total device hours divided by the number of failures. Since no failures occurred during the testing, the point MTBF and the failure rate are calculated assuming one failure.
- This MTBF and failure rate represent the performance level for which there is a 90% probability of the device doing better than the stated value. This confidence level is based on the statistics of the distribution of failures. The assumed distribution is exponential. This particular distribution is commonly used in describing useful life failures. Refer to MIL-STD-690B for details of this methodology.

Y

B. Example of Failure Rate Calculation

At 40° C with a 25% utilization (8 hours a day, 5 days a week) the device point failure rate per year can be calculated:

Utilization = (8 hrs/day x 5 days/week) / 168 hrs/week = .25

$$\frac{(0.025\%)}{(1K Hrs)} \times (25\%) \times (8760 \text{ hrs/year}) = 0.055\% \text{ per year}$$

Likewise the 90% confidence level failure rate per year is:

$$\frac{(0.057\%)}{(1K Hrs)} \times (25\%) \times (8760 \text{ hrs/year}) = 0.125\% \text{ per year}$$

(This corresponds to one out of one-thousand devices failing per year.)

II. MECHANICAL TESTS:

Test	MIL-STD-883 Reference	Test Conditions	Units Tested	Total Failed
Solderability	2003	Sn 60, Pb 40, Solder at 260° C for 3 sec	218	0
Temperature Cycling	1010	100 cycles, -55 to 100° C	60	0
Moisture Resistance	1004	10 days, 90-98% RH, -10 to 65° C, non-operating	131	0
Shock	2002	5 blows each X1, Y1, Y2 axis, 1500G, 0.5 msec pulse	200	0
Vibration Variable Frequency	2007	4, 4 minute cycles each X, Y, Z axis at 20G min, 20 to 2000 Hz	90	0
Terminal Strength	2004	1 lb. tension for 30 sec.	30	0
Lead Fatigue	2004	8 oz., 3 x 90° bends	30	0




**HEWLETT
PACKARD**
**Optoelectronics Division
Reliability Data**
Plastic Lamps
February 1992
Description

The following cumulative test results have been obtained from testing performed at HP Optoelectronics Division in accordance with the latest revision of MIL-STD-883.

Hewlett-Packard tests parts at the absolute maximum rated conditions recommended for the device. The actual performance you obtain from HP parts depends on the electrical and environmental characteristics of your application but will probably be better than the performance outlined below.

LIFE TESTS
Demonstrated Performance

					Point Typical Performance	
Test Name	Stress Test Conditions	Total Device Hours	Units Tested	Total Failed	MTBF	FailureRate (% / 1 K Hours)
High Temperature Operating Life HER, Green, and Orange and Red AlGaAs	Operating at $T_A = 55^\circ \text{C}$ $I_F = 30 \text{ mA}$	2,688,000	2,688	0	2,688,000	$\leq 0.037\%$
High Temperature Operating Life Yellow	Operating at $T_A = 55^\circ \text{C}$ $I_F = 20 \text{ mA}$	700,000	700	0	700,000	$\leq 0.143\%$
High Temperature Operating Life STD Red	Operating at $T_A = 55^\circ \text{C}$ $I_F = 50 \text{ mA}$	700,000	700	0	700,000	$\leq 0.143\%$

PRELIMINARY

②

Failure Rate Prediction

The failure rate of semiconductor devices is determined by the junction temperature of the device. The relationship between ambient temperature and actual junction temperature is given by the following:

$$T_J (^{\circ}\text{C}) = T_A (^{\circ}\text{C}) + \theta_{JA} P_{AVG}$$

where T_A = ambient temperature in $^{\circ}\text{C}$

θ_{JA} = thermal resistance of junction-to-ambient in $^{\circ}\text{C}/\text{watt}$

P_{AVG} = average power dissipated in watts

The estimated MTBF and failure rate at temperatures lower than the actual stress temperature can be determined by using an Arrhenius model for temperature acceleration. Results of such calculations are shown in the table below using an activation energy of 0.43 eV (reference MIL-HDBK-217).

I_F	Ambient Temperature ($^{\circ}\text{C}$)	Junction Temperature ($^{\circ}\text{C}$)	Point Typical Performance[1] in Time		Performance in Time[2] (90% Confidence)	
			MTBF(1)	Failure Rate (% / 1K Hours)	MTBF(2)	Failure Rate (% / 1K Hours)
30 mA DC	85	103	848,000	.118%	368,000	.271%
	75	93	1,220,000	.082%	530,000	.189%
	65	83	1,791,000	.056%	778,000	.129%
	55	73	2,688,000	.037%	1,167,000	.086%
	45	63	4,133,000	.024%	1,795,000	.056%
	35	53	6,525,000	.015%	2,834,000	.035%
	25	43	10,605,000	.009%	4,606,000	.022%

Example of Failure Rate Calculation

Assume a device operating 8 hours/day, 5 days/week. The utilization factor, given 168 hours/week is:

$$\frac{8 \text{ hours/day} \times 5 \text{ days/week}}{168 \text{ hours/week}} = 0.25$$

The point failure rate per year (8760 hours) at 40°C ambient temperature is:

$$(0.037\% / 1\text{K hours}) \times 0.25 \times (8760 \text{ hours/year}) = 0.081\% \text{ per year}$$

Similarly, 90% confidence level failure rate per year at 55°C :

$$(0.086\% / 1\text{K hours}) \times 0.25 \times (8760 \text{ hours/year}) = 0.188\% \text{ per year}$$

PRELIMINARY

②

ENVIRONMENTAL TESTS

Test Name	MIL-STD-883C Reference	Test Conditions	Units Tested	Units Failed
Temperature Cycle	1010	-55° C to 100° C; 15 min. dwell, 5 min. transfer. 20 cycles 100 cycles	9,200 9,199	1 1
Solder Heat Resistance	2003	Sn 60, pb 40, solder at 260° C for 5 seconds	9,200	0
Resistance to Solvents	2015	Solvent tested: 1-1-1 Trichlorethane, freon, TMC, 1/4 Isopropyl alcohol and 3/4 mineral spirits	134	0

MECHANICAL TESTS

Test Name	MIL-STD-883C Reference	Test Conditions	Units Tested	Units Failed
Mechanical Shock	2002	3 shocks each X ₁ , X ₂ , Z ₁ , Z ₂ , Y ₁ , Y ₂ axis, 3000 g; 0.3 msec.	60	0
Vibration Variable Frequency	2007	4 cycles, 4 minutes each X, Y, Z axis, 20 g minimum. 20 to 2000 Hz	60	0
Terminal Strength	2004 Cond. A	1 lb. for 10 seconds	117	0
Lead Fatigue	2004 Cond. B	3 oz., 3 x 30°	48	0
Physical Dimensions	2016	Device profile at 20X	47	0

Notes:

- [1] The point typical MTBF (which represents a 60% confidence level) is simply the total device hours divided by the number of failures. In the case of zero failures, one failure is assumed for this calculation
- [2] The 90% Confidence MTBF represents the minimum level of reliability performance which is expected from 90% of all samples. This confidence interval is based on the statistics of the distribution of failures. The assumed distribution of failures is exponential. This particular distribution is commonly used in describing useful life failures. Refer to MIL-STD-690B for details on this methodology.
- [3] A failure is any LED which does not emit light.

PRELIMINARY

Hewlett Packard GmbH
Components Marketing Operation
Application Lab Europe
Herrenberger Str. 124
7030 Boeblingen
Phone: [49] 7031 14-3635
Fax: [49] 7031 14-2216



Urgent Fax

Oct. 6th 1992

TO: Richard Fullalove
FROM: Uwe Thomas
Applications Engineer

PAGE 1 OF 2

SUBJECT: Respond on request for failure data on LED displays

Dear Mr. Fullalove,

I have received your fax and will answer to your questions as good as I can.

1)
Under normal operating conditions a short was never seen with our LED's. To produce a short the anode lead has to be connected to the cathode lead anyhow during operation. Because the mechanical arrangement is encapsulated with epoxy, it is impossible to bring the anode mechanical together with the cathode. The only thing I can think about, is a very high voltage applied to the leads which creates an ion track through the epoxy. At this point the chip is cracked (open) already due to the high electrical field and the 1,2mil thick wire bond will be evaporated already. Anyway this is far away from our specifications. Because Hewlett Packard monitors intensity, forward voltage and reverse voltage (at 100 uA) from every LED possible failures will be observed and bad LED's will be rejected.

2)

The graphs you send to me are looking like temperature dependend forward characteristics of a LED. With higher temperatures in a semiconductor an increasing amount of electrons is freed inside the crystal. Thus the step voltage becomes smaller and the internal resistance degrees. But this is related to temperature only and not to any leakage.

3)

Degradation is a natural thing in semiconductors. Depending on materials which are used to grow the crystal and how they are doped, degradation behaves different. Also differnt package styles are influenting degradation due to different package expansion which stresses die and wire bond. Besides this the photon current inside the chip an electron current flows always due to the never 100% clean crystal material. Stress over time increases the electron current and therefore degreeses photon current. The human eye is insensitive to a change in light output when the factor of change is not bigger than 2:1. Thus degradation of intensity has to be bigger than 50% to detect it with the human eye. Inside Hewlett Packard a LED is defined as failed, when light output degrades more than 50%! HP monitors degradation after 24h, 168h, 500h, and 1000h operating time under different extreme temperatures / drive currents and moisture stress conditions, to make sure that degradation of our devices behaves stable. Typical degradation after 1000h may be 30%. Degradation behaves like a e-function and therefore after 1000h degradation changes not much anymore.

If you require any additional specific data please let me know.

Best regards

Uwe Thomas

Mr.R.M.Fullalove
Dept. Elec.Eng.
University of Cape Town
Rondebosch
7700
South Africa
28 October 1992

Ph: [27]21 650 2813
Fax: [27]21 650 3465

E-mail: rfull@eleceng.uct.ac.za

The Chairman
Working Party 3 of ORE A155 Committee
Office for Research and Experiments
International Union of Railways
Oudenoord 500
3513EX
Utrecht
Netherlands

Dear Sir;

QUERIES RELATED TO FAILURES IN LIGHT EMITTING DIODES

Referring to Report 12 (Question A 155.3), Failure catalog for electronic components, I wish to query some of the documented LED failure modes on page 68.

In discussions with applications engineers at Hewlett Packard, it was revealed that they have never experienced short-circuits in their LEDs, due to the manner in which they are constructed. The leads to the LED dice are suspended within a clear epoxy matrix, which prevents a broken lead from dropping across the dice.

Intermittent failures and open circuits (breaks) are recognised to exist by Hewlett Packard.

I assume that increasing leakage current is taken to mean reverse leakage current under reverse-biased conditions. Could you please clarify this? If it refers to increasing forward current, then this is a temperature induced effect, since the dynamic resistance of the diode has a negative temperature coefficient.

I assume that the increasing resistance failure refers to the increase in dynamic resistance under forward-biased conditions. If so, then this is also a temperature-induced effect.

Consulting Hewlett Packard Data sheets on LED displays, I discovered that over a temperature range of -10deg to +55degC, the forward voltage varied from 1.674 to 1.554V. Also, a variation in forward current from 10mA peak to 200mA peak resulted in an increase in luminous efficiency from 85 % to 115 % (a phenomenon known as super-luminescence).

This change of 30 % is less than the 50 % required for the human eye to notice a difference.

It is also documented that a decrease in light intensity of the LED is an ageing process, and not spontaneous. Typically, LED intensity will drop to 50 % of the original level after 100,000 hours (a conservative figure quoted by Hewlett Packard). This is not noticeable to the human eye. Would it not be prudent to adopt a Reliability Centred Maintenance policy for this particular failure mode? Your opinion on this issue would be gratefully appreciated.

I would thus like to query the validity of these failure modes, and would appreciate feedback from you on whether they could be ignored in special cases.

I would like to point out that I am doing post-graduate research for the South African Railways on a fail-safe

display system for a locomotive cab-signalling application, and have chosen LED displays.

I also understand that other opto-electronic applications of LEDs may not be able to ignore these failure modes. For instance, in an optical isolator, a drop in LED intensity might not be noticeable to the human eye, but may cause the opto-isolator to switch erroneously.

Therefore, my queries refer only to the application of LEDs as displays.

If possible, could you give me your Fax number, and if available, an Electronic Mail address where I can contact you or other committee members in the future?

Kind Regards,

Richard M.Fullalove



Your reference

Your letter dated

Our reference

A 155.52
WRS/HC

Enclosures

1

Subject

Queries related to failures in LEDs

Mr R.M. Fullalove
Dept. Elec.Eng.
University of Cape Town
Rondebosch
7700
South Africa

Utrecht, 1992-11-11

Dear Sir,

I am answering your letter of 28 October 1992 as the ORE A 155 Committee was wound up in 1989 when its work was completed.

As explained in the text of the report, the catalogue was based on the experience of the railways at the time. It lists failures which must be considered in design of safety circuits. If you can be sure, from the physical construction of the component and the way it is applied, that a given failure mode cannot occur, then it may be disregarded, but such things as, for instance, voltage spikes causing breakdown of a diode, must be considered. You are correct in assuming that increasing leakage current is that under reverse-biased conditions.

As regards decrease in light intensity, the information you have is probably more extensive than that on which the catalogue was based, and on the information you quote, I agree that periodic replacement would probably be the best policy; in deciding the period, however, ambient conditions, particularly temperature, will probably be relevant.

Enclosed is a card giving our new name, address, telephone and fax numbers. We are not yet equipped for electronic mail.

Yours faithfully,

W.R. SMITH
Deputy Director of ERRI (Technical and Production)

APPENDIX F: Component Calculations

F.1) Display Module Component Selection

In order to design a 16-segment alphanumeric display with 16 digits, the HDSP-6508 (or equivalent) was selected, since this display type is readable from up to 2m with a reasonable viewing angle.

The minimum refresh rate for a multiplexed display before serious flicker occurs is 25Hz. In order to avoid any possibility of this flicker, a refresh rate of $f_R=50\text{Hz}$ was selected, giving a refresh period $T_R=20\text{ms}$.

Although there are 2 "dummy" test digits, these are selected relatively infrequently, and thus do not form part of the major display refresh loop timing calculations. Thus, pulse duration per digit is: $t_p=20\text{ms}/16=1.25\text{ms}$.

However, not all this time is spent in lighting the accessed digit, since the data has to be fetched and latched. Therefore subtract $150\mu\text{s}$ (an estimate of 150 instructions @ 12MHz @ 12 clock cycles per instruction) - this figure will change once the software is written and the exact number of instructions determined. Therefore, effective pulse duration $t_p=1.1\text{ms}$ (5.5 % duty cycle). Referring to the HDSP-6508 data sheet [30], peak segment current, $I_p=60\text{mA}$ @ $t_p=1.1\text{ms}$ @ $f_R=50\text{Hz}$.

Derate this to 50mA for design purposes, since performance curves for the ULN2803A (Digit Select Switch) do not extend to current levels of $16*60\text{mA}=960\text{mA}$. Therefore, $I_p=50\text{mA}$ per segment. Relative luminous efficiency (Luminous Intensity in Candela per unit Current) at this value is $\eta_R=105\%$. LED forward voltage, $V_F=1.65\text{V}$ @ 50mA. Maximum LED forward voltage, $V_{F(\text{max})}=1.85\text{V}+I_p*1.8\Omega=1.94\text{V}$.

APPENDIX G: Failsafe Signalling System Design

G.1) Failsafe Systems

All electronic components and systems have a finite probability of failure, including failsafe systems. However, failsafe systems use techniques to ensure that a failure will result in the system reverting to a safe (predictable) state. All failsafe systems have a probability of failure to an unsafe (unpredictable) state. This is referred to as the probability of a wrong-side failure, and must be minimized as far as possible using failsafe engineering techniques. The safety of the system (probability of wrong-side failures) can be derived from the mean time between failure of the system and the detection time of the first failure.

G.2) Safety Rules

when designing a failsafe system, it is assumed that all possible failures, at a component and system level, are *clearly identified*. There must be no design errors which will cause undetected failures [5],[6]. The time taken from the occurrence of a failure to its detection is referred to as the *fault detection time*. It is assumed that failures are independent, and that all first failures, if undetected, will cause an unsafe operation of the system. Any subsequent failure will render the first failure undetectable or cause the system to be unable to revert to a safe state.

All first faults influencing system safety must be detected within the fault detection time. Two (or more) *independent* failures cannot be allowed to occur *simultaneously*. By extension, the probability of two independent failures occurring in succession during the fault detection time of the first failure must be negligible. Failure to enforce this could lead to the system reverting to unsafe operation.

The effect of failures whose detection times are significant, must be examined in conjunction with all other failures. The effects of *interrelated* failures must be combined. These interrelated failures can be minimized by providing separate power supplies and galvanically isolating subsystems. Failure detection techniques for electronic equipment can include some, and maybe all, of the following approaches:

implemented in the signalling interlocking, is concerned with the prevention of conflicting routes or commands, undetected system failures, and any other system events that may present a danger to passengers and railway personnel. Safety can be differentiated into *absolute safety* (zero risk, statistically impossible to ensure over infinite time), and *practical safety* (minimized risk).

Practical safety is attainable by means of *signalling principles* that are enforced by *people and equipment*. In order for the signalling system to function correctly as a whole, the people (signal operators and drivers) are required to abide by signalling *rules and regulations* which are acquired through *training and experience*. The equipment must be designed to *specification* and *engineered* to be safe. Under *normal conditions* for both personnel and equipment, the system will lock points in the route before clearing a signal and hold them locked until the train passes. Collision avoidance is achieved through correct block working and interlocking to prevent the authorization of conflicting movements. Under *failure conditions*, a *threefold defense* of fail safety, high reliability, and non-provocation exists.

High reliability is ensured by selecting system components that are guaranteed with a very high likelihood to perform correctly over a predetermined service life. This is enhanced by robust design and operation below maximum limits. *Non-provocation* is implemented in the training and discipline of personnel as well as preventive design within the interlocking, in order to ensure that conflicting commands and train movements are not authorized. Historical experience with previous incidents also play a major part in compiling a database of wrong procedures and actions to avoid.

Failsafe equipment can either fail to the *wrong side*, (undetected failure, unsafe), or to the *right side*, (detected failure, possibly unsafe if ignored). It is an essential goal of failsafe system design to minimize the probability of wrong-side failures and maximize the probability of right-side failures in the event of system malfunction. In the event of a safe failure, the system can be made to *stay as last set*. This is applied to points machines, which cannot be allowed to move under failure conditions until the fault is cleared. Alternatively, the system could revert to a *no less restrictive* state. This situation applies to a signal, which would revert from a proceed aspect (green) to a red (more restrictive) aspect. These two states can either be achieved by *inherent safety* or *composite safety*.

condition occurrence rate for the system design according to its component failure rates and interconnections. Identify the potential for correlated failures, possibly by using fault trees and Markov models. Iterate the design as necessary, to meet the required MTBWSF. A preliminary reliability, safety, and Failure Modes, Effects and Criticality Analysis of the system hardware is covered in Chapter 8 (System Reliability) for this thesis. FMECA charts are listed in Appendix B.

- *Software Validation:* Set up and enforce a software validation and verification program spanning the specification, design, development, test, and acceptance process. Software safety is not discussed at present as no software has been written at this stage. Methods for verifying and validating safe system software are being developed, and will be implemented [11].
- *Integration and Acceptance Tests:* Plan and perform tests to show that the function and safety of the complete system meet all the requirements established. The tests must cover all safety-critical functions, and complete records of the testing must be kept, not only to document the steps taken, but also to make it easier to test future system modifications. Limited (static) tests will be performed for this thesis.
- *System Maintenance:* Ensure the safety of the system when making modifications to repair deficiencies or to improve functions and features.

APPENDIX H: Reliability Calculations

H.1) SYSTEM-LEVEL RELIABILITY ESTIMATION

The initial estimation of system reliability is based on the system block diagram in Figure 19. Reliability is defined as the probability that an item will operate correctly under prescribed conditions for a prescribed time. Failure rate is defined as the fraction of items failing per hour at time t . The failure rate follows the classic bathtub curve [5],[18]. Failures in the infant mortality region are due to manufacturing and design faults. In the operational lifetime region, failures occur randomly at a low, constant rate (λ). In the wear-out region, the failure rate increases exponentially. Reliability is calculated over the operational lifetime, using a constant failure rate, λ , and assuming Mean Time To Failure (MTTF) equal to the MTBF. It is also assumed that the *maintenance action rate*, $\mu > \lambda$. The Mean Time To Repair (MTTR = $1/\mu$) is 30 minutes, as required by the user.

The system MTBF for the Failsafe Display System was given provisionally as 10 000 hours by the user, with the understanding that this figure may in fact be lower in a practical implementation. It was stated that if the system MTBF is lower than 10 000 hours, it shall not result in a system MTBWSF lower than 10^7 years.

The reliability diagram for the 2-out-of-2 comparative system in Figure 19 is a relatively simple block diagram of two identical subsystems with each of the modules connected in *series*. Each module and both subsystems are critical components of the system, and a failure in any one must result in safe system shutdown. No redundancy (i.e. parallel connections) is allowed in this particular case. The system Mean Time Between Failure (MTBF) is calculated by adding the individual module failure rates, and then inverting the result.

$MTBF_{\text{system}} = 10\,000$ hours (provisional figure provided by user).

$\lambda_{\text{system}} = 1/10\,000 = 10^{-4}$ failures per hour = 100 failures/ 10^6 hours.

The Segment and Digit Modules are expected to make the greatest contribution to overall system failure rate. This is due to the relatively high discrete component count and the liberal use of optocouplers. More specifically, the Segment Module has a relatively high parts count

count due to the use of quasi-analog circuitry (window detectors/comparators) to perform the display LED proving function. The Digit Module has an opto-coupler parts count that is proportional to the number of digits desired in the display.

The Display Module will have a low parts count, made up of extremely high reliability LED displays, based on information from the data sheets [30]. The Power Module is also expected to have a low parts count, using very high reliability (though subjected to higher voltage stresses) hybrid-module DC-DC converters. The Control Module is expected to have a fairly high parts count. However, all devices will operate at 5 Volts, and few opto-couplers are expected to be used here. Based on an estimated parts count/stress level estimation for each module, the following estimated module failure rates, in failures/ 10^6 hours, will result in the provisional system failure rate given by the user:

Segment Module: $\lambda_{\text{SEGMOD}} = 40 \text{ failures}/10^6 \text{ hrs.}$

Digit Module: $\lambda_{\text{DIGMOD}} = 35 \text{ failures}/10^6 \text{ hrs.}$

Display Module: $\lambda_{\text{DISMOD}} = 2 \text{ failures}/10^6 \text{ hrs.}$

Control Module: $\lambda_{\text{CONMOD}} = 13 \text{ failures}/10^6 \text{ hours.}$

Power Module: $\lambda_{\text{PWRMOD}} = 10 \text{ failures}/10^6 \text{ hours.}$

The corresponding module MTBFs are calculated by inverting the estimated module failure rates and then multiplying by 10^6 :

$\text{MTBF}_{\text{SEGMOD}} = 25\,000 \text{ hours.}$

$\text{MTBF}_{\text{DIGMOD}} = 28\,570 \text{ hours.}$

$\text{MTBF}_{\text{DISMOD}} = 500\,000 \text{ hours.}$

$\text{MTBF}_{\text{CONMOD}} = 76\,920 \text{ hours.}$

$\text{MTBF}_{\text{PWRMOD}} = 100\,000 \text{ hours.}$

The maximum allowable failure detection time required for a MTBWSF of 10^7 years, given the provisional MTBF of 10 000 hours and a 2-out-of-2 configuration is [5]:

$$\tau \approx \frac{\text{MTBF}^2}{2 \cdot \text{MTBWSF}} = \frac{(10^4 \text{ hours})^2}{2 \cdot (10^7 \text{ years})} = 2.05 \text{ seconds} \quad (1)$$

H.2) MODULE-LEVEL RELIABILITY CALCULATIONS

Once the module-level design had been completed, a more precise module-level reliability analysis was required. This analysis was based on actual components to be used in the system, as well as exact component counts. Using this process, it was possible to compare actual reliability figures with estimates based on the system configuration block diagram and provisional requirements provided by the user. Relevant *parameters* for calculating failure rates are obtained from [31], and are as follows:

λ_p	= Device base failure rate (in Failures/ 10^6 hours).
λ_b	= Base failure rate.
π_Q	= Quality factor (commercial, plastic DIP).
π_T	= Temperature acceleration factor (40°C ambient).
π_V	= Voltage stress derating factor (max stress of 50%).
π_E	= Environmental factor (ground, mobile environment).
C_1	= Circuit complexity factor (No. of devices/gates/bits).
C_2	= Package complexity factor (No. of pins).
π_L	= Device learning factor (established devices)
π_A	= Application factor (Zener diode, BJT switch).
π_R	= Power range factor (low, medium, or high power).
π_{s2}	= Voltage stress factor of transistor.
π_C	= Transistor type (single, dual, Darlington).
π_{CV}	= Capacitance range factor.
π_P	= Pin count factor for connectors.
π_K	= Cycle factor (connector matings per 1000 hours).
N_R	= Number of resistors used in network package.

It is assumed that discrete devices operate at 50% of maximum current, voltage or power. The discrete devices generally have much higher maximum voltage ratings than the 5V at which they will run in this application. Digital ICs will run at their rated voltage. A mean junction temperature of 60°C and mean ambient temperature of 40°C is assumed. The environmental classification is **ground, mobile**. Only commercial quality plastic packaged devices of well-established technology are specified, unless unavailable.

Calculated failure rate λ_p , in failures/10⁶ hours, for the devices used in the Segment Module, Digit Module, and the Display Module are shown below:

Integrated circuits:

$$\begin{aligned}\lambda_p &= \pi_Q(C_1\pi_T\pi_V+C_2\pi_E)\pi_L \\ &= 20 \times (.01 \times 4 \times 1 + .0026 \times 4.2) \times 1 = 1.018 \quad (\text{For LM339}) \\ &= 20 \times (.01 \times .95 \times 1 + .008 \times 4.2) \times 1 = .8620 \quad (\text{For 74HCT573}) \\ &= 20 \times (.01 \times .95 \times 1 + .008 \times 4.2) \times 1 = .8620 \quad (\text{For 74HCT541})\end{aligned}\quad (2)$$

Opto-electronic devices:

$$\begin{aligned}\lambda_p &= 10 \quad (\text{TLP521-4 Data Sheet}) \\ &= 10 \quad (\text{TLP523-4 Data Sheet}) \\ &= 0.5737 \quad (\text{HDSF-6508 Data Sheet})\end{aligned}\quad (3)$$

Diodes: (Zener, 30% power stress)

$$\lambda_p = \lambda_b\pi_E\pi_A\pi_Q = .0009 \times 18 \times 1.5 \times 30 = .7290 \quad (4)$$

Octal Darlington Array: (switch, <1W, 30% rated V_{ceo} , 70% power stress)

$$\begin{aligned}\lambda_p &= \lambda_b\pi_E\pi_A\pi_Q\pi_R\pi_{S2}\pi_C = .0038 \times 18 \times .7 \times 12 \times 1 \times .3 \times .8 = .1379 \text{ per device} \\ &= 8 \times .1379 = 1.1032 \text{ per package}\end{aligned}\quad (5)$$

Resistors: (single, metal film, $R < 100K$, 30% rated power)

$$\lambda_p = \lambda_b\pi_E\pi_R\pi_Q = .0012 \times 7.8 \times 1 \times 15 = .1404 \quad (6)$$

Resistors Networks:

$$\begin{aligned}\lambda_p &= .00066 \cdot N_R\pi_T\pi_E\pi_Q \\ &= .00066 \times 8 \times 4.2 \times 7.8 \times 3 = .5198 \quad (\text{For 8-Resistor Networks}) \\ &= .00066 \times 7 \times 4.2 \times 7.8 \times 3 = .5198 \quad (\text{For 7-Resistor Networks})\end{aligned}\quad (7)$$

Capacitors: (plastic, fixed, 100nF, 85°C max, 10% rated Volts)

$$\lambda_p = \lambda_b\pi_E\pi_{CV}\pi_Q = .00063 \times 7.8 \times .97 \times 10 = .04767 \quad (8)$$

PCB Connectors: (64-pin, DIN41612)

$$\lambda_p = \lambda_b\pi_E\pi_p\pi_K = .00037 \times 17 \times 17.69 \times 2 = .2225 \quad (9)$$

Failure rates for devices in the Segment, Digit, and Display Module are shown in the table below, along with their quantities and resultant total failure rates per device type.

DEVICE	DESCRIPTION	Qty (N)	λ_p	$\lambda_{tot} = N * \lambda_p$
LM339	Quad Comparator	16	1.018	16.29
74HC573	Octal Latch	5	.8620	4.310
74HC541	Octal Tristate Buffer	10	.8620	8.620
TLP521-4	Quad Optocoupler	20	10.00	200.0
TLP523-4	Quad Opto-Darlington Coupler	4	10.00	40.00
HDSP-6508	8 Digit, 16-Segment LED Display	2	.5737	1.147
ZENERS	Reference Zener Diodes	36	.7290	26.24
ULN2803A	Octal Darlington Drivers	3	1.103	3.310
METAL RES.	Metal Film resistors	20	.1404	2.808
RES.NET-8	8-Resistor Networks	25	.5198	13.00
RES.NET-7	7-Resistor Networks	16	.5198	8.317
CAPACITORS	Wima Capacitors	15	.0477	.7150
CONNECTORS	DIN41612 (Eurocard) 64 pin Connectors	8	.2225	1.780
TOTALS:			λ_{total}	326.5

Component type failure rates are multiplied by the component type quantity. The individual component type failure rates are summed to give a total failure rate, λ_{total} :

$$\lambda_{total} = \sum_{i=1}^n N_i \cdot \lambda_{p_i} \approx 327 \text{ Failures/ } 10^6 \text{ hours} \quad (10)$$

At present the total failure rate represents the system failure rate of the Segment, Digit, and Display Modules only. (Since the Control Module design is not finalised, the calculation of the total failure rate is incomplete). From λ_{total} , the system MTBF is calculated:

$$MTBF = \frac{10^6}{\lambda_{total}} \approx 3058 \text{ hours} \quad (11)$$

This figure falls short of the users provisional requirement of $MTBF = 10\,000$ hours. This can be expected, given the relatively high failure rate contribution of opto-couplers to the system in order to provide statistical independence, and hence, safety. The system safety for the 2-out-of-2 configuration may still exceed the users requirement of $MTBWSF = 10^7$ years, provided that the fault detection time is sufficiently short:

$$MTBWSF_{2/2} \approx \frac{MTBF^2}{2 \cdot \tau} = \frac{3058 \text{ hours}^2}{2 \times .192 \text{ seconds}} = 10^7 \text{ years} \quad (12)$$

Where τ = maximum allowable time delay to fault detection = 192 ms. Therefore, it is possible to fulfill the users requirement for system safety, provided the maximum allowable fault detection time is not exceeded.

APPENDIX I: Test Results

Function:	Sub-Function:	HSDT	LSDET	HSDRV	LSDRV	HDDT	MDDT	LDDT	HDDRV	MDDRV	LDDRV	AD7	AD6	AD5	AD4	AD3	AD2	AD1	AD0
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
character " " at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Digit 9 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 9	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	0
	Latch digit 9 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	0
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
character "D" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0
Digit 10 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 10	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	0	1
	Latch digit 10 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	0	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	0	0
character "I" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	1	1	0	0	1	1	0	0
Digit 11 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 11	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	0	1	1
	Latch digit 11 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	0	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	1	0	0
character "S" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	0	1	0	0	0	1	0	0
Digit 12 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 12	1	1	0	0	1	1	1	0	1	0	1	1	1	1	0	1	1	1
	Latch digit 12 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	1	1	1	0	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	0	0	0
character "P" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1	0	0	0
Digit 13 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 13	1	1	0	0	1	1	1	0	1	0	1	1	1	0	1	1	1	1
	Latch digit 13 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	1	1	0	1	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1
character "L" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1
Digit 14 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 14	1	1	0	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1
	Latch digit 14 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	1	0	1	1	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	0	0	1	1	0	0	0	0
character "A" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	0	0	1	1	0	0	0	0
Digit 15 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 15	1	1	0	0	1	1	1	0	1	0	1	0	1	1	1	1	1	1
	Latch digit 15 (MDDRV)	1	1	0	0	1	1	1	0	0	0	1	0	1	1	1	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1
Select segments	Clear display	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
to display the	Select segments 1-8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
character "Y" at	Latch segments 1-8	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Digit 16 in the	Select segments 9-16	1	1	1	0	1	1	1	1	1	1	1	0	1	0	1	0	1	1
display.	Latch segments 9-16	1	1	0	0	1	1	1	1	1	1	1	0	1	0	1	0	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Latch LDDRV & HDDRV	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
	Select digit 16	1	1	0	0	1	1	1	0	1	0	0	1	1	1	1	1	1	1
	Latch digit 16 (MDDRV)	1	1	0	0	1	1	1	0	0	0	0	1	1	1	1	1	1	1
	Reset data bus to 1's	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1