HOW RELIABLE IS MY SAFETY CASE?†

Keith R Murphy, Head of Nuclear Safety, Atomic Weapons Establishment (AWE)
Dr Steve M Gilbert, Technical Director, Rockbourne Limited
Bronwen Lewis, Director, Partnerships Plus Limited

Safety cases are essential elements in the control of major hazards in the UK nuclear industry by aiding operators and regulators to make risk-informed decisions on the suitability of facilities, plant and operations. It is important that operators and regulators are able to make key safety decisions confidently and in the knowledge that they can depend on the safety documentation presented to them. This may lead them to ask "How reliable is this safety case?".

Incidents such as the loss of the Nimrod Aircraft XV230 in Afghanistan in 2006 illustrate the role of the safety case in averting disaster. XV230 suffered a catastrophic mid-air fire, leading to the total loss of the aircraft and the death of all 14 service personnel on board. The independent review into the disaster (Haddon-Cave, 2009) highlighted failings in the safety case process as a significant contributory factor, concluding that "*the Nimrod Safety Case was a lamentable job from start to finish*" such that "*the best opportunity to prevent the accident to XV230 was lost*".

Apart from averting disaster, it is in an organisation's interests to have an efficient and effective safety case process in order for it to assess and manage its risks – both in terms of safety and the broader business perspective. For example, AWE is investing heavily in upgrading its facilities and needs to ensure that safety risks are understood and managed, from concept through to design and implementation. If the safety case is deficient in providing a full and accurate assessment then projects may be delayed, require significant rework, incur additional cost or lack the support of our regulators. Hence it is in AWE's interest that the process by which safety cases are developed, reviewed and approved is sufficiently robust. It is also desirable to be able to demonstrate this robustness so that regulators and other stakeholders can have confidence in our capability to manage risk and deliver fit for purpose safety cases.

ORIGINS

In common with other nuclear site operators, AWE is licensed under the Nuclear Installations Act and regulated by the Office for Nuclear Regulation (ONR), which superseded the Nuclear Installations Inspectorate (NII) in 2011. A set of 36 standard licence conditions (LCs) are attached to each licence. At AWE the arrangements to meet the requirements of the licence are implemented through the Company management system. These include "*arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation*" to comply with LC14 (Safety Documentation).

In 2006, the NII released a set of revised Safety Assessment Principles (SAPs) several of which relate to LC14 and safety case processes. Recognising the importance of safety cases in the effective management of nuclear risks and the corresponding need for integrity in their development, SAP SC.1 states:

"The process for producing safety cases should be designed and operated commensurate with the hazard, using concepts applied to high reliability engineered systems."
(Nuclear Installations Inspectorate, 2006)

When SAP SC.1 was introduced, NII recognised that this was aspirational; interpreting and implementing the concept would be a challenge to the industry, and different approaches would be required to deal with the various human, organisational and cultural factors. AWE believed there to be merit in the concept and initiated a project with the aim of applying techniques for assessing the integrity of high reliability engineered safety systems to the AWE Safety Case Process. In essence, to demonstrate robustness of the Process, the approach would:

i. Identify failures and causes using a systematic process
ii. Identify safeguards and mitigation measures
iii. Specify functional requirements
iv. Substantiate & address shortfalls.

IDENTIFICATION OF SAFETY CASE PROCESSES FAILURES AND CAUSES

In the summer of 2008 a series of Safety Culture Hazard and Operability (SCHAZOP) Studies was carried out on the AWE Safety Case Process, applying the SCHAZOP technique devised by Kennedy & Kirwan, 1998. At that time, AWE had accrued more than a decade's experience of operating to LC14 requirements and the Safety Case Process was well established. As depicted by the columns in Figure 1, the AWE Safety Case Process has the following elements:

1. Planning/strategy
2. Safety case development

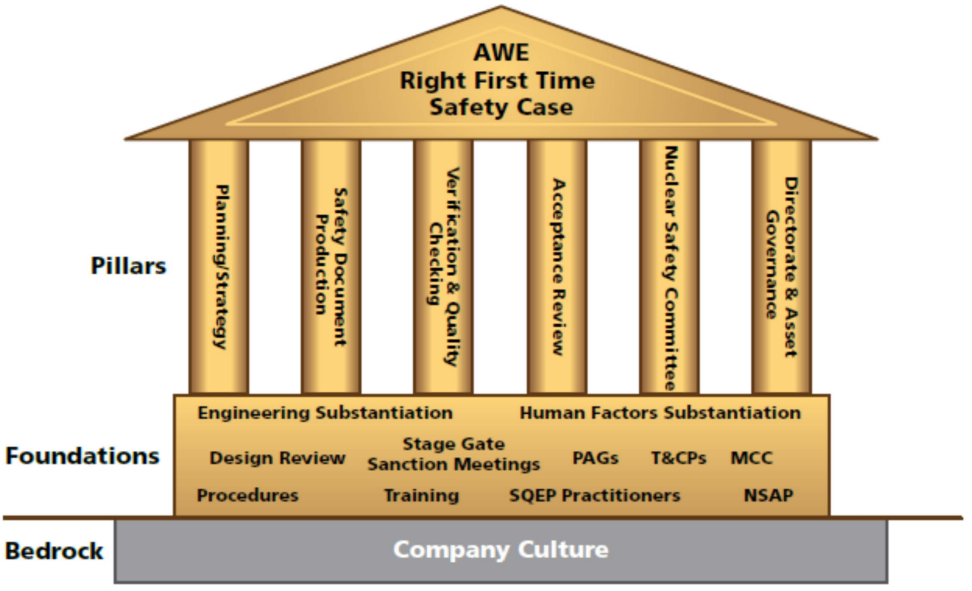

Figure 1. Simplified Representation of the Safety Case Integrity Model

3. Verification and quality checking.
4. Acceptance review (AWE's term for independent peer review).
5. Nuclear Safety Committee (senior level committee to consider and advise on matters of nuclear safety).
6. Directorate and asset governance (culminating in approval by the accountable director).

These were used as the nodes for the SCHAZOP studies which took the form of an experienced body of personnel systematically applying keywords (see Table 1) to each node, to identify potential failures, causes and control measures.

In this way any deviations that could lead to AWE's Safety Case Process being compromised were identified whilst also identifying the safeguards and mitigations that existed at the time the analysis took place.

SAFETY CASE INTEGRITY MODEL

SCHAZOP was effective in identifying potential failure mechanisms. A technique was required to turn this information into a success-oriented representation of what reliable safety case delivery should comprise. Having used SCHAZOP to identify vulnerabilities and safeguards within the process, Goal Structuring Notation (GSN) (Kelly & Weaver, 2004) was used to develop a Safety Case Integrity Model (SCIM) detailing the conditions necessary to achieve a 'Right First Time Safety Case'. More specifically, the goal that appears at the top of the GSN model is expressed as follows:

> *"The process used to produce safety cases needs to deliver consistently good quality, fit for purpose safety cases."*

Table 1. SCHAZOP keywords

Resource/Person continuity	Ownership/Understanding/ Intelligent customer
Competence/SQEP	Communication
Familiarisation	Clarity/Usability
Time	Detail/Proportionality
Process/Procedure	Control/Quality/Consistency
Information	Diversity/Independence

Figure 1 is a simplified representation of the SCIM. The pillars that support our goal stand on the foundations provided by the formal aspects of the Company's safety management system. These are underpinned by the Company's (safety) culture which is recognised as the bedrock upon which all else depends. This analogy is helpful in characterising culture as something that is deeply held and difficult to see. AWE has used Figure 1 to articulate the importance of all (formal and informal) aspects of the Company's system and to recognise the synergy between its various elements.

The SCIM reflects the complexities of the AWE Safety Case Process, i.e. the various roles, organisations, management arrangements, expectations and associated behaviours required for it to operate effectively. The SCIM was built from the detail obtained through the SCHAZOP studies and was tested by mapping across safety case failures explicitly identified in the Haddon Cave report. All of the failures identified explicitly in the review of Nimrod could be traced to a corresponding failure mode in the AWE model. This provided further confidence in the SCHAZOP-based approach and that as a product, the SCIM is complete.

The exercise also supported the concept of adapting the SCIM for use in a diagnostic capacity, i.e. in providing an indication of whether the AWE Safety Case Process is being applied effectively in practice.

SAFETY CASE ORGANISATIONAL REQUIREMENTS

Having gained confidence that the SCIM was complete the GSN model was then used to derive Safety Case Organisational Requirements (SCORes). In the spirit of SAP SC.1, the SCORes derivation and substantiation process:

i. Employed principles embodied in the derivation of safety functional requirements;
ii. Applied systems engineering principles, in particular those for requirements management; and
iii. Employed relevant good practice from the field of human factors, in particular those aspects relating to measurement of cultural and organisational factors.

The SCORes are expressed in a functional format and provide a comprehensive set of requirements which are based on the complex GSN format of the SCIM, but are designed for ease of use. For each of the nodes the SCORes range from high level purpose statements through to detailed Process Functional Requirements (PFRs).

As an example, the overarching purpose statement for Safety Case Planning/Strategy is:

> *"The Safety Case Planning/Strategy function within the AWE Safety Case Process shall produce an overview of the planned safety case production, review and approval process for a given facility/project, which shall include identification and commitment of named suitably qualified and experienced personnel to key roles."*

Each purpose statement complements the purpose statements for the other five nodes and is supported by several levels of functional requirement, right down to the PFRs. In our example, the PFRs are arranged under the following headings: corporate capability, competence and experience of the safety case team, safety case procedures, ownership of the safety case planning process, management arrangements and submissions.

The intention was to use the SCORes to substantiate the Safety Case Process, identify shortfalls and produce a Forward Action Plan of proposed improvements, following a similar approach to a Periodic Review of Safety. While the concept was sound when the process was in 'steady state', around this time AWE embarked on a major reorganisation and overhaul of its business processes, including many aspects of the AWE Safety Case Process. This provided an opportunity to use the SCORes as a means of designing, implementing, verifying and validating the revised Safety Case Process.

The SCORes benefit from a high degree of rigour, having been derived from the SCHAZOP and SCIM. The SCORes have been used in supporting requirements-driven improvements to the management arrangements and in underpinning the performance of the AWE Safety Case Process in practice.

DIAGNOSTIC TOOL

The AWE Safety Case Process is similar to some high reliability systems in that latent defects may be introduced at any point in the lifecycle and may lie dormant for considerable periods of time. These could have great significance; for example, where the potential exists to invest large sums of money in developing and implementing designs that may be fundamentally flawed.

The safety case process provides opportunities to assess facilities (in design or operation) and to deal with safety issues. Deficiencies in designs and/or safety cases may only be revealed late in the corresponding review processes, leading to delays, cost overrun and nugatory effort. It is therefore desirable to have a means of detecting early in the process whether the right conditions exist for producing a suitable quality safety case.

The aim of the Diagnostic Tool is to provide a 'health check' for a given facility/project/part of the AWE organisation and relate the findings to the SCIM. A prototype has been produced and a number of tests have demonstrated the feasibility of the concept.

The tool consists of a structured question set which has been designed to be used by subject matter experts to frame interviews with key project personnel. The SCORes have been used to indicate the type of evidence expected to be demonstrated in response.

The Diagnostic Tool continues to be developed through trial application and case study and is already providing some insights into how well the AWE Safety Case Process is operating in any particular facility/project.

Other potential applications include using it to establish the root causes of design or safety case 'failures' so that the risk of recurrence may be minimised. The Diagnostic Tool might also be utilised as part of a 'readiness review' to determine whether a facility or project is adequately prepared to proceed. Ultimately it is intended that the Diagnostic Tool may be utilised as a means of substantiating the AWE Safety Case Process through monitoring of its application in practice.

CONTINUOUS IMPROVEMENT

The key products that AWE has developed and which underpin AWE's Safety Case Process are:

- The Safety Case Integrity Model (SCIM);
- The Safety Case Organisational Requirements (SCORes); and
- The Diagnostic Tool.

These have been, and continue to be, utilised to improve the Safety Case Process and its performance. Figure 2 illustrates the various ways in which this is being

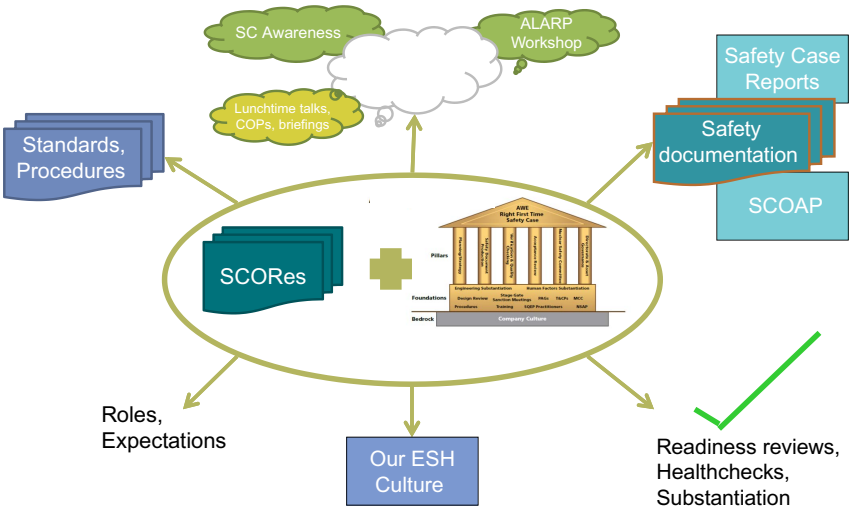

Figure 2. Improving Safety Case Delivery at AWE

achieved at AWE. The following are some examples of how the SCIM and SCORes have already been applied to good effect.

AWE STANDARDS AND PROCEDURES

The SCORes have been used to specify and then verify the content of new safety standards and procedures that define the AWE Safety Case Process. In so doing, procedural aspects of the AWE Safety Case Process have been substantiated with respect to their role in achieving robust, fit for purpose safety cases. So far, the following have been reviewed and updated against the relevant SCORes:

i. Safety Case Verification;
ii. Project/Stakeholder Review; and
iii. Safety Case Strategy & Planning.

Work continues on other procedural aspects of the process, for example, management of the safety report development phase, and the SCORes have already been of benefit in specifying what these should contain. In particular they help define the scope and interfaces between the various elements of the AWE Safety Case Process.

NUCLEAR SAFETY TRAINING

In addition to having an effective documented management system, successful application of the AWE Safety Case relies heavily on individuals within the organisation. The demands of the AWE Safety Case Process on individuals in specific roles are articulated through the SCORes and these have been fed into Training Needs Analyses (TNAs) for the ongoing development and maintenance of AWE's nuclear safety capabilities.

In addition to the technical content of procedures and training, the SCORes identify the importance of leadership, attitudes and behaviours in achieving robust safety cases. Hence, training courses have been developed in line with the Company's requirements and are tailored to the particular needs of the target audience. Examples include the leadership team, managers, practitioners and frontline workers. New training courses produced in this manner include:

i. Safety-led design: Safety case awareness for project teams
ii. Safety case awareness for facility personnel
iii. ALARP Awareness Workshop for senior managers
iv. Nuclear safety case awareness for operations and maintenance personnel.

The SCIM is featured as part of the course content to emphasise the importance of safety case integrity. Feedback from attendees has been very positive and demand for places remains strong.

Other courses are under development and through the judicious use of the SCIM and SCORes in combination with TNA, AWE is realising the benefits of having well targeted and effective training.

NIMROD REVIEW AND TRAINING COURSE

The SCIM was used to support AWE's review of the implications of the independent review into the Nimrod disaster (Haddon-Cave, 2009). All of the safety case failings from the report could be mapped onto the SCIM which provided direct read across to important elements of the AWE Safety Case Process. It enabled AWE to determine whether similar conditions might exist within its own system.

The corresponding learning was also incorporated in a one day Nimrod training course. This was effective in enhancing understanding at AWE of the potential consequences that could arise from ineffective application of safety case processes. It also emphasised the importance

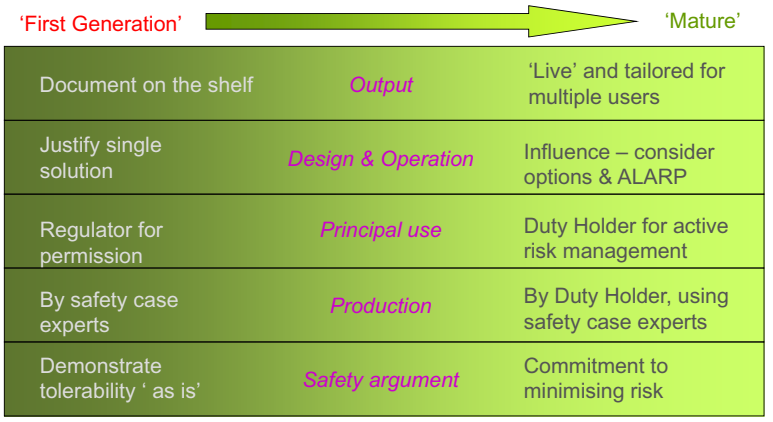

Figure 3. Safety Case Maturity Model

of individuals' contributions and active engagement in managing the risks of high hazard systems.

AWE REORGANISATION

AWE has undergone a significant period of reorganisation, during which a number of roles have disappeared, transferred or been created. The SCORes articulate the demands placed on certain roles throughout the Process, some of which have been affected by reorganisation. For example, the generic job description relating to the role of 'ESH&Q Manager' that arose from a reorganisation of how AWE delivers assurance has been based in part on characteristics and responsibilities articulated in the SCORes.

IMPROVING PERFORMANCE – PEOPLE AS PART OF THE SOLUTION

The preceding section describes a number of improvements that have already been made, mainly to the 'formal', more tangible parts of the AWE Safety Case Process. Broadly speaking, these are the aspects represented in Figure 1 as everything from the foundations upwards. It can be seen, however, that all of these 'formal' aspects are underpinned by the bedrock of the Company's culture and AWE recognises that these 'informal' aspects of its safety management system are equally important factors in its performance.

The requirement for AWE to produce safety cases has not changed since the inception of LC14 as part of nuclear site licensing in 1997. However, the way in which safety cases are developed and used at AWE has evolved as the organisation, its management systems and culture have matured. It is imperative to AWE that its safety case process performs efficiently and reliably in order to ensure safe operability in the delivery of the Company's programme.

A simple safety case maturity model (see Figure 3) has been developed to plot the organisation's progress. The left hand side corresponds to the first generation of safety cases, when AWE's objectives were to meet the expectations set by the NII to achieve nuclear site licensing standards. The right hand side corresponds to a vision of safety case process maturity, corresponding to the Company's aspirations for risk-informed safety management. Recognising that AWE has accrued over 15 years' experience of operating with safety cases under LC14, viewing maturity in this way helps engender a desire for change and a direction of travel.

The maturity model has been used with attendees at one of the regular AWE Safety Case Community of Practice (COP) meetings. The Safety Case COP meetings take place regularly every two to three months and are designed as opportunities for engagement, debate and discussion as much as means of communicating important information. The model was used as the basis for table group discussion and informal "scoring" of AWE's safety case maturity. The results indicated a fairly broad range of views of the maturity of AWE in relation to the delivery and operation of safety cases.

In order to articulate the improvement that AWE is aiming to achieve, a set of recognition statements have been developed:

i. I will hear engineers, operators, safety case personnel and other contributors working together to identify and address safety issues as part of their normal routine.
ii. I will hear designers, safety case personnel and other contributors challenging perceptions, assumptions, custom and practice.
iii. I will see that the safety argument presented in safety documentation is logical, transparent and founded firmly on evidence that relates to the true state of the design, facility, system or activity that the safety case relates to.
iv. I will hear that process operators, maintainers and other facility personnel have been engaged in the preparation of the safety case and find the outputs useful in helping them understand what they have to do to control hazards.
v. I will hear discussions about how to reduce risks further, even if the safety case concludes that risks are acceptable.

vi. I will see that decisions have been made by taking full consideration of the safety issues, that they incorporate measures to manage any residual risks and that the outcomes are reflected in safety documentation.
vii. I will see that safety documentation has undergone an appropriate process of review and approval, culminating in commitment from the person responsible to actively manage the risks that have been identified.
viii. I will see only quality assured, fit for purpose safety documentation being submitted for review and/or approval in line with the 'right first time safety case' principle.
ix. I will hear that regulators have confidence in AWE's safety case process and the safety cases it produces.

These aspirations are aimed in the main at improving the cultural context within which risks are managed. By addressing conditions, expectations, assumptions and behaviours, it is anticipated that the process will be more effective and that the various products, e.g. safety cases, will be more reliable.

MAKING SAFETY CASES REAL

Together, the recognition statements and safety case maturity model are helping AWE frame the change that it requires in the way that the safety case process is operated. The products of the safety case process will continue to satisfy LC14 but will be produced more efficiently and provide a more robust basis for risk-informed decision making.

An example of how AWE has been 'making safety cases real' for the operators and maintainers of hazardous processes is through a new product called Safety Case On A Page (SCOAP). It is designed to help personnel to manage the major hazards in their particular workplace by presenting succinct safety information pertaining to a specific area of plant in a poster format that is readily understood and displayed in the work area. Features of the SCOAP include:

- Photographs of the plant/equipment;
- Corresponding labels and simple descriptions of safety systems;
- Diagrams showing the key hazards, control measures and potential consequences; and
- Operating rules and key safety actions requiring particular attention by the operator/maintainer.

Operators and maintainers have been engaged in the development of each SCOAP to ensure it is tailored to their particular needs, which has had the added benefit of raising awareness of elements of the whole facility safety case that are of most relevance to them. At a cultural level, in providing outputs that operators and maintainers regard as useful, there is greater incentive for them to engage in the safety case process and therefore a greater sense of ownership of the safety case by facility personnel. Further, the process of presenting important parts of the safety case in this more transparent format has, in many instances, provided clarification on ambiguous or complex aspects of the source safety documentation.

The SCOAP concept is an example of how AWE is going about 'making safety cases real' for the Company as a whole. Recognising that people are essential to realising these aspirations, emphasis is currently being placed on working with individuals and teams throughout the organisation to identify and effect any changes necessary to improve safety case performance. This way of working underpins all of the elements shown in Figure 2. There are also specific approaches that aim to explicitly address individual and group behaviour and culture.

Improvements in the business as a whole provide an important context for safety case delivery. For example, the HR strategy which is driving continuous improvement in leadership, competence development, performance management and so on, can be used to lead, shape and reward positive culture and behaviours.

The SCIM and SCORes continue to be of use in confirming the roles and expectations and in support a broader programme of safety culture and change.

Another element to this improvement activity is "Our ESH Culture", an approach which engages the workforce in confirming positive and negative behaviours relating to environment, health and safety, and then undertaking gap analysis. The four behavioural themes are: standards, communication, risk management and involvement. Specific behavioural expectations can be identified within the SCORes, for example the competence and experience of the safety case team includes behaviours such as '*attitude and openness to constructive challenge'* and *'effectiveness in influencing, negotiating and communicating'*. The gap analysis provides a focus for improvement and teams can use the SCORes as a way of identifying how shortcomings can be addressed.

CONCLUSIONS

This paper describes how AWE has used concepts usually applied to high integrity engineered systems to analyse the Company's safety case process to understand potential weaknesses and corresponding demands. While the initial work was carried out in response to NII expectations a number of broader AWE business benefits have emerged as the project has evolved. This paper describes how, from the aspirational beginnings of SAP SC.1, AWE has critically examined its AWE Safety Case Process and utilised this understanding to drive improvements in its performance.

AWE has developed the SCIM and the SCORes which describe the conditions necessary to deliver consistently good quality, fit for purpose safety cases. By virtue of the techniques used and subsequent testing, the SCIM and SCORes are well founded and are fully configured to provide a sound basis for onward development and operation of the AWE Safety Case Process.

By having a secure, requirements-driven foundation, AWE has a robust framework for the development of

procedures, training, behaviours and practices to provide the conditions for 'Right First Time Safety Case' delivery. The SCIM and SCORes are being utilised to drive improvement in processes, safety culture and working practices so that safety cases realise their full potential in the management of major hazards. For AWE this will also mean that its ability to make risk-informed decisions is enhanced and provides confidence that the right outcomes will be achieved as the Company invests in its infrastructure and future capabilities.

ACKNOWLEDGEMENTS

The authors would like to thank a great number of persons actively engaged in improving safety case performance at AWE, recognising in particular the contribution made by Sally Forbes and Craig Jones.

REFERENCES

Haddon-Cave, C., 2009, The Nimrod Review: An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. London: The Stationery Office, Ref HC 1025.

Health and Safety Executive, 2006, Safety Assessment Principles for Nuclear Facilities, 2006 Edition, Revision 1.

Kelly, T. and Weaver, R., 2004, The Goal Structuring Notation – A Safety Argument Notation. Proceedings of the International Conference on Dependable Systems and Networks (DSN), Florence, Italy. IEEE Computer Society.

Kennedy, R. and Kirwan, B., 1998, Development of a Hazard and Operability-based Method for Identifying Safety Management Vulnerabilities in High Risk Systems, *Safety Science,* 30: 249–274.