B1

# An Integrated Approach to Plant Safety and Operability Assessment

D I Hambley

May 1993

AEA Technology
Reactor Services

# An Integrated Approach to Plant Safety and Operability Assessment

by

**D I Hambley**

## Summary

This paper describes the methods used within the Active Handling Department of AEA Technology to identify potential hazards posed by operations carried out in the buildings for which the AHD is responsible and to evaluate the individual risk to which critical groups are exposed. The methodology used enables the identification of plant improvements which lead to increased efficiency of operations, thus offsetting the costs of carrying out the hazard identification process.

To be presented at a meeting of the Commission of European Communities Working Group 'Hot Laboratories and Remote Handling' at Chinon, France 15/16 June 1993.

AEA Technology
Windscale
Sellafield
Seascale
Cumbria
CA20 1PF
United Kingdom

May 1993

# Contents

# 1.0 Introduction

All commercial nuclear plant within the UK must, by law, demonstrate to the Nuclear Installations Inspectorate that the operations carried out within the plant are adequately safe. The basis for satisfying this requirement is the submission of a Safety Case which includes:

- A description of the plant, operations and important safety systems.
- A description of previous operations within the facility.
- A description of the management system under normal and emergency conditions.
- A review of recent operating experience, including radiation dose uptake by operators, radioactive discharges and the state of plant and equipment.
- An assessment of the risks posed by operations within the facility.
- An assessment of the decommissioning policy for the facility.
- A review of the adequacy of the plant by comparison with current design standards.

In addition to the requirement to justify the safety of the plant there is a separate requirement to justify the safety of all modifications to the plant or equipment. The extent of these justifications depends on the potential hazard which may be generated by the modification. For a modification which may give rise to a significant hazard on or off the site all the above points would have to be addressed in the safety justification.

This paper describes the system used within the Active Handling Department of AEA Technology to identify and quantify the risks posed by operations carried out in the Windscale Active Handling Facilities. The system employed also ensures that items which are identified as requiring remedial action during the risk assessment process are tracked through to completion. The items which are identified as requiring remedial action may be safety related issues or issues which relate to the efficiency of plant operations. Resolution of the latter issues can bring about savings which more than pay for the expense of carrying out the risk assessment process.

# 2.0 Hazard Identification

The method used for the identification of hazards associated with operations in the Windscale Active Handling Facilities is Hazard and Operability studies, more commonly known as HAZOP. This methodology was developed in the chemical industry where it is now widely used and acknowledged as a major

contributor to the improved safety of modern chemical plant.

## 2.1 HAZOP TEAMS

HAZOP is a team base technique which provides a systematic method of analysing operations to determine the ways in which faults and failures may occur and the consequences of such failures. This systematic approach and the comprehensive recording procedure used within the department, provides a valuable demonstration of the completeness of the study.

The quality of the team is the major factor affecting the quality of the HAZOP process. All team members must be knowledgable about the area of plant or operations which they are representing. For operations and engineering representatives in particular it is important that they have a working knowledge of the practices on plant in addition to an understanding of the principles of operation.

The HAZOP team normally consists of four to six people, led by a team leader, who is normally independent of the design team, for a modification, or of the plant management, for plant Safety Case assessments. The core of the HAZOP team consists of the team leader, the HAZOP secretary, a representative of the operations department and a representative of the engineering/maintenance department. Other representatives would be called on to assist when additional expertise was required, eg:

- Health Physicist
- Design Engineer
- Instrument/Control Engineer
- Scientific staff responsible for new equipment

## 2.2 RISK ASSESSMENT

The other main ingredient of the HAZOP process is the information required for the study. The specification of the correct level of detail is one of the HAZOP team leader's most important tasks, since if there is insufficient detail the HAZOP process will be held up whilst the relevant information is found or, more seriously, the HAZOP will be superficial. If too much detail is provided the HAZOP can become bogged down in the detail and the exercise will be extremely costly and time consuming.

Typically each section of plant or operation is considered individually based around either a Piping and Instrumentation [P&I] diagram, for process plant, or a flow-sheet and general arrangement drawing, for operations. Supporting information could include details of flows, materials, compositions, working instructions, detailed designs or photographs of plant and equipment.

## 2.3 HAZOP ASSESSMENT

The HAZOP study is carried out by the systematic consideration of all the important stages of an operation, or sections of a process plant. For each stage of an operation or section of plant the team considers:

- The possible ways in which a change in the operation could occur. These are referred to as *deviations*. The HAZOP method uses a set of guide words to assist the team to think about what sort of events could occur.

- How these *deviations* could occur by identifying the initiating events, referred to as *causes*.

- What would happen if the *deviation* occurred, referred to as *consequences*.

- What physical or managerial control are in place either to prevent the *deviation* or to mitigate the *consequences*. These are referred to as *safeguards*.

When the team identifies a *deviation* which could lead to a hazardous *consequence*, even where protective measures exist, this is recorded as an initiating event. Normally the *consequence* is underlined to signify a hazard and a reference number given according to the type of hazard.

When the team identifies a *deviation* which could lead to a loss of production or damage to the product it is identified as an operability problem and a reference is given to it. The team normally also identify features of the design which may lead to problems during operation, eg inaccessible valves, poorly designed control panel layouts or alarm signals. These are again referred to as operability problems and are identified separately in the HAZOP records or remedial action is identified and actions are placed on the appropriate representative.

An example of the results of a HAZOP study on a design scheme for a shielded transfer system [Figure 1] is given in Table 1. An example flow-sheet for the study is given in Figure 2. The main features are:

- A description of the operation is given.

- The step of the operation under immediate consideration is given. In this case the transfer tray is normally stored inside the shielded enclosure, therefore the first step is to open the inner shield door so that the tray can be moved into the cave.

- The first guide word, or *deviation*, is applied to the step under consideration. The 'No/Not' guide word is applied to the step 'open the inner shield door'. The meeting considered that possible *causes*

for a failure of the door to open could be that the operator forgets to open the door, that one of the interlocks fails or that the power supply to the door drive units fails.

- The meeting concludes that there would be no hazard and that the only *consequence* would be a delay.

- The notes column is used to give details relevant to a particular step or equipment, give details of actions and note hazard types.

- Actions are given a reference number according to the meeting at which they were issued, details of the action are given in the notes column.

- Reviews of progress in completing actions are held periodically, for large HAZOP studies, during and at the end of the HAZOP process. Any relevant comments are added when the action is complete.

- Hazards are indicated by underlining and a hazard reference number is given in the margin.

- Action used to suggest remedial action for operability problem

### 2.4 RECORDS AND CONTROLS

On completion of the study the team leader and secretary produce a HAZOP report which contains two main sections, one summarising the results of the study and one containing the full records of the meetings, see Table 2. The full HAZOP report provides a complete record of the study including all the deviations considered and the meeting's decisions regarding potential consequences, including those which the meeting concluded were not credible.

The summary lists generated by the HAZOP process are the main output from the process. The list of hazards is forwarded for risk assessment, the list of outstanding actions, instruction changes and plant changes are placed on an action list. The action list is then incorporated into the safety justification documents which are formally reviewed by an appropriate safety committee and where necessary by the NII. The subject of ensuring completion is discussed further in Section 4.

## 3.0 Risk Assessment

The risk assessment procedure used within the Active Handling Department is based on HAzard ANalysis [HAZAN] techniques used elsewhere in the chemical and nuclear industries and the resulting assessments are often referred to as HAZANs.

## 3.1 BOUNDING SCENARIOS

The risk assessment process begins with the identification of bounding accident scenarios, based on the list of initiating events and the types of hazard derived from the HAZOP study. The use of bounding accident scenarios enables the number of individual accident scenarios to be reduced to a minimum whilst ensuring that the assessment is not optimistic. A bounding scenario for a set of fault sequences must be at least as hazardous as the most hazardous fault sequence, but must still be a credible and reasonable representation of the majority of the scenarios. Correct definition of a bounding scenario is of great importance since if the scenario is too pessimistic it may lead to the implementation of unnecessary counter measures, whilst if it is too restrictive then a much greater number of scenarios must be considered and the cost and complexity of the assessment is increased.

In some cases it is advisable to carry out an initial analysis using the minimum number of bounding scenarios, which are known to be pessimistic, since this permits early identification of the scenarios which present the greatest hazard. Thereafter the most hazardous scenarios may be split into a number of bounding scenarios for more detailed analysis. This approach ensures that effort is concentrated on those accident scenarios which present the greatest risk.

As part of the Safety Case for each plant the normal and worst case feed materials are identified. For fuel, the normal feed material in the Active Handling Department, this would be defined in terms of reactor system, irradiation conditions and cooling time. Using the worst case data, calculations are carried out to identify the radioactive composition of each type of material which can be handled in the facility. These compositions are then used as source terms for the accident scenarios. This procedure provides a measure of pessimism within the risk assessments. Different fuel compositions may be used in assessments where there is a sound case for reducing the degree of pessimism, eg examination of long stored fuel. Equally, specific cases may be made to temporarily extend the scope of the Safety Case to receive a particular fuel element with a shorter than normal cooling time.

## 3.2 HAZARD ASSESSMENT

Having identified the bounding accident scenario the hazard assessment is carried out to determine the direct and inhalation radiation dose uptakes to the operator, to an 'average' member of the work-force on the site and to a member of the public at the nearest point to the event which he/she could normally be expected to be. This is usually taken to be the nearest part of the Site boundary fence.

Direct radiation from a source is normally calculated using a computer code running on a PC which can take account of source geometry and

two-dimensional intermediate shielding.

Dose received from activity released to the environment is calculated based on the quantity of material present and the fraction which may be released. Appropriate allowance is made for any mitigation given by containment, filtration or dispersal.

## 3.3 FREQUENCY ASSESSMENT

The second part of the assessment requires an estimation of the frequency with which the initiating event, or events, may occur. This assessment requires that all the initiating events identified in the HAZOP study are addressed. The frequency of the events are modelled using fault trees and where appropriate event trees. The safeguards identified during the HAZOP study are included in the failure model, along with any potential operator actions or errors.

Human errors are normally estimated using a simple system which takes account of the type or error, the amount of time available for carrying out the task and the degree of independence between human errors within any given fault tree. Where necessary more detailed analysis, such as task analysis, is carried out.

## 3.4 RISK ASSESSMENT AND SENSITIVITY

Having obtained estimates of the potential hazard and the fault frequency the individual risk for the three critical groups are calculated using the dose conversion criteria recommended by the UK National Radiological Protection Board. These are in turn based on recommendations of the International Committee on Radiation Protection.

If the risk posed by the operations is less than the relevant criterion for a single event, an assessment is made of the sensitivity of the assessed risks to individual equipment failures or human errors. The sensitivity analysis modifies the failure frequency or probability in turn and re-calculates the resulting event frequency. If the resulting frequency would lead to a risk which is within 10% of a relevant risk criterion then the item or action is identified as critical. For each of these items additional measures are taken to minimise the probability of failure and ensure where possible that alternative safeguards are available in the event of a failure.

The individual risk estimates for each critical group for each bounding scenario are added together for comparison with corporately defined risk criteria, which have been agreed with the Nuclear Installations Inspectorate, to determine whether or not the operations are adequately safe.

All the data used in these assessments are referenced either to risk assessment databases, reports or to sequentially numbered information requests which form part of the plant records. Reference may also be

made to written instructions or drawings. In some cases the assessor may require specific actions or equipment to be provided to ensure the safety of an operation. These are forwarded to the project manager in writing by the assessor and added to the list of actions remaining from the HAZOP report.

## 4.0 Ensuring Completion

The hazard identification and risk assessment process should demonstrate that the facility can be operated adequately safely or that any proposed modification is adequately safe. Where this is not the case the assessments should identify modifications to plant or operations which will enable an adequate level of safety to be achieved. However there will normally be some outstanding issues requiring resolution when these analyses are completed and in many cases the accuracy of the assessment process relies on the completion of these items. Therefore the management of the risk assessment process must address this issue.

For a plant Safety Case any outstanding issues, from either the HAZOP or HAZAN, are included in the Action Plan for the facility which ensures that all issues raised during consideration of the Safety Case within AEA Technology or by the NII are addressed and adequately resolved.

For modifications the list of outstanding issues from the HAZOP and HAZAN stages consist of written actions which are listed in tables within the HAZOP report, or by the project manager in the case of HAZAN changes. The list of outstanding actions from both parts of the risk analysis process are combined and presented as part of the safety justification document which is submitted to the appropriate safety committee for review. For major modifications several submissions are required at different stages of the modification, eg prior to the start of construction, following construction and prior to commissioning, etc. In subsequent submissions a summary of the resolved items is given and the remaining items are listed as unresolved. It is normal that as part of the commissioning schedule, items are included to ensure that recommendations from both phases are required. In the event that they are not completed a detailed justification for operation with these items outstanding must be given in the final safety submission.

## 5.0 Operability

Although the majority of this presentation has concentrated on the identification of hazards and the assessment of risks, the second and equally important output from the HAZOP process is a list of operability problems identified during detailed examination of the operations and plant and the actions placed to resolve operability problems.

Completion of actions relating to operability issues is the responsibility of

the plant or department manager and these will normally be addressed during the design phase. However in the event of some issues remaining outstanding upon completion of the design the list of outstanding operability problems identified is provided to the manager in the HAZOP report. Resolution of operability problems raised during the HAZOP process will provide material benefits for the time invested in carrying out the HAZOP.

**Table 1**

**Example HAZOP Record Sheet**

| Line/Vessel or Step & Function | Guide word/ Deviation | Cause | Consequence | Indications/Safeguards | Action | Notes |
|---|---|---|---|---|---|---|
| OPERATION OF TRANSFER TRAY SYSTEM:<br>To transfer items on a tray out of cave system for maintenance *(a)* | | | | | | |
| 1. Open inner shield door *(b)* | No/Not *(c)* | Operator error, interlock failure, outer door failure, power failure *(c)* | Delays in movement *(d)* | | | Interlock between tray drive and inner door fully open position to prevent tray being driven into partially opened door. *(e)* |
| | More (Travel) | Limit switch failure | Door halted by ultimate stop | Physical stops | Action 1.1 *(f)* | Ensure that stops are included on detailed design<br>R2: complete *(g)* |
| | (Contam.) | Contamination on shield door is drawn into cave workshop as door is opened | Increased potential for particulate spreading into the workshop *(h)* | Routine monitoring, ventilation, beta-in-air monitor | | **B2.1** *(h)* |
| | (Radiation) | No rebate when doors moving | Potential dose uptake (direct radiation) to operator standing near door, to the side of the enclosure | Door operating controls sites well away on other side of transfer enclosure | | **B2.2** |
| | Less | Doors fails to open completely | Operability problem - delays | Tray cannot be opened until door is fully opened | Action 1.2<br><br>Action 1.3 | Ensure interlock operates when door is fully opened<br>R2: complete<br>Consider installation of window to allow operator to see into enclosure *(i)* |
| | As Well As | Operator tries to drive tray out too soon and interlock fails | Potential to damage item on tray or tray drive | Interlock | | |
| | | Operator opens outer door | Potential dose uptake (direct) by operator | Interlock prevents outer door opening if inner door is not fully closed<br>Door control located on side of transfer enclosure | | **B2.2** |
| | All other Guide words | No further problems/hazards | | | | |
| **Date:** 11 / 04 / 93 | **Project:** Example | | **Drawing Operation:** Transfer system (Flow-sheet 1.1, Drawing 0X34151 P1) | | **Meeting:** 1 | **Page:** 1 **of** 1 |

**Note:** Letters in italics, eg *(a)*, are cross references to sections of the text describing the HAZOP record sheet in Section 2.3.

## Table 2

## Contents of a HAZOP Report

| Section | Contents |
|---|---|
| | Summary Report |
| 1.1 | Scope of study |
| 1.2 | Summary of HAZOP study results |
| 2.1 | List of operations/plant sections studied |
| 2.2 | List of hazards, according to the type of hazard |
| 2.3 | List of operability problems identified |
| 2.4 | List of events which may affect other plants |
| 2.5 | List of plant changes requested, listed as completed or not completed. |
| 2.6 | List of instruction changes identified, according to whether they are completed or not. |
| 2.7 | List of actions placed at the meetings, according to whether they are completed or not. |
| | Supporting Information |
| 3.1 | Flow-sheets/P&I diagrams describing the operations/plant studied in the meetings, along with the corresponding meeting number. |
| 3.2 | Register of who attended which meeting and the main operations studies at the meeting. |
| 4.1 | Records of the meetings, interleaved with completed actions. |
| 5.1 | Copies of instructions studies |
| 5.2 | Copies of other supporting information |

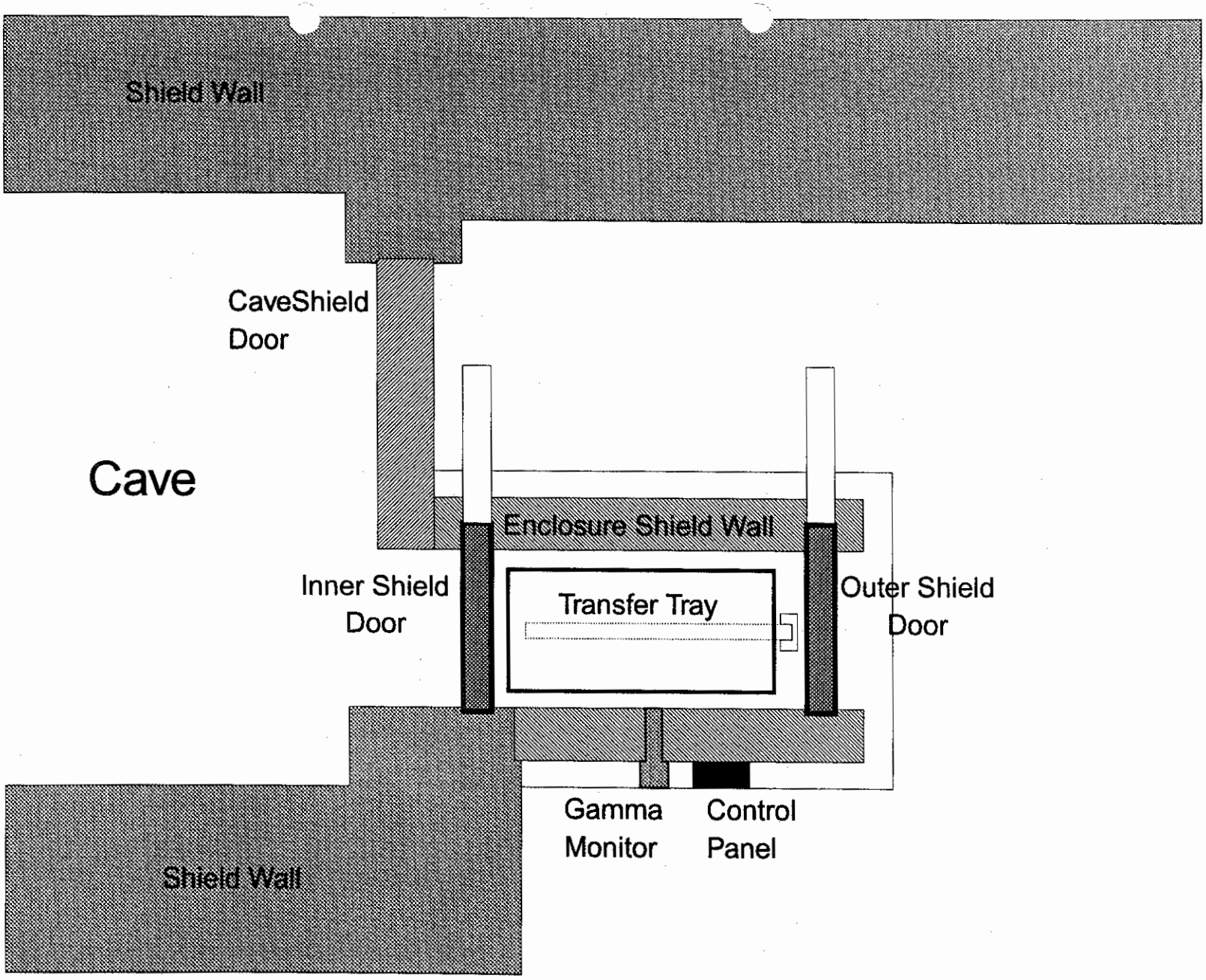
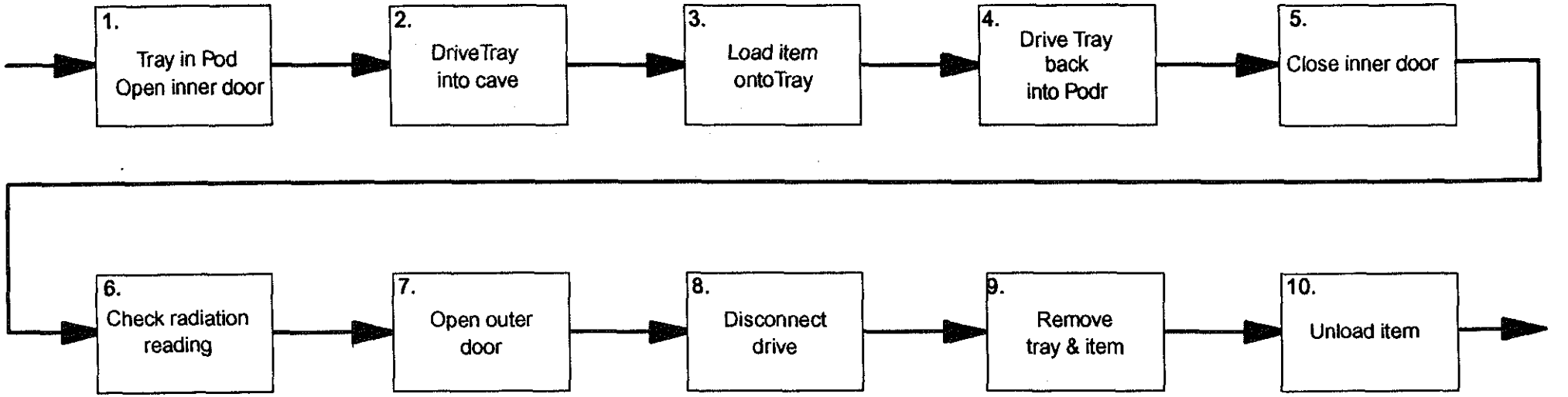



Figure 1 Example Transfer System

| PROJECT: Example | FLOWSHEET: Ex 1 | SHEET 1 OF 1 |
|---|---|---|
| OPERATION: Transfer system Operation | Drawings Ex 1 and Ex 2 | SIGNED |




| Step | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|
| Equipment & personnel | Tray, outer door, inner door<br>Drive mechanism<br><br>Process worker | Tray, inner door,<br>Drive mechanism<br><br>Process Worker | Tray, Crane, MSMs,<br>Decontaminated item<br><br>Process Worker | As step 2 | As step 1 |
| **Step** | **6.** | **7.** | **8.** | **9.** | **10.** |
| Equipment & personnel | Interlock gamma monitor, item<br><br>Process worker | Tray, outer door, inner door<br>Drive mechanism, item<br><br>Process w., HP monitor | As step 7 | As step 7 | Tray, item,<br>workshop crane<br><br>Process w., HP monitor |

Figure 2 Example Flowsheet

**DISTRIBUTION**

**Working Group Members**

| | Number of Copies |
|---|---|
| Mr G Böhme | 3 |
| Mr G Pott | 3 |
| Mr J Van de Velde | 4 |
| Mr H Carlsen | 2 |
| Mr J C Baudoin | 5 |
| Mr A Chalony | 12 |
| Mr G Trezza | 2 |
| Mr K Duijves | 2 |
| Mr R Hargreaves | 1 |
| Dr M S Stucke | 3 |
| Dr G F Hines | 1 |

**Other Copies**

| | | |
|---|---|---|
| Mr M J Gilbert | AEA Technology - Windscale | 1 |
| Mr A I Russell | AEA Technology - Windscale | 1 |
| Mr J Hopkins | AEA Technology - SRD Culcheth | 1 |
| Mr G P Snape | AEA Technology - Windscale | 1 |
| Mr J H Tratt | AEA Technology - Windscale | 1 |
| Mr D I Hambley | AEA Technology - Windscale | 2 |
| Mr M Jardine | AEA Technology - Windscale | 1 |
| Mr J Prestwood | AEA Technology - Windscale | 1 |
| Mr T S Taylor | AEA Technology - Windscale | 1 |
| Mr J McElroy | AEA Technology - Windscale | 1 |
| Dr H G Morgan | AEA Technology - Windscale | 1 |
| Mr M P Walsh | AEA Technology - Windscale | 1 |
| Dr A D King | AEA Technology - Windscale | 1 |