SPACEWIRE PHYSICAL LAYER FAULT ISOLATION

Session: Test, SpaceWire Components

Short Paper

Barry Cook

4Links Limited, Bletchley Park, MK3 6EB, England

Wahida Gasti, Sven Landstroem

ESA/ESTEC, Noordwijk, The Netherlands

E-mail: Barry@4Links.co.uk, Wahida.Gasti@esa.int, Sven.Landstroem@esa.int

ABSTRACT

The SpaceWire physical layer is required to use Low Voltage Differential Signalling (LVDS) as defined in the document ANSI/TIA/EIA-644 (A).

It has been shown that a likely failure mode in such drivers can result in high fault currents that can propagate between SpaceWire links and cause catastrophic failure of systems - including redundant systems when cross-strapping is used. Great care must be taken in power systems to limit such excessive effects.

We begin by describing the usual (LVDS) physical layer implementation, its consequence and power system requirement implications. We then consider receiver protection and its limitations. Alternative driver designs that can significantly reduce the undesirable effects resulting from component failure are described.

1 OVERVIEW

SpaceWire [1] is a relatively high speed (up to 400Mb/s) link protocol intended to be used for point-to-point data links or, in conjunction with suitable routing switches, for fault tolerant networks. The physical layer is required to use Low Voltage Differential Signalling (LVDS) as defined in the document ANSI/TIA/EIA-644 (A) [2].

Use of multiple links, whether for nominal and redundant point-to-point links, or for networks, requires interconnections between links – at least for data transfers. It has been shown [3] that a failure in one link can propagate between links unless care is taken to provide mechanisms to provide isolation between links. We consider normal operation and behaviour under failure conditions in order to suggest suitable isolation mechanisms.

2 NORMAL OPERATION

LVDS specifies a low differential output voltage, nominally 350mV, sitting at a defined common mode level, nominally 1.25V. The nominal output terminal voltages are thus between 1.075V and 1.425V. This allows an end-to-end voltage difference between ground wires (the common mode voltage range) of ±1v whilst keeping the receiver input terminal voltages between 0.075V and 2.425V.

It is often believed (and implied in [1]) that LVDS drivers must be current sources. In fact, the opposite is true – they can't be current sources. If they were current sources then the output common mode level cannot be controlled – but it is essential that it is closely controlled. Note that the standard specifies output voltages, not currents.

3 FAULT SCENARIO

The fault that concerns us here is that of the supply rail to the LVDS driver rising above its maximum level. This can be caused by a power-supply fault The common method of achieving ground isolation and secondary regulated supply voltages, is via insulated DC/DC converters which have credible failures causing over-voltage emission. Depending on the topology chosen, the over-voltage emission can be predictable (buck topology, limited value) or non-predictable (boost topology, "non-limited" value). Furthermore, the DC/DC converter may have Over-Voltage Protection (OVP) built in or it may not. In the second case, which is usual for low cost off-the-shelf DC/DC converters, the possible failure propagation paths from the supply voltage failure is a serious matter. A non protected "flyback" (i.e. boost) converter may easily cause over-voltage emission of 2-5 times nominal voltages, if not protected by OVP. Even if OVP exists, the LVDS user (the designer) must be careful on exactly what peak voltage level the DC/DC converter will emit in dynamic mode, i.e. how big the max over-shoot will be before the DC/DC converter is successfully shut-down or clamped.

Excessive supply voltage on the LVDS driver is likely to result in its failure and, unfortunately, the likely failure mode here (as it is for the regulator) is to propagate the excessive voltage to its output pins. This voltage is passed to the input pins of the receiver and, after causing this device to fail, might be passed to the receiver supply rail. This catastrophic failure scenario is rarely assumed or analysed in the FMECA analysis on system design level. The analysis is often depending on the equipment designer's knowledge about power supplies and in fact often overlooked.

Power supply regulators are most commonly designed only to source current, not to sink DC current supplied from high voltages on device input pins. Excessive signal input voltage can result in a rise in supply voltage at the receiver – leading in turn to failure of nearby transmitters and propagation of the fault to other receivers etc. The effect may, in this way, be passed to redundant circuits. See Figure 1 (taken from [3]).

4 CONTROLLING THE FAULT AT SOURCE

The first line to consider is preventing the initial fault damaging the LVDS drivers. Some sort of supply rail over-voltage detector and limiter would appear to be enough.

We must, however, consider the practicality of such devices … they must allow a normal supply rail voltage – for example, 3.3V nominal (acceptable range 3.0 to 3.6V) – and clamp an excessive voltage – 4V maximum in this example. That is a small difference which in a true worst-case analysis may be very hard to prove.

We must also consider whether the protection device can clamp the rail voltage cleanly or whether there will be a transient over-voltage, possibly caused by intentional or stray inductance in the circuit. Even a transient can cause damage: semiconductors are noted for the speed at which they fail with over-voltage stress.

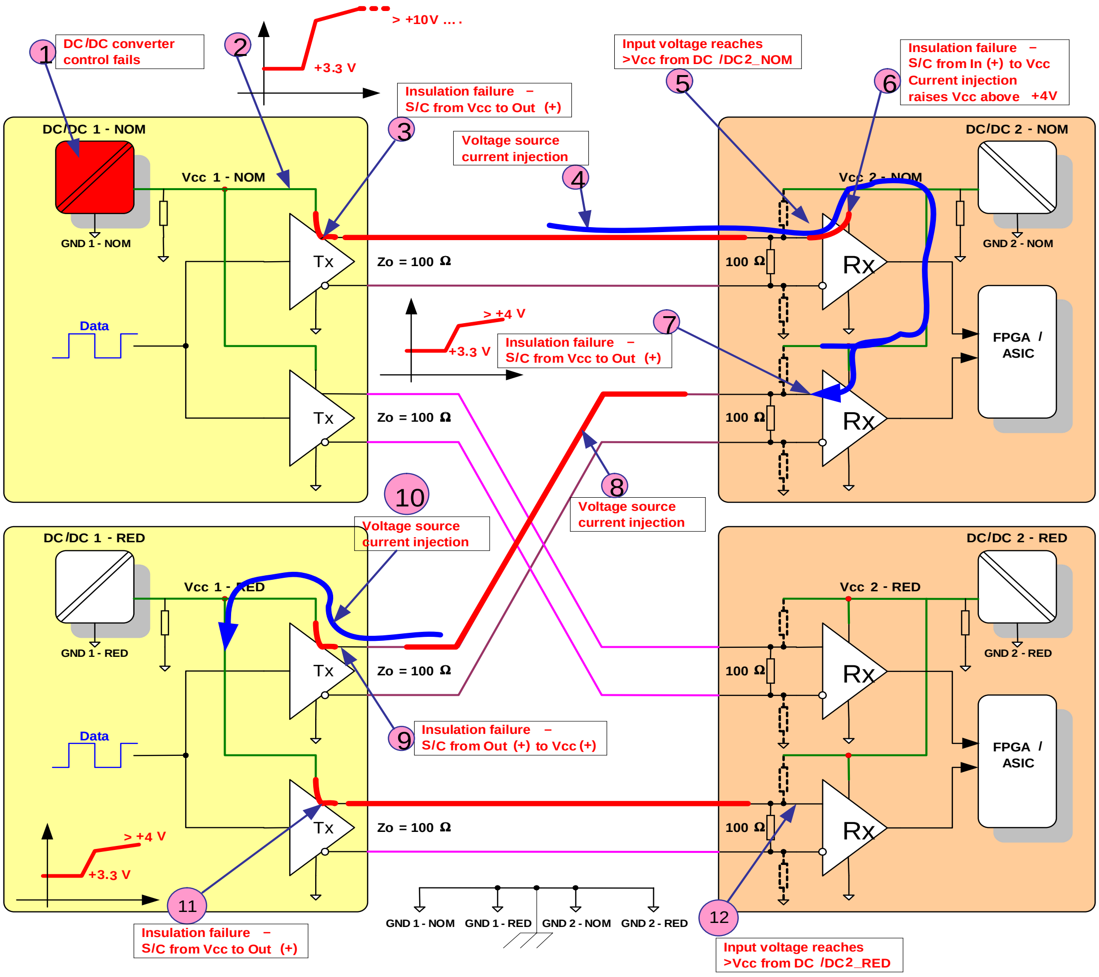
1
DC/DC converter control fails
2
> +10V ....
+3.3 V
Insulation failure – S/C from Vcc to Out (+)
3
Voltage source current injection
4
Input voltage reaches >Vcc from DC /DC2_NOM
5
Insulation failure – S/C from In (+) to Vcc Current injection raises Vcc above +4V
6
DC/DC 1 - NOM
Vcc 1 - NOM
GND 1 - NOM
Tx
Data
Tx
Zo = 100 Ω
Zo = 100 Ω
DC/DC 2 - NOM
Vcc 2 - NOM
GND 2 - NOM
100 Ω
Rx
100 Ω
Rx
FPGA / ASIC
> +4 V
+3.3 V
Insulation failure – S/C from Vcc to Out (+)
7
8
Voltage source current injection
10
Voltage source current injection
DC/DC 1 - RED
Vcc 1 - RED
GND 1 - RED
Tx
Data
Tx
Zo = 100 Ω
Zo = 100 Ω
> +4 V
+3.3 V
9
Insulation failure – S/C from Out (+) to Vcc (+)
11
Insulation failure – S/C from Vcc to Out (+)
GND 1 - NOM
GND 1 - RED
GND 2 - NOM
GND 2 - RED
DC/DC 2 - RED
Vcc 2 - RED
GND 2 - RED
100 Ω
Rx
100 Ω
Rx
FPGA / ASIC
12
Input voltage reaches >Vcc from DC /DC2_RED

Figure 1 How a fault can cause damage to both nominal and redundant circuits.

5 LIMITING PROPAGATION

It may be possible to arrange input clamping or isolation circuits at the receiver inputs. The circuits used must not excessively load the signal lines (capacitively, for example) and as a result will tend to be small and thus have limited current and energy absorbing capability. It is essential that the fault current available from a compromised LVDS transmitter is limited to a safe value – at nowhere the level available from a supply bus.

We cannot rely on the LVDS transmitter chip to do this – it will have been damaged by this fault situation. We need to provide a reliable current limiting device that will not be easily damaged by excessive voltage – and if it is damaged will be sure to fail open-circuit. A simple resistor has the correct properties (dependant on technology, but thick-film SMD resistors and hole mounted metal-film resistors are accepted by most agencies as S/C free).

A driver circuit such as that shown in figure 2 where series resistors and, optionally, a parallel resistor are used with complementary logic-swing outputs can be used to produce LVDS signal levels. One suitable combination uses a 2.5V supply, 300Ω series resistors (R_s = 300) and no parallel resistor (R_p = ∞). It produces correct common mode and differential LVDS voltage levels. Its output resistance of 300Ω in each signal wire limits fault currents into a receiver – with a driver over-supply of

15V the current is limited to less than 50mA on each wire, a level that could be safely absorbed by receiver protection devices. This circuit is equivalent to a reasonable, but not perfect, current source (the higher the series resistor value, the better the current source). The required supply current is 3.5mA (9mW consumption), exactly the current needed to develop the required load voltage across a 100 Ω termination. Similar circuits may also be used with 3.3V or 5V supplies with the advantage of having higher valued series resistors to further limit fault currents, but the disadvantage of consuming more power.

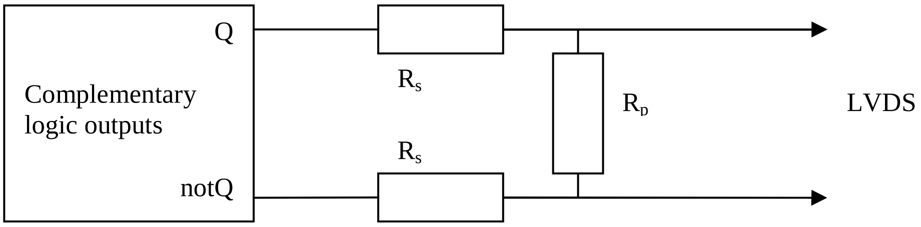

Figure 2 LVDS transmitter from complementary logic output and resistors

6 EMC

In addition to transferring data the signal lines must no be susceptible to interference from electro-magnetic fields.

Experience from IEEE1355 (which was developed into SpaceWire, keeping the same physical layer) reveals that differential drivers are often poor in this regard – their output characteristic is far from linear. It was common-mode noise on the signal lines was converted, by the drivers, into differential noise. Series resistance serves to linearise the outputs and improve EMC performance. A degree of source termination can also improve the situation – leading to consideration of re-scaling the series resistors in Figure 2 to allow the addition of a parallel resistor. The circuit used by Actel™ is very good in providing a near ideal source termination.

7 Conclusions

Far from being non-LVDS compliant, an LVDS output circuit containing real, non-integrated, resistors meets the LVDS standard, has a safe failure mode and is likely to improve EMC characteristics.

8 References

1. The ECSS-E-50-12 Working Group, "**ECSS-E-50-12A 24 January 2003**, SpaceWire - Links, nodes, routers and networks", published by the ECSS Secretariat, ESA-ESTEC, Requirements & Standards Division, Noordwijk, The Netherlands

2. ANSI/TIA/EIA-644-A-2001 "**Electrical Characteristics of Low Voltage Differential Signaling (LVDS) Interface Circuits**"

3. "**SpaceWire Link interface: LVDS, Power & Cross-strapping Aspects**" Sven Landstroem and Wahida Gasti Presentation at the SpaceWire working group meeting #11, Noordwijk, June 10&11 2008