Learning from incidents involving electrical/electronic/ programmable electronic safety-related systems – Project outline

Mark Bowell, Technology Division, Health and Safety Executive
George Cleland, Adelard
Luke Emmet, Adelard

Introduction

As technology develops, economic activity varies and cultural attitudes change, the factors influencing accident situations in industry also change. One area of substantial technological development has been the way in which the massive increase in computational power has allowed sweeping changes in the control of safety-related systems applied to plant and equipment. The UK Health and Safety Executive (HSE) needs to stay abreast of these changes and of their influence on accident situations in order to provide industry with best advice on how to achieve safe working environments.

As part of this process, HSE has initiated a programme of work that will eventually provide:

- guidance for those responsible on how to learn from their own incident data;
- a means for HSE to ensure that it has the best information attainable on incidents involving electrical/electronic/programmable electronic (E/E/PE) safety-related systems;
- a stimulus to industry through a successor to "Out of Control" [1].

The Electrical and Control Systems Unit within HSE's Technology Division strongly contributed to the international standard IEC 61508 "Functional safety of electrical/ electronic/programmable electronic safety-related systems" [2]. This sets out specific requirements for systems involving computer control, within a high level framework that defines the safety lifecycle and safety management activities that should be followed.

One of these requirements is the need to learn from experience. Subclause 6.2.1 of IEC 61508-1 states that responsible organisations or individuals should consider specifying, implementing and monitoring the progress of:

> "procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations are made to minimise the probability of a repeat occurrence."

The above requirement presents a goal to be achieved and, as is often the case with goal based objectives, does not say how this should be done. The implementation details will depend on the organisation that is trying to learn, its maturity in terms of data collection and analysis, and the criticality of the systems that it is responsible for. The terminology, concepts and approach of IEC 61508 will provide grounding for the programme.

In addition to the requirements of standards, organisations are increasingly realising the importance of their knowledge assets. They are keen to have those aspects of this knowledge base, which are currently tied to individuals, shared throughout the company. The recent interest in concepts such as organisational learning, corporate memory, and knowledge management reflect this concern. Those in the safety-critical arena have an even greater need

to adopt these approaches, as expertise is in short supply and currently tied very much to key individuals and occasionally certain high-performance teams.

The HSE guidance document "Out of Control" analysed the causes of 34 incidents involving control systems, and presented the results as a pie chart showing the relative occurrence of primary causes by lifecycle phase. The intention is that its successor will contain results for a greater number of incidents, work within the framework of IEC 61508, and demonstrate the usefulness of incident information.

As a first step, HSE has contracted a consortium, led by Adelard and also involving the Glasgow (University) Accident Analysis Group (GAAG) [3] and Blacksafe Consulting, to carry out a 7-month interactive project that will:

1) identify and evaluate existing schemes for classifying causes from incident data and generating lessons to avoid recurrence of similar incidents;
2) select and modify an existing scheme or schemes, or derive a new one, in order to create a method for analysing and classifying incident data to match the principles and activities of IEC 61508;
3) test the new method using data from a small number of real incidents; and
4) identify and present the significant strengths and weaknesses of the proposed method and how it fits in with wider issues such as incident reporting, incident investigation and process improvement.

This project is part of HSE's longer-term programme to provide best advice in this field.

Technical approach

Phase 1 – Evaluation of existing schemes and stakeholder consultation

In this phase the project will evaluate existing schemes and undertake a requirements capture and analysis exercise with the main stakeholders. Although the scheme itself will address the requirements emerging from IEC 61508, we will consult on the most relevant level of support needed. For example, some industries or organisations may be looking for an overall process that they can customise, whereas others may be looking for more concrete artefacts in the form of tool support and an explicit method.

First, the project will identity and classify a selection of existing schemes from a literature review, and prior knowledge – Glasgow Accident Analysis Group has already undertaken an extensive review of these techniques. Many of these are themselves a synthesis of established approaches for particular applications. Other recent work [4]-[11] is applicable here.

In order to appropriately evaluate alternative schemes it is important to identify desirable characteristics for the new scheme. These will also be used to inform evaluation of the scheme itself. Characteristics for consideration include consistency, coverage, generality, configurability, usability, simplicity, extensibility, and understandability.

These will be developed and defined to best meet the following criteria:

– satisfaction of HSE's overall project objectives;
– effectiveness in learning all possible lessons and preventing further incidents;
– usefulness to relevant parties (taking current practice into account);
– simplicity, usability and understanding;

– ease of training;
– consistency of results;
– compatibility with IEC 61508 concepts and activities;
– flexibility when applied to data of varying detail and quality; and
– visibility of assumptions and of level of confidence in analysis results.

The characteristics above are not all mutually compatible. For example, an engineer and a usability expert might assess causes of an incident differently. Both views might be equally valid, but there may not be a consistent assessment. On the other hand coverage is improved. Other trade-offs should become clear in the analysis, and balancing decisions will be made.

Based on the results of the initial evaluation, the project will identify a number of candidate schemes that have desirable characteristics and will consult the stakeholders in these schemes. This will establish both user requirements and current best practice and experience in actually deploying incident reporting and analysis schemes. Adelard's consultation process involves the development of briefing material followed by interview or desktop analysis. Briefing notes are used to guide discussions, but are not rigidly followed. Instead the interview process is allowed to develop freely. This usually results in a richer discussion, sometimes uncovering unexpected threads. The briefing notes are reviewed again towards the end of the meeting to ensure all planned areas have been covered.

The briefing material and subsequent interviews will address the key concerns of:
– how companies collect and use their own incident data, impediments to data collection,
– what characterises reliable incident data and how this is acted upon when available,
– the perceived applicability of data when taken from other companies, applications or sectors.

The following table is indicative of the type of coverage that will be sought.

Stakeholder **Domain**	Procurers	System Suppliers	Users	Maintainers	Assessors/ licensors/ regulators	Standards/ guidance developers	Academics and consultants
Process	I	I	I	I	I	I	E
Offshore	I		I				
Machinery		I	I				
Nuclear	I	I			I	E	
Railways					E, I		
Marine	E		E				
Medical		E	E		E		E
Aviation		E			E, I		E
Defence	E					E	E

I implies interview, *E* experience capture from a review of material

Consultation activities will be varied, and optimised for the organisation approached and expected benefit. Activities will include face-to-face meetings, telephone interviews, and in some cases observation of schemes in use. In addition the task will include, where appropriate, pre- or post-consultation desk reviews. Previous consultation exercises have shown that interviewees will often have more than one role and that there are diminishing returns on the amount of new information as coverage increases. The later stages often act as validation of earlier findings.

Phase 2 – Develop new scheme

Phase 1 will reveal the best existing schemes to form the basis for the scheme to be developed. Phase 2 will develop a candidate new scheme and a software prototype, will identify candidate data to use in its evaluation, and will run an open consultation workshop.

In developing the new scheme, the project will specify the changes required to existing schemes to satisfy the new scheme's requirements, especially those relating to compatibility with IEC 61508. Compatibility issues include:

- interface to the main safety lifecycle phases for the E/E/PE safety-related systems,
- interface to activities in IEC 61508, e.g. looking at the phase of the product development where a fault was inserted,
- identification of criticality of systems and components and relating these to the safety integrity level (keeping in mind that the safety integrity level applies to safety functions),
- the relationship to the risk apportionment model in the standard,
- relationship to the software and hardware techniques,
- correct use of terminology from IEC 61508.

The work will also take into account sector specific derivatives such as IEC 61511.

A new scheme will be developed based on these findings together and a rationale presented.

The project will build an example web-based implementation of the proposed scheme that other organisations can use as a basis for their own system. This will be designed using rapid application technology, and will support enough of the scheme for the evaluation in phase 3.

During the consultation a small number of candidate organisations will be identified to assist with running of the evaluation phase. Working with them the project will identify incident data to be used on the trials, taking into account the range of criticalities and the different types of user likely to be involved in such schemes. The scheme characteristics developed in Phase 1 will be key factors in identifying candidate data and organisations.

A position paper will describe the work to date, including an outline of the scheme, and its rationale. The project will run a consultation workshop to which stakeholders will be invited. Feedback from this workshop will be valuable in positioning evaluation of the scheme and refining the final version.

Phase 3 – Evaluation of the new scheme

Simple usability testing will be conducted in-house as a sanity check for the scheme before conducting the external evaluation. Testers will not have been involved in the project up to this point, but they will be familiar with similar reporting schemes.

Following this, and based upon the data gathered and organisations identified in Phases 1 and 2, the scheme will be evaluated using field trials. This will involve two organisations from different domains, with at least three users from each organisation. Stakeholders with differing viewpoints will be included in the study, and the number and scale of incidents should be representative. Concentrating on high impact, large-scale events is not appropriate as these will be visible and handled specially. Instead the project will look at typical event sets and evaluate how effective the scheme is at drawing out appropriate conclusions and patterns.

The results of these tests will be evaluated against the test criteria. This information will be used to produce a set of recommendations for upgrading the scheme.

Phase 4 – Consolidation of and deployment support for scheme

This phase will provide a detailed rationale for the new scheme (based on output of Phase 2), and will update the scheme according to the recommendations from Phase 3.

The prototype software developed during Phase 2 will also be updated to reflect the new scheme.

An appraisal of the scheme will include its strengths, weaknesses and trade-offs that have been made in its development.

The scheme developed will be generic, implementing the requirements of IEC 61508. Practical use of the scheme will require guidance on how it should be customised for specific use. The project will draft guidance in this area, and also draft limited domain guidance for at least one domain. The audience will be base-level industry users, i.e. those with low levels of current capability or sophistication in such schemes.

More sophisticated users will be able to use the scheme in more flexible and powerful ways, building it into a safety and process improvement model, including potential use of the software tools developed on this project. Draft customisation guidelines will be produced which could support such users in deploying the scheme most appropriately for their level of sophistication.

The classification and analysis scheme developed is only part of the whole process of incident reporting. The project will summarise concerns and strategies on the wider issues of process improvement, incident reporting and incident investigation. The issues to be considered include:

- fragmentation and cohesion of industry sectors;
- change in style of standards from prescriptive to goal based;
- maintenance of competencies in older technologies with maturing workforces;
- professional trajectories - dilution of culture; and
- organisational and individual resistance to reporting.

Way forward

HSE will use the results of this project to draft and publish guidelines on how companies can learn from their own incidents that involve E/E/PE safety-related systems.

After these guidelines have been published, our aim is to work in conjunction with several companies to gather and make available anonymised categorised incident data and analysis results from a large number of incidents. This will help HSE to:

- publish new guidance material to supplement “Out of Control”;
- determine technical priorities for HSE inspections where applicable and appropriate;
- justify HSE's policy, technical priorities and resource usage;
- develop HSE's input to standards and guidance;
- demonstrate that learning from incident data is both feasible and beneficial; and
- increase the awareness of industry and other organisations to common problems.

Acknowledgements

The authors would like to acknowledge input to this work from other project members, in particular Robin Bloomfield and Peter Bishop of Adelard, and Chris Johnson of Glasgow University.

References

[1] HSE, “Out of Control”. Health and Safety Executive, ISBN 0 7176 0847 6, 1995.

[2] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, 2000. See http://www.iec.ch/61508 for further details.

[3] Glasgow Accident Analysis Group (web site) http://www.dcs.gla.ac.uk/research/gaag/.

[4] J Henderson, C Whittington & K Wright. Accident investigation -The drivers, methods and outcomes, http://www.hse.gov .uk/research/crr_pdf/2001/crr01344.pdf.

[5] A D Livingston, G Jackson & K Priestley. Root causes analysis: Literature review, http://www.hse.gov .uk/research/crr_pdf/2001/crr01325.pdf.

[6] F Koornneef, “Organised Learning from Small Scale Incidents”, Delft University Press, ISBN 90-407-2092-4, 2000.

[7] Eurocontrol, “Reporting and Assessment of Safety Occurrences in ATM”, Eurocontrol Safety Regulatory Requirement, ESARR2, Edition 2, 03-11-2000.

[8] NASA, “NASA Procedures and Guidelines for Mishap Reporting”, Safety and Risk Management Division, Washington DC, USA, NASA PG 8621.1, 2001. See http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm.

[9] "Final Report of a Study to Evaluate the Feasibility and Effectiveness of a Sentinel Reporting System for Adverse Event Reporting of Medical Device use in User Facilities", Food and Drug Administration, Office of Surveillance and Biometrics, Center for Devices and Radiological Health". See http://www.fda.gov/cdrh/postsurv/medsunappendixa.html.

[10] T S Ferry, Modern accident investigation and analysis, 1988, Wylie, ISBN 047 16248.

[11] E D Rademaeker and J P Pineau (Eds). Accident databases as a management tool, Proceedings of the 15th ESReDA Seminar, Antwerp, 16-17 November 1998, ESReDA.