Production of TATB: A case study in making the risks of explosives manufacture as low as reasonably practicable

by

Dr Peter Allan Moreton,
MBTB Ltd,

SAFEX Topical Papers Series
Paper no 03/2006

About the author

Dr Peter Moreton is a chemist by training, having completed a PhD in analytical/environmental chemistry in 1984. His interest in explosives began while he was doing post-doctoral research at the Royal Military College of Science. At this time he became involved in the application of risk assessment techniques to ensure safe storage of explosives, particularly in situations where the standard quantity-distance prescriptions could not be met.

He was a senior consultant with the UK Atomic Energy Authority from 1987 to 1999, developing and applying risk assessment techniques to a variety of hazardous activities, including the storage and transportation of explosives and ammunition. He was instrumental in developing the Explosives Incidents Database Advisory Service (EIDAS) in the early 1990s. This service was originally developed on behalf of the UK Health and Safety Executive (HSE) and the UK Ministry of Defence, and he has continued to maintain EIDAS on behalf of these organizations to the present day.

Since 2000, Dr Moreton has worked as a freelance safety consultant, trading under the name of MBTB Ltd. His clients include the HSE, MoD, the Confederation of British Industry, as well as a number of explosives manufacturing companies based in the UK.

Contact details:
28 Hazelborough Close,
Warrington, Cheshire, WA3 6UL
ENGLAND
Tel: 0044 1925 831175
Fax: 0044 1925 831175
email: petermoreton@msn.com

The author wishes to acknowledge the contribution of Messrs John Strickland and Adrian Francis of BAE Systems, Land Systems (Munitions and Ordnance) Ltd who have primary responsibility for the safety of the process described in this paper

INTRODUCTION

Risk assessment has been the subject of much discussion in various forums during recent years. This has coincided with a move by the regulatory authorities in a number of countries towards the adoption of risk assessment as a means of assessing the safety of operations involving explosives. Indeed in some countries there is now a legal requirement for such assessments to be undertaken. In the European Union, for example, the Seveso II Directive requires that formal risk assessments be carried out at all installations holding more than specified threshold inventories of explosives materials. The aim of these assessments is to show that risks are adequately controlled and that all necessary measures have been taken to reduce them as low as reasonably practicable.

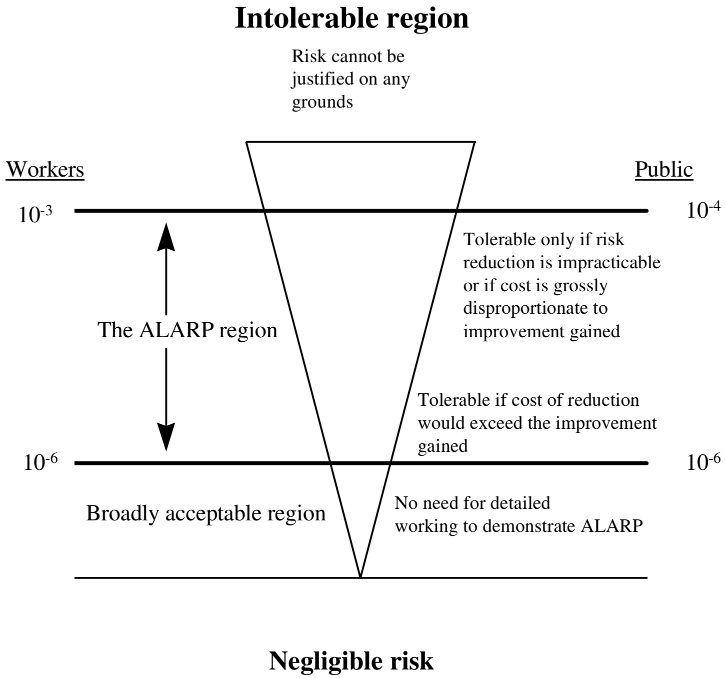
The term “as low as reasonably practicable” (ALARP) implies that absolute safety is not always achievable. Most importantly, the term suggests that a balance has to be struck between the cost of safety measures and the risk reduction achieved by those measures. Looked at another way, a risk assessment aims to provide an answer to that all important question of “how safe is safe enough?”

Hitherto, much effort has been devoted to developing procedures for quantifying risks, both to people who work with explosives and members of the public who live, work or travel nearby to installations where explosives are present. A number of computer programs, such as SAFER[1], have been developed to aide quantification of such risks. Quantified risks estimates may then be compared with tolerability criteria to determine whether any corrective action is needed. In this regard it has become common practice to place assessed risks into one of three bands, as shown in Figure 1 on the following page

.
Risks to specified individuals that are greater than a certain level are regarded as intolerable save perhaps in exceptional circumstances, such as wartime. In the UK this level is set at 1 in 1000 and 1 in 10,000 per annum for the chance of fatal injury to workers and members of the public respectively. At the other end of the scale, a risk of fatal injury of less than 1 in 1,000,000 per annum is deemed to be broadly acceptable. Between these two thresholds there is a grey area, where risks are only tolerable provided all necessary measures have been taken to reduce them as low as reasonably practicable –

this area is sometimes referred to as “tolerable if ALARP”. It is noteworthy that this three-band approach to evaluating risks for explosives operations was first proposed as far back as 1986 [2].

Figure 1: The Tolerability of Risk Framework



In practice, many explosives manufacturing plants are found to pose risks that fall within the middle band shown in Figure 1. In such cases regulatory authorities may require convincing arguments that all reasonably practicable risk-reduction measures have been taken. It is with this requirement in mind that the present paper has been written. The paper outlines a procedure for ensuring ALARP risk reduction for explosive manufacture by reference to one such operation: manufacture of TATB.

BRIEF DETAILS OF PROCESS

TATB (1,3,5-triamino-2,4,6-trinitrobenzene) is a highly stable explosive material that has a number of military applications. It is manufactured by BAE in a two-step process in which 1,3,5-trichlorobenzene (TCB) is first nitrated to produce an intermediate compound,1,3,5-trichloro-2,4,6-trinitrobenzene (TCTNB), which is then subsequently aminated to produce the final product.

The process makes use of concentrated acids, which are also powerful oxidizing agents, hot solvent, toxic organic compounds and gaseous ammonia. The process thus presents a number of hazards – acid-burn, fire and toxic – as well as a potential danger of explosion. Brief details of the process are as follows:

A quantity of 30% oleum is pumped to a glass-lined nitration vessel. Nitric acid (100% HNO_3) is slowly added with cooling, the temperature being maintained at 90° C. Once the acid has been mixed and is at the right temperature, the required quantity of molten TCB is added. The TCB reacts with the mixed acid exothermically to produce first the mono-nitrate and then the di-nitrate. This reaction proceeds adiabatically and the temperature within the nitration vessel increases to about 140º C. However, this is not sufficient to drive the trinitration reaction; so towards the end of the reaction period, steam is passed into the jacket surrounding the vessel to raise the temperature to the required value. The trinitration reaction is kinetically slow and the whole nitration process takes about four hours to complete. At the end of this period, the contents are cooled and diluted and the intermediate product filtered off. The spent acid is returned to the Acids Section of the plant for re-concentration.

At the beginning of the second stage of the process, the intermediate is first washed and then dissolved in toluene before being charged into the amination vessel. Additional quantities of toluene and water are added, and the vessel is then sealed and heated. Gaseous ammonia is introduced and the amination reaction proceeds at 152℃ and 5 bar pressure for 4 to 6 hours. When the reaction is complete the contents are cooled and then diluted with water before being discharged to the filter press. The TATB cake is steamed in the press, washed, partly dried with compressed air, and then blended and packaged. The toluene in the filtrate is recovered by distillation.

There is a potential for the following types of Major Accidents to occur in the production building:

Detonation of TCTNB or TATB
Thermal runaway in nitration vessel
Toluene fire in building
Spillage/escape of hazardous/toxic substances

There are many safeguards in place to help prevent such accidents arising, including inherently safe design features, procedural measures and engineered measures that are designed to reduce the likelihood of faults arising and automatically correct those that do occur. Steps have also been taken to reduce the potential consequences of accidents in the unlikely event that all the safeguards fail. All of these measures, taken together, form a hierarchical approach to safety. This is now discussed in the following section.

SAFETY PHILOSOPHY

BAE adopts a hierarchical approach to safety to ensure that the risks arising from its explosives manufacturing operations are as low as reasonably practicable. In this approach (1) inherently safe design is used as far as possible, backed up where necessary by (2) measures to reduce the likelihood of accidents occurring and finally by (3) measures to ameliorate the consequences of any accidents that do occur.

Inherently safe design

The principal inherently-safe design feature is the use of a synthetic route that does not involve the production of sensitive intermediate compounds or by-products, and for which the thermodynamics of the reactions are such that elaborate control measures are not required to keep the process within the design parameters – in a sense, the process “runs itself”. The intermediate compound, TCTNB, is completely insensitive when wet, and even in the dry state has a very high Figure of Insensitiveness (169). This intermediate is thus not inherently susceptible to accidental initiation.

The by-products produced in the reaction are also insensitive. Apart from the gaseous by-products[a] NO_X and SO_3, the only other compounds produced in the nitration are 1,3,5-trichloro-2,4-dinitrobenzene and 1,2,3,5- tetrachloro- 4,6-dinitrobenzene. Both of these compounds have a lower oxygen balance than TCTNB and do not in any way increase the sensitiveness of the intermediate product.

The above considerations are important as there are in fact a number of ways in which TATB can be manufactured, some of which do involve production of sensitive intermediates, such as 1,3,5-trihydroxy-2,4,6-trinitrobenzene (trinitro-phloro-glucinol), a compound that can be easily exploded by mechanical forces and heat when in a dry state. Indeed the sensitive nature of this compound was an essential cause of one fatal accident during manufacture of TATB elsewhere.

Measures to reduce the chance of accidents occurring

The insensitive nature of the intermediate and final products notwithstanding, BAE recognizes that the production process is still hazardous and accordingly takes appropriate measures to prevent accidents arising. These measures are based on long-established good practice (as enshrined, for example, in the MoD Explosives Regulations, Approved Codes of Practice issued by regulatory authorities, and internationally-recognized engineering design standards), as well as any additional safeguards as deemed necessary from structured analyses of the potential causes of accidents.

In general, potential causes of accidents and appropriate safeguards are identified at the design stage when the processes are subject to conventional HAZOP studies. However, with the advent of the Seveso II Directive, three further analyses have been carried out to provide further assurance that all reasonably practical safety measures have been taken. These analyses comprised: an Accident Review, a Human Factors study and a pseudo-HAZOP study. Each of these analyses is now described in turn.

---

[a] The quantities produced are small: the nitration vessel is kept under slight negative pressure from an air eductor and any NO_X or SO_3 evolved are scrubbed with a continuous flow of water in a packed column.

Accident Review

An assessment of the safety of any operation logically begins with a study of the causes of past accidents (if any) involving that operation. This is to ensure that the lessons learnt from those accidents have been assimilated in both the engineering design and the operating procedures for the plant. Details of past accidents involving relevant process, i.e. nitration, filtration and amination, were obtained from the EIDAS Database[3], the search parameters being set to look for reports that matched the following criteria:

1. The accident occurred during the last 50 years;

2. The details of the accident were reported by a competent authority, either in the UK or abroad;

3. The immediate cause of the accident was known or had been reduced to a small set of definite possibilities.

A large number of reports were found for nitration incidents, though only two of these referred to manufacture of TATB. An analysis of the details revealed many elements of commonality and suggested that the immediate causes could be grouped under five broad headings as follows:

Faulty equipment

Most of the accidents under this heading were directly due to the wearing and subsequent failure of items of plant equipment, such as cooling coils within nitration vessels. In one case a valve failed after a botched maintenance operation and in other cases failure was clearly the result of poor initial deign, e.g. use of rubber/plastic hoses with poor connections to metal plant.

Incorrect ingredients

A number of accidents were reported as having been directly due to this cause. In some cases insufficient nitric acid was added to the nitration vessel and this led to unstable conditions. In other cases contaminants were present in the reagents or the reactor vessels.

Operative Error

The term "operative error" implies that the operative failed to follow written instructions or did not exercise due care and attention when carrying out those instructions. In some cases – and this often a matter of subjective judgment – it might be argued that there were underlying causes leading to such failure, such as lack of competency, inadequate training and poor supervision.

Procedure in error

The term "procedure in error" implies that the procedure followed was inherently unsafe, though this might not have been reasonably foreseen before the occurrence of the accidents in question. Again, this is often a matter of subjective opinion, and in some cases it might be argued that problems would have been anticipated had a more detailed risk assessment been carried out prior to the inauguration of the process.

External events

This category includes all incidents that did not originate from faults with the process in question. The category includes such events as lightening strikes, vegetation fires and explosion elsewhere on site.

The details of each accident identified in the EIDAS search were examined under the appropriate heading to determine whether a similar accident could occur during production of TATB, what the consequences of such an accident would be, what existing safeguards are in place and whether any additional safeguards are required to ensure that risks are ALARP.

This process is illustrated by reference to the circumstances of one particular accident that resulted in the destruction of an RDX plant in the 1950s.

Location: UK, Bridgwater Date: 29/06/1951
The RDX plant was destroyed by explosion, resulting in the deaths of six workers. Debris was thrown out to a distance of about 400ft. Windows, ceilings and roofs were damaged in properties beyond the

factory confines, out to a distance of about 1.75 miles. There were, however, no casualties outside the factory.

While the Court of Inquiry came to no definite conclusion as to the exact cause of the explosion, it is most probable that the immediate cause was corrosion by nitric acid of the end of the shaft of one of the stirrers in one of the diluter vessels, resulting in the boss coming off and the blade impacting RDX crystals coated on to a cooling coil. Underlying this immediate cause were a number irregularities in that the plant was being run outside the original design specifications at the time of the accident

Table 1: Example worksheet from the Accident Review Study

Could a similar accident occur during production of TATB?

The nitration vessel in the TATB production building does not contain cooling coils and there are no areas in the vessel where TCTNB "ice" could form. But even if the stirrer in the vessel were to detach and impact solid TCTNB it is extremely unlikely that an explosion would occur, given that the F of I of dry TCTNB is 169 (i.e. relatively insensitive). Such a scenario is even less likely in the amination vessel – TATB is so insensitive that an F of I figure cannot be determined on a Rotter Impact Machine, though a value of >190 is normally quoted. TATB is insensitive in all other respects: F of F > 5.2; temperature of ignition is 360º C; fails to ignite by flash, but supports a train if ignited; no ignition at 4.5 J.

Consequences of a similar occurrence during production of TATB

Whilst a detached stirrer would be extremely unlikely to initiate a detonation, it is recognized that such an event would cause a loss of agitation in the nitration vessel and that this could possibly result in the formation of hot spots, which in turn could lead to an uncontrolled exotherm. This is particularly true at the start of the operation, when concentrated nitric acid (CAN) is mixed with oleum. In these circumstances, TCB could be added to the vessel without prior correct mixing of the acids. This potentially could lead to a vigorous reaction that could cause the lid of the nitrator vessel to lift. However, workers in the building would receive prior warning of such an event from the high-temperature alarm attached to the vessel. Failure to evacuate the building in these circumstances could result in fatal injury to any persons present.

Safeguards against a similar occurrence during production of TATB

The stirrer is constructed from steel and is glass coated. There are three blades on the stirrer, each of which is individually welded to the shaft and therefore simultaneous failure of all three blades is highly unlikely. The stirrer is tested before start-up as part of the calibration and interlock checks.

Before the stirrer could shear, some corrosion by acid would be necessary and this would be quickly detected as in this circumstance blow-over to the dilution vessel could not be achieved.

There is a rotation detector attached to the stirrer. The detector is attached to the nut that holds the stirrer in place, so mis-assembly of the stirrer would be quickly detected. This arrangement holds for nitrators and aminators.

There are two visual indicators to show that the stirrer is rotating.

In the event that the blades had detached from the stirrer, the operatives would be alerted by the noise from the vessel.

There is an interlock that cuts the feed of CNA in the event that the temperature in the vessel exceeds 90°C. There are three independent temperature probes linked to the interlocking system.

Are any further safety measures required?

It is suggested that consideration be given to implementing the following two measures further to ensure that risks are ALARP:

1. Install a temperature alarm set to 165°C linked to the evacuation alarm.
2. Include an instruction in the Manufacturing Instructions to evacuate building if the temperature exceeds 165°C.

Human Factors Study

The second exercise was designed to identify problems that might arise as a result of human error. Human error has in the past been a major cause of accidents in the explosives industry and thus it is clearly important that processes are made as “forgiving” as possible. An essential aim of the exercise was to establish the robustness of the process, and in particular whether sufficient automatic safeguards are present to prevent simple errors escalating to more serious events. To this end the Manufacturing Instructions were examined in detail and a number of “what if” type questions were asked in regard to each:

What if the operative failed to perform the instruction?
What if the operative performed only part of the instruction?
What if the operative performed the instruction erroneously?
What if the operative performed the instructions in the incorrect order?
What if the operative performed actions in addition to those given in the process instructions?
Are there any other ways in which a hazard could arise from actions of operatives?

This type of analysis is illustrated in the table below, which considers the potential causes and consequences of a failure to carry out an instruction pertaining to the early stages of the process, in which the operative requests the Acid Section to pump the requisite amount of CNA to the building. Consideration is also given to the adequacy of the safeguards in place to prevent errors arising during this operation.

Table 2: Example worksheet from the Human Factors Study
Instruction: Check the phone is operational and inform the Acid Section to commence pumping CNA.

GW	Causes	Consequences	Safeguards
Omit to carry out instruction	See Causes 1 – 5 below	Operation does not proceed if CNA is not available.	See general Human Factors Safeguards 1 – 8 below
Carry out only part of the instruction	See Causes 1 – 5 below	If less than the required amount of CNA is added to the nitration vessel, the reaction will not go to completion. This would result in a reduced yield but would not pose a danger.	See general Human Factors Safeguards 1 – 8 below

GW	**Causes**	**Consequences**	**Safeguards**
Carry out instruction erroneously	See Causes 1 – 5 below	The addition of weak nitric (instead of CNA) to the nitration vessel would lead to a rapid temperature rise and the subsequent shutting of the CNA inlet valve by the interlocking system. A failure of the interlocking system could lead to a violent reaction and release of acid fume to the scrubber	See general Human Factors Safeguards 1 – 8 below The specific gravity of the CNA is checked at the Acid Section before dispatch to the TATB production builsing.

In general there are a number of potential causes of human error, including:

1. Negligence
2. Complacency
3. Time saving
4. Lack of supervision
5. Low level of competence
6. Malicious action

The safeguards in place to prevent such error, so far as is reasonably practicable, are:

1 Recruitment policy: All employees and contractors are vetted against counter terrorist procedures to the UK Ministry of Defence standard.

2 Induction Training: All new employees undergo induction training, which covers the dangers of the materials handled on site, manual handling operations, use of personal protective equipment and emergency procedures, including use of safe havens and muster points.

3 On-the-job Training: New recruits would not be sent to work immediately in the TATB Production Building, but rather would first acquire experience in packing-and-filling-type operations. Only after having demonstrated a suitable aptitude would personnel then undergo training in the use of more advanced processing equipment, such as nitrators and aminators. Personnel would need to complete a minimum six-month probationary period and then undergo special appraisal before being selected to work in the production building. New members of the team would start as panel operatives under the direct supervision of experienced staff. The new members would then have to demonstrate competency, which would require that they pass a written test as well as satisfy supervisory staff, before becoming full members of the team.

Members of staff tasked with training new operatives must also have successfully completed a validation process, which is also assessed by written examination. This particular measure was implemented following a gap analysis to identify further safety measures that might reasonably be undertaken – it is seen as a further measure in reducing risks as low as reasonably practicable. The validation process is overseen by an external organization. Trained operatives are re-validated at set periods. BAE also run in-house Explosives Safety Courses for supervisors and front-line managers.

4 Manufacturing Instructions: It is recognized that the provision of clear, concise and accurate Manufacturing Instructions is an important measure in reducing the likelihood of human error. The Manufacturing Instructions for the building cover all aspects of its operation, including normal running and emergency procedures. The actions to be taken in the event of specific faults arising are clearly described, including power failure, mechanical failure of stirrers and pumps, failure of air supply, spillages of hazardous substances, fire in the building and approaching thunderstorms. The requirements for personal protective equipment (PPE) – i.e. type, location and circumstances under which to be worn – are also clearly described, as are the requirements for recording and logging process parameters.

There is a separate Use List for the building, which specifies the standard items, furniture, tools, cleaning materials and environmental sampling kits that are allowed to be present in the building.

There is a set of batch sheets and a run sheet associated with the Manufacturing Instructions and these are completed every time the process is run. The batch sheets record process parameters, such as feed rates, temperatures, pressures, etc., and any changes made to these parameters. These sheets thus provide documentary evidence that the process has been completed within the design parameters. The run sheet requires signature by operatives at various points in the operation to verify that tasks have been completed. There is also a run board that is completed in a similar manner to the run sheet; this functions as a double checklist.

All of these documents are controlled and have been produced in compliance with the quality standards ISO 9000/2000 and ISO 14001 for environmental management.

A building logbook is also maintained. This records the times and amounts of reactants added to vessels, any unusual occurrences, any faults requiring maintenance, etc. The logbook and the run board help ensure process history information is communicated between shifts.

5 Supervision: A named building leader would have charge of the building under the supervision of the shift leader. The shift leader reports directly to the Production Manager. The Product Manager is the building owner and holds the budget for the building and is responsible for the batch sheets, without which the process cannot run. The Product Manager reports to the Production Manager who in turn reports to the Site Manager. The two-person rule is in force in the building for the most hazardous phases of the operation, i.e. no lone working, during oleum handling, running of the nitration operation (until reaction nears completion), start of the amination operation.

6 Safety Culture: The company has a well-documented Safety Management System, which is subject to review in line with changing legislation and business requirements. The control of the safety manual rests with the Head of Quality, Assurance, Security and Safety, Health and Environment (SHE) for the company.

Safety culture includes the following facets: (1) a bias towards a "non-blame culture" – operatives are encouraged to report errors/mistakes (e.g. addition of wrong material or incorrect amount of material) to management, and can easily contact Product Managers, Team Leaders and Shift Leaders by two-way radio; (2) the production operatives can refuse to work in the building if they consider it to be unsafe and indeed have the authority to shut down the process; (3) operatives are not put under time pressure – there are no time penalties and no fixed breaks, all breaks being staggered; (4) all unusual occurrences are investigated and reported; (5) there is a SHE committee that meets on a regular basis and this committee ensures that any lessons learnt from unusual occurrences are acted on.

To reinforce safety culture, all employees have been issued with an Employee Safety, Health and Environment Guide. This action was taken following a gap analysis by the company to identify further safety measures that might reasonably be undertaken – it is seen as a further measure in reducing risks as low as reasonably practicable.

7 Health surveillance: Operatives undergo medicals in compliance with the UK Control of Substances Hazardous to Health Regulations. This helps to guard against errors that might arise from mental health problems, e.g. depression.

8 Site security: A company specializing in security is contracted to provide a manned guarding service to the site. The on-site team has responsibility for: (1) Access Control of site staff, visitors and deliveries; (2) patrolling the site with regard to designated buildings, document storage and perimeter fences; (3) response to alarm activation of designated buildings; (4) Control Room duties, to include monitoring of the alarm system and implementation of site procedures with regard to summoning external assistance. It is considered that these measures provide an appropriate level of defence against malicious action.

A principle aim of the Human Factors Study was to verify that there are sufficient engineered safeguards in place to prevent simple errors by operatives escalating to Major Accidents. This was indeed found to be the case. However, it should be stressed that the interlocking systems, etc., are very much regarded as backup lines of defence and that the competence of the operatives should be such that these backup systems are very rarely, if at all, called on to perform.

The reliability of the interlocking systems is maintained through a programme of periodic inspection and testing. Appropriate inspection and testing intervals can be established by carrying out a Safety Integrity Level (SIL) Analysis of the process instrumentation and control systems. A description of SIL analysis is beyond the scope of the present paper, but guidance on the procedure has been published elsewhere[4].

Pseudo HAZOP

While the Accident Review gave assurance that the lessons learnt from past accidents are adequately reflected in the engineering design and the Manufacturing Instructions for the process, it did not in itself provide a guarantee that the process is sufficiently safe. This is because the approach is “retrospective” rather than “proactive”. A proactive approach is required to identify all theoretical potential causes of accidents, including those that have not materialized in practice. To this end a pseudo HAZOP study was performed in which the parameters consisted of the various types of energetic stimuli (impact, friction, heat, static discharge, etc.) capable of initiating explosives material. An example worksheet generated in this type of analysis is shown in the following table, which considers the potential consequences and safeguards against static discharges.

Table 3: Example worksheet from the Pseudo-HAZOP Study

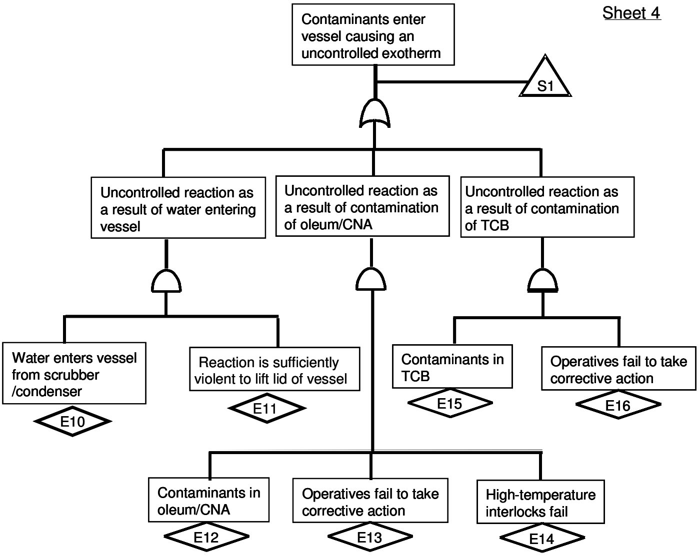
GW	Causes	Consequences	Safeguards	Comments
Static discharge	Static charge on persons or objects	Potential fire and smoke hazard. Main concern is that a static discharge could ignite a toluene spill, i.e. potential for toluene vapour to be ignited if static discharge occurred at same time as toluene leak. Possibility of fire spreading to toluene or TCTNB/TATB	Equipment is grounded and bonded to standards specified in the MoD Explosives Regulations. Earthing is checked on a regular basis Toluene is run through stainless steel pipes to avoid possibility of static build up. Toluene storage vessels are external to building and there are flame arrestors to prevent fire spreading to process. Toluene is sucked into the aminator from the dissolver by vacuum to eliminate	Electrical pre-startup checks are specified in the Maintenance Plan for the building As a further precaution, consider earthing toluene drums during discharge to toluene storage vessel.

GW	Causes	Consequences	Safeguards	Comments
			oxygen. Contents of aminator are blown to the press by nitrogen Wet TCTNB/TATB is not sensitive to initiation by static discharges, so first degree precautions are appropriate. All process equipment, with the exception of the sample trays and poly trucks are enclosed. Aminator vessels are completely sealed. Floor is usually damp	

RESULTS OF THE ACCIDENT REVIEW, HUMAN FACTORS AND PSEUDO-HAZOP STUDIES

The information gathered from the above studies allowed a set of fault trees to be drawn to illustrate graphically the various potential accident initiators and the associated safeguards that would have to fail for accidents to materialize in practice. An example fault tree is shown in Figure 2, which considers the potential fault sequences leading to an uncontrolled exothermic reaction in the nitration vessel as a result of contaminants entering the process.

Figure 2: Potential routes leading to an uncontrolled exothermic reaction in the nitration vessel resulting from contamination



The tree shows that are a number of potential routes leading to this type of accident. The following cut set shows one such route resulting from the presence of contaminants in the oleum or CNA.

E12: Contaminants in oleum/CNA
E13: Operatives fail to take corrective action
E14: High-temperature interlock fails

The ALARP demonstration requires that each cut set is considered in detail to determine whether further measures are necessary to reduce the identified risk.

E12: Contaminants in raw ingredients

Contaminants could be present in the raw materials as a result of errors made by either the suppliers or personnel on site. In the present case there have been no such problems from either source, but the danger from the former is exemplified by an accident that occurred some years ago during the manufacture of RDX on site. In this case the supplier of hexamine (one of the raw ingredients used in the process) had added powdered aluminium to the material so as to improve its flow quality. The aluminium reacted with the CNA to cause a small fire in both the nitration vessel and the hexamine feed line, though this was quickly extinguished and no damage was done.

Current safeguards

The safeguards against this identified fault are as follows:

- The CNA is manufactured on site and is supplied directly from the Acids Section to the production building, the specific gravity of the CNA being checked at the Acid Section before dispatch.

- Oleum is bought in with a certificate of conformance and is stored in UN approved drums. These drums are unique to oleum on the site, a fact that reduces the chance that oleum could be confused with other types of material stored on site.

- The cleaning and inspection procedure that is followed at the start of each campaign should ensure that no foreign objects are present in process equipment.

- The operatives are required to report anything that seems unusual in the appearance of reagents particularly as a change in appearance or consistency might indicate contamination.

E13: Operatives fail to take corrective action

The oleum is subject to inspection by the operatives before use and it is likely, though not absolutely certain, that the presence of contaminants would be picked up at this stage. The CNA, however, is fed directly to the process from the Acids Section. Were the CNA or oleum to be off-specification in a dangerous way, the problem would become immediately apparent on the opening of the valve on the CNA line. In this case excess gas/fume would be heard/seen to be vented to the scrubber and in such circumstances it could be expected that the operatives would immediately shut off the feed of CNA. Corrective action might not be taken for one of two reasons: (1) failure of the temperature monitoring system and (2) human error.

Redundancy provides the main safeguard against problems arising from instrument failure: there are three independent temperature probes linked to the interlocking system.

The main safeguards against human error are recruitment policy, training, written Manufacturing Instructions, the requirement to complete tick sheets and record process parameters as the operation proceeds, supervision and experience – see section on Human Factors study.

E14: High-temperature interlock fails

A violent reaction would produce a rapid temperature rise inside the vessel, and once the temperature reached 90º C the high-temperature interlock would automatically close the valve on the CNA line. There is a chance that the interlocking system could fail to work on demand, though it is difficult to quantify a precise failure probability. In general it is recognized that a reliability of about 99.9% is the most that can be achieved for such systems.

In order to determine whether additional safeguards are needed on the ALARP principle, it is first necessary to estimate the likelihood of the identified fault sequence arising. In practice very real difficulties are encountered in quantifying accident probabilities; in many cases such quantification necessarily has to relay on engineering judgement rather than empirical data. Accordingly, the authors believe that in assessing accident likelihood a semi-quantitative scheme is more appropriate than fully quantified estimates – which may covey a spurious level of accuracy. The scheme used in the present study is summarized in the table below.

Table 4: Semi-quantitative terms to express accident likelihood

Likelihood	Definition	Approximate frequency band (per year)
Likely	Likely to occur a number of times in a year	$F > 1$
Occasional	Could occur in plant lifetime	$1 > F > 10^{-2}$
Unlikely	Unlikely to occur	$10^{-2} > F > 10^{-4}$
Remote	High unlikely, but may exceptionally occur	$10^{-4} > F > 10^{-6}$
Incredible	Extremely unlikely that the event will ever occur	$F < 10^{-6}$

In the present case, the likelihood of the identified faults arising were assessed as follows:

E12: Contaminants in raw ingredients

There is no experience of the identified fault with the process under consideration. Operating experience accumulated to date would suggest that the chance is no greater than “occasional”, i.e. perhaps as low as 10^{-2} per year.

E13: Operatives fail to take corrective action

While there is a chance that the operatives could fail to take corrective action, the chance of this event is difficult to quantify precisely. Much would depend on the experience of the operatives, and given that this process is operated by long serving personnel the chance of failure is judged to be no greater than “occasional”.

E14: High-temperature interlock fails

As previously noted, it is difficult to quantify precise failure probabilities for interlocking systems, though it is generally recognized that a reliability of about 99.9% is the most that can be achieved for such systems. In the present case the failure probability is judged to be of the order $10^{-2} – 10^{-3}$

The overall chance of the fault sequence arising is thus considered to be “remote”, i.e. perhaps as low as 10^{-6} per annum.

There is one further line of defence that would protect the production personnel should the accident occur, and that is emergency evacuation. The chance of such an evacuation being successfully conducted has been enhanced by the fitting of an evacuation alarm linked to a high temperature sensor set to 165ºC. There is still a chance that this important last line of defence could fail, but this is considered to be no greater than “occasional”. The frequency of the identified fault sequence leading to fatal injury is thus assessed to be sufficiently low as to make the risk “broadly acceptable”, and accordingly no further risk reduction measures are proposed in regard to this potential fault sequence.

MEASURES TO AMELIORATE THE CONSEQUENCES OF ACCIDENTS

In the event that all safeguards failed, there are measures in place that would ameliorate the consequences of any Major Accident. These measures include:

- Large distances to the nearest public amenities and inhabited buildings off site (much in excess of those specified by the regulatory authority), which would in practice offer the public complete immunity against the lethal effects of any Major Accidents that might occur in the building

- Compliance with the regulatory authority’s internal quantity-distance prescriptions, which would offer a high level of protection to workers in adjacent process buildings on the site

- Evacuation procedures, which would offer an important last line of defence for the operatives working in the building

- On-site and off-site emergency plans

CONCLUSIONS

This paper has outlined a procedure for ensuring that the risks involved in manufacturing explosives are as low as reasonably practicable. The procedure is based on a hierarchical approach to safety in which processes are made as inherently safe as possible, backed up by measures to reduce the likelihood of accidents occurring and further measures to ameliorate the consequences of any that do occur.

The procedure requires that careful consideration is given to the potential causes of accidents, and this is done by conducting accident reviews, human factors studies and HAZOP-type exercises. The success of these exercises requires ready access to information on past explosives accidents and input from personnel covering a very wide range of disciplines, including, just to name a few: explosives chemistry, explosion effects, chemical engineering and process instrumentation and control. The procedure is labour-intensive, requires input from experts in a number of disciplines, and, it has to be stated, is commensurately costly. Nonetheless, BAE has undertaken this procedure through a commitment to achieving a high level of protection for people and the environment from all potential sources of Major Accidents, and moreover to ensuring that the risks of these accidents are not intolerable and have been reduced as low as reasonably practicable.

REFERENCES

1 Hardwick M and Pfitzer T, *Safety Assessment for Explosives Risk (SAFER) Model Status*, Minutes of the Thirty-first Explosives Safety Seminar, San Antonio, Texas, US Department of Defense Explosives Safety Board, 2004.

2 Clifton J J, Edmondson J N, Hartley F R, Moreton P A, *Application of risk assessment in the field of explosives and ammunition safety*, Minutes of the Twenty-second Explosives Safety Seminar, Anaheim, California, US Department of Defense Explosives Safety Board, 1986.

3 Moreton P A, Lang G L and Sexstone P A, *The Explosives Incidents Database Advisory Service (EIDAS)*, Minutes of the Twenty-seventh Explosives Safety Seminar, Las Vegas, Nevada, US Department of Defense Explosives Safety Board, 1996.

4 Gulland, W G, *Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons*, Safety-critical Systems Symposium 2004, Meriden, Warwickshire, The Safety Systems Club, 2004.

About SAFEX International

SAFEX International is a global organisation with the fundamental objective of improving the safety of operations and their impact on people and the environment. Operations cover the development, manufacture, storage, and transport of commercial explosives, military explosives and pyrotechnic products throughout the world. The term “explosives” includes initiating devices, propellants, industrial and military powders as well as the raw and intermediate materials associated with the explosives industry.

Current membership of **SAFEX** is over 100 companies from all the continents in the world and operating in more than 40 different countries.

SAFEX is a non-profit making association of manufacturers of explosives and was founded in 1954 with the aim of exchanging experiences within the explosives industry. The way **SAFEX** works is to exchange safety, health and environmental (SHE) information about major accidents, serious incidents, and near-misses. The objective is to avoid other manufacturers experiencing the same or similar events. In this way **SAFEX** contributes to improving the health and safety of operators within the explosives business as well as the well-being and standing of the explosives industry. As a voluntary organisation, **SAFEX** is not organised for the pecuniary gain of any of its members.