Another EMC resource
from EMC Standards

How to do Risk Assessment (Part 2)

Helping you solve your EMC problems

9 Bracken View, Brocton, Stafford ST17 0TF T:+44 (0) 1785 660247 E:info@emcstandards.co.uk

Cherry Clough Consultants

How to do Risk Assessment (Part 2)

In last month's issue, Keith Armstrong introduced the topic of risk assessment. This time, he turns his attention to the potential ways in which hazards can arise, complete with an analysis of the likelihood of such occurrences

EurIng Keith Armstrong C.Eng MIET

keith.armstrong@cherryclough.com

Originally published in PSB Magazine, May 2009, http://www.psbonthenet.net, and reproduced here with their kind permission

An earlier column, PSB March 2009, introduced the European Directives that are commonly relevant to panel and system builders as regards safety, and discussed the role of Risk Assessment in complying with them and in reducing a company's exposure to financial risks.

Then in the April edition I started to describe how to actually do a risk assessment. This column continues this subject, to be completed in future columns (including how to deal with risks that are found not to be adequately controlled by the usual safety test standards).

Part 1 described Risk Graphs and how to use them to discover if a risk needed to be reduced. But it did not describe how to determine the hazards that can arise, and their probabilities – the input data required by such graphs. So this is the subject for this edition.

Unfortunately, there is no standard, correct and formal way to analyse risks – there is always the need for human judgement – and therefore for appropriate competence, skill and experience. A list of appropriate methods are given in section 3.7 of [1], some of them standardised, some not.

'Inductive' methods (sometimes called ''consequence' or 'bottom-up' methods), such as Failure Modes and Effects Analysis (FMEA) or Event Tree Analysis (ETA) generally start with a low-level error or failure, for example in a resistor or capacitor, and try to determine whether it could lead to a hazardous situation.

'Deductive' methods (sometimes called 'causal' or 'top-down' methods), such as HAZOP or Fault Tree Analysis (FTA) start with the hazardous situations and try to determine what could have caused them.

'Brainstorming' techniques identify all kinds of possibilities, then determine whether they could increase any risks. If the result is undesirable, the causes of the originally brainstormed possibilities are then determined to see what could cause them and help identify the risk level. Established brainstorming methods exist, and even if not directly relevant for an application, their approaches may still have some value. It is important to include a wide variety of people in a 'brainstorming session, including field service engineers, repairers, not just designers. And the person in charge should be from outside the project (ideally outside the company) and so able to focus on getting the process correct rather than getting involved in the issues.

To achieve a good 'coverage' of potential hazards and their probabilities for causing harm, it is usually necessary to use *at least* one inductive and one deductive method. FMEA and HAZOP-like techniques are often used together on projects, and another common pairing is Fault-Tree Analysis (FTA) and Event Tree Analysis (ETA). 'Brainstorming' is *always* recommended as well, to help identify faults and foresee use/misuse that the more formal methods would otherwise overlook.

A risk analysis should also consider hazards identified by *any* means: previous incidents; checklists; design reviews; human task analysis; etc. But, whatever techniques are used, good hazard identification and risk assessment depends on experience and imagination. Unfortunately, many manufacturers simply apply standardised methods in a 'rote' or 'mechanical' way, often using junior engineers with insufficient experience, just to put a tick in a management procedure box – a practice that safety experts warn against [2] [3]. Some of the issues that are usually overlooked follow below.

The concept of 'single-fault safety' is inappropriate. Instead, all of the independent faults that *could* occur simultaneously should be taken into account to see if the resulting risk requires reduction. For example, if there were ten independent faults that could each cause a particular hazard to occur, and if each had a probability of occurring once in every 100 years, then we would expect the hazard to occur once every 10 years on average. If, in a particular design, four independent faults would have to occur before a hazard could occur, and if each fault was random and could occur once in every year, then we would expect the hazard to occur on average once every four years.

Another common and often incorrect assumption is that failures occur at random (as in the above two examples). In fact many of the faults in electronic and programmable technologies are reliably triggered by

certain EMI and/or physical events, or sometimes simply by unanticipated combinations of perfectly correct inputs. These are called 'systematic' faults, and the only way to prevent them is by careful design and appropriate verification and validation techniques.

Yet another incorrect assumption is that failures or faults are permanent, when in fact they can be as temporary as an intermittent connection or transient EMI event, or momentary change in some parameter, that causes a delayed, degraded, distorted or false signal. The terms 'failure' and fault' need to be extended to include all undesirable events, and should not be assumed to mean (for example) simply all-or-nothing events such as permanent short-circuits or open-circuits.

Some EMI and physical events can cause what is known as common-cause or common-mode failures. For example overheating and/or overvoltages on the electrical power supply can cause two or more electronic devices to malfunction at the same time. Electrical transients, high temperatures, and ionising radiation can all conspire to cause semiconductor devices to 'latch-up', in which state all of their inputs and outputs can assume fixed and possibly undesirable levels, and correct operation can only be recovered by cycling the power to the device (assuming the device has not been overheated by unrestricted power supply current during its latch-up).

Reasonably foreseeable use/misuse is another very important issue that must be taken fully into account during brainstorming. Safety design should never assume that someone would never do anything because it would be 'too stupid'. People often do apparently stupid things during a moment of inattention or confusion (e.g. caused by poor human interface design), or when in a panic.

References:

[1] Guide on EMC for Functional Safety, The IET, 2008, www.theiet.org/factfiles/emc/index.cfm

[2] "The Reality of Risks", Erik Hollnagel, Safety Critical Systems Club Newsletter, Vol. 17, No. 2, January 2008, pp 20-22, www.safety-club.org.uk

[3] "Are 'Safety Cases' Working?", Tim Kelly, Safety Critical Systems Club Newsletter, Vol. 17, No. 2, January 2008, pp 31-33, www.safety-club.org.uk

The EMC Directive and UK Regulations, and their official guides, plus a great deal of useful and practical information on EMC and EMI, are available as described in the document: '*Some Useful References on EMI and EMC*' posted on this site.

EMI and EMC is often ignored (incorrectly) in risk assessments. People believe that as long as they ensure that the equipment passes the relevant EMC tests under the EMC Directive, maybe with the immunity test levels increased, this is sufficient. **But this approach is quite wrong**, and it is trivially easy to show why. Instead, read and apply the IET's new Guide on EMC for Functional Safety, 180 pages, August 2008, (which replaces the IEE's 2000 Guide). Free download from: www.theiet.org/factfiles/emc/index.cfm, and available as a reasonably-priced (£27) colour-printed-book from www.emcacademy.org/books.asp.