

Programmable Electronic Systems: De-mystifying the Jargon

The last ten years or so have seen considerable growth in the use of Programmable Logic Controllers (PLCs) in safety-critical applications. This was expected, because PLCs had been successfully used much earlier as logic solvers for normal control operations, and they were found to offer much more flexibility than older systems.

Initially there was a reluctance to use programmable electronic equipment in safety critical applications because failure modes, particularly in software, were difficult to predict and control. As confidence grew, regular PLCs began to be used for safety functions, but it was soon realised that this still posed significant risk. It became necessary to design devices specifically for safety applications.

By 1999, international standards were developed and unified to help deal with the proliferation of programmable electronic safety-related systems. Unfortunately a combination of committees, foreign language translations and a legalistic approach has created guidelines that only a few technocrats can fully understand.

What is SIL?

How can managers assure themselves that proper diligence is being applied to these systems when technical jargon tends to be the norm? Foremost is the concept of Safety Integrity Level (SIL). Ask five technocrats for a definition, and expect five or more explanations – ranging from concise and understandable to completely unintelligible!

A simple definition of SIL: "A measure of the improvement needed to bring a system from its current state to an acceptable level of safety."

This immediately raises the questions: What is acceptable? Acceptable to whom? How do we measure improvement?

Some people think safety is freedom from risk. A better definition is "freedom from unacceptable risk". Unacceptable thus becomes a community standard that can change with time and communities. For those old enough, just recall safety standards that once applied to motor vehicles – when seat belts, air bags and ABS brakes did not exist.

What risk is acceptable to the community?

Let's say that a safety critical function in a mining application is being modified in some way. A common example of this occurs when outdated relay-based electrical equipment is replaced by modern programmable electronic systems. This is not to say that the relay system is technically unacceptable – but components have reached the end of their economic lives and replacement parts are difficult and costly to obtain.

The question arises, how safe should the new system be? Clearly it would need to be at least as safe as the system it is replacing – and perhaps considerably safer now that community standards have advanced in the intervening period.

Industry safety statistics provide a few more clues. It could be argued that new systems ought to be designed to provide levels of safety that are considerably better than industry average – things will not improve if new systems merely aim to reach average performance.

Risk and reliability engineering helps quantify safety targets and the levels of reliability currently being achieved. Engineers rely on performance data such as failure modes, dangerous failure proportions and failure rates for the

various hardware and software devices used. It is possible to estimate existing and expected improved reliabilities in a way that permits a numerical risk reduction factor or target to be specified.

This leads to a **more quantitative definition of SIL**: “A numerical measure of the risk reduction targeted or achieved by implementing a safety-related function.”

The standards list four levels of integrity, each representing a ten-fold improvement – or risk reduction – from the previous level. SIL 1 represents the least risk reduction (a factor of between 10 and 100), whilst SIL 4 represents a risk reduction factor of between 10 000 and 100 000.

How is SIL applied?

Imagine a safety system where if the system fails, a person will likely be killed. It is first necessary to estimate how often such failures could occur, then decide whether this is an acceptable risk. Deciding how often is not an easy task, but let's say operating experience suggests that fatalities could occur once in 30 years. Is this acceptable?

Suppose that industry average performance for this kind of incident is one fatality in 100 years. Clearly our current performance is below average and therefore unacceptable. If changes are proposed for the safety system, they should at least aim to reduce the risk by a factor of three.

There is a strong argument to say that the risk ought to be reduced by much more than three, perhaps by 10 or more. If a reduction of between 10 and 100 is chosen as a target, then the new safety system would need to be designed to achieve SIL 1.

One reason for choosing conservative targets lies in the confidence that can (or cannot) be had in estimated failure rates, industry data and the like. Much of the data is generic, making it hard to apply to specific situations. Order of magnitude errors are to be expected – adopting a conservative approach is prudent.

What SILs are being achieved in industry applications?

What happens if safety systems fail in chemical processing, railway signalling, aircraft control systems or nuclear power plants? Questions about consequences – and likelihoods – of system failures in these industries are being asked all the time. What improvement in system failure rates is required in order to produce outcomes acceptable to the community?

Answers typically range from SIL 1 and 2 in the chemical industries, to SIL 3 in railways and aviation, to SIL 4 in nuclear plants. In coal mining, system failures – and their consequences – in shuttle cars, ventilation controls, longwall systems and winders typically require risk reductions of SIL 2 or more.

Reference:

1. AS IEC 61508 – 1999: Functional safety of electrical/electronic/programmable electronic safety-related systems.

For more information, please contact:

Advitech Pty Limited
1 Elizabeth Street
Tighes Hill Newcastle NSW 2297

Tel 02 4961 6544
mail@advitech.com.au
<http://www.advitech.com.au>



Copyright © 2007
Advitech Pty Limited

The information in this document is of a general nature and is not intended to provide a complete and comprehensive discussion on every topic. While every precaution has been taken to ensure the accuracy of the information, Advitech Pty Limited accepts no responsibility for inadvertent errors or omissions. The information contained in this document is subject to change without notice.