SAFETY CULTURE; CORNERSTONE OF THE NUCLEAR SAFETY CASE

R.J. Cullen
Pöyry Energy, Warrington, UK

Engineering substantiation forms a major part of the modern standards nuclear safety case and increasingly within safety cases for the process industries: substantiation is itself dependent on safety management systems or so-called "safety culture" to ensure engineered systems perform as required. It follows therefore that the existence of a good safety culture is a prerequisite for a good safety case. The converse is also true; the existence of a poor safety culture will lead to a substandard safety case no matter how convincingly the safety argument is presented.

It is during the implementation of the Safety Case that the dependency of the safety argument on safety culture becomes apparent. This paper looks at where in the safety case the dependencies on safety culture exist and also examines safety case implementation strategy employed by nuclear chemical plant which highlight these dependencies and how they are managed. In this way lessons can be learnt by safety case assessors and managers about the importance of safety culture underpinning the safety case and how it should not be taken for granted in developing the safety argument. Although this paper takes the nuclear safety case as its basis, the discussion will be equally applicable to all safety cases within the process industries.

INTRODUCTION

The modern standards nuclear safety case has gone through significant changes over the past 3 decades; evolving from the first set of Fully Developed Safety Cases fdSC first produced in 1987 for BNFL to the comprehensive set of documents currently produced by UK Licensees. Initially, the adequacy of a safety case (development of a robust safety argument) was largely dependent on a demonstration that numerical targets had been met (probabilistic assessment). The inherent drawback with this singular approach was that there was no clear demonstration that the specified engineering required to achieve compliance would deliver its stated safety function. Hence a further iteration of safety case methodology came about, the need to base the adequacy of safety on a demonstrable set of engineering (hazard) controls with defined safety functions and a demonstration that such functions could be met. This is the basis of engineering substantiation, the deterministic approach to the demonstration of the adequacy of safety. The safety case becomes therefore an engineering-based formal demonstration of the adequacy of safety of a facility at every stage of its life from inception, build, commissioning, operation and eventual decommissioning. This is well understood both within and outside the safety community. Equally well understood, but often under estimated is the role that safety culture plays both in the development and in the implementation of the safety case.

Although this paper uses the nuclear safety case as its basis, the role that safety culture plays within the case is equally applicable to safety cases within the process industries. This is because there is no difference in the need to demonstrate safety adequacy in non nuclear plant and process. Where this involves engineering substantiation as the pivotal element then the implicit role of safety culture becomes significant.

This paper aims to focus attention on the importance of safety culture in each stage of safety case production and implementation. Examples from existing plant and process will be used to illustrate the points made. In this way attention is drawn to the many occasions on which safety professionals make assumptions about the validity of an extant safety culture in the formation of a safety argument without necessarily questioning or validating them. This can lead to a safety argument which looks good on paper but fails in practice. In highlighting the importance to safety assessors and safety case managers of the need to understand the role that safety culture plays in the assumptions made and arguments presented in the safety case, safety professionals are better placed to advise plant personnel on the impact that their behaviour makes on the safety arguments specified in the safety case.

To understand how these assumptions are arrived at and made it is first necessary to define safety culture before examining the common elements which make up the modern standards nuclear safety case. In this way a better understanding can be developed about where assumptions are made regarding safety culture in safety case development and implementation.

SAFETY CULTURE

The term "safety culture" was first introduced by the International Nuclear Safety Advisory Group (INSAG) following the Chernobyl nuclear accident. With reference to this and subsequent accidents it was concluded that it was not necessarily the safety management systems which were at fault but the safety climate and culture within which these management systems existed[1]. There are many different definitions of the term but the one most widely adopted is that developed by the Advisory Committee on the Safety of Nuclear Installations (ACSNI):

[1]ACSNI 1993.

"The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management."

(HSE 1993)

A much simpler, more easily digestible but equally cogent definition was coined by the Confederation of British Industry, CBI:

"The way we do things around here."

(CBI 1990)

Both these definitions put people rather than procedures at the heart of the meaning of safety culture and the focus is on how people behave. With regard to safety it is how people behave safely and the motivation that is offered in order that safe behaviours dominate. Simplistically therefore a "good" safety culture is where plant personnel behave with due regard for safety and are continually encouraged to do so such that potential faults are avoided and hazards are minimized. A "bad" or non existent safety culture is one within which plant personnel have little or no regard for safe practices, no encouragement is offered and the potential for faults to develop into hazardous situations is particularly high. A "good" or "bad" safety culture can exist independently of the presence and availability of well-defined safety policies and procedures. If the motivation (and hence behaviour) to utilize and adhere to such policies and procedures is not present (or not continually reinforced) then no matter how good such documents are in describing what ought to be happening, safety culture will be poor or non existent.

The Health & Safety Executive (HSE) has produced guidelines on what factors contribute to a good safety culture or conversely are absent in a poor one.[2] These relate to things like management interest, employee empowerment for safety, no-blame culture and good communications.

Much has been written about safety culture but for the purposes of this paper the essential point to be made is that safety culture is people-based and its development is dependent on the proactive nature of plant management towards its workers in promoting and maintaining "safe" behaviours. This process is not immediately apparent in the Safety Case, nevertheless its presence is assumed during both its development and implementation. The following sections will establish the essential elements of the safety case; then examine within them how safety case authors and managers make assumptions as to how plant personnel will behave and base safety arguments on those assumptions.

[2]HSE Human Factors Briefing Note No. 7.

ESSENTIAL ELEMENTS OF THE NUCLEAR SAFETY CASE

It is a requirement of the Nuclear Site Licence[3] that nuclear facilities have an extant safety case covering plant and process. This applies at all stage of plant and process life: design, build, commissioning, operation and decommissioning activities. The format and language of nuclear safety cases across the various Licensees which operate nuclear plant and processes can vary greatly but, for a well produced safety case, it is easy to see the presence of the essential common elements which must be present.

PLANT & PROCESS DESCRIPTION

This essentially defines the scope and content of the Safety Case. This covers not just the plant and process (at a defined stage in its development) but also clearly defines the boundaries and interfaces, other plant dependencies as well as input and output process streams. It is purely descriptive and does not contain any safety argument; it is the basis on which the safety argument is developed and justified.

HAZARD IDENTIFICATION

This is generally seen as the most important part of the safety case: with respect to the written demonstration of safety, the production of the safety case, this is true. Hazard identification covers not just the formal identification processes (HAZOP, HAZID etc.) but also takes account of the experiences and lessons learnt from similar plant and process to that being considered. When hazard identification involves the use of a multi-discipline team that includes among others plant operators (or operators from a similar plant if the one under consideration is still at the design stage) then this inclusion enriches the identification process with input from a "real" set of operations.

HAZARD ASSESSMENT

Identified hazards are assessed against standard risk criteria. Each Licensee defines his own criteria but essentially they encompass the requirements of the NII Safety Assessment Principles, SAPs.[4] Hazards are categorised according to their severity. For radiological hazards, severity is generally defined in terms of operator or public dose with reference to the requirements of the Ionizing Radiation Regulations, IRRs.[5] For non-radiological and other process hazards, severity is defined in terms of potential for injury or death to affected individuals or groups. Using standard assessment techniques (consequence analysis, Probabilistic Safety Assessment etc.) the requirement for hazard controls is identified. Hazard controls are (ideally) robust engineering measures backed up by administrative (procedural) measures which ensure that the hazard cannot occur and give rise to the specified consequences. Defence in depth

[3]Nuclear Site Licence Condition 14
[4]NII SAPs 2006
[5]IRRs 1999.

is achieved by defining diverse protection (commensurate with the severity of the hazard) and mitigators which would reduce the consequences (and hence severity) of the hazard in the unlikely event of the failure of the (preventative) hazard controls. Assessment is both deterministic – confirmation that suitable and sufficient hazard controls are in place such that the overall risk is deemed acceptable; and probabilistic – a logical and numerical analysis of fault development and its termination by the specified controls which leads to a comparison against numerical targets. Compliance with such targets is a further demonstration of acceptable safety.

ENGINEERING SUBSTANTIATION

Specifying engineering measures to provide the required hazard control is one thing, ensuring that it can actually carry out the task is another. This emphasis on the need for engineering substantiation, an essential element of the safety case, is a relatively recent development in safety case methodology. The safety assessor determines the engineering requirements (the safety functional requirements, SFRs) that will ensure safety; the engineers determine how that function can be achieved. Put simply can the engineering do what is specified in the SFRs? In order that this is achieved, substantiation of the performance is needed to demonstrate that the SFRs are met. In terms of the development of the safety case this is the formal meeting between safety and the rest of the design team; the culmination of safety in design development. This is the opportunity to confirm that the designers understand the safety case requirements, the need for specific safety functions (performance requirements) and that the safety assessors are realistic in their expectation of equipment performance. This so-called "reconciliation" series of meetings between designers and safety ensure common understanding develops regarding the importance to safety of plant and process equipment and is pivotal in the development of robust engineering substantiation. Substantiation of the design intent (e.g. that a pump will deliver the required liquor flowrate) assumes that the engineering measure is operated and maintained as required by the design intent. Licensees also carry out substantiation of procedural requirements on the basis that, together with the engineering, they support the demonstration of adequate safety. This "parallel" substantiation process includes such activities as human factors (task analysis) and analysis of operating instructions.

SAFETY MANAGEMENT

Every safety case requires a formal demonstration that top level safety policies are present to which the Licensee adheres and that there are local safety procedures in place (or in development for a plant in the design stage) which are followed by the workforce. This section defines activities such as safety responsibilities, the need for training, review of accidents, learning from experience etc.

ALARP

The preceding sections of the safety case will have demonstrated that the risk from identified hazards is acceptably low. However there is a legal requirement in a nuclear safety case to ensure that risks from potential hazards are not just acceptable but are as Low as Reasonably Practicable or ALARP. Could more be done to reduce the risk still further – additional safeguards, engineered and/or procedural? The NII SAPs[6] offer a numerical basis for the development of a robust ALARP argument in the Safety Case. Developed from the Tolerability of Risk philosophy, levels are set above which the risk (from a potential hazard) is considered intolerable (Basic Safety Limit, BSO) and below which the risk is broadly acceptable (Basic Safety Objective, BSO). Hazard risk that is determined to be between these two levels requires an ALARP argument to ensure its acceptability. That does not mean to say that all hazard risks determined to be below the BSO are automatically considered ALARP. The Licensee must always demonstrate for all identified hazards that the risks are ALARP no matter how numerically "acceptable" they appear to be. The BSO simply represents that risk level below which the NII would not normally seek improvements but this does not absolve the Licensee from ensuring such risks are always ALARP. Licensees have a formal ALARP review process which demonstrates that ALARP has been explicitly considered within the safety case.

ACCEPTANCE AND REVIEW

The safety case undergoes a structured QA and peer review process (utilising both experienced individuals and committees) before it is submitted to the regulator under the terms of the site licence. Independent (or Peer) Review of the safety case is seen as an important indicator of quality by the regulator, ensuring that the quality of both the source data used in the construction of the safety case and the safety argument is complete, comprehensive and fit for purpose. On its formal acceptance by the regulator the case is implemented and becomes live. The live safety case is then subject to a formal periodic review. Licensees are required under the terms of the site licence to carry out a full reassessment of the safety case at defined time intervals (usually five years) or whenever the plant status changes (e.g. from commissioning to operations, operations to end-of-life shutdown). Plant and process modifications within a current plant state (e.g. during operations) which affect the safety case are treated within a formal assessment process which ensures that the safety case is always current, live and relevant.

ASSUMPTIONS ABOUT SAFETY CULTURE IN SAFETY CASE DEVELOPMENT

Having examined what is meant by safety culture (in broad terms) and what essential elements must be present within

[6]NII SAPs Paras. 568–638

the nuclear safety case, this section will examine how, in developing the safety case, safety case authors and managers make assumptions about the presence of safety culture – either what will be present during proposed operations or what is considered to be present during current operations. Table 1 lists each essential element present together with assumptions made which relate to safety culture. The point to note is that such assumptions are often implicit, value judgements made by the safety assessor/author. For example a HAZOP chairman may rely on the information given by plant operators as to how things are done when such information is pertinent to the study. This may lead in part to a judgement made by the HAZOP team that a particular potential hazard is not deemed credible. This is fine provided that a safety culture is in place which supports the operators' assertions. If, instead, an operator describes plant practices as to how they *ought* to be carried out when in fact the prevailing safety culture on plant precludes this, then a totally erroneous view is offered to the HAZOP team which may lead to poor judgements as to the potential for hazards to occur; this will have a knock-on effect on the upcoming hazard assessment and control.

Similar assumptions about the existence of safety culture are made by assessors in the deterministic and probabilistic assessment sections of the safety case. To demonstrate adequate safety, suitable and sufficient engineering and procedural measures are defined commensurate with the severity (consequence) of the hazard. The safety (performance) requirements are specified and these requirements are substantiated by the engineers and, in the case of procedures, by human factors specialists.

The substantiation process is a demonstration that the equipment/procedures will do what it (or they) are required to do. Implicit in this is that, because plant operators are part of the substantiation, then they will also perform as required in both how they use and maintain the equipment. The assumption is made that a positive safety culture exists such that operators behave in the way that will allow equipment and procedures to perform their safety functions as specified in the assessment. The resulting safety argument is therefore strongly dependent on safety culture but this is not apparent in the safety case.

In order to develop the probabilistic approach which complements the deterministic assessment and allows a comparison with specified numerical criteria, numerical

Table 1. Typical assumptions made about safety culture

Safety case element	Description	Activity within which assumption is made
Plant & process description	Scope of the safety case, boundaries and interfaces. Clear description of the plant and process	No assumptions made as to how well the plant is operated. Concept of safety culture does not appear here.
Hazard identification	Learning from experience	Examination of similar operations (past and present), accident and near-miss data.
	Team-based systematic study	Presence of plant operators. Their contribution to the study may focus on what should be done rather than what is done. This can lead to assumptions about how safety is managed and the likely potential for hazardous situations to be recognised and controlled.
Hazard assessment	Normal operations and credible fault conditions. Derivation of engineering and procedural hazard controls, specification of safety function and performance requirements such that, if achieved then there is the demonstration of acceptable risk	Use of numerical data (e.g. reliability data and human error probabilities). Maintenance activities.
Engineering substantiation	Demonstration that the safety function and performance requirements specified in the assessment can be met.	Equipment use and maintenance
Safety management	Safety policy, safety instructions. Responsibilities for safety	Operator understanding of the need for safety. Operator awareness of why safety is important. Nurturing of good safety practices.
ALARP	Determination that suitable and sufficient safety features are present to demonstrate adequate safety	No additional assumptions made.
Acceptance & review	Maintenance of the quality of the safety case submission. Ensures that it is always live and current	No additional assumptions made.

data relating to equipment reliability and human performance is used to generate the logical analysis. There is some account taken of safety culture in using operating plant-specific reliability data since it relates to real operations often over a long period of time. It therefore takes account of how operators behave over that period. Use of manufacturer's data in determining equipment reliability however assumes that the operator will behave in the correct way with regards to operating and maintaining the equipment.

When it comes to determining human reliability (potential for human error), the safety case author and often the human factors specialist will assume that a good safety culture is present. The basis for the task analysis (from which human error probabilities are derived) often mentions the existence of "Suitably Qualified and Experienced Persons, SQEP, operators" "familiarity with the task" etc.: all of which is correct within a robust safety culture but is most definitely absent (in whole or in part) for a safety culture that is deficient or non existent. Hence the overall numerical analysis (and demonstration of compliance with criteria) always assumes that safety culture is present, alive and strong.

There is no suggestion here that making these assumptions throughout safety case development is in any way, wrong. What is important is that safety case authors, assessors and manager are aware of them, of where the dependences on the presence of a good safety culture lie within the safety argument. In this way their visibility can be enhanced during the implementation stage of the safety case ensuring that plant operators fully understand what is expected of them and are encouraged to behave accordingly.

SAFETY CASE IMPLEMENTATION

Appendix 1 is a typical safety case implementation checklist. Different Licensees have differences in language, style and format but the basic elements are as presented in the table. It illustrates what needs to be completed, approved and in place before the new safety case can be implemented. A signature sheet (not shown) ensures that relevant disciplines (engineering, process and maintenance for example) understand, check and sign off the completed list. This is their demonstration that they accept and understand the requirements of the safety case. Implementation is the real test of the of the safety case; can what is required of plant and process personnel in the safety argument be translated from what should be carried out to what actually is carried out on a day to day basis? A key component of successful implementation is the confirmation that the safety case is complete and comprehensive and approval for its implementation has been given by the regulator.

The visibility of the safety case to the plant operator is that concise set of documents which detail equipment and procedures necessary for plant safety, how they should be operated and maintained. These define limits and conditions and contain instructions which ensure the safety of the plant under normal and credible fault conditions. Having the visibility of the safety case made available to plant operators does not guarantee their understanding of its requirements. It can be seen from the checklist that implementation includes requirements to ensure operators understand the safety case requirements and, as a result, carry them out.

Examples of on-plant techniques which help to ensure operator understanding include:

- Development of a training programme tailored to the specifics of the safety case. Operator training is carried out to ensure operators are aware of and understand the requirements of the safety case. Training logs are updated and signed off to demonstrate that operators have been made aware of the new requirements. To ensure the success of the training, operators, particularly those with safety-significant roles, undergo exams and refresher training (as needed) to maintain their SQEP status.
- Toolbox talks. These are regular interactive sessions between supervisors and operators which focus on issues affecting the day to day running of the plant. They can be used to explain (and test understanding) of what is safety significant equipment and how it is supposed to operate, highlight the need for good housekeeping or share information of potential safety issues (e.g. learning from experience). They are an opportunity to share and enhance common understanding.
- Safety inspections/Walkdowns. Opportunities to inspect safety-significant equipment to ensure its defined safety function is being carried out, and/or to identify safety shortfalls which need addressing. The physical act of carrying out such inspections tests the understanding of operators and supervisors alike and ensures that their knowledge of the plant safety systems is always relevant and up to date.

The success, or otherwise, of these techniques is directly proportional to the presence of a good safety culture. Operators who are valued, well trained and motivated with "good" safety behaviours are more likely to respond to the need to understand (and hence implement correctly) the requirements of the safety case. Successful implementation of the safety case into the operating arena is firmly linked to the need for plant personnel to understand the requirements of the safety case and to carry them out correctly. As described above there are a number of techniques used to do this; their success is dependent on the presence of a strong safety culture. As will be seen in the next section if there is a lack of understanding of the safety case requirements by plant personnel then the safety argument will be deficient.

ASSUMPTIONS ABOUT SAFETY CULTURE DURING IMPLEMENTATION

Implementation of the safety case takes it from a written safety argument to the day to day demonstration that the plant is being operated within the defined safe limits. Here, as noted above, the expectation is that an already existing safety culture is a crucial pre-requisite for successful implementation. This expectation is borne out in the requirement for up to date training of operators in what is expected of them in operating the plant to the new or updated safety case requirements. However the reality can be somewhat different which can bring into question the assumption that successful implementation of the safety case must mean that there is a good safety culture present.

Discussions with a safety case manager at a nuclear licensed site yielded an example[7] of where the safety case argument required a certain set of operator behaviours for a plant operation that would result in a safe lifting operation. When the operation was observed it was carried out less than safely and it was clear that the operators did not understand the requirements of the safety case regarding this lifting operation. The details have been reproduced verbatim in Appendix 1 from the manager's observations and serve to show that an assumption of the presence of safety culture as supporting the safety argument within the safety case may not always be valid. In this instance the safety argument assumed that the operators knew, understood and implemented the safety case requirements. This did not happen, hence the safety argument in this area was deficient. The safety case manager concluded that there were deficiencies in supervision and training; operators were not sufficiently aware of their safety responsibilities. Action was taken to remedy the identified shortfalls.

That safety case Manager's awareness that improvements in safety culture were needed in order that adequate knowledge and understanding of the safety case requirements came about echoes my own experience some years ago as a shift leader in charge of several process workers on a nuclear processes pilot plant. Plant operators need to understand not just that something or some action is required for safety purposes but why that action is important. On the above mentioned pilot plant I was responsible for operator training in plant operations and the need to observe the safety requirements. As well as structured training sessions for operators; before each plant run operators were involved in the purpose and scope of the planned operations. In a sense they had shared ownership of the operations, were contributors to the success (or otherwise) of the plant run. Operators understood why tasks they had to carry out, had to be carried out in a certain way – whether they related to sampling operations or the maintenance of a safe plant state.

The example of the lifting operation and my experience of training plant operators show that an understanding of the requirements (and assumptions made) in the safety case is the key to ensuring their validity. A good understanding of requirements will only result from a good safety culture – operators encouraged to want to understand and own the work they do. This clearly demonstrates that a good safety culture has to be a prerequisite to a good safety case, good safety argument with all its assumptions about how operators behave can only exist when those assumptions are valid, their validity is dependent on a good safety culture being present. It is important that safety case authors, assessors and managers understand this throughout the development and implementation of a safety case. The presence of a good safety culture is truly the cornerstone of the safety case.

[7]Personal Communication, B. Drew.

CONCLUSION

Safety case authors and managers make assumptions about safety culture when developing and implementing the safety case for a new or current plant. They are woven into the fabric of the safety argument. This is right and proper provided that authors and managers ensure that those assumptions are valid. It is all too easy to think that what is assumed about safety culture will in fact exist. If the assumption is wrong and the safety culture is poor or non existent then numerical and other analytical data which rely on it will be suspect which in extreme cases can render the safety argument invalid and the whole safety case falls apart.

What this paper has tried to highlight is that safety case authors and managers should be more aware of when assumptions about the presence of safety culture are made and if necessary they are questioned to ensure that they are valid. The need to validate assumptions about safety culture can be carried forward from the development to the implementation stage and addressed there as part of the need to ensure operator understanding of the (new) safety case before it comes into force.

REFERENCES

1. Advisory Committee on the Safety of Nuclear Installations 1993. Definition taken from Gadd and Collins "Safety Culture: A Review of the Literature." HSL/2002/25. Health & Safety Executive, 2002.
2. HSE Human Factors Briefing Note No. 7 "Safety Culture" Health & Safety Executive.
3. Nuclear Site Licence Conditions. Health & Safety Executive.
4. Safety Assessment Principles, 1st Edition, Revision 1. Health & Safety Executive, 2006.
5. Ionizing Radiations Regulations, 1999.
6. Safety Assessment Principles, 1st Edition, Revision 1. Health & Safety Executive, 2006.
7. Personal Communication, B. Drew. Safety Case Manager, 2009.

APPENDIX 1: A TYPICAL SAFETY CASE IMPLEMENTATION CHECKLIST

The following documentation to be have been through "due process", complete and approved

- Complete Safety Case and top level summary report (if applicable). Ensure issues from supporting documents (e.g. commissioning documentation) have been addressed and closed out.
- Criticality and Operational Plant-Specific Documentation.

- Plant complex (Facility); Safety Related Equipment, Safety Features and Operating Assumptions.
- Safety Memoranda.
- Plant Modification raised to Implement the new Safety Case.
- Pre-Implementation review of Safety Case.

NII Submission made

Plant Instructions and Documentation to be reviewed and amended to reflect the new Safety Case

- Operator Instructions
- Maintenance Instructions
- Emergency Instructions
- Surveillance Schedule
- Alarm Prioritisation and Schedule
- Operator Rounds
- Logs
- Plant Maintenance Schedule

The following activities complete and closed out

- On plant Safety System Labelling.
- Verification and Functional Testing of Safety Systems, Safety Functions.
- Pre-implementation Operator Training delivered, competencies reviewed and training logs updated.

APPENDIX 2: IMPROVING SAFETY CULTURE FOR THE SAFETY CASE. THE SAFETY CASE MANAGER'S VIEW

The following text is a reflection from a facility safety case manager (Reference 6).

"During the process of moving from a Pre-Operational Safety Report to an Operational Safety Case for a radiological facility, a human factors review was undertaken. The review identified several specific areas of safety culture that required improvement. One important observation was that the quality of facility operating procedures varied considerably. The approach to development of the documents, the format of documents and the manner of use were the main areas of focus. It was recognised that the procedural documents were written by very knowledgeable and experienced scientific and technical staff and therefore the technical content was accurate and comprehensive.

Before the review findings were actioned, a non-nuclear lifting operation was observed by a bystander. The lift was being undertaken at first floor level above an access opening to the ground floor. The ground floor area below was accessible to passers by yet there were no operators on the ground floor restricting the otherwise free access to an area where items had the potential to fall from height and cause fatal injury.

On investigation into the near-miss incident it became clear that the trained operators had read the operating procedure for the task once, the first time they had performed it, but had not used the procedure at any time during the following 18 months, the task was performed at least weekly, this in frequent reference to procedures for non-nuclear tasks appeared to be common. The operating procedure contained a clear instruction in bold type at the top of the first page stating that one of the operators must stand guard on the ground floor at all times during the lift. This instruction had been derived in the POSR and was clearly marked as such using the company abbreviation which indicated the safety significance of the instruction, making it akin to an Operating Rule, albeit a non-nuclear operation.

When asked if they understood the abbreviation, the operators replied that they did not. They understood that there was a need to station someone on the ground floor but this had not been done due to a mix up in communication and a lack of importance assigned to the task by the operators.

This near-miss incident indicated that there was limited staff knowledge or understanding of the Safety Case and its outputs. When delving further it was seen that although the POSR was fit for purpose and its outputs had been represented in the operating procedures, the safety significance of the outputs had not been adequately articulated to the staff and the need to learn and follow operating procedures closely had not been disseminated adequately to the staff.

There are many ways in which the likelihood of the operators following procedures could be increased.

The operation could have been authorised by the work control office in such a way as to force the procedure to be read before the relevant keys were issued.
The supervision could have been increased.
The operators could have been regularly examined on their knowledge of procedures.

All of the above are accepted methods of ensuring tasks are completed as designed, albeit using a piecemeal approach. If operators can be educated about the major hazards identified in the safety case, why specific engineered and procedural safety measures have been put in place and what consequences have been identified in the event of the equipment failing or the procedures breaking down, they should begin to take more of a personal interest and develop a reasoned, rational approach to safety. If this training had been undertaken and if the operating procedure, in the case of the lifting operation, were written using modern understanding of human factors it is less likely that the near miss incident would have occurred.

When a human can understand the what, why and how of a dangerous situation they become engaged in the safety process. Once engaged, a well written, meaningful rule or instruction has more weight, rather than being a corner to be cut.

This education process has now begun in the above facility; staff have started safety case awareness training and training to write operating procedures with human factors in mind. A review of the safety culture is planned for a year hence, it is hoped that the occurrence of near misses arising from the old fashioned operating procedure process will be a thing of the past . . ."