NEWSLETTER Issue no 57

Summer 2007

Contents

Edited by Dr Ian Lawrenson OBE

Further information regarding the articles in this issue is available from Simon Whalley on 020 7665 2230
email hazards.forum@ice.org.uk

1. John Lee

We are sorry to have to announce the death of John Lee on 24 May 2007, after a long illness. He had been Secretary of the Hazards forum since 1999. Although ill, he continued to work for the Forum, retiring only at the end of March.

John spent most of his career with the Health and Safety Executive where he was Head of the Unit covering the Civil, Structural and the Plant and Machinery disciplines of the Technology Division prior to his retirement in 1999. In his areas of responsibility, he provided professional leadership to the team of specialist inspectors engaged in the formulation and implementation of technical standards both national and international, the investigation of incidents, preparation of guidance and the provision of specialist advice and technical input to policy making. He was also responsible for liaison with the specialist inspectors in the Field Consultant Groups distributed around HSE's regional organisation. Central to his role was the interpretation in a variety of engineering contexts of the ALARP principle embodied in Health and Safety law and this required much technical interaction with industry on new developments as well as the management of a substantial research programme in order to codify good practice.

Aside from his job-related duties, John was active in the affairs of the Engineering Institutions; he was a member of both the Institution of Mechanical Engineers and the Institution of Engineering and Technology (formerly the IEE). He played a leading role in the establishment and operation of the Inter-Institutional Group on Health and Safety. He took great pride and satisfaction in his work to improve health and safety and he strove to engender greater awareness of the importance of risk reduction at all stages of the design process and the contribution that improved education of undergraduate engineers in risk topics could make in the longer term. Following his early retirement from HSE for personal reasons, he carried out a project on behalf of HSE in which he surveyed the views of universities, industry and other stakeholders on the education of engineers in risk concepts. This was very revealing in a number of ways but, perhaps more importantly, it identified specific actions which needed to be taken.

He joined the Hazards Forum in 1999, as Secretary in succession to Ian Lawrenson. He embraced his new role with enthusiasm and early on he was instrumental in establishing the Working Group of the Forum (in collaboration with the Civils, Mechanicals and Electricals) which produced the report 'Public Understanding of Risk: an Agenda for Action' in 2000. He was instrumental in launching the Hazards Forums series of evening events, and in expanding the membership. He was elected a Distinguished Member of the Hazards Forum by the Executive in March.

He was a courteous and patient man of great personal integrity as well as being very affable and well-liked and respected by all who worked with him. He will be greatly missed.

He is survived by his wife Gill, his daughter Susan and his grandchildren.

2. Introduction to Safety Integrity Levels (SILs)

Ron Bell OBE

Ron Bell Consulting Limited

---

1. Introduction

Over the past 25 years there have been a number of initiatives worldwide to develop guidelines and standards to enable the safe exploitation of electrical, electronic and programmable electronic systems used for safety applications (referred to hereafter as electronic safety-related systems). In the context of industrial applications a major standards initiative has been focussed on the international standard IEC 61508[1] and is emerging as a key standard in many industrial sectors. A key concept in this standard is that of the 'Safety Integrity Level' (SIL). This brief introduction is intended to indicate (1) why the concept is necessary and (2) the way the concept is applied.

2. What is functional safety?

Safety is defined as the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment. The concept of functional safety has been developed to cover that aspect of safety which is dependent on electronic safety-related systems.

'Functional safety' is defined as that part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. For example, an over temperature protection device employing a thermal sensor in the windings of an electric motor, which will de-energise the motor before the windings could overheat, is an example of functional safety. Functional safety is essentially about safety being achieved through the application of electronic safety-related systems.

In simple terms, we are trying to achieve a tolerable risk for the application, through the use of an electronic safety-system. This is achievable if the potentially hazardous events are properly identified and effective action is taken to prevent the potentially hazardous event becoming a reality. In order to achieve this it is essential that the safety requirements specification, for the design of the electronic safety-related system, contains two key pieces of information, namely:

The functions to be performed by the electronic safety-related system. These functions are called '**safety functions**'; and,

The safety performance of the safety functions in order to achieve the target tolerable risk. The safety performance, in this context means the degree to which we can rely on the safety functions being carried out when they are needed. The safety performance is called the **Safety Integrity**. The higher the safety integrity the more confidence there is that the safety functions will be carried out when required (ie the higher the safety integrity, the lower the rate of dangerous failures that would prevent the safety function from being performed).

If the safety function is performed the hazardous event will not take place. **The safety function is determined from the hazard analysis.** In order to meet the tolerable risk for the specified hazardous event, it is necessary that the safety integrity of the safety function is commensurate with the risk reduction required to achieve a tolerable risk. T**he safety integrity of the safety function is determined from the risk assessment.**

A safety-related system is a system that has the:

Functionality to carry out the safety functions; and,

The ability to carry out the safety functions with the required Safety Integrity.

A safety-related system will carry out many safety functions and must be of sufficient Safety Integrity to carry out the safety function with the highest SIL (unless special measures are taken). This is illustrated in Figure 1.

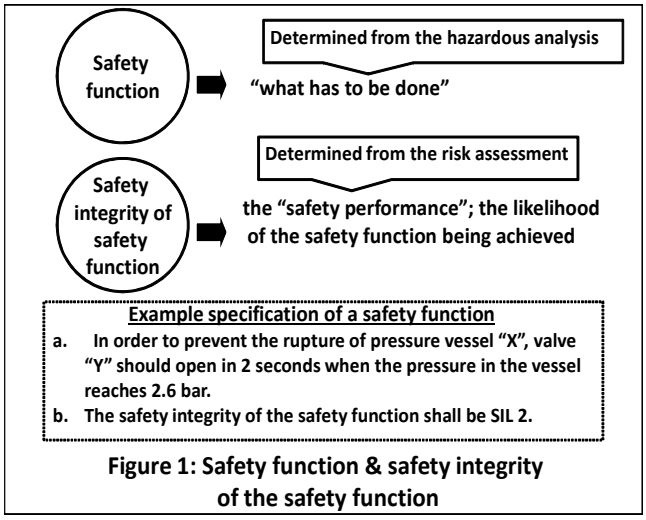

Figure 1: Safety function & safety integrity of the safety function

3. Strategy to Achieve Functional Safety

The strategy for achieving functional safety is made up of the following key elements:

Management of functional safety;
Technical requirements for each phase of the systems safety lifecycles;
Competence of persons;
Functional safety assessment.

In the context of the technical requirements (see above), the phases for the system safety lifecycle include the following:

Safety requirements specification;
Design and implementation;
Installation and commissioning;
Operation and maintenance;
Changes after commissioning.

Evidence of the need to adopt an approach that covers all phases of the safety lifecycle is illustrated in a study undertaken by the Health and Safety Executive[2]. The study analysed a number of accidents and incidents involving safety-related control systems. Figure 2 shows the primary cause of failure for each lifecycle phase.

Note: It is acknowledged that because of the small sample size the results of the analysis have low statistical significance, and therefore care needs to be taken in using these results to generalise for all control system failures. Even so, there are many useful lessons to be learned from summaries of incidents such as these.

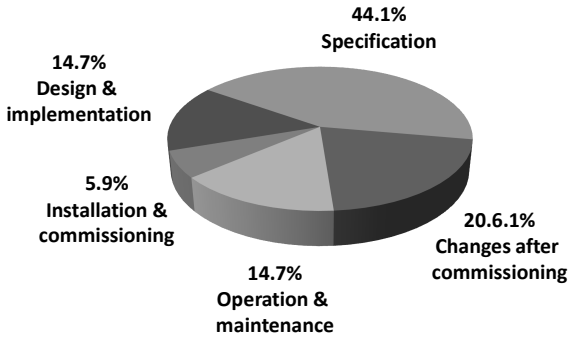

Figure 2: Primary cause, by phase, of control system failures

The analysis suggests that most control system failures may have their root cause in an inadequate specification. In some cases this was because insufficient hazard analysis of the equipment under control had been carried out; in others it was because the impact on the specification of a critical failure mode, of the control system, had not been properly assessed.

Based on the HSE study, more than 60% of failures were 'built in' to the safety-related system before being taken into service. Whilst the primary causes by phase will vary depending upon the sector and complexity of the application, what is self-evident is that it is important that all phases of the lifecycle be addressed if functional safety is to be achieved.

4. **Safety Integrity Levels**

The failure categories in IEC 61508 relate to failures arising from;

Random hardware failures:

Random hardware failures arise from degradation mechanisms in the hardware. It is difficult to determine exactly when a random hardware failure will occur but it is possible to predict, through reliability modelling, the failure rate with reasonable confidence.

Systematic failures:

In connection with electronic safety-related systems, particularly those that are programmable, it is not usually possible to model with reasonable confidence the systematic failures of complex systems. Also, it not possible to predict, in the same way as with random hardware failures, what the failure rate is likely to be. A characteristic of a systematic failure is that once the failure mode has been identified and rectified, then that particular failure mode will not arise again. Systematic failures arise from:

Errors in the safety requirements specification;
Errors in the software;
Failures arising from electromagnetic interference because of inadequate electromagnetic immunity;
Errors made during maintenance:
etc

IEC 61508 sets four **Safety Integrity Levels (SILs)**; SIL 1 is the lowest and SIL 4 is the highest level of Safety Integrity. Each SIL has a specified **target failure measure** (e.g. 1.5 x 10^{-6} probability of dangerous failure per hour for a SIL 2 safety function operating in a high demand mode of operation). It is the SIL of the safety function(s) to be carried out by a safety-related system that determines the measures that need to be taken in the design of the safety-related system.

Safety integrity is made up of:

Hardware Safety Integrity (in relation to random hardware failures); and
Systematic Safety Integrity (in relation to systematic failures).

The design strategy is to:

Develop design measures to tackle random hardware failures to achieve an adequate level of Hardware Safety Integrity; and
Develop design measures to tackle systematic failures to achieve an adequate level of Systematic Safety Integrity.

The SIL that has been determined, for a specified safety function, is used as the basis for the design measures for the achievement of the Safety Integrity for the electronic safety-related. The required Safety Integrity is achieved by using the SIL for the basis of the design measures for both Hardware Safety Integrity and Systematic Safety Integrity. The approach adopted is as follows:

Hardware Safety Integrity: This comprises two elements:

Achievement of the quantitative target failure measure for the specified SIL (through modelling of the random hardware failures);and

Architectural Constraints related to the specified SIL. The concept of architectural constraints is intended to provide added robustness to the design by providing tolerance against specified failures. The higher the SIL the greater the degree of robustness.

Systematic Safety Integrity: 'Packages' of measures are used for different systematic failure mechanisms and these are in general qualitative measures with increasing rigour, assurance and confidence the higher the SIL.

The above concepts are illustrated in Figure 3.

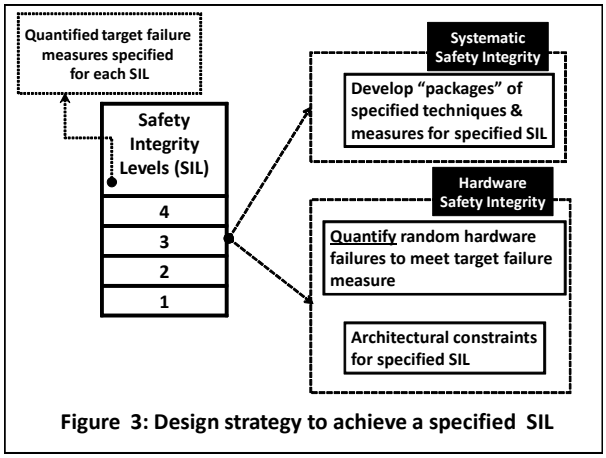

Figure 3: Design strategy to achieve a specified SIL

It can be seen from Figure 3 that:

For each safety integrity level (SIL) there is a quantified target failure measure.

The SIL is used as a basis for achievement of the Hardware Safety Integrity.

The SIL is used as a basis for achievement of the Systematic Safety Integrity.

Determination of the SIL is of fundamental importance. Once determined, the SIL is the key parameter that drives the design requirements for both the Hardware Safety Integrity and the Systematic Safety Integrity which are the constituent elements of the Safety Integrity.

5. References

1. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0-7
2. Health and Safety Executive (1995): 'Out of Control (why control systems go wrong and how to prevent failure)'. HSE Books 2003. ISBN 0 7176 2192 8. <www.hsebooks.co.uk>

6. Further information

IEE Functional Safety Professional Network http://www.iee.org/OnComms/pn/functionalsafety/
Functional and IEC 61508*
IEC61508 Brochure*
FAQ's on IEC61508*

* available on the IEC Functional Safety Zone (see www.iec.ch/functionalsafety).

Ron Bell spent several years in the telecommunications industry before joining the Health and Safety Executive (HSE) in 1976 as specialist in safety critical control systems.

From 1992 until his retirement from HSE in May 2006, he was head of the Electrical and Control Systems Group responsible for the development of technical policies and for taking the lead within HSE for international standards development in the field of electrical engineering and safety-related control systems that had an impact across HSE.

In 1988 he was appointed as one of the five UK members of the Channel Tunnel Safety Authority by the Health and Safety Commission, with responsibility, as UK Chair of the Civil Engineering and General Equipment Working Group, for advising the CTSA on all aspects of safety critical equipment of the Tunnel infrastructure.

He chaired the international IEC Task group that assessed the viability of developing an international standard for safety critical computer systems and then went on to chair one of the two (IEC) working groups responsible for developing IEC 61508. He currently chairs one of the two teams responsible for the revision of this standard.

In 2006 he set up his own consultancy business specialising in the functional safety of safety critical systems including the management of functional safety competence management systems.

He was awarded the OBE in 2006.

3. A Lull in the North Atlantic?

Why were the forecasts for the 2006 hurricane season wrong? Most experts believed that Katrina and the other 2005 hurricanes, which led to record insured losses of $80bn, were a sign of above-average storm activity to come, but the 2006 North Atlantic hurricane season fell far short of the high levels of activity forecast by all the reputed institutes. There were only ten named tropical storms, five of which reached hurricane force.

This is in line with the average over the past 56 years, when there were around ten named cyclones per year, including six of hurricane force. With only two hurricanes of category 3 or more (ie with wind speeds of over 178 km/h), 2006 was below the 1900–2006 average (three) and well below the average for 1995–2006 (about four).

Scientific reasons for the low level of activity

Sea surface temperature

Many scientific papers published last year provided further evidence that sea surface temperature is one of the main parameters of storm activity in the North Atlantic. Following all-time highs between June and October 2005 sea surface temperatures in the main hurricane breeding ground of the tropical North Atlantic were lower in 2006. However, they were nonetheless high, the deviation above the 1961 – 1990 average (+0.59°C) being the third-highest since the beginning of the period under observation. Furthermore, sea temperatures in 2006 were high enough to have triggered an extremely active season. Accordingly, to find the reasons for the lower level of activity, we need to look elsewhere.

Dryness

The main reasons for the small number of cyclones were widespread atmospheric dryness over the tropical North Atlantic and the effect of El Niño in the Pacific, which developed rapidly in the period between August and October. The dry, warm layer of air increases the energy barrier that must be overcome to allow warm, moist air to rise up from the surface of the water, where it can subsequently produce tall thunderclouds and result in cyclones. The air over the sea therefore required more convective energy in order to rise up through this layer. This hampered the formation of clouds and storms. This dryness is caused by high concentrations of mineral particles in the atmosphere which absorb solar radiation, thus warming the surrounding layer of air and making it drier. This concentration of particles, which can span the entire Atlantic from Africa to Central America, is caused by sand blown from the Sahara.

El Niño is another phenomenon which has a drying effect on the air. Over the Caribbean and tropical Atlantic in particular, displacement of the circulation patterns can bring about a downward motion. As the air sinks, it becomes warmer and drier. Analyses show that, between June and November 2006, the moisture content of the middle atmosphere over the tropical North Atlantic was consistently below the long-term average. Indirect evidence of this is an above-average water vapour brightness temperature due to a lack of water vapour in the atmosphere.

Vertical wind shear

A further mechanism plays a major role in the formation of hurricanes: different wind forces in the upper and lower atmosphere. The greater the difference in wind force and direction, the lower the propensity for tropical cyclones to develop. This vertical wind shear is a factor whose annual cycle affects the typical course of the hurricane season. In September, vertical wind shear is at a minimum whilst activity, on average, is at a maximum. Wind shear is a very effective means of controlling cyclone activity. Typically, it increases from October onwards, bringing the hurricane season to a close.

Distribution of the different mechanisms at play across the season

The 2006 season got off to an earlier than average start, the first named tropical storm forming on 11 June. In June and July, sea surface temperatures were 0.5–1.0°C cooler and the air over the eastern

tropical Atlantic drier than in 2005. Accordingly, activity in those two months was far less pronounced than in 2005 (with three storms compared with
seven) and in keeping with the 1995–2005 average. In August 2006, there were three storms – well above the long-term average but below the average for the previous 12 years. This was mainly due to the effects described above, of mineral particles swept up from the sand of the Sahara, producing warm, dry air. Vertical wind shear was also high at the beginning and towards the end of the month, a factor not conducive to cyclones. In September, activity increased to just below the mean for the previous 12 years, vertical wind shear in the tropical Atlantic and Caribbean being below average

The North Atlantic hurricane season ended relatively early, at the beginning of October, westerly winds in the upper atmosphere having strengthened due to the rapid development of El Nino; wind shear had accordingly increased sharply.

Future storm activity

After the remarkably subdued 2006 Atlantic hurricane season, this year's season might well be more active. The Tropical Storm Risk venture, involving the insurance industry with the Benfield UCL Hazard Research Centre, UCL and the Met Office, forecasts a return to livelier activity in 2007. They forecast that Atlantic Basin and US land-falling tropical cyclone activity will be 60% above the 1950 - 2006 norm, with around 15 or 16 tropical storms and perhaps 8 or 9 hurricanes.

The full report and further information is available at http//tsr.mssi.ucl.ac.uk

---

4. Forthcoming Hazards Forum Events

The following evening events are planned by the Hazards Forum for the period September 2007 to March 2008:

3 October 2007	Risks associated with Organisational Change
20 November 2007	Managing Risks re the London Olympics
11 March 2008	AGM plus event.

These dates are provisional and will be confirmed later.

Attendance at Evening Events is by invitation only. Those wishing to attend should contact the Secretariat, Simon Whalley on 0207 665 2230, or at hazards.forum.ice.org.uk

---

5. NASA Earth Observatory

Earth scientists around the world use NASA satellite imagery to study the causes and effects of natural hazards. The goal in sharing these images is to help people visualize where and when natural hazards occur, and to help mitigate their effects. These images are freely available to the public for re-use or re-publication.

By taking out a subscription (free of charge) to 'Natural Hazards' you will receive once a week or once a day, a short notice by email from the Earth Observatory: Natural Hazards telling you about the latest events and letting you view the images on the site.

A subscription may be made by accessing http://earthobservatory.nasa.gov/NaturalHazards/

6. 'Science in Parliament'

As a member of the Parliamentary and Scientific Committee the Hazards Forum receives a copy of the Committee's journal *'Science in Parliament'*, which is published quarterly. As it is not feasible to circulate our copy of the journal widely, the contents of each issue are shown in the Hazards Forum Newsletter. Any member who wishes to see any of the articles should contact the Editor at ilawrenson@theiet.org

Spring 2007 Volume 64 Number 1

Spring 2007 Volume 64 Number 1

7. Membership of the Hazards Forum 2007

Distinguished Members

Professor P A Bennett, FREng
Professor Sir Bernard Crossland, CBE FRS FREng
Dr S N Mustow, CBE FREng
Dr A C Patterson, CBE FREng
Professor P O Wolf, FREng
Professor Sir Frederick Warner, FRS FREng

Institutional, Corporate and Individual Members include:

British Computer Society
British Hydrological Society
British Psychological Society
City University
Cranfield University
Ergonomics Society
Eurogears Ltd
Geological Society
Institute of Measurement and Control
Institution of Chemical Engineers
Institution of Civil Engineers
Institution of Engineering and Technology
Institution of Mechanical Engineers
Institution of Materials, Minerals and Mining
Institution of Occupational Safety and Health
Institution of Structural Engineers
Lancaster University
Met Office
National Health and Safety Groups Council
Risk Management Solutions Ltd
Risk Support Ltd
Royal Academy of Engineering
Royal Society of Chemistry
Safety and Reliability Society
Society of Industrial Emergency Service Officers
University of Nottingham
University of York

BP plc
Corus Group
CSE International Ltd
DSTL
Healh and Safety Executive
Lloyd's Register
NEBOSH
Rail and Safety Standards Board
Shell UK Ltd
United Utilities

Mr Ade Adeyemo
Dr John Bond
Mrs Patricia Bond
Mr Iain Carter
Mr Nigel Cheetham
Mr Frank Crawley
Mr Graham Dalzell
Dr Chris Elliott
Mr David Eves CB
Mr Robert Foster
Mr Robert Gilchrist
Mr Frank Groszmann
Mr Brian Neale
Mr Peter Livock
Dr J McQuaid CB
Mr Mark Paradies
Mr Fred Pell
Mr Michael Selfe
Mr Gordon Senior CBE
Mr Ed Spence
Mr Brian G J Thompson
Mr Simon Turner