Another EMC resource
from EMC Standards

# How to do Risk Assessment (Part 4)

*Helping you solve your EMC problems*

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

# How to do Risk Assessment (Part 4)

**Risk assessment needs to be available during the initial stages of a project so that the 'Safety Requirements Specification', which guides the rest of the project, can be created. But since neither hardware nor software designs exist at this early stage, methods such as FMEA, Fault Tree, and so on, cannot yet be applied. We must create an 'Initial Risk Assessment', as Keith Armstrong explains**

> *"Obviously [when writing our Initial Risk Assessment] we will have to use a lot of engineering estimates and expert judgements, and these are always best done at the lowest level of detail that we can possibly contemplate at the time. Broad, sweeping estimates or judgements are easy to get wrong, often leading to large delays and costs during design, assembly and/or verification"*

Part 2 of this mini-series on doing hazard analyses and risk assessments made it clear that simply performing an FMEA (or any rote procedure) at the end of a project, is not enough. In fact, it is very far from what is required to ensure that our projects achieve tolerable safety risks for users and third parties, and tolerable financial risks for ourselves - whilst also achieving cost and time savings (or at least not adding significantly to costs or timescales).

Cherry Clough Consultants was started by Keith Armstrong in 1990 to help manufacturers reduce costs, time-scales and warranty costs whilst complying with the EMC Directive and other regulations.

Keith has a great deal of experience with the EMC of control panels, systems and installations, of all types and sizes, and with Tim Williams, wrote the only textbook on the subject: "EMC for Systems and Installations" (Newnes, 2000, ISBN 0-7506-4167-3, www.bh.com/newnes, RS Components P/No. 377-6463).

The 'Publications & Downloads' pages at www.cherryclough.com contain a great deal of helpful and practical information on EMC.

Part 2 showed us that a proper, defensible risk assessment must take into account the fact that:

- Faults do not only occur randomly, 'systematic' faults can also happen
- Several faults can occur at any one time, whether random or systematic
- People can behave in what appear to be the most amazingly stupid ways (and when they do, we can still be blamed if our equipment causes harm)
- Where electromagnetic interference (EMI or RFI) could possibly cause errors or malfunctions that could in turn increase safety risks - merely passing the normal EMC tests required by the EMC or R&TTE Directives, or by medical, military or aerospace standards will not be sufficient for demonstrating that tolerable safety risks have been achieved (see [1]).

Parts 1- 3 have showed us how to fill in everything in the first 5 columns of our risk assessment spreadsheet, leaving only column 6 - the final risk - to be calculated. We can easily calculate this from the previous 5 spreadsheet columns, and of course we must ensure that it falls below the level of risk considered tolerable for that hazard in that application, which we will often have found from an appropriate Risk Graph (see Part 1) - but may have to work out the hard way for ourselves.

We need our risk assessment to be available during the initial stages of a project, so that we can create what IEC 61508 [2] calls the 'Safety Requirements Specification' (SRS) that guides

the rest of the project (design, purchasing, assembly/construction, verification, commissioning, validation, operation, maintenance, etc., etc.) and will eventually be used for its final safety validation.

But since neither hardware nor software designs exist at this early stage, methods such as FMEA, Fault Tree, etc. cannot yet be applied. We must create an 'Initial Risk Assessment'!

Some of the methods mentioned in section 3.7 of [1] will be useful when writing our Initial Risk Assessment. Obviously we will have to use a lot of engineering estimates and expert judgements, and these are always best done at the lowest level of detail that we can possibly contemplate at the time. Broad, sweeping estimates or judgements are easy to get wrong, often leading to large delays and costs during design, assembly and/or verification.

During the subsequent stages of design, development, purchasing, assembly/construction, verification, etc., a great deal of very detailed information will become available on all of the mechanics, hardware and software. Other techniques, such as some of those listed in Section 3.7 of [1], should be applied to this data as it becomes available, to guide each of these stages and their on-going verification in real-time, to help achieve the overall goals of the Initial Risk Assessment.

Where our project has a defined customer, he should be asked if he prefers certain hazard and risk assessment methods to be employed. Some manufacturers will specify the ones they insist upon. But the hazards assessment and risk analysis work we do should not be limited to using only the methods required or preferred by the customer.

It is important to be aware that it is very well-known within the safety engineering community that there is no one method or technique, or group of them, which can be relied upon to provide the necessary hazard and risk assessment for any project - there is always the need for experienced and expert judgement. So we must never think that all we need to do is get some junior engineers to go through some rote methodology such as FMEA.

As shown in the Figures attached to Part 3 of this mini-series, all foreseeable hazards and all of their risks should be analysed at every iteration of the hazard/risk assessment, even where the hazards were considered negligible at the previous iteration. This is because changes to the design or marketing might add new hazards or increase the risks of existing ones.

In this way, our Initial Risk Assessment accumulates wider and deeper analyses, eventually producing - at the very end of our project - its 'Final Risk Assessment'.

This is a vitally important part of the safety documentation of our project, but it is the process of creating it, during the actual design, development and realisation activities, that is the important thing that enables the achievement of the desired levels of risk (or risk-reductions) whilst also achieving cost and time savings (or at least not adding significantly to the costs or timescales).

*"It is important to be aware that it is very well-known within the safety engineering community that there is no one method or technique, or group of them, which can be relied upon to provide the necessary hazard and risk assessment for any project - there is always the need for experienced and expert judgement"*

So our hazard analysis and risk assessment must be a 'live' document that should guide the project from its very conception, throughout its entire lifecycle (see Figure 0.4 of [1]) - as the design, marketing and customer expectations change, obsolete components are replaced, improved manufacturing techniques adopted, etc.

*"Changes to the design or marketing during a project might add new hazards, or increase the risks of existing ones"*

Changes in a project's hazard analysis and risk assessment do not always stop when the customer has fully paid our invoices. Whenever changes, modifications or upgrades are proposed throughout the lifecycle, it is necessary to revisit the hazard and risk analysis, to guide their design, construction, verification, etc.

I hope you have enjoyed this little series on Risk Assessment! In the next issue we'll get back to EMC design issues.

*References:*

[1] "Guide on EMC for Functional Safety", The IET, 2008, especially sections 3.4, 3.5, 3.7, 4.2.1, 4.2.2, free download from www.theiet.org/factfiles/emc/index.cfm, or as colour-printed book, ISBN 978-0-9555118-2-0, for £27 plus p&p from http://www.emcacademy.org/books.asp.

[2] IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", in seven parts, http://webstore.iec.ch