 © 2003 Crown Copyright

KEY ELEMENTS OF RISK DECISIONS IN THE CONTROL OF MAJOR ACCIDENTS HAZARDS

Andrew G. Rushton
Methodology and Standards Development Unit, Hazardous Installations Directorate, HSE

© Crown Copyright 2003. Reproduced with the permission of the Controller of Her Majesty's Stationery Office.

COMAH Safety Reports must show that all measures necessary are in place to prevent control or mitigate relevant major accidents.
Many Operators consider that they have in place all reasonably practicable risk reduction measures, but have difficulty presenting their position to the Competent Authority, particularly in relation to "predictive aspects". Usually, most fundamentally, this is because the Operator does not set out how their process of risk management provides the necessary assurance that the risk is not intolerable and all necessary measures are in place. Often the description of necessary steps leading to risk decisions is incomplete.
This paper clarifies the flow of information which needs to exist in a risk control system and which, therefore, underlies the regulators' view of how predictive aspects are handled in safety reports. The link to a specific goal-based standard (BS IEC 61508) is described.
The Operator should be able to show that the relevant decision makers were, where necessary, aware of the risk criteria, the "risk picture" and the costs of practicable risk reduction measures.
Where initial attempts at the demonstrations required by COMAH have been ineffective, this is likely to be remedied by setting out the thought process underlying risk decisions more clearly, rather than just by providing more detail.

KEYWORDS: COMAH, risk, information, predictive, criteria

INTRODUCTION

The "Seveso II" directive aimed to improve control of major accident hazards from hazardous substances. It is implemented in the United Kingdom, in part, by the Control of Major Accident Hazards Regulations (COMAH)[1].

"Operators" of "establishment" where COMAH Regulation 7 applies ("top tier COMAH sites") are required to prepare a Safety Report and present it to the Competent Authority (CA), comprised of the Health and Safety Executive (HSE) and the Environment Agency or the Scottish Environmental Protection Agency. A requirement of the Safety Report is that it includes demonstrations which indicate acceptable control of major accident hazards.

Operators of COMAH establishments have found the preparation and presentation of demonstrations in Safety Reports challenging, particularly in relation to "predictive aspects"[2].

This paper aims to set out the background against which these predictive aspects are viewed by the regulators (the "Competent Authority"). It should help Operators to understand the CA's perspective and help Operators to avoid common faults in the preparation and presentation of predictive aspects of their reports.

Key steps necessary to support risk decisions are identified. The relationship between case-specific risks and risk criteria is described. The implications for reporting a risk analysis within a Safety Report are identified. Attention to these implications can help lead to successful demonstration that all necessary measures may have been taken.

KEY STEPS IN SUPPORT OF RISK DECISIONS

The essence of making the necessary demonstrations in a Safety Report is to show that all necessary measures to prevent control and mitigate major accidents have been taken. In relation to safety, this generally involves the following four key steps in support of risk decisions:

i) identification of potential major accidents or "major accident scenarios";
ii) assessment of the approximate consequences and approximate expected frequency of the identified major accidents;
iii) classification of the overall risk position (with respect to individuals and groups) as either broadly acceptable or tolerable if risks are reduced as low as reasonably practicable (ALARP), *in other words a decision that the overall position is not intolerable*;
iv) consideration of what further measures could be taken and justification for not taking these measures, *in other words a decision that further measures are not reasonably practicable*.

Sometimes reference to and use of industry-wide standards may be considered to cover the later steps. This will be relatively rare for top-tier COMAH sites and even then will usually only apply to individual risk to people at the establishment. More commonly - for high and multiple hazards, for complex and novel plant, and for assessment of risk with respect to groups, or *societal risk* - case-specific attention to all four steps is necessary.

In the process of classifying an overall risk position, or "risk picture", it may be found that the position is intolerable. In such cases the position will need to be altered (by suspending the activity or introducing further risk reduction measures). An intolerable position should not, therefore, be an outcome of risk analysis that is reported. For this reason this outcome has been excluded from the above steps.

In the course of considering further measures, the justification for not taking a measure may be found to be too weak. In such cases the measure is necessary and will need to be taken. A position of not having taken a necessary measure should not be an outcome of risk analysis that is reported. For this reason this outcome has been excluded from the above steps.

In the sense that further measures may become available or may become more cost-effective, or improved science may lead to a revised estimate of probability or consequence of an accident, maintaining risk "ALARP" is a process of continuous review and improvement. This does not mean that, where reasonably practicable measures have been identified, then it is satisfactory to describe a forward plan which will, if and when implemented, achieve the demonstrations required.

EXPERIENCE IN REVIEWING REPORTED RISK ANALYSIS

Many Operators consider that they have in place all reasonably practicable risk reduction measures, but have difficulty presenting their position to the Competent Authority. Usually, most fundamentally, this is because the Operator does not set out how their process of risk management achieves the steps set out above. Often the steps are incomplete or the later steps are completely omitted (or merely implied). Sometimes the flow of information from one step to the next is unclear, so that the robustness of the overall approach is not evident.

When they are challenged about how their report achieves the steps set out above, many Operators perceive that the CA cannot be satisfied without much more quantification and/or much more detailed information. More quantification or detailed information may indeed be appropriate, but this is not usually the key to improving the Report. No amount of additional quantification or information may compensate for incompleteness in reporting the necessary steps taken in support of risk decisions.

Sometimes the problem will lie in the description of the risk control process in the Safety Report, rather than in the operating practices at the establishment. However, the presumption should be that where hazards are high there might be unusual risk reduction measures (i.e. measures not prescribed by codes or standards) which are necessary in the particular circumstances. The Operator needs to set out the thought process – considering what can go wrong with what result, assessing the risk picture, considering what defences are in place and why more cannot be done – which will ensure that such unusual, but necessary, measures are implemented.

In order to conduct and report risk analysis and risk control successfully, an Operator must understand the relationship of risk criteria to case-specific risk. The Operator must employ suitable risk criteria when considering both the risk posed by their operations and the opportunities for further risk reduction measures.

RISK CRITERIA AND THEIR RELATIONSHIP TO RISKS FROM MAJOR ACCIDENT SCENARIOS

A criterion which, for example, discriminates between a position where the risk to an individual at work is intolerable and a position where the risk is tolerable if risks are rendered ALARP may be termed a “risk criterion”.

The classification of the overall risk positions (in relation to individuals and groups) requires an Operator to have in mind risk criteria.

The COMAH Regulations are “goal-setting”, in recognition of the scale, complexity and evolving nature of the regulated activities. It is generally agreed that such activities are not suited to prescriptive controls.

The Regulations are not prescriptive, so there is no recipe to follow in making the required demonstrations. There is, on the other hand, a philosophy of risk control, underlying COMAH and other legislation, which provides a framework for adequate treatment of “predictive” aspects in Safety Reports.

HSE has set out indicative criteria for risks to people[3] which will be used in support of regulatory decisions. Clearly the relationship of any Operator-specified criteria to those indicated by HSE will be considered when HSE makes regulatory decisions as part of the COMAH CA.

A significant feature of risk criteria is that they relate to the relationships of a risk controller to the person or group at risk. These relationships are not restricted to COMAH regulated hazards, nor further restricted to individual major accident hazards. Therefore there is strictly no mapping between risk criteria and particular hazards or scenarios. For this reason methods which imply such a mapping, such as frequency-consequence matrices must be used with caution[4]. Individual risk to the more active people at work in the process industries from hazards other than those regulated by COMAH will rarely be negligible. Whilst much of the risk analysis in a Safety Report will be focussed on major accident scenarios as defined in the COMAH regulations, the risk picture which the Operator reports (and reflects on in reaching decisions on risk reduction measures) should be informed by a broader perspective.

SUPPORT TOOLS FOR RISK ANALYSIS

Sophisticated tools supporting risk analysis (e.g. for gas dispersion modelling) may be appropriate aids to judgement. This does not imply that such tools are always required. Whether or not such tools are used, it will usually be necessary to show that all the steps in risk analysis necessary to prepare for risk decisions are understood and followed when managing major hazards at the establishment.

In other words, sophisticated tools may be a necessary support to risk decisions but are not a substitute for risk decisions.

With or without a sophisticated approach, the Operator needs to be making decisions about what can go wrong, what the consequences would be, what measures are in place and why no more should be done.

DECISIONS ON WHAT ARE THE NECESSARY MEASURES

Figure 1 sets out, in outline, the flow of information in major hazard risk analysis and decision-making. This flow of information is essential to ensuring that a proper conclusion is reached on what are the necessary risk control measures.

In principle, Operators will decide that the necessary measures are complete (in the sense that they are all the measures necessary). This will allow them to set out a *justification for not adopting any further risk reduction measure* (final box in the Figure). To reach this conclusion, the Operator generally needs to make two critical decisions. Firstly, having in mind the risk to groups and individuals (the *risk picture*), a decision can be made that the risk is not intolerable. Secondly, and where risks are only tolerable if rendered ALARP, having in mind the available *further practicable risk reduction measures* and their costs, a decision can be made whether or not to deploy each measure.

Knowledge of the *risk picture* requires knowledge of the *risk criteria*, the *COMAH risks* and other relevant risks (*other risks*). Knowledge of the *COMAH risks* requires knowledge of the *consequences* of major accident scenarios and the predicted *frequency* of major accident scenarios. The *consequence assessment* and *frequency assessment* generally requires many inputs some of which are indicated in Figure 1.

Knowledge of the available *further practicable risk reduction measures* (and their costs) in turn requires a mechanism for identifying (and costing) such measures.

The process of risk analysis is complete when the decision maker is able to conclude either that the risks are broadly acceptable or that no further risk reduction measures are reasonably practicable (because the cost is grossly disproportionate to the benefit[4]).

From a regulator's perspective, the most satisfactory way of demonstrating that the risk analysis and decision making may have been concluded in a satisfactory way is to show that the decision makers had all the information that they needed to follow the process outlined above (and have followed this or a comparable process).

QUANTIFICATION OF ELEMENTS OF THE RISK ANALYSIS

Some approximate quantification of consequences of major accident scenarios, frequencies of major accident scenarios and costs of risk reduction measures will generally be necessary in order to achieve the purposes of risk analysis to support risk decisions reliably and transparently. Using judgement to allocate case-specific variables (such as predicted frequency) to bands of values, within quantified limits, will usually be both appropriate (because of the lack of accuracy in available estimation methods) and sufficient. The correct allocation is crucial to discovering whether the necessary measures are complete. Where it is proportionate (because the consequences are high), or where the uncertainty in the judgement is high, then the decision will be sensitive to the depth and strength of the analysis. In such cases it will be reasonable to support the judgement with further quantitative or qualitative analysis (more detailed analysis and/or "sensitivity" analysis) or to upgrade the allocation to a more pessimistic band.

Some would regard the process of allocation to (quantified) bands as qualitative, others may regard it as unnecessarily quantitative. The case for this minimal level of quantification is clearly seen wherever the decision making process involves collaboration.

For example, one person may estimate the frequency of a scenario as "unlikely". If another person attaches a different meaning to the word "unlikely" when setting out the risk criteria, or if a third person has another meaning in mind when judging the benefit of eliminating the scenario, then it is difficult to see how the overall decision making process can be relied upon to deliver all the necessary measures.

It has to be accepted that estimates of each contributory factor underlying a decision will be uncertain, but this is not a justification for not making the necessary estimates.

Methods for proceeding with risk analysis have been discussed by Carter et al[5], who also describe an approach to estimating the overall position in relation to societal risk. Gadd et al[6] have recently reviewed pitfalls in risk assessment, many of which are particularly pertinent to the support of risk decisions in the control of major accident hazards.

DEMONSTRATION

Whatever support tools are used, the Operator usually and ultimately will rely on an expert group or person making decisions (about whether to deploy a risk reducing measure).

It may well be that "expert judgement" is used, and is appropriate, for some or all contributory decisions. It will generally be practicable for an expert to express their reasoning in a (minimally) quantitative way. Where there is not minimal quantification, then auditing the decision making process or revisiting a decision in the light of changing circumstances will be difficult or impossible.

For decisions on whether the risks are tolerable (if ALARP) or broadly acceptable, the Operator should be able to show that the decision making person or group was aware of the relevant criteria and the risk picture and show that the decision was informed by a reasonable (but not necessarily detailed) estimate of the consequences and likelihood of the hazard in question. For a justification of not implementing a further risk reduction measure, the operator should additionally be able to show that the person or group had some awareness of the approximate cost of the proposed measure.

Where these conditions for decision making cannot be shown, then it is hard to see how the Operator can be confident that appropriate decisions are being made and how the decisions arising can be revisited as circumstances change (for example in response to increased activity or reduced cost of a risk reduction measure). In particular it is hard to see what check there is against a drift into an intolerable position.

The Safety Report needs therefore to provide answers to these questions:

- How does the Operator perform hazard identification (HAZID) and what satisfies the Operator that this approach to HAZID is suitable and sufficient in all the circumstances of their business?
- How does the Operator estimate the frequency and consequences of potential major accidents?
- How does the Operator judge the overall risk position to be tolerable (or more rarely broadly acceptable)?
- How does the operator ensure that opportunities to take further measures are identified and reviewed appropriately?
- What justification does the operator have for not taking any practicable further measures and what satisfies the operator that this approach to justifying taking any further measures is suitable and sufficient in all the circumstances of their business?

A Report is unlikely to be satisfactory in relation to predictive aspects if it does not clearly and preferably explicitly deal with these questions.

This does not mean that every Report must have a uniform and high level of quantification and detail. It does mean that a narrative style of report which makes clear the flow of information leading to decisions on risk tolerability and deployment (or not) of measures is helpful. Where links between details of fact and decisions of risk control are not presented, then an increase in detail is unlikely to remove concerns about predictive aspects.

GOAL SETTING FOR IMPLEMENTING INSTRUMENTED PROTECTIVE SYSTEMS

BS IEC 61508[7] supports the specification and implementation (etc.) of safety-related systems utilising electrical, electronic or programmable electronic technologies. Publication of a related process-industries sector-specific standard (BS IEC 61511) is imminent.

The standard links the “safety requirements specification” of the safety-related systems to risk criteria through a “Safety Integrity Level” (SIL). The “necessary risk reduction” is the reduction in risk that has to be achieved to meet the “tolerable” risk for a specific situation. In other words, the standard supposes that, for a particular application, a target of

risk reduction by the protective system can be identified and this will lead to specification of the necessary SIL. Figure 2 shows the outline of how risk reduction can be allocated.

In the context of COMAH, the target risk reduction may be relatively complex. For example the aim may be to reduce an intolerable risk to a tolerable one but then to reduce the risk further if reasonably practicable.

To apply BS IEC 61508, therefore, an Operator of a top tier COMAH site will generally need to set out the overall approach to risk control in order, in this case, to generate the target risk reduction for a protective system.

Often Safety Reports describe the SIL achieved in the implemented protective system without reference to any process for allocating risk reduction to that system. This does not provide any justification for the selection or acceptance of the system implemented. Sometimes it is stated or implied that, on the basis of the SIL achieved and the consequent reduction of risk from a particular hazard or collection of hazards, the Operator can conclude that they have directly met an appropriate risk criterion. This approach, which supposes risk criteria apply to the relationship between risks from equipment or hazards to individuals or groups, is not generally compatible with HSE's view that risk criteria are applicable to the relationship between all the risks in the control of one *dutyholder* (the Operator in the context of COMAH) and the individual or group at risk. The annex outlines how these two views differ and why they are not compatible (in general and in the context of COMAH in particular).

In some cases the Operator has treated the electrical/electronic/programmable electronic system (for which a SIL has been established) in isolation without reference to other (e.g. mechanical) risk reduction measures. Clearly this can make the task of showing that the risks are acceptably low more difficult.

DISCUSSION

In the COMAH regime, it is not generally sufficient for an Operator to employ competent people, on whom they rely to make decisions about – for example – the appropriate SIL of an instrumented protective system. One purpose of the Safety Report is to make these decisions and their basis explicit (however much or little they rely on sophisticated decision aids). If the Operator cannot write down how it makes these decisions, then the charitable conclusion is that it does not know how it makes these decisions but it has employed staff who do know; the less charitable conclusion is that the necessary decisions have not been made.

Of course the CA is more likely to challenge Operators' risk decisions where they do not appear to be proportionately sophisticated, but the CA will be most concerned to see evidence of the application of a complete approach to risk decision making which, in principle, *can* deliver appropriate decisions, however unsophisticated.

CONCLUSIONS

Operators of COMAH establishments have found the preparation and presentation of demonstrations in Safety Reports challenging, particularly in relation to "predictive aspects".

There is a philosophy of risk control, underlying COMAH and other legislation, which provides a framework (but no prescription) for adequate treatment of "predictive" aspects in Safety Reports.

The Operator should be able to show that the relevant decision makers were, where necessary, aware of risk criteria, the "risk picture" and the costs of practicable risk reduction measures. A model for the essential flow of information, needed to support risk decisions in the control of major accident hazards, has been presented (Figure 1).

Where initial attempts at the demonstrations required by COMAH are ineffective, this is likely to be remedied by setting out more clearly the thought process underlying risk decisions, rather than just by providing more detail.

The regulator is, of course, more likely to challenge Operators' decisions where they do not appear to be proportionately sophisticated, but the regulator will be most concerned to see evidence of a complete approach to risk decision which can deliver appropriate results.

DISCLAIMER

The views expressed in this paper are those of the author alone and are not a statement of HSE policy.

1 Health & Safety Executive, 1999, 'A guide to the Control of Major Accident Hazards regulations 1999, L111, HSE Books.

2 Health & Safety Executive, 2002, COMAH Safety Report Assessment Manual (revised), available at http://www.hse.gov.uk

3 Health & Safety Executive, 2001, 'Reducing Risks, Protecting People, HSE's decision-making process', HSE Books, see also http://www.hse.gov.uk/dst/alarp1.htm etc.

4 Middleton M & Franks A, September 2001, 'Using Risk Matrices', The Chemical Engineer.

5 Carter DA, Hirst IL, Maddison TE and Porter SR, 2003, 'Appropriate risk assessment methods for major accident establishments', Trans I Chem E (B) Proc Safety and Envtl Prot, accepted for publication.

6 Gadd S, Keeley D and Balmforth H (2002) 'Good practice and pitfalls in risk assessment' HSL research report, in preparation.

7 BS IEC 61508, 1998, Functional safety of electrical/electronic/programmable electronic safety related systems.

 © 2003 Crown Copyright

ANNEX: RISK IN THE CONTROL OF A DUTYHOLDER AND RISK FROM A HAZARD

INTRODUCTION

The question is often asked: "What do I have to do to make the risk from my plant (or equipment) acceptable". There is no simple answer. This annex describes some features of the type of risk approach described by HSE which lead to the answer being context dependent. Two extreme positions are described which, hopefully, shed light on why there is no simple answer.

FEATURES OF HSE'S RISK APPROACH WHICH COMPLICATE ITS APPLICATION TO SINGLE HAZARDS

The risk criteria set out in "R2P2"[3] suggest that, in general, a dutyholder must find that risks are not intolerable and (where risks are not broadly acceptable) must find that further risk reduction measures are not reasonably practicable.

These criteria, however, relate to all the risks arising in the relationship of a risk controller (the dutyholder) with the person or group at risk. These relationships are not restricted to risks arising from COMAH regulated hazards, nor further restricted to any individual major accident hazard. Therefore there is strictly no mapping between risk criteria and risk from a singular hazard (perhaps associated with one plant or one piece of equipment).

Application of the "ALARP" principle requires the costs and benefits of further risk reduction measures to be considered, but the costs and (particularly) the benefits are affected by the operating context of the hazard. Most typically, in the context of COMAH, the benefit to be gained will increase with the number of people likely to be affected by a particular scenario.

Societal risk criteria are different in quality to individual risk criteria. Generally, satisfying individual risk criteria does not guarantee that any societal risk criteria have been satisfied.

Three needs arise, therefore, which can affect the risk picture and/or the reasonable practicability of further risk reduction measures:

i) the need to consider all relevant risk under control of the dutyholder (not just the risk from one plant/equipment);
ii) the need to distinguish between ostensibly identical hazards where one instance of the hazard has potential for harming more than one person (or, more generally, where the cost and benefit of a risk reduction measure in one application can be distinguished from the cost and benefit of the same measure in a different application);
iii) the need to consider societal risk.

In principle a collection of risks, each one "tolerable" if it existed in isolation, can produce an "intolerable" position.

The benefit of deploying a further risk reduction measure will generally increase if more than one person could be harmed by the hazard that is to be controlled.

A single measure may reduce the risks from several hazards, so that in the particular application of that measure the benefit is increased.

When the societal risk picture is evaluated it may be that further measures are required (which would not have been required on the basis of individual risk assessment).

IMPLICATIONS FOR RISK MANAGEMENT

The problem is that individuals in a risk-controlling organisation will often only have direct responsibility for one hazard or a small sub-set of the hazards controlled by the dutyholder. It is tempting to try to re-cast the overall requirement as a need to find that risks *from my plant* are not intolerable (etc.). In the context of COMAH this temptation should usually be resisted and there is a need for the bigger picture to be considered.

At one extreme there may be no significant societal risks and, with the exception of a single hazard, there are no significant risks of death to an individual. In this case application of a general approach (for risk of death) *as if* it applied to the single hazard will not lead to serious error. At the other extreme, there may be significant societal risks and several hazards each of which has potential (in a single incident) of causing harm to many people.

CONCLUSION (OF ANNEX)

A risk control approach intended to encompass all the risks arising in the relationship of a risk controller to a person or group cannot generally be applied to single hazards where other hazards are significant.

Whether or not risk reduction measures are reasonably practicable can depend on the operating context of a hazard. In the context of COMAH, where the emphasis is on sites presenting many hazards and on scenarios in which many people could be harmed, a strong dependence of the reasonable practicability of measures on the particular operating context can be expected.

 © 2003 Crown Copyright

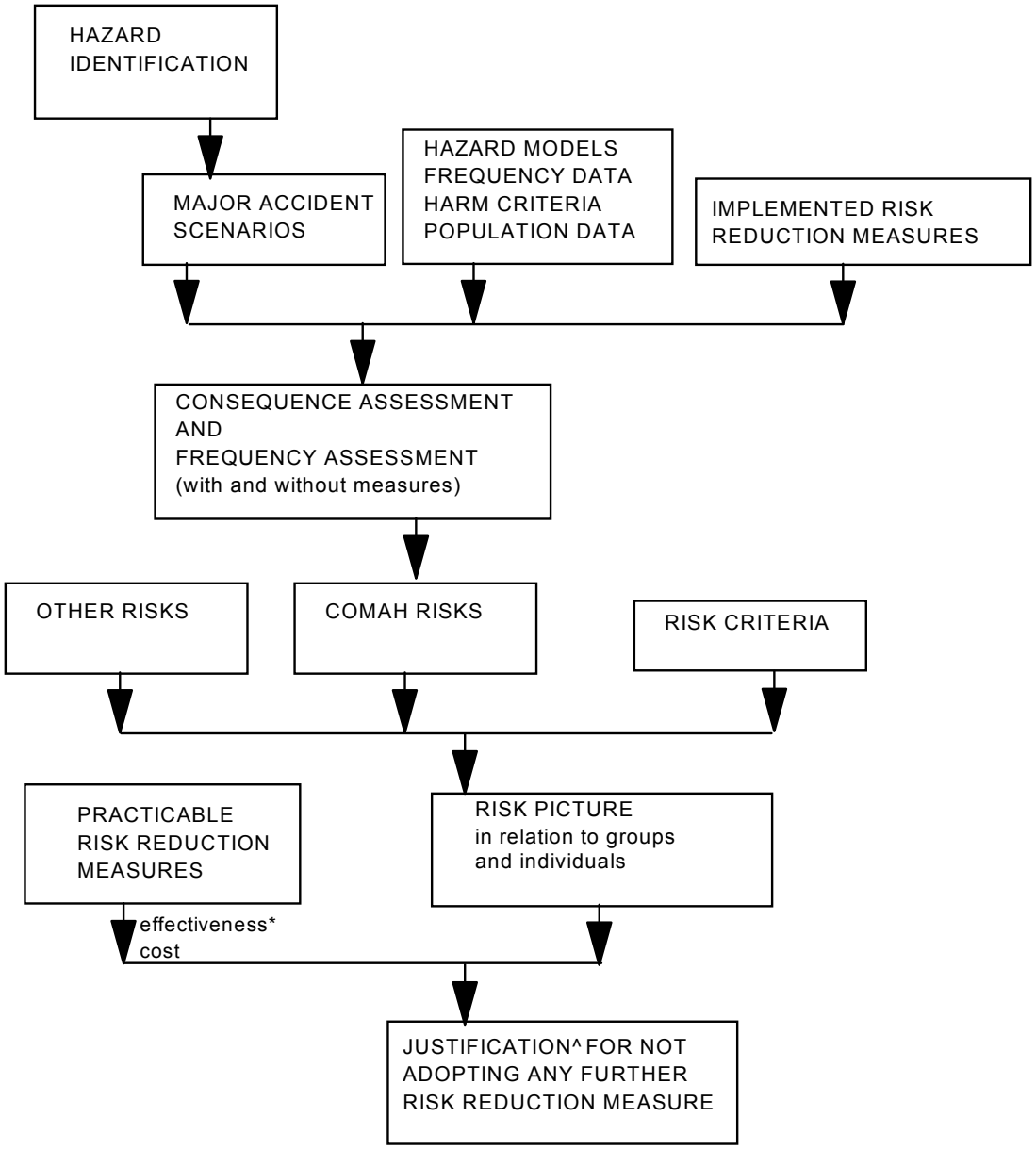

Figure 1. The flow of information in major hazard risk analysis
Note that in the process of establishing an acceptable position there will be iteration (not shown in the figure) if any element of the "risk picture" is intolerable or any further risk reduction measure is found to be reasonably practicable.

 © 2003 Crown Copyright

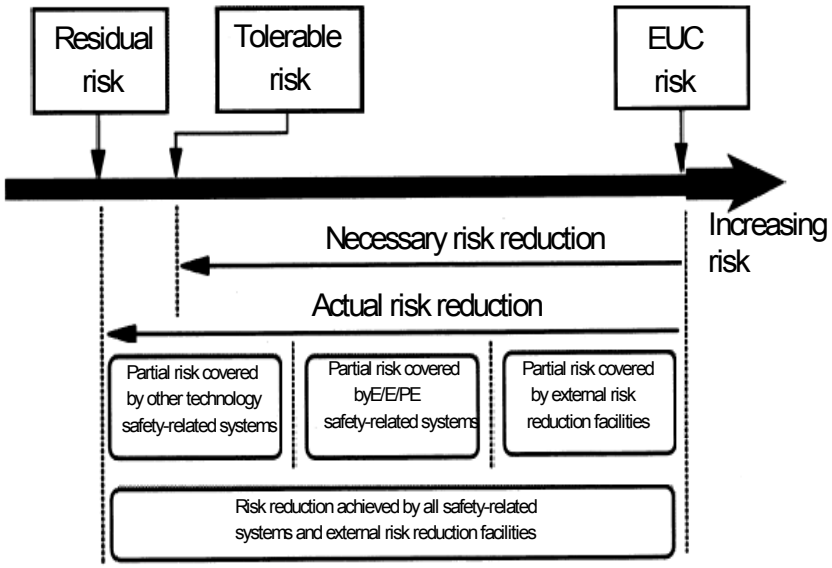

Figure 2. "Risk Reduction General Concepts", reproduced from BS IEC 61508 - 5, Figure A.1, courtesy of the British Standards Institution.
EUC = equipment under control
E/E/PE = electrical/electronic/programmable electronic