Application Report
SLVAEQ6–April 2020

Failure Containment in Spacecraft Point-of-Load Power Supplies

ABSTRACT

Failure containment is a design approach that makes sure failures in one functional block do not propagate to another. It is an important part of spacecraft design. Because interface circuits, by definition, provide a connection between different functional blocks, they are a potential path for failure propagation. Proper design of interface circuits is therefore critical for mission success. This application report describes how to use the TPS50601A-SP, TPS7H1101A-SP, and TPS7H2201-SP devices to generate a fail-safe supply voltage for high-speed transceiver circuits.

Contents

List of Figures

Trademarks

All trademarks are the property of their respective owners.

1 Introduction

Electronic hardware designed for use in space must be robust enough to meet the mission requirements. And since even high-reliability components are not immune to failure, spacecraft designers must consider failure modes and their impact on spacecraft operability. Failure containment is an important design principle that lets spacecraft designers address failure modes at system level, which reduces the analysis of a complex spacecraft to something more manageable.

The goal of failure containment is to limit the effect of failures on the overall system. Referring to Figure 1, a failure that occurs in Block A is *contained* if only Block A is affected. On the other hand, a failure in Block B that subsequently causes Block C to fail has not been contained. In such cases we say that the failure has *propagated* from Block B to Block C. Failure containment is an important part of spacecraft design, because without it failures can potentially propagate throughout an entire spacecraft, resulting in a destructive domino effect. It is important enough that spacecraft design requirements may formally require it: for example, section 4.2.1a of the European Space Agency's *Space engineering: Electrical and electronic* [1] states that: *A single failure shall not propagate outside a single reconfigurable element.*

This application report describes various approaches to circuit design that can be used to contain failures within a particular block.

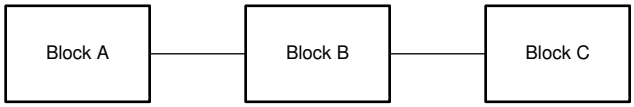

Figure 1. Interconnected Functional Blocks

2 Transceivers as a Failure Propagation Path

Transceivers are commonly used to interface between different functional blocks and are therefore often a potential path for failure propagation. When a transceiver's supply voltage exceeds its absolute maximum rating, it can fail. In this case, "failure" means that the device is damaged in some way. Typically, the worst thing that can happen is that the supply voltage appears on one or more of the transceiver's I/O pins and is transmitted to the corresponding transceiver device at the other end of the communication link. If this failure voltage is greater than the maximum voltage the corresponding transceiver device can withstand, the failure will propagate across the interface.

Many transceiver devices used in modern spacecraft use low-voltage processes and components to achieve their high speed, and there is often not much headroom between the recommended supply voltage and the absolute maximum supply voltage (beyond which the device may fail). For example, TI's TLK2711-SP rad-hard Gigabit transceiver has a recommended supply voltage of 2.5 V (2.6 V at higher frequencies) and absolute maximum rating of 3 V.

Figure 2 shows part of the power tree of a spacecraft subsystem. An isolated DC-DC converter generates a 5-V rail from the 28-V satellite bus, and a non-isolated DC-DC converter generates a 3.3-V rail from the 5 V. The 3.3-V rail supplies a transceiver that connects the function to other subsystems in the spacecraft.

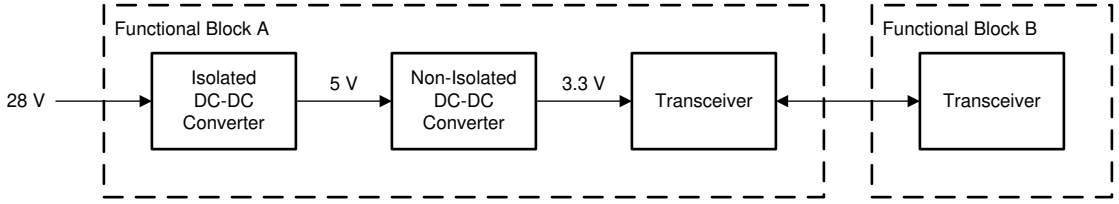

Figure 2. Typical Transceiver Power Tree

A Failure Modes, Effects and Criticality Analysis (FMECA) of the subsystem shown in Figure 2 shows that the non-isolated DC-DC converter can, for a number of different reasons, fail with its output permanently high. If this occurs, the supply voltage of the transceiver will be 5 V instead of 3.3 V. This exceeds the absolute maximum rating of transceiver devices such as the TLK2711-SP, and can cause them to fail. This failure can, in turn, propagate to another functional block. Because it is impossible to predict exactly how a device will fail, FMECAs typically consider worst-case credible failures (see [2]). Although conservative, this approach is more expedient than trying to argue the case for more nuanced failure modes (which a semiconductor manufacturer is in any case unlikely to want to guarantee). The rest of this document mainly addresses the failure case when the switch pin of a DC-DC converter fails short-circuited to the input. In practice, the circuit is unlikely to fail with a perfect short-circuit between the two pins, and we would expect some residual resistance, but for the purposes of this analysis we assume the worst.

To prevent failure propagation, then, a 3.3-V power supply is needed in which no single component failure can cause the output to exceed 4 V.

The following discussion considers the circuit and components of the TPS50601A-SP Evaluation Module (EVM), modified where necessary. No attempt was made to optimize dynamic performance or efficiency beyond the standard EVM configuration. Though customers' circuits may differ from the EVM, the following principles are generally applicable to a wide range of applications.

2.1 A closer look at the problem

Figure 3 provides a closer look at the power stage of a DC-DC converter. In practical circuits, the load is likely to be more complex than the simple resistor R_L used to represent the load here, but a resistor is sufficient for the purposes of this analysis.

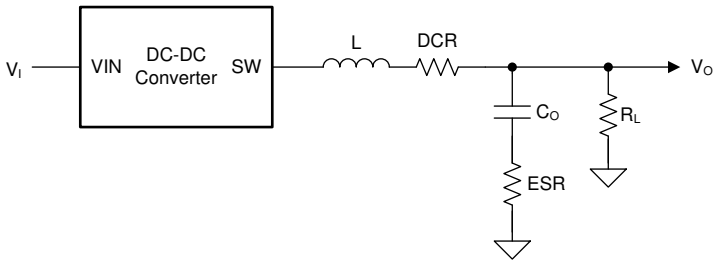

Figure 3. DC-DC Converter Power Stage

When the switch pin SW (sometimes referred to as the phase node) of the DC-DC converter fails high, L and C_O form an underdamped second-order system that rings for a few cycles before settling at a voltage equal to V_I, as shown in Figure 4. In most practical cases, R_L >> DCR + ESR and has little effect on the dynamic response of the system. L and C_O set the oscillation frequency of the system, which in such an underdamped system is closed to the natural frequency.

$$f_n = \frac{1}{2\pi\sqrt{LC_O}} \quad (1)$$

where

- f_n is the natural frequency of the output filter in hertz
- L is the inductance of the output filter in henries
- C_O is the capacitance of the output filter in farads

The peak output voltage is given by

$$V_{OM} = 2V_{I(2)} - V_{O(1)}$$

where

- V_{OM} is the peak output voltage in volts
- $V_{I(2)}$ is the input voltage during the failure condition in volts
- $V_{O(1)}$ is the output voltage before the failure condition in volts (2)

In practice, the inductor's DC resistance (DCR) and the capacitor's equivalent series resistance (ESR) damp the peak voltage to a lower value. With the components used in this example, the maximum instantaneous voltage appearing on V_O is 6.3 V.

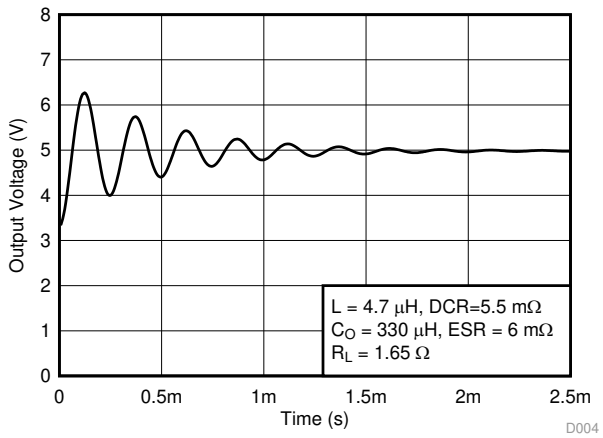

Figure 4. Underdamped Output Response Following Failure

The rate of change output voltage is sinusoidal in shape and is set by the natural frequency of the system and the damping factor. In the case when there is no damping the rate of change of the instantaneous output voltage is

$$\frac{dv_O}{dt} = \left(V_{I(2)} - V_{O(1)}\right)\frac{1}{\sqrt{LC_O}} \quad (3)$$

The maximum rate of change occurs when the instantaneous output voltage equals the input voltage (5 V in this case). Figure 5 shows an expanded view of the waveform described by Equation 3.

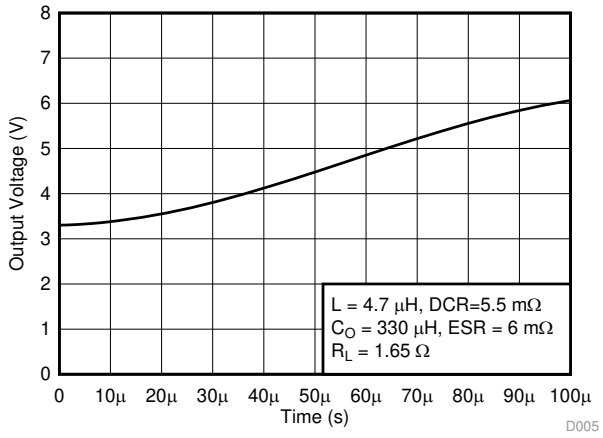

Figure 5. Underdamped Output Response Following Failure – Expanded View

3 Two-Stage Regulation

Figure 6 shows the simplest approach to contain such a failure. A linear regulator adds a second stage of voltage regulation, so that even if the output of the DC-DC converter fails high, the linear regulator continues to regulate the output voltage to 3.3 V.

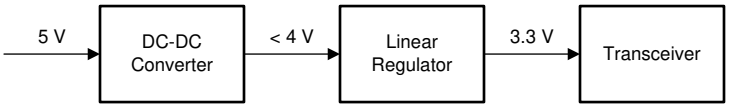

Figure 6. Two-Stage Regulation Approach

Figure 6 shows a detailed schematic for this approach when a TPS50601A DC-DC converter and a TPS7H1101 LDO are cascaded to generate a 3.3-V supply voltage.

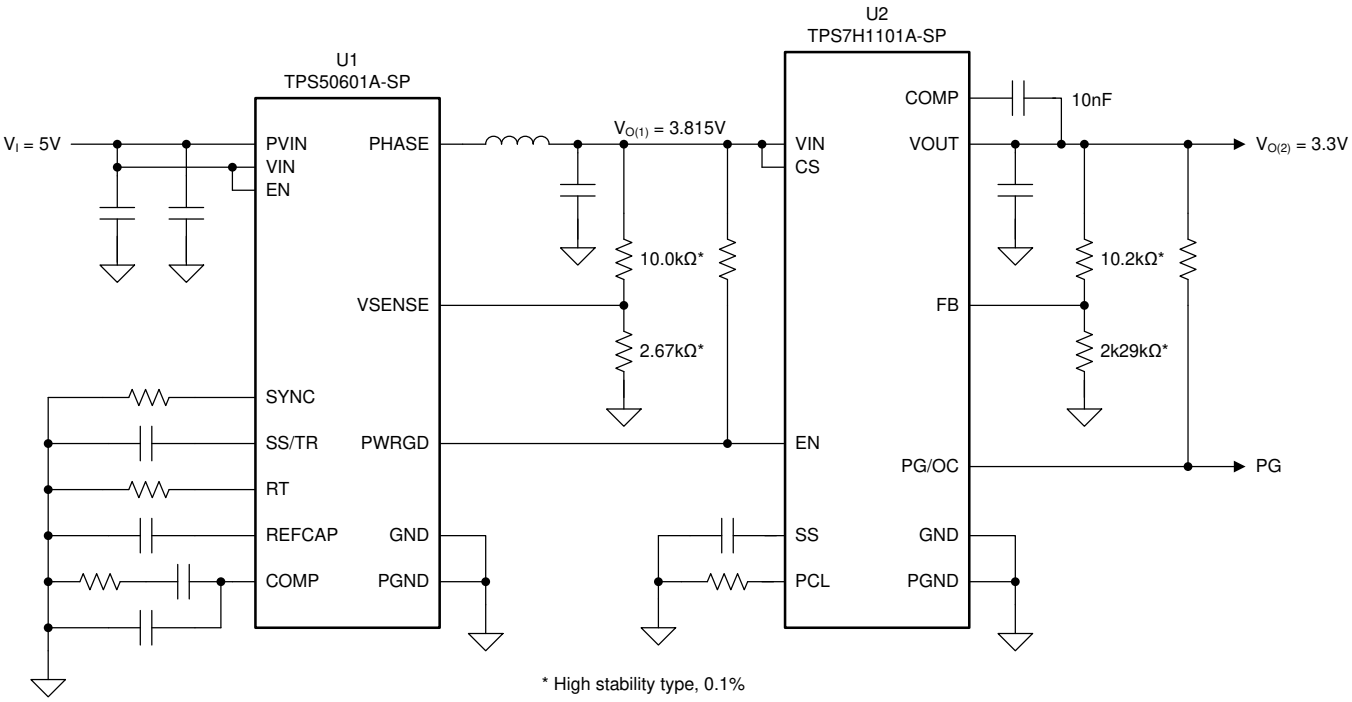

Figure 7. Two-Stage Regulation Circuit

The output voltage of the TPS7H1101-SP linear regulator (U2) is set to 3.3 V. The output of the TPS50601A-SP DC-DC converter (U1) is set to 3.815 V. This voltage is high enough to ensure that U2 operates correctly under all steady-state and transient conditions, but low enough to ensure that, if *U2* fails with its output high, the transceiver supply voltage (V_{O2}) will not exceed 4 V.

Figure 8 shows the response of the circuit in Figure 7 to the failure case when $V_{O(1)}$ suddenly increases from 3.815 V to 5 V. Channel 1 is $V_{O(1)}$ and channel 2 is $V_{O(2)}$ (ac-coupled). The maximum perturbation on $V_{O(2)}$ is 100 mV, which is well below the transceivers absolute maximum rating.

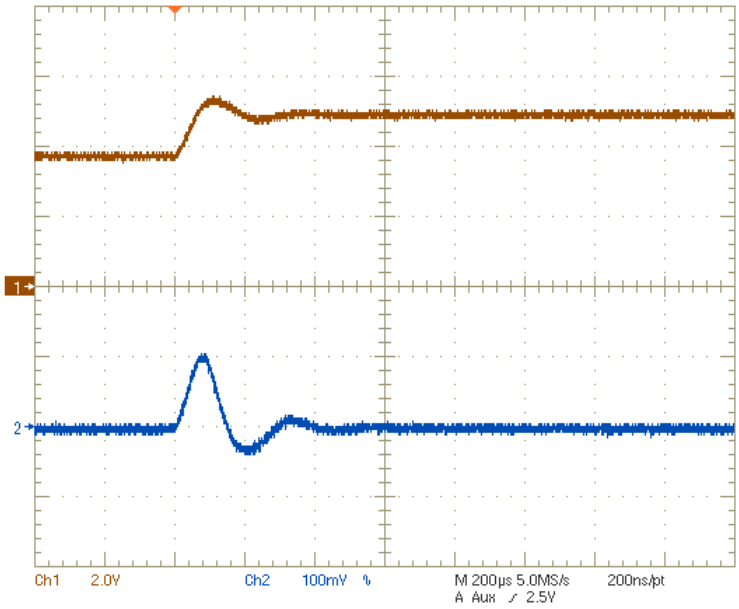

Figure 8. Response of Figure 6's Circuit to a Failure Condition

Note that during a failure condition, the power dissipation in U2 is more than three times higher than during normal operation. If the system cannot adequately dissipate the increased power dissipation, U2 should be turned off to prevent overheating. The circuit shown in Figure 9 can be used to disable U2 when U1's output exceeds 4.5 V.

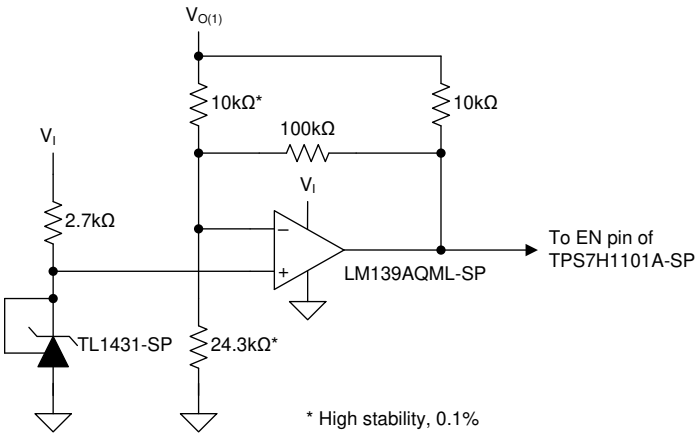

Figure 9. Overvoltage Detection Circuit

4 Downstream Load Switch

Figure 10 shows an alternative approach, in which the overvoltage protection (OVP) function of a TPS7H2201-SP load switch (U2) disconnects the transceiver supply if it detects an imminent overvoltage condition. This approach is particularly suitable to applications with a small load on the output of the load switch; for example, if a small number of transceiver devices are supplied by the load switch, but the rest of the circuitry supplied directly from the output of the DC-DC converter.

In this application, the DC-DC converter's output voltage is set to 2.5 V and U2 is configured for a worst-case overvoltage threshold of 3.774 V. This OVP threshold is high enough to prevent false triggering under normal steady-state and transient conditions, but low enough to prevent output voltages higher than 4 V appearing on the output.

When U2 turns off in response to an overvoltage condition, the output filter of the DC-DC converter circuit is almost completely unloaded. In this underdamped state, its voltage can swing close to the theoretical maximum of 7.5 V. The TPS7H2201-SP has an absolute maximum rating of 7.5 V, so can withstand this voltage, but designers are advised to consider this point when modifying this circuit for output voltages below 2.5 V. One option would be to use an output capacitor with higher ESR than the very low 6-mΩ component used in the TPS50601A-SP EVM, although this will increase output ripple voltage and may necessitate tweaking of the compensation components.

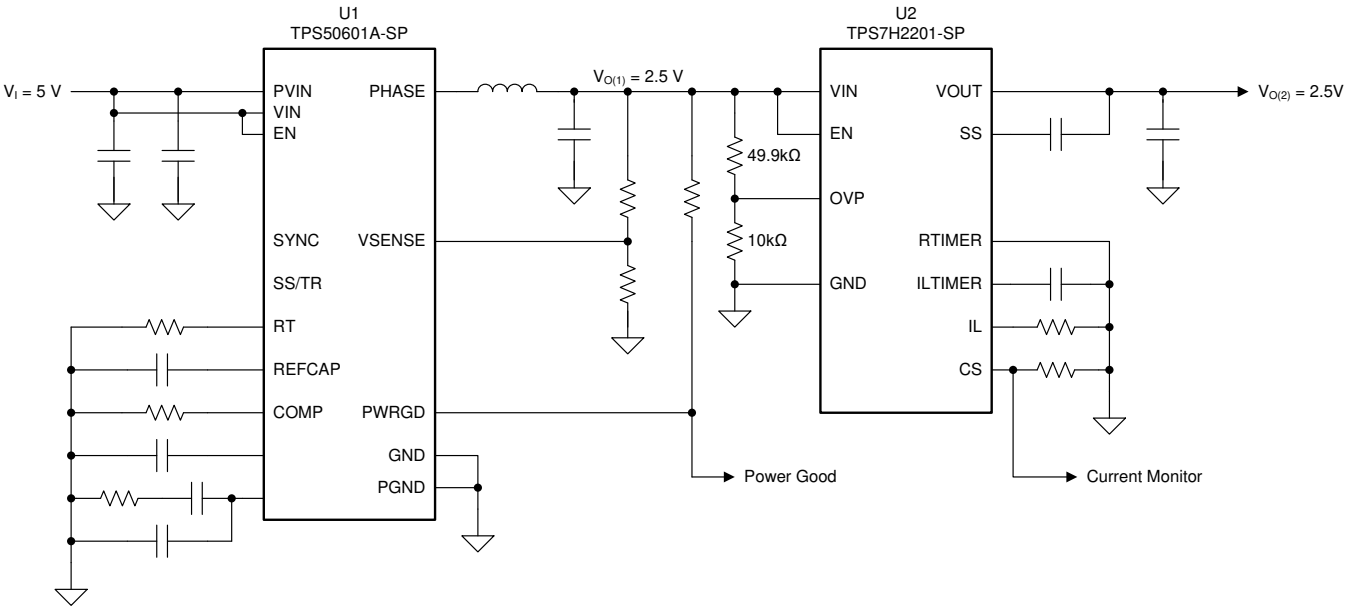

Figure 10. Downstream Load Switch – Internal OVP Comparator

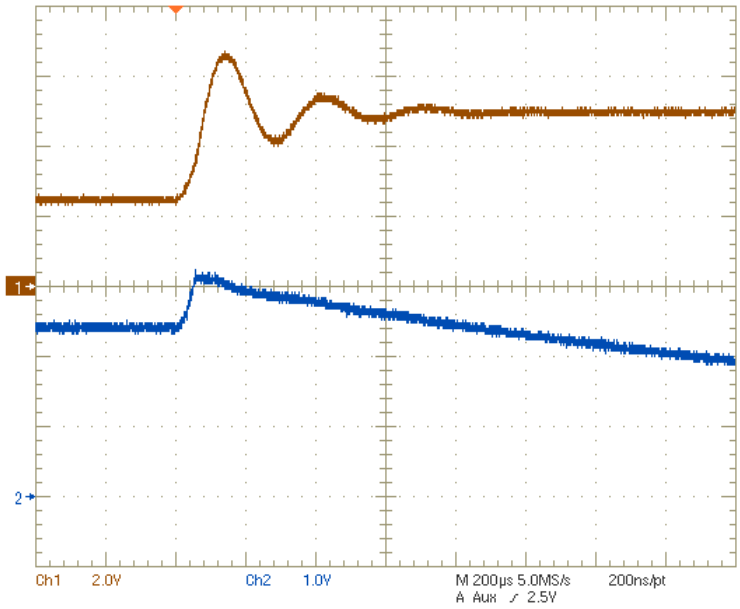

Figure 11. Response of Figure 10's Circuit to a Failure Condition

The circuit shown in Figure 10 is not suitable for 3.3-V outputs because the tolerance of U2's OVP threshold voltage means that under worst-case conditions the output voltage could exceed 4 V. The circuit shown in Figure 12 overcomes this problem by using a TL1431-SP (U3) and ¼ of an LM139AQML-SP (U4) as a more accurate voltage comparator. With the resistor values shown, the rising and falling thresholds are 3.779 V and 3.435 V, respectively.

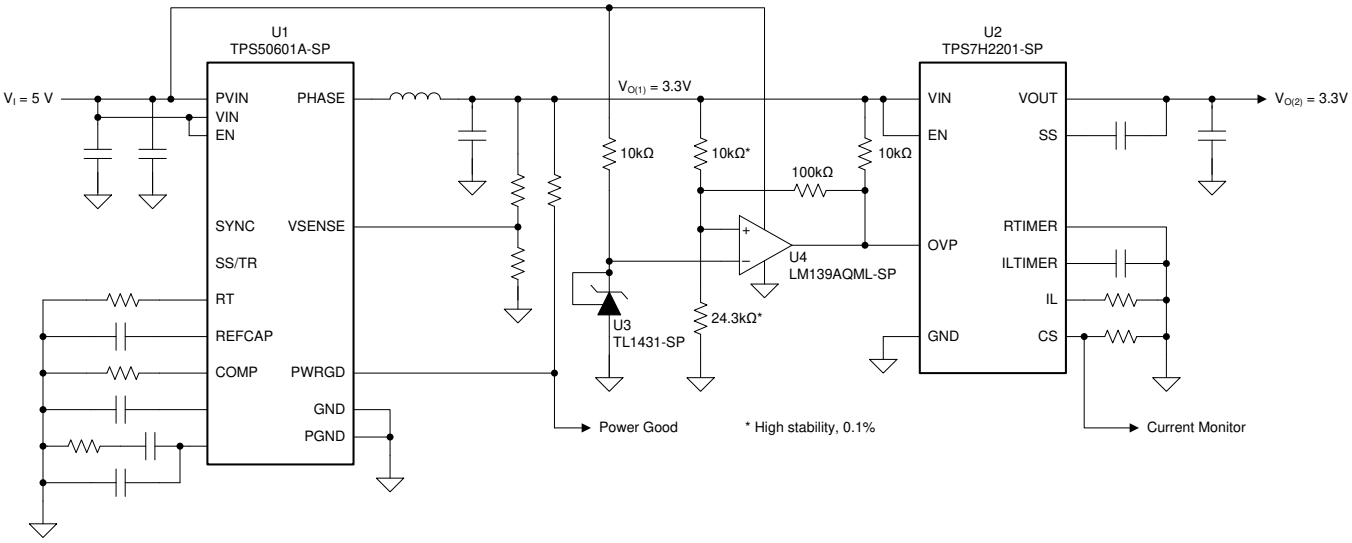

Figure 12. Downstream Load Switch – External OVP Comparator

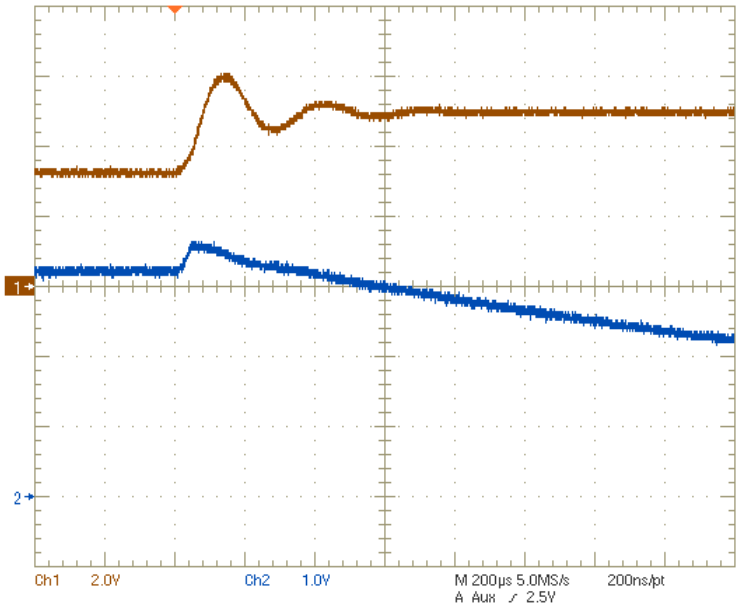

Figure 13. Response of Figure 12's Circuit to a Failure Condition

5 Upstream Load Switch

Figure 14 shows the basic configuration of this solution. In this circuit, a DC-DC converter fed by an upstream load switch supplies the load directly. A comparator monitors the output voltage and, if it detects an overvoltage condition, sets a latch which disables the load switch.

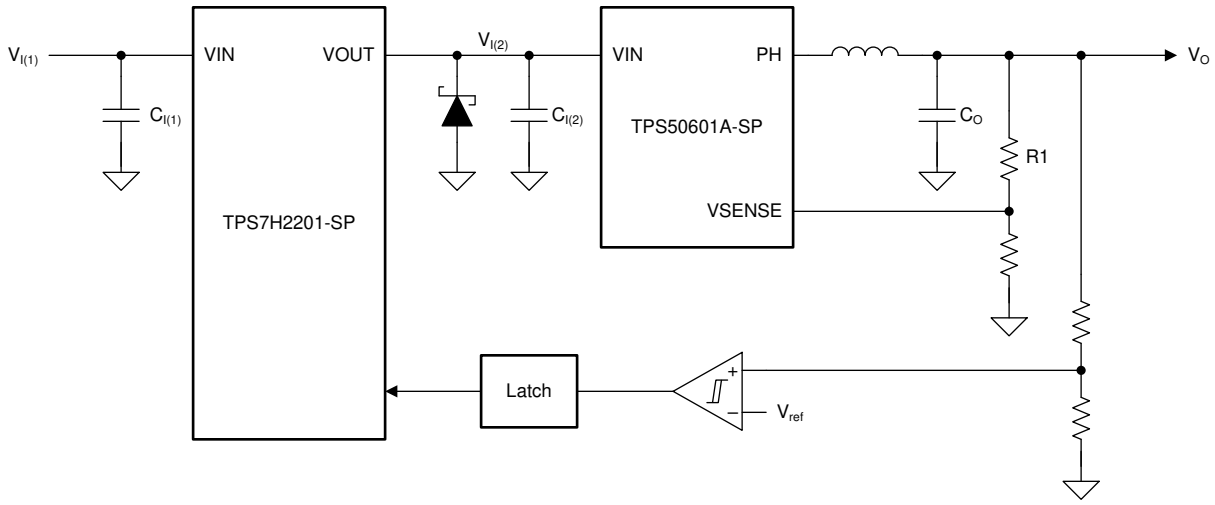

Figure 14. Upstream Load Switch

The discontinuous input current of the TPS50601A necessitates substantial input capacitance. Some capacitance must be placed close to the VIN pins of the DC-DC converter in order to ensure proper operation, but the bulk of the input capacitance must be placed in front of the load switch. This is because energy stored in $C_{I(2)}$ continues to supply the DC-DC converter for a short time after the load switch opens. In the case that resistor R1 fails open-circuit, the converter will continue to increase its output until the charge in $C_{I(2)}$ has depleted. In the case that the converter's high-side switch fails short-circuit, $C_{I(2)}$ forms a capacitor divider with C_O and the underdamped ringing on V_O appears, inverted, on $V_{I(2)}$. The amplitude of the $V_{I(2)}$ waveform depends on the ratio of $C_{I(2)}$ to C_O, and in may be large enough to pull the $V_{I(2)}$ node negative. The Schottky diode connected to $V_{I(2)}$ protects the DC-DC converter and the load switch against this eventuality. Figure 15 shows how the circuit in Figure 14 behaves when the TPS50601A-SP fails with a short-circuit between the VIN and PH pins (simulated response).

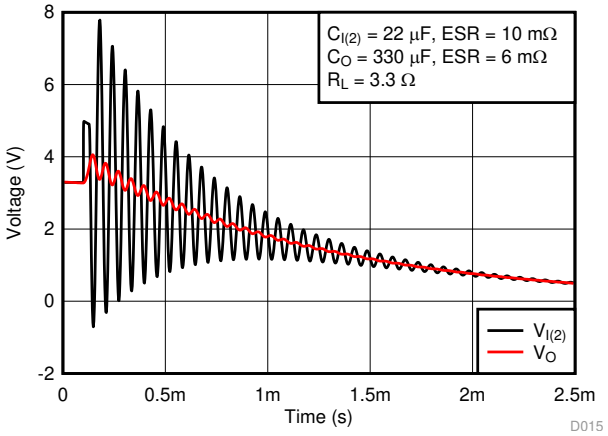

Figure 15. Response of Figure 14's Circuit to a Failure Condition

6 Test Setup

There are practical difficulties in evaluating failure cases, not least because we usually only want to evaluate them, not cause permanent damage to components. This is especially true when working with space-grade components, which tend to be expensive and more difficult to get hold of than devices intended for commercial use.

One way to force the output of a DC-DC converter high is to short the lower feedback resistor. However, this method depends on the closed-loop bandwidth of the converter, which will always be slower than the worst-case. The preferred method is to use the test setup shown in Figure 16 to emulate the response of the DC-DC converter's output to a worst-case failure; that is, when the converter's high-side switch output fails permanently on, with the voltage on the switch pin equal to the supply voltage. The pulse generator generates a pulse whose low level is equal to the nominal output voltage of the DC-DC converter during normal operation. The high level of the pulse is equal to the output voltage of the DC-DC converter during failure (in this case, 5 V). The unity-gain power amplifier buffers the pulse and supplies the equipment under test, in this case one of TI's evaluation modules. The series-connected inductor, together with the EVM's input capacitance represent the output filter of the upstream DC-DC converter. For best results, these components should be identical to the ones used in the final design.

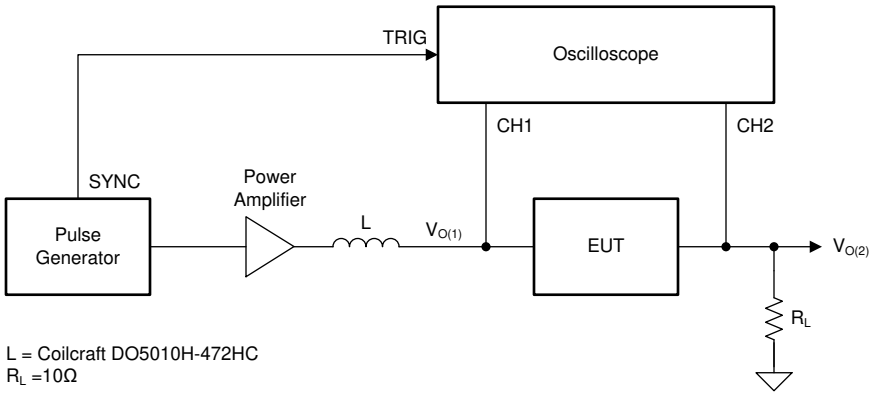

Figure 16. Test Setup

7 Summary

Failure containment is an important part of spacecraft electronics design. Because of their function connecting different functional blocks together, transceiver circuits are a potential path for failure propagation, and must be designed in a way that makes sure a single failure does not propagate anywhere else.

The high-speed requirements of modern transceiver devices often mandate the use of low-voltage processes and components, which in turn may limit the headroom between recommended operating voltage and absolute maximum voltage. The design of a voltage regulator circuit to supply such transceivers is often non-trivial, requiring careful choice of architecture and components.

Of the approaches presented in this application report, the linear post-regulator is the easiest to implement. This circuit's behavior is largely independent of the upstream DC-DC converter's dynamic response, which greatly simplifies circuit analysis. Downstream load switches – using internal or external OVP comparators – are the next easiest to implement and, with careful consideration, can be used effectively in practical applications. Using a DC-DC converter with an upstream load switch promises good performance but requires great attention to detail and intimate knowledge of the dynamic behavior of the rest of the circuit.

8 References

1. *Space engineering: Electrical and electronic (ECSS-E-ST-20C)*
2. *Space product assurance: Failure modes, effects (and criticality) analysis (FMEA/FMECA) (ECSS-Q-ST-30-02C)*
3. Texas Instruments, *TPS7H2201EVM-CVAL Evaluation Module (EVM) User's Guide*
4. Texas Instruments, *TPS50601ASPEVM 6-A Regulator Evaluation Module User's Guide*
5. Texas Instruments, *TPS7H1101SPEVM User's Guide*

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265