EXPLORING THE ROLE AND CONTENT OF THE SAFETY CASE

Helen Conlin[1], Philip G. Brabazon[2], King Lee[1]
[1]Parsons Brinckerhoff Ltd.
[2]University of Nottingham

It is a requirement to provide a safety case for all of the Major Accident Hazard (MAH) industries. The prime purpose of the safety case is for the Dutyholder to demonstrate to the Regulator there are effective means for ensuring safe operation in accordance with a goal setting safety regulation regime. This paper will take forward ideas presented in Expert Advice to the Ladbroke Grove Rail Inquiry Part 2(6) in regard to the principles of a safety regulation regime and the role and content of the safety case.

Currently, with local variations within different major hazard sectors, it is common for a Safety Case (SC) to describe an organisation's technical systems and processes and its Safety Management System (SMS). These sections are accompanied by a risk assessment which attempts to demonstrate that through these measures and perhaps further identified control measures, risk has been reduced to As Low As Reasonably Practical (ALARP). This paper criticises the current norm, accusing it of producing unbalanced documents that fail to present a complete and strong argument for why the organisation's arrangement lead to continuing safe operation.

The completeness and strength of an argument can be rated by comparison to theories and models of argument construction e.g. Toulmin et al 1979(39). The strength of an argument is limited by the quality of knowledge and science used as the basis. In the field of safety the quality of science varies depending on the context, for example more confidence can be placed in the understanding of the science of materials and structures than in the understanding of organisational behaviour. Consequently, in general, the conditions under which hardware components and structures fail can be forecast with greater certainty than the performance of a team of people tackling a complex problem. The benefit of using formal argument structures is that constituent parts of an argument are made explicit, increasing the visibility of incomplete and weak arguments. Validation of the Safety Case would entail appraisal of the constituents of the argument.

This paper explores the application of an argument model, commenting on the viability and benefit of its adoption. This paper also considers the degree to which the proposed approach is implemented in other fields such as insurance, aerospace and defence.

Safety Case (SC), argument, Toulmin, Safety Management System (SMS), Regulator

THE BENEFITS OF COMPLETE AND STRONG ARGUMENT IN SAFETY CASES

This paper proposes that the SC should set out an argument for why an activity is as safe as it needs to be. That those involved in the operation of a MAH facility should make a case for how their activities lead to continuing safe operation of that facility and form a plan for strengthening the argument. This is consistent with the requirements of a goal setting safety regime.

The term 'argument' is being applied in place of 'demonstration' which is used in the regulations defining the Safety Case/Safety Report regimes(12,13,16,18,20,19,20,21,22,23,24). This is due to there being no dictionary definition of demonstration which reflects the meaning implied in such safety regulations. The regulations imply the need for a reasoned explanation rather than a scientific proof of safety. Scientific proof is the available definition of demonstration, however this is not achievable within the current understanding of safety science.

A concern is that the present SC process is drifting from the intention of the SC regime. Benefit has been gained from SC's, but for further benefits the SC process needs a prod. A SC regime puts the onus on the Dutyholder to find ways of operating safely. When brought in to a sector the SC regime stimulates considerable thought. A criticism is that the reflection can stagnate, and a reason for this is that the regulations are not pushing Dutyholders to produce SC's with complete or strong arguments. The approach of demanding Dutyholders to put forward a convincing argument for why they are safe and to seek to continually strengthen the argument is a remedy.

FORMS OF ARGUMENTS

For centuries, philosophers have believed that arguments can either be explained by absolute means or by relative means. These positions briefly are:

- Positivism and the belief that there is only one absolute logic and one form of approach to rational understanding (i.e. truth) called absolutism.
- The counter-position known as relativism with many logics.

Toulmin's model for argument[39] sits outside both these positions. Using either of these methods according to Toulmin[38] is irrational to the modern argument. First, Toulmin claims that by using a relative method, no standards for the claims are made because the analysis of the argument is only relative to that particular argument. Additionally, Toulmin believes that absolutism or foundationalism is irrelevant in the modern era. He claims absolutism is irrelevant for several reasons. First is the fact that this absolute logic is based in mathematics and geometry. Therefore the concepts which are contained in them are field dependent. Hence, Toulmin argues that there is no room for these viewpoints in other areas of logic. Secondly, Toulmin believes that due to there being a definite grey area in some arguments, they do not allow for the absolutism position that answers are either correct or incorrect. The overall problem that Toulmin expresses about absolutism is that its rules are so strict that it just does not apply to modern reasoning.

Certainly the field of safety science is unsuited to the use of absolute logic and the analyses of SC arguments must be capable of comparison within a regulatory framework.

THEORIES OF ARGUMENT

Argument theories and models can provide assistance for constructing a SC argument for continued safe operation and for validation of such an argument.

An argument involves putting forward reasons to influence someone's belief that what you are proposing is the case[11]. An argument has at least two components, a point and a reason(9):

- making a point (or statement)
  by
- providing sufficient reason (or evidence) for the point to be accepted by others.

These elements are related and the movement can go either way to form the argument:

- a movement from either a point to a reason
  or
- from evidence to conclusion (the point)

The movement from one to the other can be supported by other components called inferential devices. These are rules or principles which permit the making of a claim on the basis of some evidence (or warrants). These components are explored further below. For the purposes of constructing a SC argument the movement would be from a point (activities lead to continuing safe operation) to the reasons for this with support from evidence.

Some theories/models of argumentation and argument analysis are introduced below.

CORAX

Corax[2] outlined the concept of argument in two areas. First, he believed argumentation is practical. Second, he contended that probability is a factor that affects this concept. Corax detailed what he called ‘practical disputation’ or argument. Additionally, Corax incorporated probability into his definition of argumentation. Unlike hard sciences that advocate certainty, he asserted that argumentation was a process of debate wherein exploration is encouraged as opposed to certainty. In fact, the term ‘reasonable doubt’ used in our judicial system stems from this Greek idea. Hikins[10] writes, ‘Corax, as far as we know, was the first to notice the importance of probability in public argument and discuss it in a book on rhetoric. From this point on, the concept of probability persists as a central term in rhetorical history to the present day.’

TOULMIN

Various models of argument have been developed, the leading one being the Toulmin et al (1979) model[39]. According to this model, an argument has several constituents - claim, grounds, warrants, backing, qualifier and rebuttals. The model may be used for constructing an argument and for analysing arguments. The argument components are defined as follows:

- claim: ‘the assertion put forward publicly for general acceptance’ – proposition;
- grounds: ‘the specific facts relied on to support a given claim’ – data or facts;
- warrants: ‘statements indicating how the facts are connected to the claim’ – explanation of how the data supports the proposition;
- backing: ‘generalisations making explicit the body of experience relied on to establish the trustworthiness of the ways of arguing in any particular case’ – credentials or general information in support of the explanation;
- qualifier: ‘phrases that show what kind and degree of reliance is to be placed on the conclusions, given the arguments available to support them’ – the strength of the claim; and,
- rebuttals: ‘the extraordinary or exceptional circumstances that might undermine the force of the supporting arguments’ – under what conditions may the claim not be true, counter examples.

Toulmin et al. say the first four elements need to be present for an argument to be *sound*. The last two are required for an argument to be *strong*.

The Toulmin structure of argument is illustrated in Figure 1. A challenge can be made to any or all elements. Is the claim justified? Are the evidence, warrant and backing justified? Additionally, we can ask whether the claim stands up to major challenges? Is it sufficiently robust? The validation of a SC argument would ask such questions, a further method of analysing argumentation is introduced in the next section.

FISHERS METHOD OF CRITICAL READING

Fisher (1993)[7] provides a systematic technique for reading analytically which allows evaluation of any argument to be done by analysis of its formal structure. Words that are used to structure an argument are the focus for the analysis. Words such as *thus* and *therefore* are highlighted because they are used to link evidence with claims and suggest inference, reasons and conclusions. Fisher's approach provides a systematic set of procedures for the analysis and subsequent evaluation of an argument, for example, one procedure seeks to extract the conclusions and reasons of an argument.

Fisher's method is based on what he calls the assertability question, it questions both the premises and the conclusions of an argument. The main assertability question is: what argument (what *you* need to believe) or evidence (what *you* would need to know) would justify the acceptance of the conclusion? Note, this question is not attempting to establish truth, it is about establishing justified reasons for accepting an assertion[9]. This analysis method may lead to the problems associated with a relative analysis of argumentation in that due to the analysis only being relative to a particular argument there is a lack of standards being applied to the claims.

REVIEW OF CURRENT SITUATION

The sequence of implementation of MAH industry regulations is summarised below:

- Nuclear, 1971 [12,13];
- CIMAH, 1984 [14];
- Offshore, 1992 [16,20,22];
- Railway, 1994 [18,24];
- Pipelines, 1996 [21];
- COMAH, 1999 [23].

Throughout this time the Regulator's approach to the structure and content of the SC has evolved. The Nuclear regulatory regime[12,13,15,17] is based upon the Regulator granting a license to operate, part of this exercise requires production of a SC by the Dutyholder. The nuclear site license has conditions attached which define areas of nuclear safety which the licensee should pay attention to ensure safe operation of the site. Some conditions impose specific duties whilst others require the licensee to devise and implement adequate arrangements in particular areas. Schedule 14[17] on Safety Documentation states that: *'the licensee shall make and implement adequate 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*'. Note the use of 'justify' rather than 'demonstration'. Supporting the Nuclear

Site Licence conditions[17] are the Safety Assessment Principles for Nuclear Plants[15]. These principles define how the Dutyholder will be assessed for safety, they do not specify content, rather they provide a benchmark for safety both in general terms through the fundamental principles and in specific areas such as Equipment Qualification and Reliability. The approach used within Nuclear SC's is similar to other MAH SC's, it is the rigour and robustness of the 'arguments' used to justify safety which differs.

The use of the word demonstration is most apparent within the COMAH regulations[23] and guidance[25,26] and is explored further below.

DEMONSTRATION WITHIN COMAH

The COMAH regulations[23] require that a number of demonstrations relating to SMS are provided, major accident scenarios are identified and the necessary measures have been implemented, the measures have adequate safety and reliability and an onsite emergency plan has been developed.

COMAH safety report guidance defines demonstration as 'to show, justify or make the case/argument through the information given'[26]. In particular this requires:

- A sufficiently rigorous and systematic process;
- A link between the measures taken and the major accident scenario;
- Provision of prima-facie evidence that the necessary measures have been taken.

Part of the problem limiting the successful achievement of the level of demonstration required by COMAH may be that the document is described as a 'safety report' and not a 'safety case'.

CURRENT PROBLEMS

Industry has difficulties in understanding and meeting the requirements of demonstration. This was highlighted as a problem in the early days of COMAH[4]. However, it has continued to be a reported problem[5].

The HSE have suggested a certain structure for the safety report and its content[25,26]. This structure may not be most appropriate to present a logical safety argument.

Current COMAH safety report argument is often restricted to one section and can be incoherent and disjointed due to excessive cross referencing to descriptive sections of the document plus there is limited analysis e.g. whether the SMS is a good one and why it was chosen compared to other available models. Does this arise due to the prescriptive nature of the guidance for safety report content? Is it a problem due to inadequacies of the previous CIMAH regime and attempts by Dutyholders to 'bolt-on' sections for a new regime such as COMAH?

The main element of the report which contains safety arguments is the risk assessment section which tries to identify all major accident scenarios and assess them. Most other sections of safety reports are descriptive. However, often the link between risk assessment and control measures is weak. Information on safety control measures tends to be descriptive rather than showing that they are fit for purpose. Additionally the risk assessment generally starts at a low level and does not question why, for example, a particular process route has been selected and discuss alternatives that were considered and rejected e.g. alkylation process within oil refining and alternatives to the use of hydrofluoric acid.

Appreciating that risk assessments take many forms, it is considered that applying the forms of qualitative or quantitative risk assessments typically used for analysing engineering systems for analysing an organisation would be very demanding and prone to error. Simplistically, it is routine in a risk assessment of an engineering system to decompose the system into its constituent components and to determine how the states of the components can combine to cause the system to fail. Applying a similar approach to analysis of an organisation has not proven successful. The use of benchmarking through comparison with one or more 'best practice' models is an approach commonly used for assessing organisations. To make a strong argument for the use of a best practice model it would be expected that the Dutyholder would argue for the validity of the model and obtain favourable ratings from an unbiased assessment. The use of 'leading indicators' of safety performance is another approach related to benchmarking. As catastrophes are rare, not suffering a catastrophe is not proof that safety controls are sufficient and fully effective. The idea is that 'leading' indicators allow the 'safeness' of an organisation to be assessed. These types of approaches to demonstrating safety do not fall easily within the risk assessment based model to demonstrating safety.

Most safety reports tend to describe the SMS and do not demonstrate that the SMS is designed to manage the hazards. Additionally, most safety reports are prepared by safety professionals who focus on technical issues. There is generally little content on other organisational factors.

Many safety reports strive to present a favourable picture of a site's operations. However, safety reports would be more realistic and credible if they demonstrated the adequacy of the safety control measures through defining the assumptions, limitations and potential and planned improvements.

OTHER SECTORS

Other MAH industries have slightly different approaches to SC development. Some of the differences in regulations and practices are briefly described below.

The Offshore Safety Case regime(16,20,22) uses the concept of performance standards and a verification scheme. This requires the safety requirements of a safety critical system to be defined (normally by safety assessment) and a verification scheme to be set up to ensure the safety system is suitably managed throughout its life cycle.

The railway and defence industries tend to adopt the system engineering approach to safety assessment and safety case development. In particular the specification of system requirements and apportionment of requirements allows the precise safety requirements and validation criteria to be defined. By taking a life cycle approach the safety plan describes the management arrangement responsible for delivering the safety for each phase of the life cycle(1,34,32). The life cycle approach adopted within the rail industry stems from a British Standard(1) and industry guidance(34) not HSE published regulations(18,24) and guidance(19).

However, all the SC regulations tend to define a similar structure and content of a SC. Further, SC regulations only require limited demonstration to defined aspects not to the entire SC. Generally, the regulations only require demonstration of technical safety measures taken using risk assessment; whilst other SC sections need only present a description. For example, the Railways Safety Case assessment criteria(27) states that different terms (such as description of, particular of, particular to demonstrate) are used in the regulations to indicate the level of detail to be provided in the SC and to some extent defines the type and robustness of arguments required.

ARGUMENT WITHIN THE SAFETY CASE REGIME

A role of SC regulations should be to stimulate deep questioning by a Dutyholder of their beliefs about safety and their approach to safety, and encourage Dutyholders to look beyond their immediate horizons for safety knowledge that prompts re-evaluation and improvement. Regulations can do this by requiring Dutyholders to present a critical and comprehensive argument to justify their safety controls. They should impose the need to consider what is critical to safety and defend the arrangements; e.g. does the Dutyholder judge their organisational design to be critical and if they do then the Dutyholder should argue for why their organisation is adequate rather than just describe it. However, the regulations should not prescribe a list of the sub-arguments to be presented. It is for the Dutyholder to decide the completeness of the argument. This approach is consistent with the precautionary principle, which shifts the burden of proof in demonstrating presence of risk or degree of safety towards the hazard creator. The presumption should be that the hazard creator should provide, as a minimum, the information needed for decision-making(28).

Two tasks for the regulator are the evaluation of the validity of the argument and the veracity of its components. Validation is an intellectual task which evaluates whether the grounds, warrants, backing and rebuttals are complete and of sufficient strength to make the claim of safe operation. Verification involves checking data and confirming that what is said to occur is actually done (effectively). Additionally the regulator can take note of how the Dutyholder has gone about constructing the argument, such as how the Dutyholder has prevented vested interests from biasing the argument.

In setting out how SC's are to be evaluated, a question is whether the regulations should specify not only the safety criteria a Dutyholder is aiming for (e.g. ALARP) but whether they should set out also the standard of proof that the SC is to be judged on. Options for standards are: beyond all possible doubt, beyond a reasonable doubt, on a balance of probabilities.

Such an approach can assist in deciding when the precautionary principle should be invoked as it will bring to the surface aspects of the argument for which there is insufficient science to build confidence(28).

CONTENT OF AN ARGUMENT BASED SAFETY CASE

An argument based SC should contain a critical appraisal and justification of the Dutyholder's governance of risk. Should such a SC include a description of the SMS? Is a hazard log and a quantitative risk assessment necessary? The answer is they are if they make the argument sound and/or strong but not if they do not. It is unlikely that they are sufficient. The inclusion of a SMS description, for example, begs the question – why this SMS? The type of SC that raises concerns is one in which a SMS is described that is an adaptation of an international standard or uses a template from a respected third party organisation, and the implied argument is that this

SMS must be good because of its origin and association. The reader of a SC is less impressed by the description of the SMS than by a line of reasoning that convinces of the suitability of the SMS for the purpose of achieving ALARP (or other criteria adopted by the Dutyholder). A reader is less convinced by a claim from the Dutyholder 'we have a procedure for every hazard' than by a reasoned explanation as to why the SMS is appropriate to the Dutyholder's activities and organisation; that the principles underpinning the SMS have benefited, and will continue to benefit, from sound safety science; that the Dutyholder can assure that the principles are being put into practice in a balanced and effective manner. The implication is that the SMS is an output from an SMS governance process and the SC is a critique of this process as well as of the SMS itself.

If a SC were to be structured according to Toulmin's model it could open with a statement encompassing a *claim*, its *grounds* and *qualifier(s)*, an example being "this Dutyholder configures and manages its operation so that, using the test of risks to be 'as low as is reasonably practicable', its operations are safe to the public, employees and the environment" (Figure 2).

The SC would then contain the warrants, backing and rebuttals to underpin the argument. In regard to the rebuttal, one form of query the SC should provide defence against is 'wouldn't the XYZ model of SMS be better for this Dutyholder than the model they are using?' There are contrasting views as to how to manage safety in organisation (e.g. the conflicting viewpoint of the protagonists of high reliability organisations as opposed to Normal accident theorists(36)) and given the developing state of some areas of safety science, particularly in regard to soft issues, disputes will continue for the foreseeable future. However, one could read many, many safety cases and remain ignorant of these debates and the issues of contention. A demonstration of awareness and understanding of the limits of current safety science and of new and emerging theories and knowledge will assist greatly in bringing to light the strengths and weaknesses of arguments in a SC.

Confidence in an argument is influenced by how the argument was developed. Confidence may be undermined if the authors of the SC were at a distance from the operations, or if the SC were produced in a rush. Therefore the SC should describe how the argument has been developed, over what timescale and who has been involved.

The SC should include a plan from the Dutyholder for strengthening their argument, as well as a plan for reducing risks as is currently required.

IMPLICATIONS OF USE OF ARGUMENT

FOR REGULATORS

Proposing the use of argument for SC's appears consistent with the Regulations(12,13,16,18,20,19,20,21,22,23,24) and HSE's approach(15,17,19,25,26,27), substituting argument for demonstration provides a process for achieving the desired SC regime output.

The use of validation and verification techniques for evaluating the strength and soundness of arguments has been explored above. Use of an argument structure for the SC should aid SC assessment (and in some regimes acceptance), the validation phase; and inspection, the verification phase. The validation phase demands expertise and extensive knowledge of safety in the particular relevant industry. The verification phase involves inspection, requiring access to the organisation and a number of its staff. Verification requires an open relationship and trust between the evaluators and the parties under examination. The skills and knowledge requirements for validation and verification of a SC based on argument do not appear to be different from those currently required from the Regulator for SC assessment and site inspection activities.

Pushing safety science to the fore within Dutyholder arguments would require wider appreciation of such science within the Regulatory bodies. The counter argument to this would be that safety science is not sufficient. However bringing safety science to the fore is helpful to highlight the need for more research through questioning existing knowledge and understanding and therefore stimulating improvement.

Adoption of an argument orientated approach to SC's is likely to require the production of process orientated guidance. This guidance would not wish to provide detailed example arguments which could lead to formulaic argument based SC's and would not generate the benefits available from an argument based SC approach. Dutyholders would be likely to require guidance on how to formulate an argument and how to analyse an argument for strength and soundness. However the detailed contents and development of a Dutyholder's argument for continued safe operation would have to be unique to that MAH facility.

FOR DUTYHOLDERS

The relationship the SC has with other parts of a Dutyholder's SMS is likely to change as rather than sitting within the SMS, the argument based SC would exist at a much higher level. The SMS would form part of the argument for continued safe operation, in particular why a particular SMS model has been selected and others rejected. The detailed procedures and guidance within the SMS may be examined during the verification (inspection) phase of a SC regime but would not be contained within the SC argument. The reduction in detail which is included within the SC means there would be less requirement to update. Although detailed procedures and guidance at lower levels of the management systems will change, it is unlikely that the underlying principles will unless there are significant advances in safety science or a major change in the Dutyholder's organisational philosophy due to e.g. a change in ownership.

Due to the well appreciated fact that organisational factors have a significant influence on safety; in order to form an argument for how safe an activity is, such as operating a chemical plant, it is necessary to justify the configuration of the organisation as well as hardware. There are several routes available for doing this. This requires an approach which actively benchmarks organisational structure, policies, processes, working practices and performance against 'best practice' models. Therefore in order to form strong arguments Dutyholders are likely to need to introduce increased use of such benchmarking tools. Similarly, the use of 'leading indicators' of safety performance is likely to need to increase amongst Dutyholders so that they may base their argument on why they are safe on the selection of leading indicators used and the ratings being achieved against them. There would need to be a discussion within the Dutyholding organisation around the uncertainty as to how quickly safety management controls decay and therefore the frequency of measurement of leading indicators. These additional requirements are unlikely to be identified through the existing SC structure with the emphasis on technical risk assessment and limited organisational factor content.

For Dutyholders to increase use of benchmarking and leading indicators, many will need to increase their understanding of organisational influencing factors and improve the skill balance between technical risk and other factors. The skills required to construct arguments will need to be resourced either by developing them within the Dutyholding organisation or by outsourcing. The use of argumentation is common within the social sciences but not so common within engineering and physical science disciplines where traditionally Safety specialists emanate and the use of absolutism and 'truth' is preferred. Even where risk assessment is used as a tool, many safety specialists prefer to have a defined acceptable/unacceptable cut-off point and to assign (often arbitrary) numbers to probability and consequence to allow a simple decision on the level of risk to be made and to prescribe certain levels of control measures to the different risk levels rather than to systematically analyse whether the assessed risk is ALARP and consider further control measures which may be required. That is, often the SC is produced by following a prescriptive set of instructions which stifle true thought about whether defined activities are as safe as they need to be because it is easier to write a SC that way and then to audit the SC against the internal procedure. The use of argumentation would require a rethink on how a SC is written and a critical review of the Dutyholders activities in order to construct a sound and strong argument which can be validated and verified. It requires a much higher level assessment of the basis of operation than is generally found in current SC's.

It is almost certainly the case that Dutyholders will conclude their arguments can be strengthened by greater understanding of safety science. Consequently there will be a motivation for research and some of this will merit sector wide effort. A criticism made in several safety reviews of the rail industry was a drop in research effort following privatisation(40,37,35). Part of the blame was the lack or weakness of facilitating organisations, but it is argued here the SC regime at the time was a contributor in that it did not drive Dutyholders into formulating and pursuing research agendas.

EXAMPLES OF USE OF ARGUMENT APPROACH TO SAFETY AND RISK

We have already explored the extent to which argument is used with existing SC's. This section provides examples of how argument has been applied to the safety and risk domain within other sectors or disciplines.

The insurance industry uses validation and verification techniques when evaluating the safety of a facility's activities. The validation part of the evaluation entails checking for the use of approved tools and techniques such as HAZOP, FMEA. The use of these tools suggests a minimum level of safety performance. The confirmed use and quality of the application of such tools is verified through site visits and inspections. Insurance companies actively seek new tools which they may add to their approved list to further improve their validation and verification capability, including tools outside the technical risk area, and may even advise clients of suitable tools to apply. The benefit of such an approach is the targeting of the insurance company's resources to allow efficient and effective, dependent on expertise of insurance company employees, evaluation of the safety of a facility's activities. The insurer's role has similarities with that of the Regulator (although there are also significant difference such as the relationship with the Public and legal compliance). However both parties aim to validate and verify the safety of a facility's activities but there are significant differences in approach, particularly to validation, which for the Regulator is how it evaluates the SC. If a SC were structured as an argument then the validation techniques used by the Regulator could incorporate the approach used by insurance companies to evaluate the claim of safe operation. For example the use of workforce involvement techniques and continuous improvement by a MAH company may be evaluated favourably at the validation phase of the SC as based on relevant predictive theories of theory. The actual extent and perceived successful application of such theories would be verified through site visits and interviews with employees.

The argument based approach to safety cases has been researched within the UK, led by the University of York, and has led to the development of Safety Argument Manager (SAM) software[29]. The research sought to develop an overall safety argument by assembling 'micro-arguments' based on the Toulmin model. The initial phase of the research found the Toulmin model too restrictive and not readily applicable to the types of argument commonly found within real safety cases. The SAM software aims to provide support for the high level argument of the safety case and for the supporting evidence, particularly safety analysis techniques. The software uses a goal based notation for structuring the high level argument of the SC and manages the interrelationships that exist between the most common safety analysis techniques e.g. between Fault Tree Analysis and Failure Modes and Effects Analysis. The author[29] considers that the safety case consists of four elements:

- Requirements – the safety objectives that must be addressed to assure safety
- Evidence – information from study, analysis and test of the system in question
- Argument – showing how the evidence indicates compliance with the requirements
- Context – identifying the basis of the argument presented.

The argument links the evidence to the requirements and all three must be valid for the defined context.

The goal structures used within SAM to present the structure of a safety argument consists of goals, strategies, solutions (roughly equivalent to claims, warrants and evidence within the Toulmin model) and context. Context may be associated with goals, strategies or solutions. The author links the Goal Structuring Notation (GSN) to the four elements of the safety case argument. Requirements are represented as top level goals. Evidence is represented as solutions. Contextual information is represented as context, assumptions, justifications and models. Argument is communicated through the structuring of goals supported by sub-goals. The GSN used within SAM extends Toulmin's form of argument representation to present a notation which the author believes applies particularly well to the safety justification domain[29]. The author[29] acknowledges that the concept of goal decomposition has been applied in areas other than argumentation, particularly in requirements engineering.

The GSN approach has been applied within the railway, aerospace and defence industries. Users are reported[29] as finding the approach helpful for understanding the scope and complexity of safety cases and providing a basis for an executive summary of the safety justification.

The 'Air Traffic Management (ATM) system criticality raises issues in balancing actors responsibility (ARIBA)' project[(33)] utilised the SAM tool (including GSN) to develop a safety case for an advanced ATM system; constructing the High Level Argument and identifying relevant Supporting Evidence. The ARIBA project defined the safety case as 'a consistent and coherent set of arguments used to justify the safety of a system at all stages in its lifecycle'. The project found the principal benefit of the safety case argument approach was that it provides a structure to the evidence presented to justify the system. Additionally '*that the need to structure a coherent argument from general principles through to the functions to carry out the tasks required a holistic view to be taken of the safety argument. It becomes more difficult to pre-judge the impact of changes, and to get 'locked in' to considering some narrow range of issues*[(34)].'

The examples included within the above references on SAM[(29,33)] have tended to focus on technical control measures for assuring safety and not tackled the organisational contribution. Therefore it is not clear from reviewing these sources how applicable the GSN and SAM tools would be to an overall argument based safety case incorporating organisational and technical aspects. However due to the close relationship with the Toulmin model it is foreseeable that they could be applicable.

The next example is from research seeking to build computer systems which can reason autonomously about alternative actions, informed by predictions of their possible consequences[(30)]. Due to difficulties in estimating and agreeing quantitative probabilities the authors have explored qualitative approaches to practical reasoning and in particular, the application of argumentation. The specific application is scientific reasoning about the possible carcinogenicity of some chemical substance. One of the benefits found by the authors of such an approach was that argumentation permits coherent reasoning about the consequences and likelihood's of alternative courses of action even when expressed in qualitative terms. Another paper by these authors[(31)] further develops this approach. The carcinogen risk assessment usually involves the comparison and resolution of multiple and diverse evidence, which may conflict. Use of argumentation allows the reasons for claims to be represented in association with the claims themselves and cases for and against a particular claim to be compared. This paper also states that an argumentation formulation permits the representation of quantitative and qualitative information in the reasoning process. Their argument structure is informed by Toulmin's structure.

Further research from the human health risk domain[(3)] explores a concept of scientific rationality which involves systematic comparison of alternative risk estimates.

The final example proposes the use of argumentation for medical decisions by artificial intelligence systems[(8)]. The paper asserts that argumentation has far greater representational power than traditional mathematical formalisms based on probability or other quantitative concepts, that it is more versatile and robust under conditions of lack of knowledge. The author comments that where it is possible to directly compare strict probabilistic methods and the author's argumentation based decision process, greater precision does not generally lead to better decision making. The author has found argumentation to be a very practical technique for decision making in systems because it provides a simple method for comparing the relative persuasiveness of competing claims without requiring a comprehensive body of quantitative knowledge of the world. The basic structure of the argument is drawn from Toulmin's model.

DISCUSSION

What are the likely counter-arguments to this proposal?

Firstly is it achievable? It relies on safety science. Perhaps the truth is that SC lack arguments because there is insufficient safety science to support arguments. No doubt safety science has plenty of scope for development but we do not accept there is insufficient. However, the degree of confidence in the science is inconsistent. For example; generally, a greater degree of confidence can be placed in the understanding of the science of engineering materials and structures than in the understanding of organisational behaviour. That is, the conditions under which hardware components and structures fail can be forecast with greater certainty than the performance of a team of people tackling a complex problem. However, by bringing safety science to the fore, the use of argument could drive improvement in areas where further research is required.

Secondly, it may be argued that this is a consultants agenda, and that writing a SC should involve the workforce and is a powerful motivation for improvement. This is a naïve argument for several reasons.

There is the obvious concern that the staff and workforce do not have the necessary knowledge E.g. If you were to visit a facility in an earthquake zone. Would you be convinced by the knowledge and experience of those who work there about the seismic stability of the area or by the analysis of an expert seismologist? Organisational design, management of safety and human factors are not 'common sense' but difficult issues. Many of the theories are emerging, incomplete and contradictory. Workforce involvement and continuous improvement are relevant theories of predictive safety and are likely to be evaluated favourably during the validation phase of the SC evaluation, however these approaches are a means of positively influencing safety culture and when applied successfully are consistent with an organisation's full range of activities. That is, the SC is not a particularly useful tool for developing workforce involvement and continuous improvement and there are many more effective means and in itself, involving the workforce in the SC is not going to lead to cultural change.

Additionally, writing the SC is a one-off exercise. It will be updated and reviewed, but are companies really willing to repeat the initial resource commitment every few years? This is highly unlikely. Hence if a SC initiates significant change, it is a one-off event. Use of argument within SC's would be more likely to lead to critical examination of an organisation's activities rather than a justification of the status quo. Therefore it would be more likely to initiate any required changes to improve safety.

Further, is this argument claiming that the SC is an on-line management tool? But is it not the case (usually) that procedures and other material are on-line and the SC is updated periodically to reflect the on-line material that is actually in active use? The SC is poorly suited to becoming a hands-on management tool because it is difficult to envisage how such a document could be made sufficiently dynamic to facilitate daily use in parallel to regulatory requirements. If a company claims that the SC is in the front line of their SMS it should cause concern because it suggests inflexibility and a potential lack of understanding about the function of a SMS.

It would be very beneficial for the workforce (and stakeholders) to be able to read a clear argument which explains how a MAH facility's activities lead to continuing safe operation of that facility within a SC which also forms a plan for strengthening the argument.

CONCLUSIONS

This paper seeks to show that there are weaknesses associated with the current demonstration model and proposes an alternative argument model. The use of argument for SC's appears consistent with the Regulations and HSE's approach, substituting argument for demonstration provides a process for achieving the desired SC regime output.

Some benefits of the argument approach:

- Dutyholders would be led to think about the completeness of their argument and the degree of confidence in it.
- Would encourage linking of organisational as well as hardware controls to hazards.
- Revealing soundness and strength/weakness of arguments has the potential to improve the transparency of SC's.
- Argument approach draws attention to safety science and has the potential to stimulate improvement.
- The requirement for the Dutyholder to plan to strengthen the argument (as well as reducing risks) has the potential to stimulate research and development.
- Use of an argument model would assist the Regulator during the validation and verification phases of SC assessment.

REFERENCES

1. British Standards Institute, 1999. Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). BS EN 50126:1999
2. Corax, 5th Century BC. Art of Rhetoric (reported, none of original text known to have survived)
3. Crawford-Brown, D., 2000. Scientific Models of Human Health Risk Analysis in Legal and Policy Decisions, Carolina Environment Program, University of North Carolina.
4. ENDS December 1999, Issue No. 299
5. ENDS October 2001, Issue No. 321
6. Entec UK Ltd., 2000. A Railway Safety Case Regime. Class Number EF 14. Ladbroke Grove Rail Inquiry. Part 2. Rail Safety. Core Documents. Piece Number 184
7. Fisher, A., 1993. The logic of real arguments. Cambridge University Press, Cambridge
8. Fox, J., 2000. Arguments about beliefs and actions: Decision making in the real world. Imperial Cancer Research Fund Laboratories
9. Hart, C., 1998. Doing a literature review, releasing the social science research imagination, Ch4 Argumentation Analysis. London, Sage

10. Hikins, J, 1996. Remarks on The Development of Rhetoric. Kendall-Hunt
11. Hinderer D.E, 1992. Building Arguments. Belmont, California. Wadsworth
12. HMSO, 1965. Nuclear Installations Act
13. HMSO, 1971. Atomic Energy and Radioactive Substances, Licensing and Regulation of Sites. The Nuclear Installations Regulations.
14. HSE, 1984. Control of Industrial Major Accident Hazards (CIMAH) Regulations SI 1984/1902
15. HSE, 1992. Safety assessment principles for nuclear plants
16. HSE, 1992. Offshore Installations (Safety Case) Regulations
17. HSE, 1994. Nuclear Site License Conditions, Notes for Applicants
18. HSE, 1994. Railways (Safety Case) Regulations
19. HSE Books, 1994. Railway safety cases. Railways (Safety Case) Regulations, 1994. Guidance on Regulations, L52
20. HSE, 1995. Offshore Installations (Prevention, Fire, Explosion and Emergency Response) Regulations, SI 1995/743
21. HSE, 1996. The Pipelines Safety Regulations SI1996/825
22. HSE, 1996. Offshore Installations and Wells (Design and Construction, etc.) Regulations, SI 1996/913
23. HSE, 1999. Control of Major Accident Hazards (COMAH) Regulations SI 1999/743
24. HSE, 1999. Railway Safety Regulations SI 1999/2244
25. HSE, 1999. Guide to the COMAH regulations, L111
26. HSE, 1999. Preparing Safety Report, COMAH Regulations, HSG 190
27. HSE, 2002. Railways Safety Case Assessment Manual
28. HSE, United Kingdom Interdepartmental Liaison Group on Risk Assessment (UK-ILGRA), 2002. The Precautionary Principle: Policy and Application
29. Kelly, T. P., 1998. Arguing Safety – A Systematic Approach to Managing Safety Cases, University of York
30. McBurney, P and Parsons, S., 1999. Truth or Consequences: Using argumentation to reason about risk. Presented at BPS Symposium on Practical Reasoning, London.
31. McBurney, P and Parsons, S., 2000. Dialectical Argumentation for Reasoning about Chemical Carcinogenicity, University of Liverpool
32. Ministry of Defence, 1996. 00-56 Safety Management Requirements for Defence Systems. Defence Standard
33. Pygott, C., Furze, R., Thompson, I. And Kelly, C – WP5 Final Report, Safety Case Assessment Approach for Air Traffic Management (ATM), ATM system criticality raises issues in balancing actors responsibility (ARIBA), DERA
34. Railtrack, 2000. Ensuring Safety Management Issue 3, Yellow Book 3, Volumes 1 and 2, Fundamentals and Guidance, BS EN 50126
35. Rowlands (DETR), 2000. Review of Railtrack Safety and Standards Directorate
36. Sagan, S., 1993. The limits of safety: Organisations, accidents and nuclear weapons. Princeton Paperbacks
37. Tansley, 1999. The Tansley Report-review of arrangements for standard setting and application on the main railway network; interim report
38. Toulmin, S, 1958. The Uses of Argument. Cambridge University Press, Cambridge.

39. Toulmin S, Reike R and Janik A, 1979. An Introduction to Reasoning, New York: Collier Macmillan
40. Uff, Professor J., 2000. Report into The Southall Rail Crash

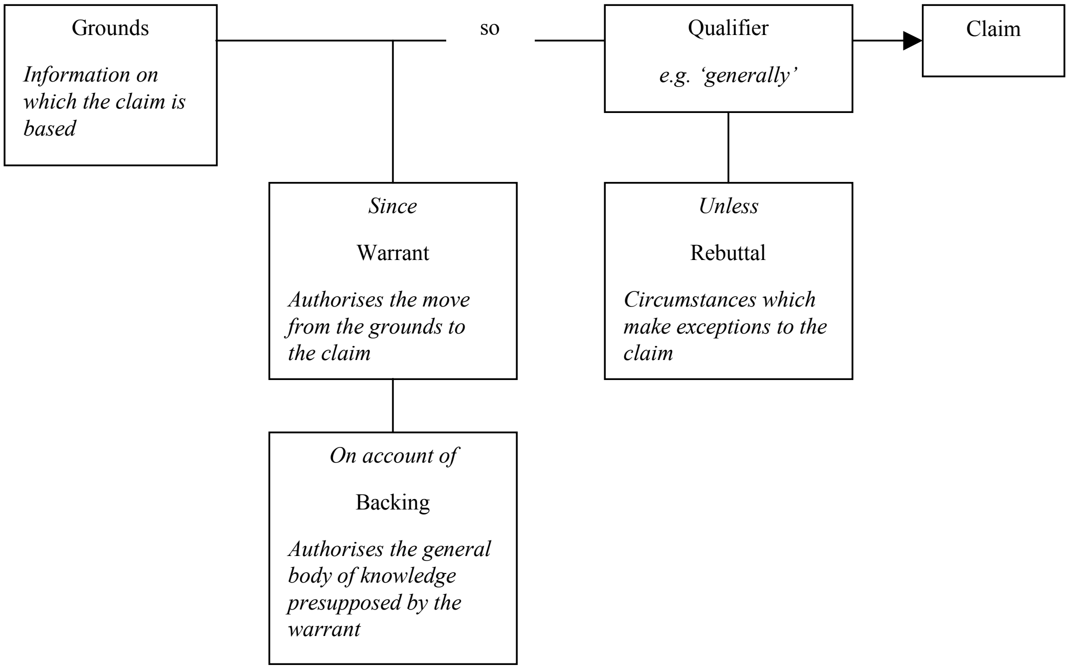
Grounds
Information on which the claim is based
so
Qualifier
e.g. 'generally'
Claim
Since
Warrant
Authorises the move from the grounds to the claim
Unless
Rebuttal
Circumstances which make exceptions to the claim
On account of
Backing
Authorises the general body of knowledge presupposed by the warrant

Figure 1. Toulmin's argument structure

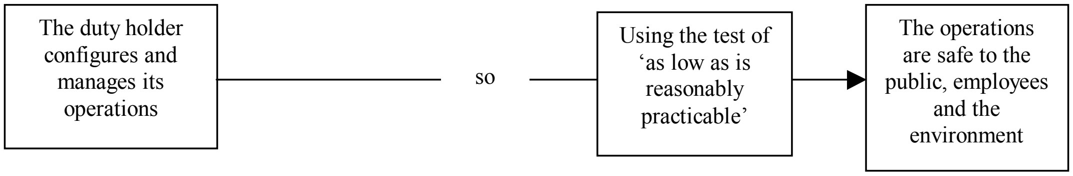
The duty holder configures and manages its operations
so
Using the test of 'as low as is reasonably practicable'
The operations are safe to the public, employees and the environment

Figure 2. An example of a dutyholders opening claim presented in Toulmin's structure