

# UC Berkeley

## Research Reports

### Title

Power System Reliability for Precision Docking and Electronic Guidance Systems

### Permalink

<https://escholarship.org/uc/item/3qg2r5f4>

### Authors

Nesgaard, Carsten

Sanders, Seth

Zhang, Wei-Bin

### Publication Date

2005-11-01

CALIFORNIA PATH PROGRAM  
INSTITUTE OF TRANSPORTATION STUDIES  
UNIVERSITY OF CALIFORNIA, BERKELEY

## **Power System Reliability for Precision Docking and Electronic Guidance Systems**

**Carsten Nesgaard**  
**Seth Sanders**  
**Wei-Bin Zhang**

**California PATH Research Report**  
**UCB-ITS-PRR-2005-38**

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation, and the United States Department of Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

Final Report for RTA 64A0028

November 2005

ISSN 1055-1425

# **Power System Reliability for Precision Docking and Electronic Guidance Systems**

## **Part III report for Development of Precision Docking Function for Bus Rapid transit**

Carsten Nesgaard, Seth Sanders and Wei-Bin Zhang

### **1. Introduction**

BRT has demonstrated its effectiveness to be a portion of the ‘backbone’ of an integrated transit network. It has become an effective means for attracting non-traditional transit riders and therefore can help to reduce urban transportation needs and traffic congestion. Many California transit agencies are planning to deploy BRT and have considered the use of dedicated lanes for BRT to be a very attractive option as it is less affected by automobile traffic and therefore can provide rail-like quality of service. In 1999, Caltrans generated a Caltrans Action Request (CAR) to request participation in the Bus Rapid Transit Project with VTA and other local transit providers. The future of BRT in California, as envisioned by Caltrans, would include a system of coordinated transit infrastructure, equipment, and operations that will give preference to buses on local urban transportation systems and the High Occupancy Vehicles (HOVs) lanes at congested corridors. The goal of the BRT service is to attract riders from single-occupancy vehicles, which could result in congestion relief without major infrastructure expansion. In the long-term, the proposed project may integrate the currently separate local transportation systems and transit services (offered by multiple transit agencies in a region) to provide express transit services enabled by interconnectivity between local systems and the State highway HOV system. Under the Caltrans Action Request, a BRT research program is established. One of the elements of this program is “Development of Precision Docking Function for Bus Rapid transit (named ‘Precision Docking’ or BPD from hereon)”.

Precision docking -- an innovative technology that enable bus to perform rail like level boarding has shown great potential for allowing fast boarding and alighting and therefore reducing the total trip time and improving service reliability and quality for BRT system. The bus precision docking seeks to achieve, with the help of electronic guidance technologies, a high docking accuracy and consistency that allows fast loading and unloading of passengers with special needs. In addition to the potential of serving as a major component of an advanced bus stop, such an automation capability would also reduce the skill and training requirements on the bus driver as well as the stress associated with achieving the high accuracy by the driver. In addition to precision docking, electronic guidance technologies also support a number of critical functions for BRT and transit applications. Once a bus is instrumented with electronic guidance, it can provide lane assist along dedicated BRT lanes. In the applications where dedicated lanes are not available, lane assist can facilitate efficient operation at Queue Jump Lanes and can significantly benefit Bus Priority Systems. Electronic guidance can also support application at a bus depot where BPD technology can be useful as a component of the concept of Advanced Maintenance Station.

PATH has demonstrated precision docking function on automobiles. The objective of the BPD project is to develop and enhance the precision docking system for real-world bus operations. At the project early stage, Caltrans and PATH have decided to develop and demonstrate automated BRT using three automated buses (Demo 2003). Because of the synergy of these two programs, and due

to the safety critical nature of precision docking/lane assist functions, PATH and Caltrans have determined to focus this project to safety designs of precision docking system. The two projects will complement each other and the mutual goal is to accelerate the deployment of precision docking/lane assist technologies.

This final reports the fault analysis of precision docking system and safety design of the safety critical elements for precision docking system. The report includes three Parts, including:

Part I provides a description of the Precision Docking System and reports analysis for fault diagnosis and safety design of automated steering controller and Electronic Control Unit (ECU) for steering actuator. It also reports a demonstration PATH conducted during the National Intelligent Vehicle Initiative demonstration organized by the US Department of Transportation Joint Program Office.

Part II report an analysis and design for a reliable direct drive for the steering wheel column of buses.

Part III reports power system reliability.

The report below is the Part III report: Power Reliability.

## **2. Power system configuration:**

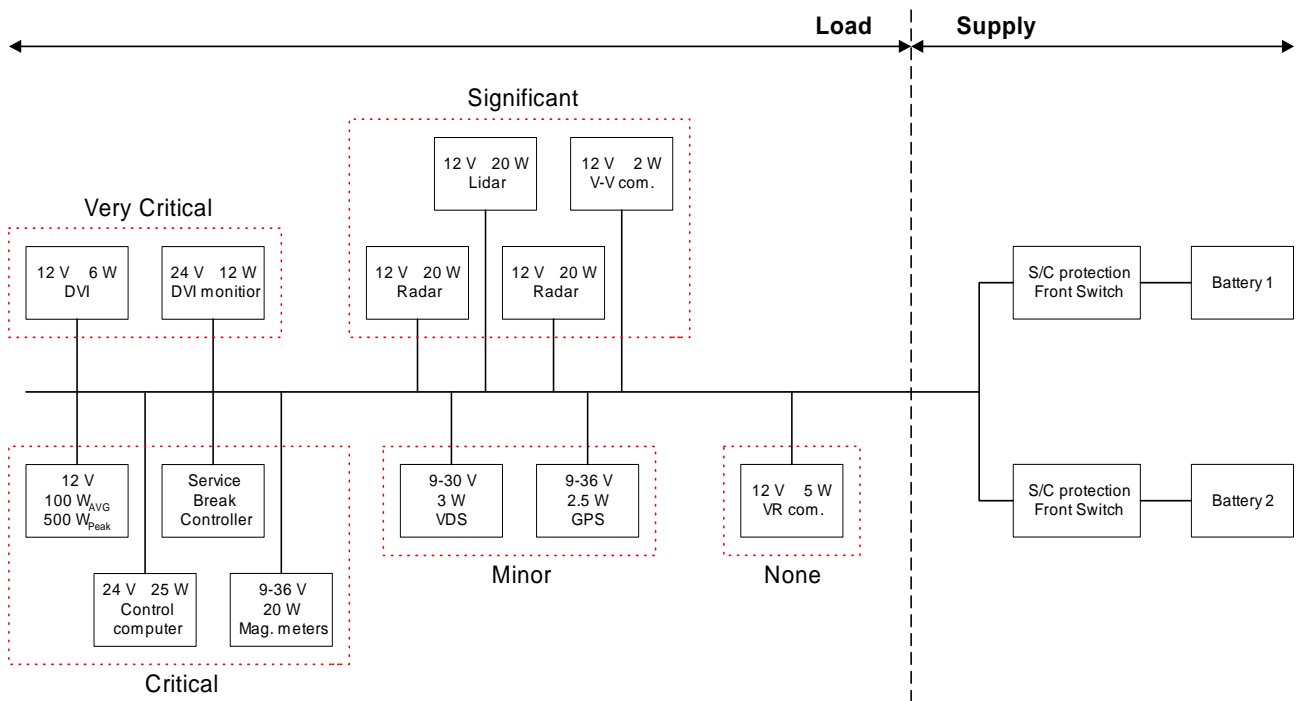
The power system is one of the most critical parts of almost any system. Due to the sever consequences of a guidance system failure in the application at hand it is of vital importance to ensure a stable and continuous output voltage to the subsequent systems. This report contributes to an identification of critical parts of the power system as well as to a classification of techniques for increasing the overall power system reliability.

To comply with the general guidelines of the UpTime Institute the input power has to come from at least two different and independent sources. This is a rather stringent requirement that limits its implementation to systems comprised of multiple power sources. In systems with only a single power source these guidelines are not applicable for which reason such systems cannot be classified as fault tolerant. However, even if the system cannot be classified as fault tolerant from a system point of view does not prevent it from being fault tolerant at a subsystem level. Furthermore, even though true fault tolerance might not be obtainable, improvements to the overall system reliability is still possible by means of different techniques.

In this particular application the failure rate of the battery is very low – meaning that the challenge in terms of reliability is the voltage conversions to the interconnected subsystems.

This report will provide an examination of the power system with intend to optimize reliability as well as overall system performance. The foundation of the analysis is a Functional Failure Modes Effects and Criticality Analysis (FFMECA) followed by a description of hardware redundancy implementations. The FFMECA is performed at a block level and indicates a prioritized criticality evaluation of each block.

In order to establish the criticality of the power system the following configuration has been established:



**Figure 1 : Power system criticality analysis**

The individual blocks are rated according to the following criticality list:

- 1 **Very critical** (This block is essential for human safety)
- 2 **Critical** (Loss of this block causes system malfunction)
- 3 **Significant** (Loss of this block causes important system degradation)
- 4 **Minor** (Loss of this block causes only minor system degradation)
- 5 **None** (Loss of this block has no effect on overall system performance might cause a surveillance circuit to loose power)

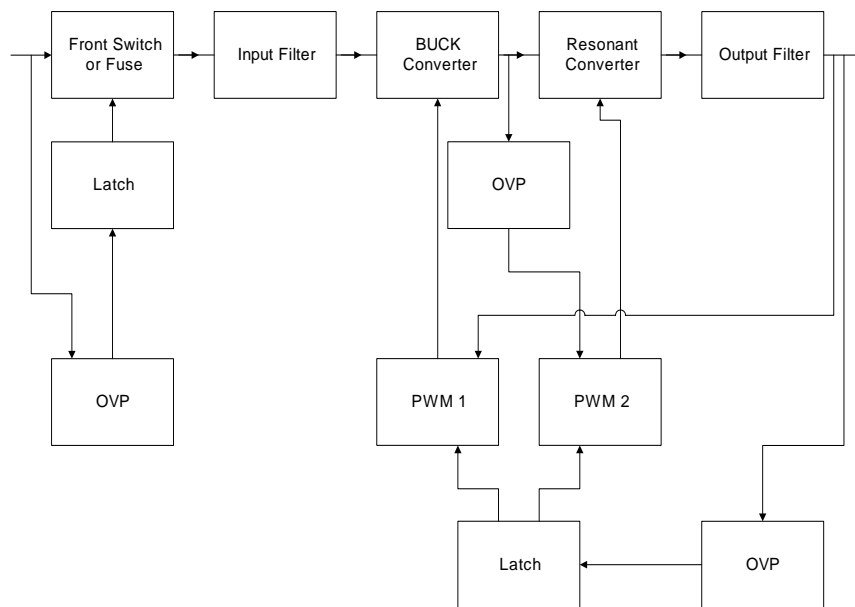
Based on above list the following Functional Failure Mode Effects and Criticality Analysis is established:

Block	Functional effect	Voltage level	Criticality	Power rating
Control computer	System malfunction	24V	2	25W
Differential GPS system	Loss of exact location	9-36V	4	2.5W
Driver vehicle interface	Loss of control	12V	1	6W
Lidar	Deteriorated avoidance system	12V	3	20W
Magnetometers	Loss of guidance	9-36V	2	20W
Radar	Deteriorated avoidance system	12V	3	20W
Safety monitor computer	Loss of control	24V	1	12W
Service brake controller	System malfunction	-	2	-
Steering actuator	Loss of steering	12V	2	100W (500W)
Vehicle dynamics sensor	Loss of motion detection	9-30V	4	3W
V-R communication	Loss of roadside communication	12V	5	5W
V-V communication	Loss of avoidance communication	12V	3	2W

### 3. Preliminary topology evaluation:

Due to the severity of certain system malfunctions a high degree of overall system reliability is required. To further increase the overall reliability fault resilience is build into the electrical design

resulting in a single point failure free system. The proposed converter design that complies with the latter requirement is shown Figure 2.

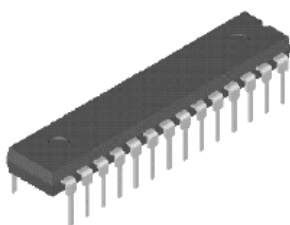


**Figure 2 : Individual converter realization**

The system is comprised of a buck converter followed by a resonant converter operated at a 50% - 50% duty-cycle - thus serving as a DC-DC transformer. To ensure that no single failure can short out the input power bus a front switch is inserted in series with each individual converter. This front switch also serves as a current limitation during system startup and/or converter replacement. Controlled converter shut-down in case of fault occurrence is ensured by the build in latch, which also prevents the system from operating in a state where one or more converters are trying to restart after being shut-down (hick-up mode).

#### 4. Reliability considerations:

Considering the individual component failure rates it becomes apparent that the reliability of the entire system is determined by the component/components most likely to fail. For this reason this section provides the reliability data for the three most unreliable components – the controller IC, the MOSFET transistor and the filter capacitors.



**Controller IC**



**MOSFET transistor**



**Filter capacitor**

The probability of component survival for a specified period of time (survivability) of the three components is calculated based on the following assumptions:

- The control IC considered is a standard controller for DC/DC converter applications and is comprised of approx. 3,500 transistors.
- The switching device under consideration is a standard low voltage MOSFET transistor (64V) for use in switching applications with power ratings up to 100W.
- Due to the requirements of fairly low output voltage ripple a large amount of capacitance is needed at the system output. For this reason the capacitors considered are electrolytic capacitors with a voltage rating complying with the standard derating requirements of 75%.

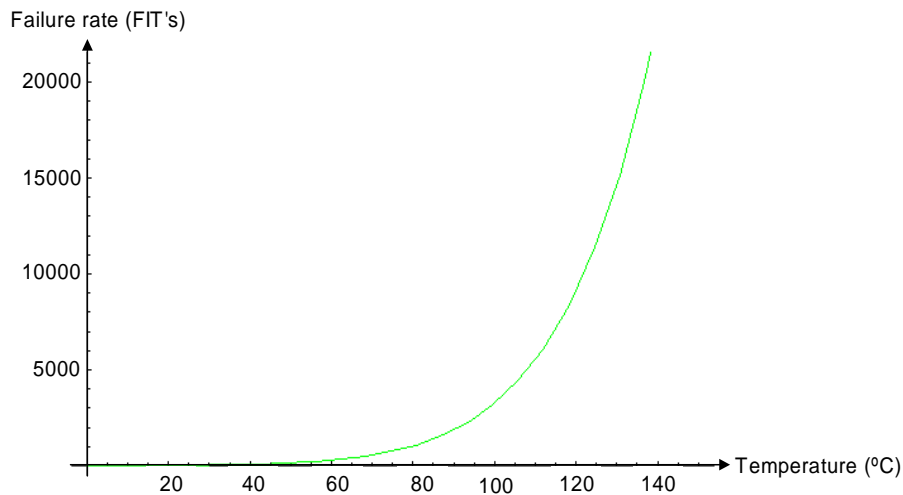
Using the point failure rate estimates found in MIL-HDBK-217 the following three equations can be deduced:

$$\lambda_{\text{MOSFET}} = 120 \cdot e^{-1925 \cdot \left( \frac{1}{T+273} - \frac{1}{298} \right)}$$

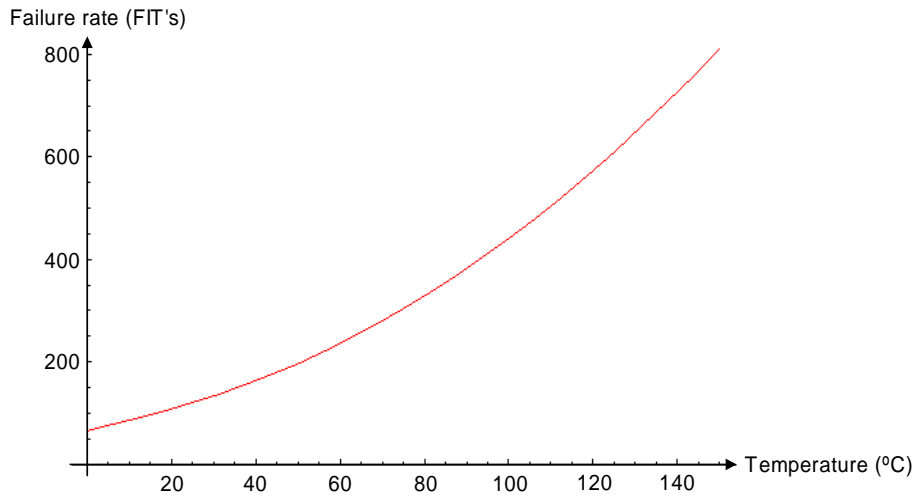
$$\lambda_{\text{Control IC}} = 1000 \cdot \left( 0.02 \cdot e^{-\frac{0.65}{8.617 \cdot 10^{-5}} \cdot \left( \frac{1}{T+273} - \frac{1}{298} \right)} + 0.0013 \right)$$

$$\lambda_{\text{Capacitor}} = 0.0254 \cdot \left( \left( \frac{s}{0.5} \right)^3 + 1 \right) \cdot e^{5.09 \cdot \left( \frac{T+273}{378} \right)^5}$$

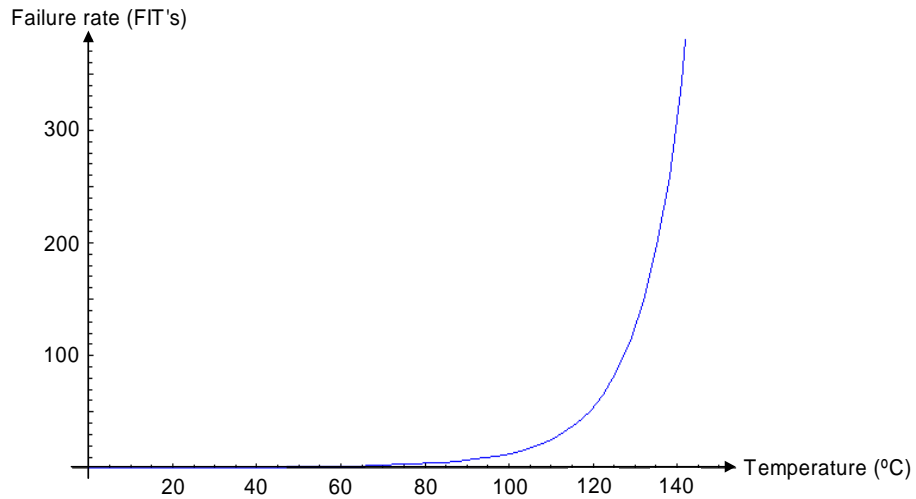
A graphical illustration of the temperature dependency of component reliability is shown below:



**Figure 3 : Control IC failure rate as a function of junction temperature**



**Figure 4 : MOSFET transistor failure rate as a function of junction temperature**

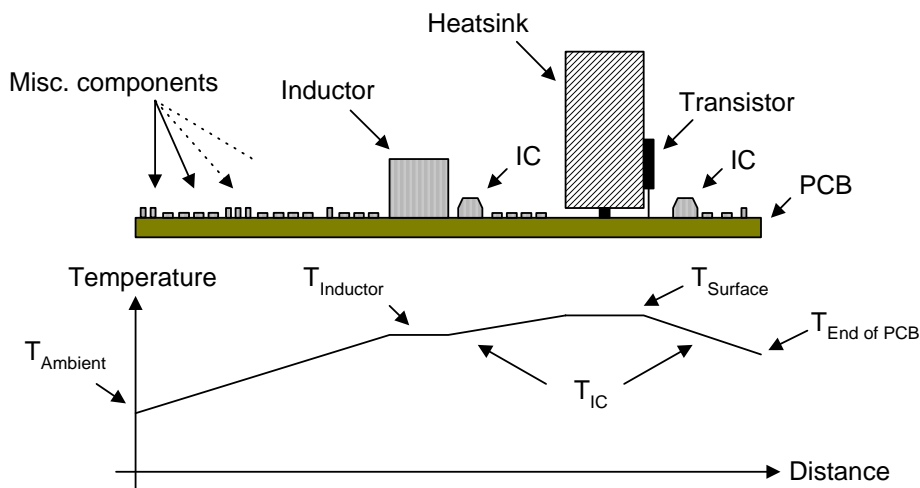


**Figure 5 : Filter capacitor failure rate as a function of internal temperature**

It should be noted that the failure rate of the capacitors are calculated based on 3 sets of equations applicable in 3 different temperature intervals. The detailed derivation of these equations are omitted in this report but can be provided in the form of a ‘Mathematica’ document.

From Figure 3, Figure 4 and Figure 5 it can be seen that the control IC is by far the most unreliable component. Therefore, proper circuit layout is of vital importance for the overall system reliability. As a trade-off between thermal considerations and electrical requirements the printed circuit board layout shown in Figure 6 (top) is chosen for each converter. Based on circuit simulations the resulting operating temperature distribution, shown in Figure 6 (bottom), can be established.





**Figure 6 : Converter temperature distribution**

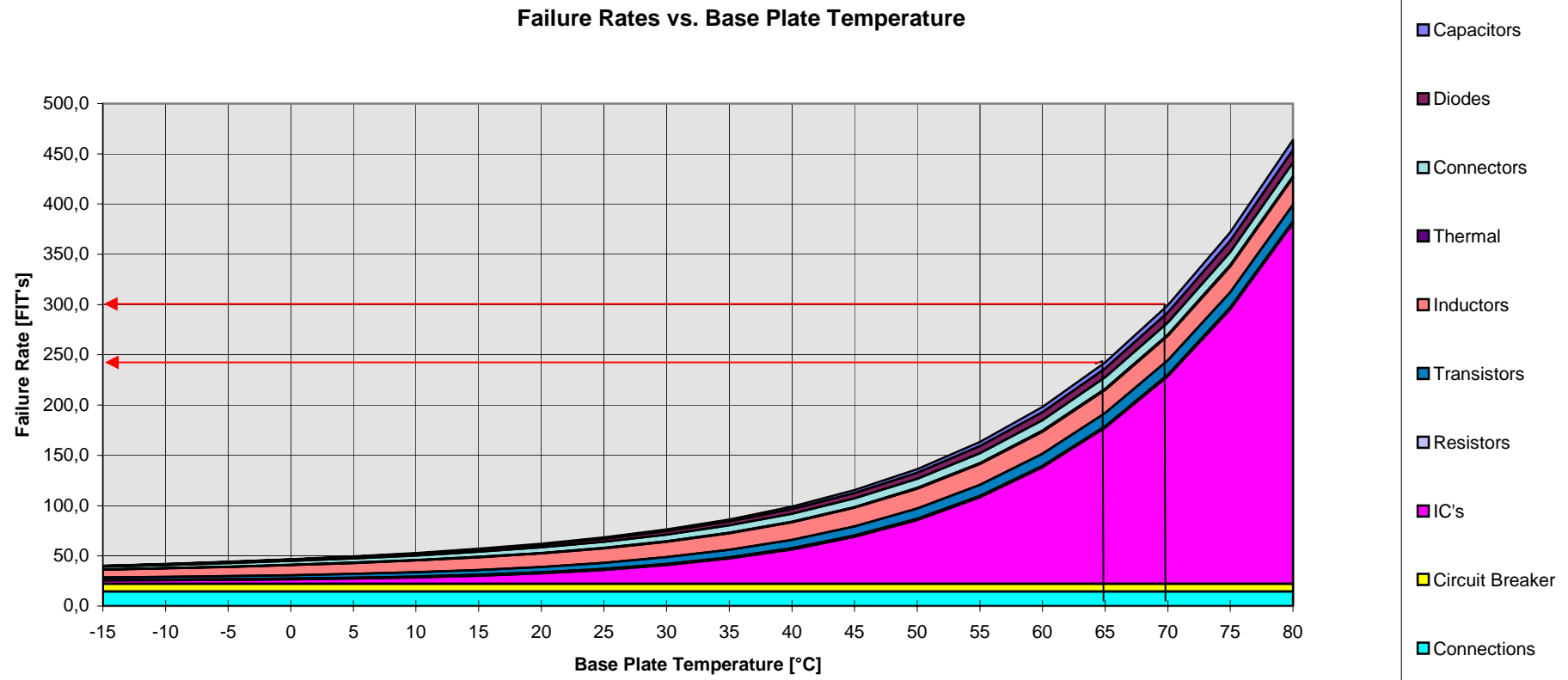
The obtainable mean time between failures for a system comprised of commercially available parts should be expected within the MTBF range:  $2 \cdot 10^5$  to  $5 \cdot 10^5$ . These numbers apply to a single converter unit, thus implying that better system performance is achievable by means of reliability enhancement techniques.

An example of a rather expensive reliability improvement technique is the use of screened components for the power system implementation. A graphical illustration of the accumulated failure rates of a single DC/DC converter can be seen on the next page. The resulting MTBF at the desired operating temperature is within  $3.3 \cdot 10^6$  to  $4.3 \cdot 10^6$ , which is considerably better than the MTBF values mentioned in the previous paragraph.

Further reliability enhancement techniques will be described in a subsequent section.

## Failure rate shown include:

- PWM Control IC (UC1825), Load Share IC (UC1907)
- Output filter inductor and capacitor, input filter inductor and capacitor,
- Current transformer
- Components external to the IC's



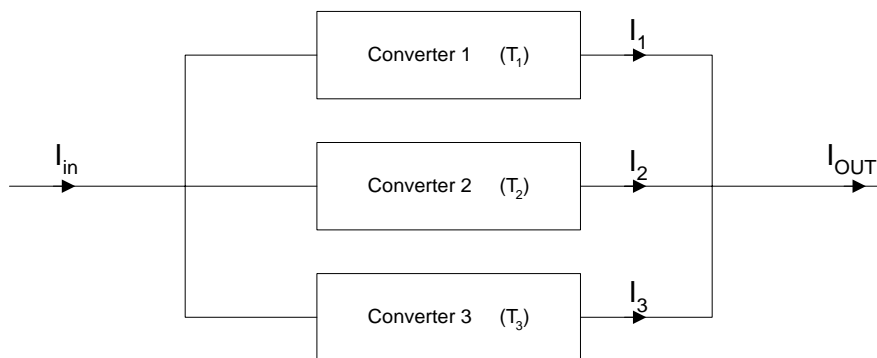
**5°C drop in temperature results in an MTBF increase of approximately  $1 \cdot 10^6$**

## 5. Redundancy concept:

In order to improve the reliability of the system, one or more spare converters can be added to form a redundant configuration. On the assumption that the proposed converter configurations can be implemented within acceptable reliability limits (MTBF of approx.  $1 \cdot 10^6$ ) several techniques in terms of redundancy are applicable. If the spare converters are kept on stand-by until a functioning converter fails, the system is said to be cold redundant whereas if all converters are operated at the same time the system is said to be hot redundant.

In case one converter fails, the hot redundant system automatically resumes operation without noticeable system affect while the cold redundant system requires a series of system procedures to be performed prior to returning to normal system operation. The latter case causes system downtime, but has the advantage of adding an unused converter to the system – meaning that aging and reliability issues in most cases can be disregarded for the cold spare.

If two or more ordinary power converters are connected to the same load, small difference in the output voltage will cause unequal current sharing among the converters. Typically, one or more of the converters will operate in current limitation and some may not supply any current at all. This system does not perform dynamically as expected, since the current loop gain decreases. The result is deteriorated load step response. Furthermore, the converters operating in current limitation do not conform to the component derating requirements unless each converter is over-designed.



**Figure 7 : Redundant power system**

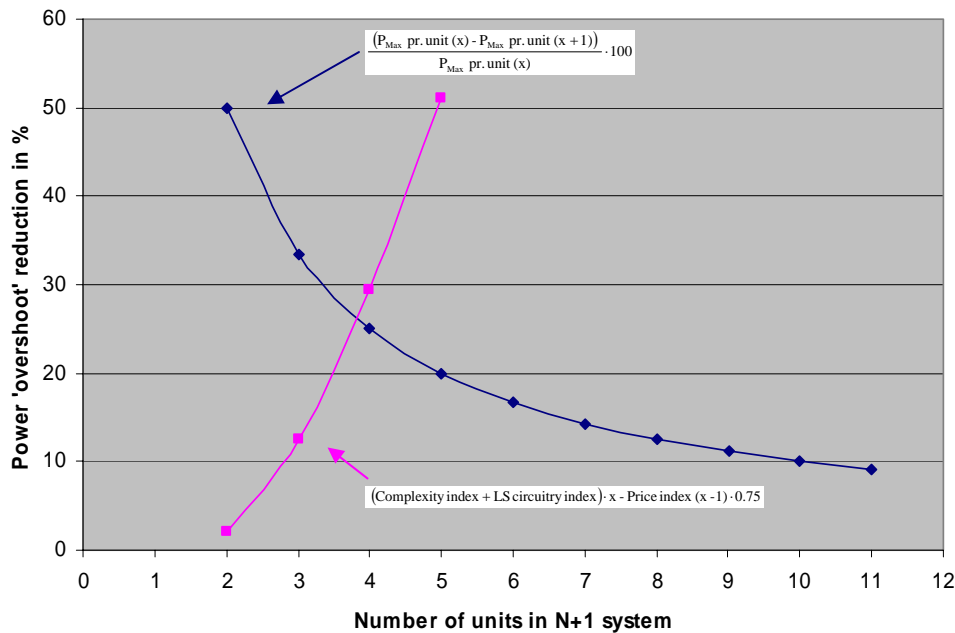
The lack of system performance in parallel-configurations calls for active load sharing. The load sharing among the proposed converters is based on current mode control. The output current is measured and compared to an internal reference in the current controller. The output from the current controller alters the duty-cycle generated by the PWM controller so that each converter's current contribution can be modified. This current modifying capability of each converter is combined with a current sharing bus through which the converters communicate. In turn, this results in equal current sharing among the parallel-connected converters.

Traditionally the current sharing bus is implemented by means of a single wire to which each converter is connected. This configuration is simple and very effective as long as the wire stays intact. If for some reason the current sharing bus is damaged, some converters might still share part of the output current while others might not supply any current at all. From a dynamic point of view this causes the system to become slow reacting and possibly unstable due to the lack of load sharing feedback. To eliminate the failure mode of single wire open failure each converter is diode connected to a ring configuration of the current sharing bus.

To protect against output voltage loss in case of a single point failure (shorted output) each converter has to be connected to the common output voltage bus via an OR'ing device or through a

fuse. The latter case is a single-fault protection that impedes future reconnecting attempts. A more detailed description of the pros and cons of fuse-connecting the individual converters to the output bus are provided in a subsequent section.

When using parallel-connected converters for power system reliability enhancement the choice of redundancy configuration must be established. The most common approach is a N+1 redundant configuration where one extra converter is added to the system. This approach enables the system to tolerate one fault while still providing the required output power. The most straight forward implementation of such a N+1 redundant system is the design of two identical converters each capable of supplying the maximum load current. However, this approach results in a 100% power ‘overshoot’ – meaning that the available system power is twice that required by the specifications. Increasing the number of converter units reduces this power ‘overshoot’. For a N+1 redundant power system Figure 8 shows the percent-wise decrease in power ‘overshoot’ as the number of converter units increases. The other curve is an index that takes into account the decrease in converter unit cost price, the increase in circuit complexity and the increase in load sharing circuitry costs – all a function of the number of converter units. The index is based on component cost (pr. 1000 pieces) and standard load sharing implementation circuitry. It should be noted that the index curve in many situations will change as a function of the number of units when large scale manufacturing is employed and/or different load sharing techniques are used.



**Figure 8 : Percent-wise decrease in power ‘overshoot’**

From Figure 8 it can be seen that the two curves intersect somewhere between 3 and 4 converter units. This point is the optimum in the configuration at hand. However, as indicated above this optimum point is most likely to shift to either side along the axis of abscissas when other power system implementations are considered.

From a reliability point of view the number of converter units should be kept to a minimum. As an example, a N+1 redundant system comprised of 4 converter units is 40% more likely to fail at any given time than a N+1 redundant power system comprised of 3 converter units. The same tendency holds when transitioning from a 3 converter system to a 2 converter system. However, due to the percent-wise larger increase in component count in the latter case the probability of system failure

is 65% higher in a N+1 redundant 3 converter system than that of a N+1 redundant 2 converter system. From these calculations it can be seen that as the number of converter units increase a smaller and smaller gain in reliability is achieved when substituting an X unit system with an X-1 unit system.

In order to calculate the reliability improvement obtainable with different number of converters in a given parallel-configuration the following set of equations are established:

$$P_{2-1} = (e^{\lambda_1 \cdot T} + e^{\lambda_2 \cdot T} - 1) \cdot e^{-(\lambda_1 + \lambda_2) \cdot T}$$

$$P_{3-2} = (e^{\lambda_1 \cdot T} + e^{\lambda_2 \cdot T} + e^{\lambda_3 \cdot T} - 2) \cdot e^{-(\lambda_1 + \lambda_2 + \lambda_3) \cdot T}$$

$$P_{4-3} = (e^{\lambda_1 \cdot T} + e^{\lambda_2 \cdot T} + e^{\lambda_3 \cdot T} + e^{\lambda_4 \cdot T} - 3) \cdot e^{-(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4) \cdot T}$$

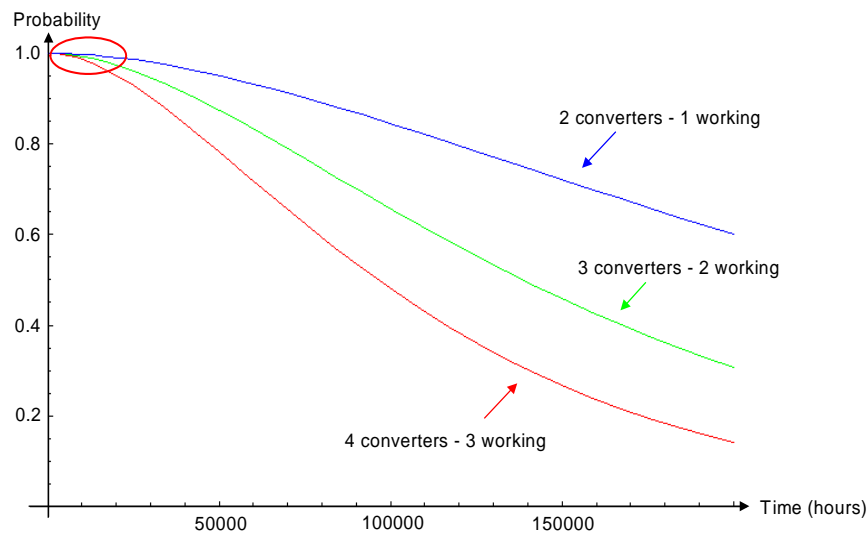
The equations are derived using the exponential distribution with a constant hazard rate for all components combined with the binominal coefficients for successful system operation. It should be noted that the equations allow for reliability calculations of converters with different accumulated failure rates. In the special case of equal failure rates the 3 equations can be further simplified:

$$P_{2-1} = (2 \cdot e^{\lambda \cdot T} - 1) \cdot e^{-2 \cdot \lambda \cdot T}$$

$$P_{3-2} = (3 \cdot e^{\lambda \cdot T} - 2) \cdot e^{-3 \cdot \lambda \cdot T}$$

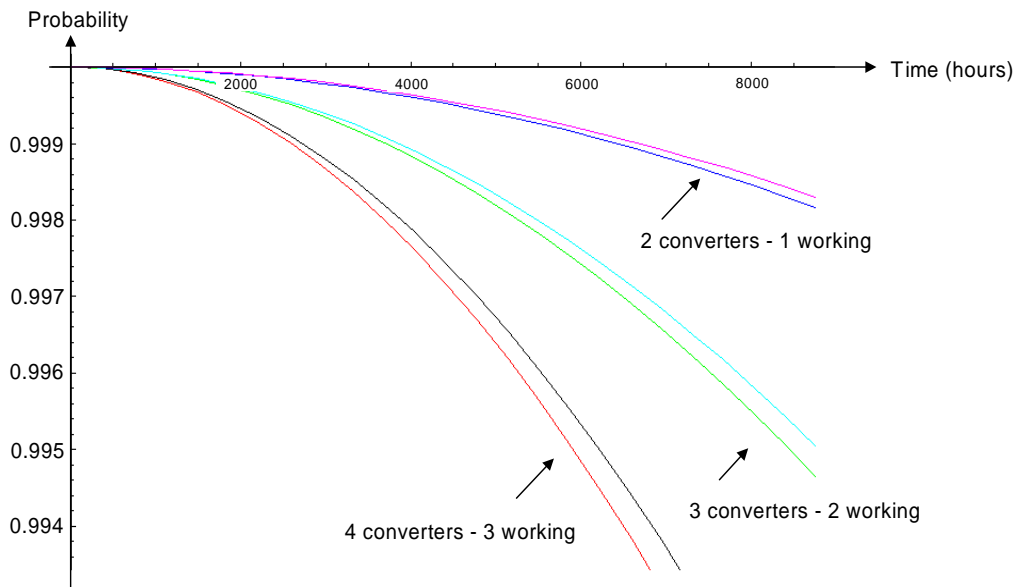
$$P_{4-3} = (4 \cdot e^{\lambda \cdot T} - 3) \cdot e^{-4 \cdot \lambda \cdot T}$$

Plotting the equations as a function of time provides a visual assessment of the different configurations:



**Figure 9 : Probability of system survival as a function of time**

As expected Figure 9 shows that the system comprised of 2 converters provides the best overall reliability whereas the system comprised of 4 converters performs worst reliability-wise. In Figure 9 a red circle indicates the normal range of system life. A more detailed view of this section can be seen in Figure 10.



**Figure 10 : Enhanced view of circled time interval shown in Figure 9**

The curves shown above the probability functions for the 3 different configurations are the system probability of survival for the special case where all converters have the same failure rate. It can be seen that equalizing the failure rates results in improved system reliability. Ensuring equal failure rate can be accomplished by means of thermally distributing each converter's current contribution. Due to IEEE regulations a detailed description of this latter technique cannot be provided in this report since papers have been submitted to both the Applied Power Electronics Conference and Exposition 2004 and the Power Electronics Specialists Conference 2004. However, the real-world implementation of the proposed power system will incorporate this new load sharing technique.

## 6. Fuse protection:

If a redundant system supplies a common load, it is important to ensure that none of the converters fail in a manner that shorts the output power bus, since this will disable the entire power system. In other words it is important that each converter is single failure tolerant towards short circuiting the power supply outputs. One way of ensuring this is by inserting fuses in series with each converter output. Unfortunately, a fuse can sustain several times its nominal current rating for prolonged periods of time. Therefore a large current is needed to blow the fuse in a timely manner. The current rating needed to blow a traditional fuse within 1 ms. is on the order of 4 times the nominal current. This sets a lower limit on the number of parallel-connected converters since the remaining converters have to supply the large current needed to blow the fuse of the faulty converter. At the same time the remaining converters must maintain the proper current level at the load. Further details of pre-arcing time vs. multiple integers of nominal current can be found in fuse manufactures datasheets (for instance SCHURTER).

However, from a reliability point of view the use of fuses has an overall system impact that results in lower converter failure rate. Whether to use fuse protection or some means of actively limiting the current-flow to one direction should be based on system assessments for each particular application. In this application a mix of fuses and active semiconductors will be used. The fuses will be used as buffers at each converter's input while each converter's output is actively OR'ed to the common output voltage bus.

## 7. Parts level redundancy:

Having described the redundancy concept at a system level it is worth noting that similar approaches apply at the parts level. The common approach in assessing system reliability is based on a probability of component failure. This approach assumes two failure modes – a working part and a failed part. However, most components have several failure modes each with their own probability of occurrence.

As an example the free-wheeling diode of the buck converter is considered. By means of traditional reliability evaluation of electronic parts the following two states can be determined:

- Part working
- Part failed

The probability of the buck converter free-wheeling diode failing within a year is 0.08%. Considering the multiple failure modes of the free-wheeling diode the following states can be determined:

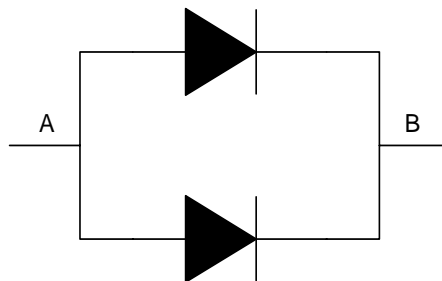
- Part working
- Part failed - short circuit
- Part failed - open circuit

In order to take corrective actions towards the part failures it is necessary to know the distribution of short circuit failures and open circuit failures. These data can be found in numerous component standards. The data used in this report is as follows:

- Part failed - short circuit            35%
- Part failed - open circuit            65%

The percentages indicate that 35% of the probability of diode failure – the diode fails short circuit while the remaining 65% of the probability of diode failure – the diode fails open circuit.

Continuous buck converter operation requires a path for the inductor current during the off-period, meaning that an open circuit is not a valid state. At the same time this current path should be blocked during the on-period, meaning that a short circuit is not a valid state either. Optimization of this current path using the above information can be accomplished by parallel-connecting two diodes as shown in Figure 11.



**Figure 11 : Parallel-connection of two diodes increases the reliability**

For the probability assessment it should be noted that the two failure modes are mutually exclusive, meaning that once a diode has failed open circuit it cannot fail short circuit. This information is important when deducing the minimal cut set used to assess the probability of diode survival in the parallel-configuration. The following equation forms the minimal cut set:

$$R_{\text{Parallel}} = P_{\text{Normal operation}}^2 + 2 \cdot P_{\text{Normal operation}} \cdot P_{\text{Open circuit}}$$

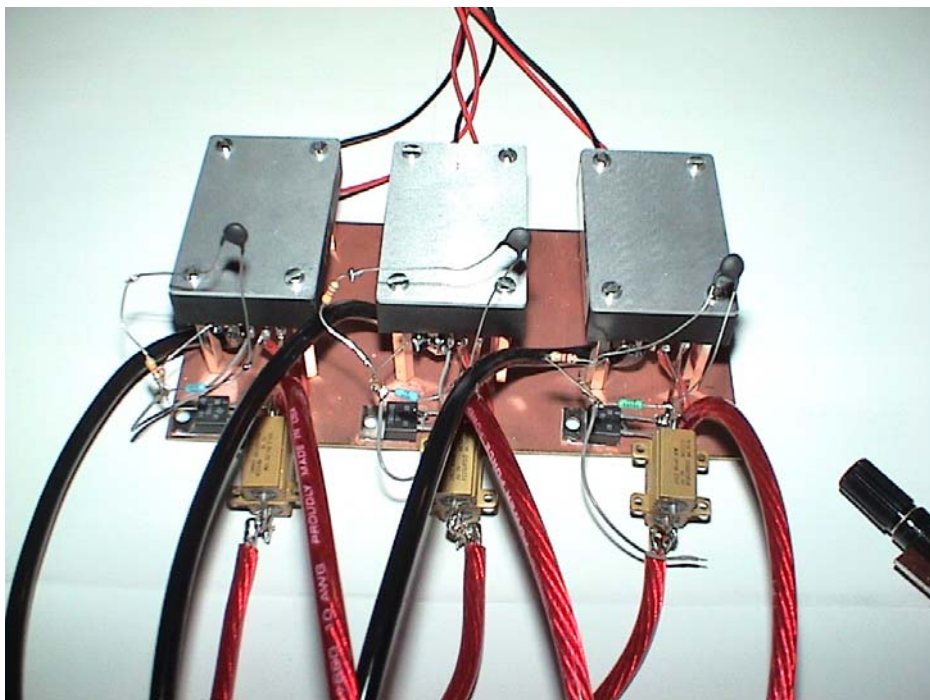
Inserting values for the two cases (single diode and parallel-connected diodes) results in the following probabilities of component survival within 1 year:

$$\begin{aligned} P_{\text{Single}} &= 0.999219 \\ P_{\text{Parallel}} &= 0.999453 \end{aligned}$$

The value for the parallel-connected diodes might not seem that different from the result of the single diode, but in terms of unavailability (1-Probability) it amounts to almost a 30% reduction in overall probability of component failure. Similar approaches can be taken in parallel-connecting other parts throughout the system. However, it should be noted that this technique only applies to multiple failure mode components having different probabilities of failing in one state or the other.

## 8. Actual system:

An image of the real-world implementation of the power system for the control computers, magnetometers, Doppler radar and lidar can be seen in Figure 12.



**Figure 12 : Real-world power system**

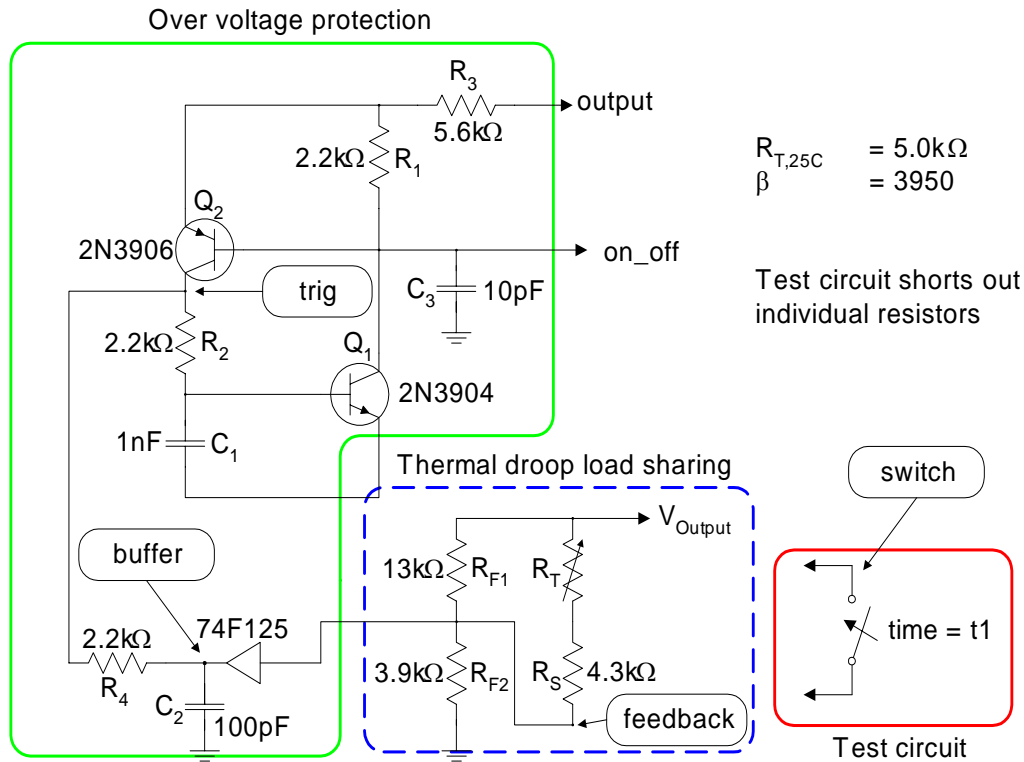
The realization of the power system and the design of components are described in the document ‘Precision Docking Project Power System’ presented at the last project meeting. Therefore this section only provides the results and the simulations for the overvoltage protection circuitry that



was designed to prevent unacceptable failure modes from propagating through the system. A schematic of the thermal droop load sharing circuitry added to each converter is illustrated in Figure 13.

### Overvoltage protection

To prevent overvoltage faults in the power system the following overvoltage protection circuit has been designed:



**Figure 13 : Droop load sharing with overvoltage protection circuit**

A basic FMECA for the thermal droop load sharing network components is performed. The result can be seen in the table below:

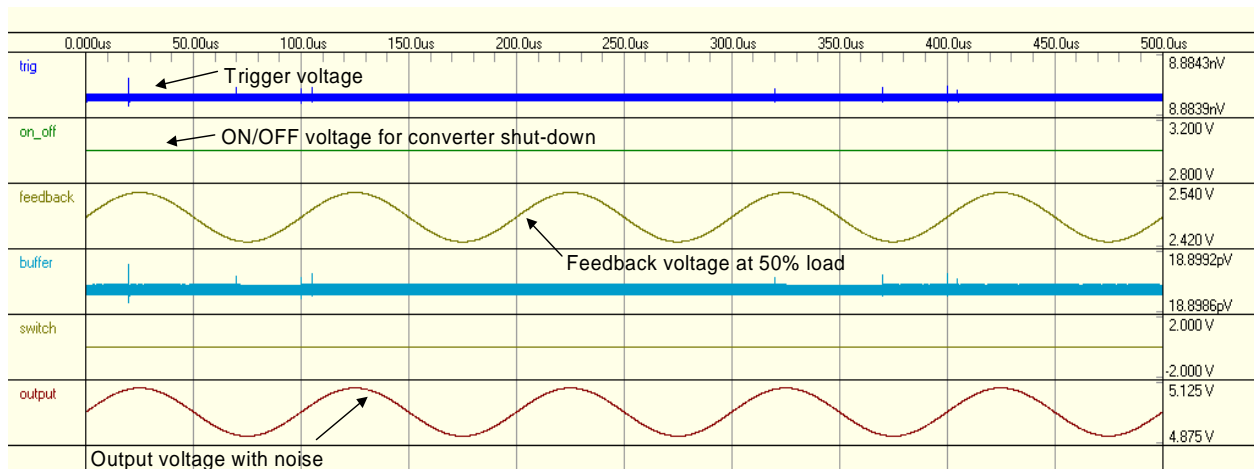
Part	Failure mode	Failure effect	Criticality
R <sub>T</sub>	Short circuit	Over voltage situation	2
	Open Circuit	None	4
R <sub>S</sub>	Short circuit	None	4
	Open Circuit	None	4
R <sub>F1</sub>	Short circuit	Over voltage situation	2
	Open Circuit	None	4
R <sub>F2</sub>	Short circuit	None	4
	Open Circuit	Over voltage situation	2

The 3 failure modes causing an over voltage situation is examined by means of the test circuit shown in Figure 13. At a predetermined moment the test circuit closes the switch, thus causing a

short circuit of its terminals. To make sure the over voltage circuit does not trigger prematurely the test circuit incorporates a time delay of  $20\mu\text{s}$ .

### Simulation results

Figure 14 shows the normal operating mode of the converter. The curves show the node voltages at 50% of full load, which is equivalent to 7.5A. The buffer (buffer) and trigger (trig) voltages are zero, although the curves show some noise in the nano and pico volt range. The output voltage (output) is 5V with a sinusoidal ripple voltage of  $\pm 100\text{mV}$  that represents both the natural converter voltage ripple as well as random noise. The fact that the feedback voltage is a scaled replica of the output voltage is used to trigger the over voltage protection in case the feedback voltage exceeds 2.7V. It should be noted that the non-linear characteristics of the thermistor must be taken into account in order for the feedback voltage to be a true scaled replica of the output voltage.

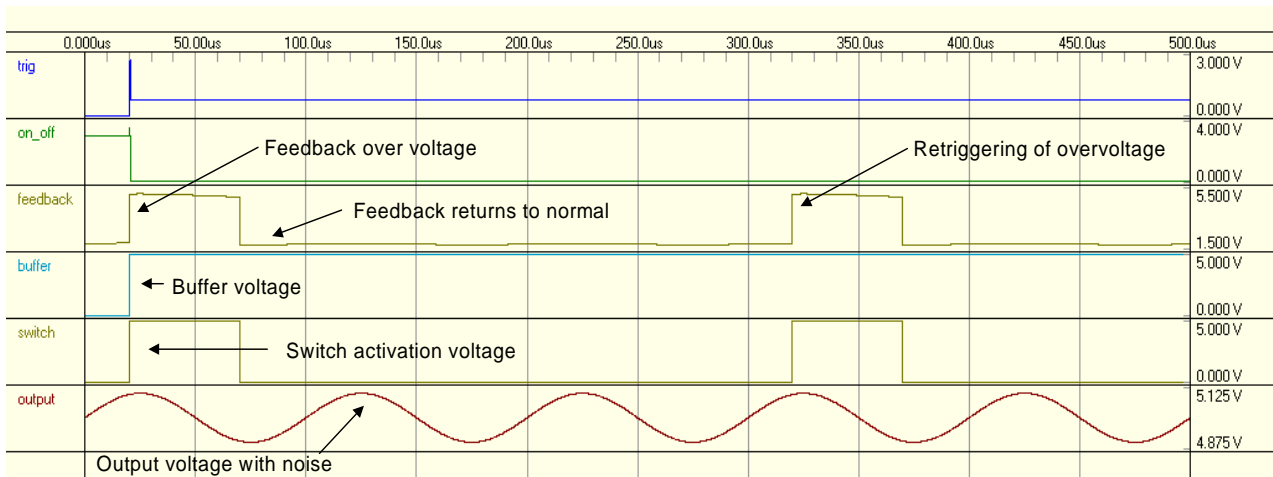


**Figure 14 : Waveforms during normal operation**

Close examination of the 3 failure modes leading to over voltages reveals that the exact same timing behavior occurs in all situations. For this reason, only one set of waveforms are provided. The 3 failure modes examined are:

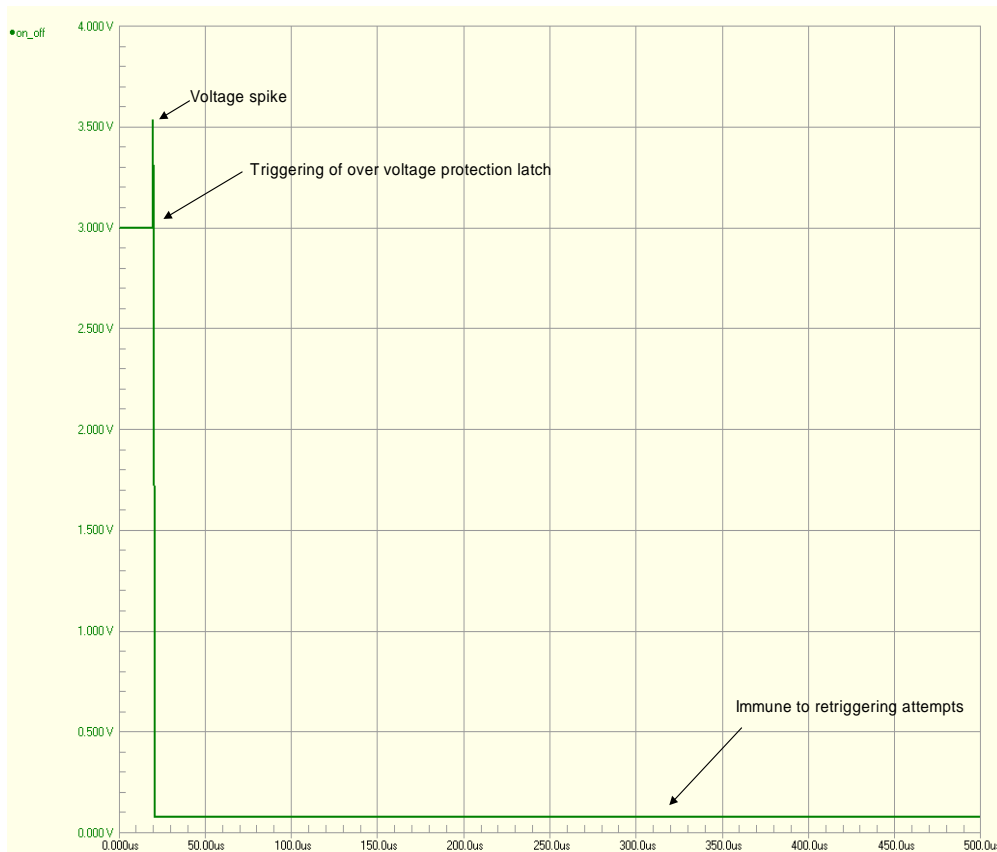
- $R_T$  short circuit
- $R_{F1}$  short circuit
- $R_{F2}$  open circuit

Figure 15 shows the node voltages from which the protection circuit response can be observed.



**Figure 15 : Waveforms during abnormal operation**

At the instant the test circuit closes the switch and causes an over voltage situation the buffer voltage (buffer) generates the trigger signal (trig) that activates the ON/OFF latch (on\_off). Figure 16 shows a close up view of the on\_off voltage during abnormal system operation.



**Figure 16 : Enhanced view of the on\_off voltage during abnormal operation**

The reaction time from over-voltage detection to converter shut-down is 663ns. This reaction time can be minimized at the cost of a larger voltage spike. According to the manufacturer’s datasheet the voltage at the ON/OFF pin should be limited to 3V. Currently a 533mV voltage spike results from the circuit configuration but can be minimized if more capacitance is added to C<sub>1</sub> and C<sub>2</sub>. Larger capacitors results in longer charge times, which in turn prolongs the reaction time of the

overvoltage protection. Very fast-reacting protection circuits and low voltage spikes at the converter TRIM input during circuit triggering are contradictory requirements and a trade-off must be made. In this case a relatively fast-reacting protection circuit is essential for system survival, therefore the voltage spike that results have to be accepted.

Once the over voltage protection has detected an over-voltage from the converter it would be desirable if the converter never attempted to restart and possibly cause another over-voltage situation. The overvoltage protection latch ensures that retriggering attempts are ignored and the converter stays off-line. From the switch voltage (switch) shown in Figure 15 it can be seen that a retriggering is attempted 300 $\mu$ s after the first over voltage situation. Furthermore, although the feedback voltage (feedback) returns to normal 50 $\mu$ s after triggering the overvoltage protection, the ON/OFF latch remains in the low state, thus keeping the converter in the off state.

## **9. Summary:**

The power system can be implemented using a wide verity of techniques – each resulting in optimization of reliability, mass, cost or circuit complexity. Since there are no requirements towards mass and circuit complexity these parameters are secondary concerns, for which reason it is recommended that the approach taken should be based on a trade-off between the needed system reliability and power system cost.

With the severe consequences of for instance control computer malfunction it is recommended that the power system is implemented using the redundancy technique and associated thermal load sharing. Since large scale implementation is desirable, power system realization by means of off-the-shelf converters have been examined. The conclusion was that the best approach for the application at hand was a power system comprised of 3 parallel-connected sharing the common load by utilizing the new thermal droop load sharing technique proposed in the document ‘Precision Docking Project Power System’.