Design Power Supply with Uvervoltage Protection Acceptable for SIL4 application According EN50129

Jaroslav Fait

Abstract—This abstract is aimed for Number specification.

Index Terms—SIL4, WayGuard, Bistabil relay

I. Single Points of Failure in a simple setup

Systems can be made robust by adding redundancy in all potential SPOFs (single point of failure) [1]. For example on the figure 1, two sensors are powered by simplex element - power source. If the power supply breaks (overvoltage/undervoltage), it can compromise any safety margin gained in using dual sensors.

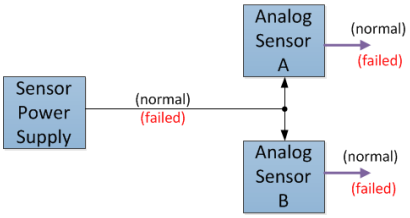

Fig. 1. Simplex component failure may brings in matching but incorrect results in the dual sensors

Redundancy can be achieved at various levels. The assessment of a potential SPOF involves identifying the critical components of a complex system that would provoke a total systems failure in case of malfunction. Highly reliable systems should not rely on any such individual component.

II. Dual Computer Architecture

When microcomputers were introduced in mid 1980s, diagnostic functions became the main force of the CPUs. In applying microcomputers to railway signalling, conventional safety measures based on the asymmetric nature of component failure modes are not available. Instead, however, microcomputers enable high-frequency diagnosis, and this leads to composite fail-safety and reactive fail-safety as well Rastocny2013

The Dual Computer Architecture is the adoption of identical duplicate CPU configuration (identical software). Computer hardware, power supply, and interconnects (and sensors) are all duplicated, as is shown in figure 2. Each of the groups is referred to as a channel.

Assumption:

1) Hardware in the channels is independent: A hardware failure in a channel has no effect on the correct performance of other channels.

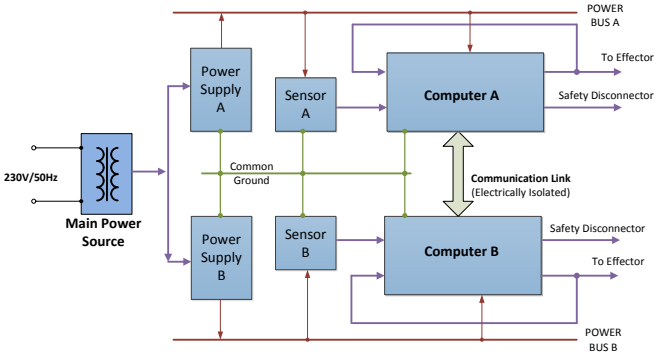

Fig. 2. Redundant CPU Architecture

2) The communication path is electrically isolated from the computers: A hardware failure (such as a short circuit) in the connecting path will not propagate to computers.

In safety discussion, whether or not a safe state can be defined also plays a big role power supply concept, because wrong supplying can easy lead to common cause failure.

A common cause failure occurs when several failures have the same origin. Common cause failures are either common event failures, where the cause is a single external event, or common mode failures, where two systems fail in the same way for the same reason. Common mode failures can occur at different times because of a design defect or a repeated external event

For example overvoltage on the Main Power Supply's output on figure 2 can leads to same failure of all Auxiliary Power supplies, which can compromise all parts of the Fail-Safe.

The benefit of component duplication can be defeated by common-cause failure (CCF) or common-mode failures (CMF)

III. Crowbar Protection

Crowbar protection is a fail-safe protection mechanism which pulls the voltage below the trigger level, usually close to ground. A clamp prevents the voltage from exceeding a preset level. Thus, a crowbar will not automatically return to normal operation when the overvoltage condition is removed; power must be removed entirely to stop its conduction. Crowbar protection can also refer to a circuit which has its sole purpose to cause a fuse to blow by subjecting it to high current.

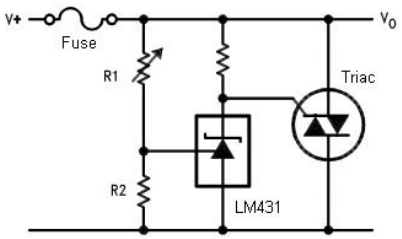

Fig. 3. Simple Crowbar Protection with SCR

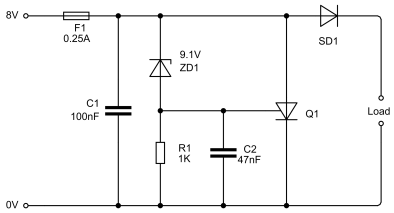

Fig. 4. Simple Crowbar Protection with SCR

References

[1] Definition single point of failure, (Date last accessed 11-August-2017). [Online]. Available: https://en.wikipedia.org/wiki/Single_point_of_failure.