Report Cover Page

ACERA Project
0606
Title
Tools for Anticipating Potential Problems in Biosecurity Applications
Author(s) / Address (es)
Jean Cross, University of New South Wales
Material Type and Status (Internal draft, Final Technical or Project report, Manuscript, Manual, Software)
Final Project report
Summary

This report provides a broad overview of techniques used in safety and reliability engineering to identify the nature and causes of risk. The report assesses the potential for these methods to be deployed in biosecurity operations, to reduce unanticipated failures effectively. It uses two case studies to illustrate them; the foot and mouth outbreak in Surrey, UK, and a hypothetical incursion of equine influenza.

The report finds that control charts and syndromic surveillance tools may be useful in border quarantine and post-border surveillance systems where routine time series data are collected. They may provide early warning of changes in the nature and frequency of risks on pathways.

Process-based methods such as Failure Mode and Effect Analysis, (FMEA), Hazard and Operability Studies (HAZOP), and Hazard and Critical Control Point analysis (HACCP) can be time-consuming but may have a place in biosecurity in assessing existing operational procedures, identifying weaknesses, and anticipating faults especially when failures are critical. For instance, HACCP may be useful for assessing the possibility of substituting one management system (or set of quarantine measures) for another, evaluating system equivalence and the potential for failures in the candidate system.

Causal analysis techniques are applied typically after a serious system failure. Examples demonstrate that complex systems are not easily identified from this type of analysis, even after the event. This is a critical point for biosecurity applications. Systems that depend on complex human factors require explicit analysis using tools developed for such situations.

'Human factors analysis' aims to describe, predict, and manage human behaviour to achieve operational goals. These methods provide a framework for understanding how systems can become error-prone, and how procedures may be implemented to anticipate and remedy these situations. Application of human factors analysis to the two case studies illustrates how it may have been useful in elaborating the causes of failure and identifying systemic changes that would reduce the chances of repetition of such events. The report concludes by outlining barrier techniques, foresight and scenario planning methods that may usefully support human factors analysis.

ACERA Use only	Received By:	Date:
	ACERA / AMSI SAC Approval:	Date:
	DAFF Endorsement: ( ) Yes ( ) No	Date:

Tools for Anticipating Potential Problems in Biosecurity Applications

ACERA Project No. 0606

Jean Cross
University of New South Wales

September 2011

Acknowledgements

This report is a product of the Australian Centre of Excellence for Risk Analysis (ACERA). In preparing this report, the authors acknowledge the financial and other support provided by the Australian Government Department of Agriculture, Fisheries and Forestry (DAFF), the University of Melbourne, Australian Mathematical Sciences Institute (AMSI), and the Australian Research Centre for Urban Ecology (ARCUE).

Disclaimer

This report has been prepared by consultants for the Australian Centre of Excellence for Risk Analysis (ACERA) and the views expressed do not necessarily reflect those of ACERA. ACERA cannot guarantee the accuracy of the report, and does not accept liability for any loss or damage incurred as a result of relying on its accuracy.

List of Tables

List of Figures

Executive Summary

The ISO 31010 standard on Risk Management – Risk Assessment Techniques lists many methods of risk assessment, many of which concentrate on events that might cause harm, controls that might fail, and targets that might be affected. All are applied within logical structures that attempt to identify weaknesses in a timeline or process. This project reviews a number of risk identification techniques used in reliability and process engineering to evaluate the potential for their use in biosecurity.

The review of current practice in biosecurity in Australia (DAFF) and New Zealand (MAF) established that the deployment of risk identification tools was patchy, limited mainly to some foresight activities for emerging animal diseases. In some circumstances, risk identification is specified by international agreements, limiting the extent to which tools can be deployed in routine operations. In other circumstances, corporate groups considered risk identification to be outside the scope of their activities. The review of these activities in Animal Health Australia suggested a revised, structured approach should be adopted to improve risk identification and priority-setting.

In contrast, DEFRA in the UK has invested substantially in risk identification techniques over the last few years, developing and deploying a range of structured methods. These developments have been stimulated in part by the Bovine Spongiform Encephalopathy (BSE) and foot-and-mouth disease (FMD) outbreaks and have led to whole-of-government initiatives on horizon scanning, foresight, and setting biosecurity priorities.

To illustrate the potential of the tools, two case studies are offered: an outbreak of FMD caused by the escape of virus from a laboratory and a hypothetical incursion of equine influenza (EI). The events are outlined as a precursor to hypothetical assessments evaluating how the tools might be used to help understand these events better.

Control charts and syndromic surveillance tools may be useful in biosecurity environments, especially in quarantine systems where routine time-series data may provide early warning of changes in the frequency of hazards on pathways. Post-border surveillance may also provide opportunities for their deployment. Control charts have been trialled in engineering systems for decades where their simplicity means they are effective in maintaining system control, even when operators have limited technical training. These operational conditions reflect some of those in border operations.

Informal expert networks are often very effective at identifying emerging threats. Foresight can be supported by a range of software tools dedicated to the early detection of emerging diseases pests and pathogens (e.g. ProMed and GPHIN). These and related tools and platforms are developing rapidly, as are the statistical data-mining tools that find and synthesise relevant information. OCVO has begun to develop protocols and implement systems, and ACERA is developing systems for aquatic and plant health (ACERA Report).

Process-based methods take as their starting point a process and work through it to consider problems that might arise at each step. Methods considered here include Failure Mode and Effect Analysis, (FMEA), Hazard and Operability Studies (HAZOP) and Hazard and Critical Control Point analysis (HACCP). In general, these methods can be time-consuming and may not be often practical to implement on a routine basis. They may have a place in biosecurity in assessing existing operational procedures, identifying weaknesses, and anticipating faults, especially when failures are critical. For instance, HACCP may be useful in areas of biosecurity concerned with systems management. When assessing the possibility of substituting one management system (or set of quarantine measures) for

another, HACCP may provide a useful framework for evaluating system equivalence and the potential for failures in the candidate system.

Causal analysis techniques are applied, typically after a serious system failure, as a tool of investigation, and as a logical way to explore potential causes of failures. Causal analysis focuses on underlying problems. Applications and examples in the report demonstrate that complex systems are not easily identified from this type of analysis, even after the event. This is a critical point for biosecurity applications. Systems that depend on complex human factors require explicit analysis using tools developed for such situations. Theoretically, root cause analysis techniques could identify the problems that occurred. There is, however, insufficient evidence of the successful use of the techniques in a proactive way for problems involving human and organisational failures to be able to indicate how well they would work in these circumstances.

'Human factors analysis' refers to the class of methods from behavioural science that aims to describe, predict, and manage human behaviour to achieve operational goals. Human factors methods are used in engineering to help design systems and procedures to work efficiently and to minimise error. These methods provide a framework for understanding how systems can become error-prone, and how procedures may be implemented to anticipate and remedy these situations. Resilience engineering removes the focus completely from identifying the potential for individual error and procedural failure, and looks at management decisions, organisational structures, communications, and foresight or mindfulness. As measures of organisational resilience are developed further, they could be used as part of an auditing tool to identify where a more detailed analysis of organisational weaknesses would be beneficial.

Application of human factors analysis to the two case hypothetical cases illustrates how they may be useful in elaborating causes and identifying systemic changes that may reduce the chances of such events. The report outlines a few structured methods, barrier techniques, foresight, and scenario methods that might assist in supporting human factors analysis. Finally, the report documents the potential for human factors analysis to improve the system-wide performance of biosecurity operations in Australia.

PART A CURRENT PRACTICE

1. Introduction

1.1. Objectives

The objectives of this project were:

- to review and benchmark risk identification techniques used in biosecurity in Australia and those in use overseas (particularly in the UK and New Zealand);
- to report on any limitations or perceived limitations in the techniques;
- to review formal techniques for identifying risks used in other industries and applications, and
- to evaluate the potential for use of these techniques in the biosecurity context.

1.2. Scope

The scope of this project covers techniques which identify hazards, the nature of the harm, and the circumstances and pathways by which harm can occur. Techniques that seek to find the magnitude of consequences and likelihood are outside the scope.

The report seeks to review risk identification techniques that have application to biosecurity. In the context of this report, risks to biosecurity are taken to incorporate risks of relevance to agriculture, fisheries and forestry industries, and to the government agencies that regulate and support them. The focus is on risks that affect the ability of an industry to remain profitable, competitive, and sustainable. Business risks, project risks and other risks that are applicable to all industries, are not part of the scope

1.3. Definitions

Risk-related terms do not have universal definitions, and are often used differently in health- and environment-related areas than when used in engineering-related areas. In looking at the application to biosecurity of techniques developed initially for engineering problems, it is therefore important to clarify terminology.

1.3.1. Hazard

The term ‘hazard’ refers to a source of harm; something with the intrinsic property of being harmful. Some definitions recognise the idea that the property of being harmful depends on circumstances; something may be harmful in some circumstances but not in others (Hayes 2002). Some definitions include dangerous activities; others are limited to ‘things’ such as substances, or in the case of biosecurity, pests and diseases. Makin and Winder (2008), in an occupational health and safety (OHS) context, suggest that the term should be broadened to include anything (including system and organisational problems) that leads directly or indirectly to harm, so that when hazards are identified, all factors contributing to loss are identified. A broad definition of hazard, however, is unhelpful here as it allows for dissimilar hazards too easily, making it potentially difficult to compare the level of risk they may pose. For example, under a broad definition, the risk of having inexperienced staff may be compared with the risk of contracting a disease. Thus, in this paper, the term ‘hazard’ is limited to the source of harm. Hazardous activities and conditions are incorporated through consideration of exposure pathways and conditions. Hazard assessment refers to techniques for gaining a greater understanding of the source of harm and the circumstances under which it may lead to harm.

1.3.2. Risk

Hanson (2004) describes five common technical interpretations of the word ‘risk’, of which there are two distinct classes of meaning. The first is a description of the nature of a harm that might occur and

the circumstances under which it may occur. As pointed out by Hayes (2002), a source of harm may have several end-points and the same end-point may be reached from several different sources of harm. Thus to describe a single 'risk', the set of circumstances or conditions of exposure by which a particular hazard leads to a particular end-point needs to be specified. This meaning of risk is illustrated by the sentence, 'there is a risk that a diseased animal might enter the country and infect Australian populations resulting in financial loss to the industry'.

The second common usage of the word is, 'a measure to which a number can be ascribed, related to the extent to which the potential outcomes are of concern to us' (Knight 1921). Traditionally, this number is obtained by multiplying a measure of consequences by their likelihood. For example, the World Organisation for Animal Health (OIE 2011) defines risk, in the context of import risk analysis, as 'the likelihood of the occurrence and the likely magnitude of the biological and economic consequences of an adverse event or effect to animal or human health.' This expression of risk is the statistical expectation of unwanted events (Hanson 2004).

For clarity, in this paper the term 'level of risk' is used to refer to the magnitude of a risk. In the context of this report, the magnitude of risk is the statistical expectation of unwanted events.

1.4. Risk analysis

Four risk analysis/management frameworks are used in the Australian Government Department of Agriculture Forestry and Fisheries (DAFF, Hennessey and Barry 2006), reflecting different national and international standards and guidelines used in different sectors. They all describe a similar process of identifying hazards, pathways, and consequences, estimating the likelihood and consequences of harm, evaluating this information, making and implementing decisions, and communicating as appropriate. The frameworks differ in the following ways:

- The Codex Alimentarius and AS/NZS4360 consider that risk assessment includes hazard identification, whereas the International Plant Protection Convention (IPPC) and OIE frameworks reserve the term 'risk assessment' for estimating the level of risk and understanding the information necessary to do this.
- AS/NZS4360 differs from the other models in considering risk evaluation to be part of risk assessment rather than risk management. This standard uses the term 'risk management' for the entire process, reserving the term 'risk analysis' for the sub-step of risk assessment that is about understanding and measuring a level of risk

The frameworks differ in terminology rather than in basic concept. In this report, the Codex Alimentarius definitions for risk analysis and risk assessment are used.

2. Review of Australian practice

2.1. Method

The method involved:

- a review of documentation supplied by the Department of Agriculture Fisheries and Forestry (DAFF) and on the web, including sample import risk assessments, to see the extent to which formal techniques were recommended or used;
- the collection of information relating to the methods used for the identification phase of risk assessments in DAFF through discussions with DAFF personnel;
- a review of a project carried out for Animal Health Australia for outcomes relevant to identifying risks;
- the collection of information about how biosecurity risks are assessed overseas and on failures that have occurred through a review of documents and visits to the United Kingdom (UK) and New Zealand; and
- a literature review of the application of formal techniques of risk identification used in other industries, and a desktop exercise to consider their potential to predict problems in biosecurity applications.

Although risk perception is an important element of many of the procedures outlined here, the science of risk perception and the science and practice of risk communication were beyond the scope of this report. They have been addressed in several other ACERA reports (notably, reports ACERA 0608, ACERA 0611 and ACERA 0801).

2.1.1. Interviews

Brief introductory meetings were held with representatives from Biosecurity Australia, Australian Quarantine and Inspection Service (AQIS), Product Integrity Animal and Plant Health Division (PIAPH) (Plant Protection, now the Office of the Chief Plant Protection Officer), and Bureau of Rural Sciences (BRS). The people participating were nominated by BRS in discussion with the appropriate section. In some cases, only one person was seen; in others, there was a group. Relatively short interviews were held. The aim of the meeting was to elicit general information on the extent to which formal methods of risk identification are used or needed within DAFF. It was originally intended that these introductory unstructured interviews would form the basis for wider, structured, and more in-depth questions later. However, the individuals interviewed discussed their understanding of risk identification and directed us to documentation explaining their methods, so in-depth interviews were not held.

2.2. Results of document review

2.2.1. Methods of hazard and risk identification in international standards

The risk assessment models used OIE, IPPC, and the Codex Alimentarius all take a scenario-analysis approach to describe the series of events and pathways that might occur to cause harm (scenario analysis is discussed in this report below). The scenario may be explicitly displayed diagrammatically

in import risk assessments following these codes, or may be displayed in the structure of the report detailing the risk assessment. For example, Figure 1 shows an example of part of a scenario-based framework from the UK risk assessment on illegal meat imports (Hartnett *et al.* 2003).

Generally, hazards are identified from searches of international information sources including electronic databases, scientific literature, risk analyses performed by other countries, and input from individual experts. The starting point for the searches depends on the application. For example, in an import risk assessment, the commodity forms the starting point. Risk analysis may also be initiated by discovery of a new pathway, a new pest or the revision of policies and priorities (IPPC 2004). The IPPC standard provides a checklist of some situations that might lead to identification of a new pest or pathway, but no specific techniques for identification are suggested. Generally, the standards describe what has to occur but do not specify methods for how this should be done. Their aim is to define required outcomes rather than detailed methods.

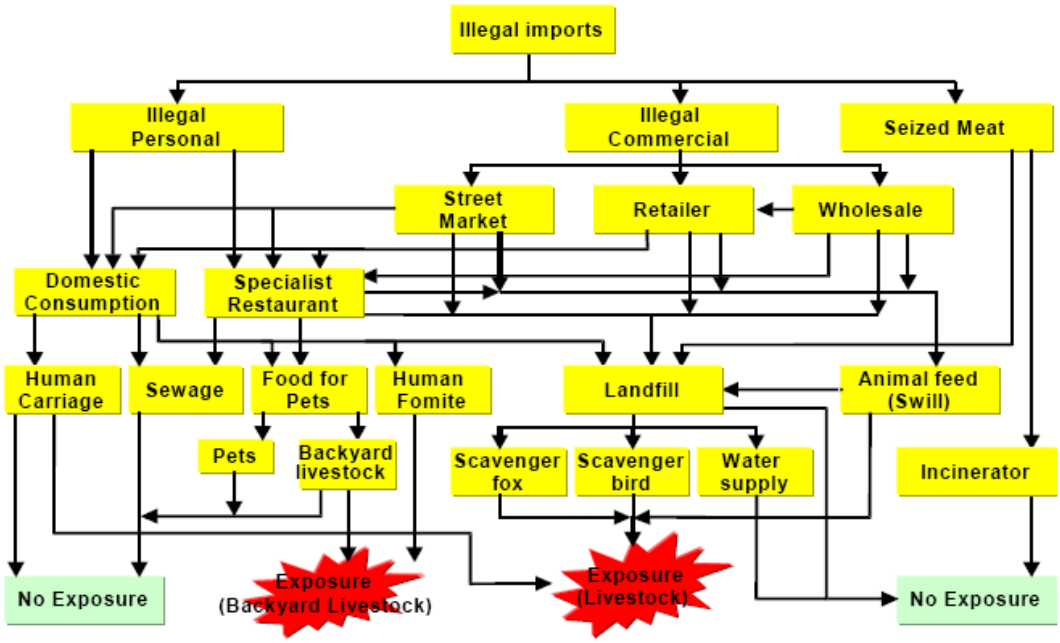

Figure 1. Framework for quantitative modelling of the flow of illegal contaminated meat from import to livestock exposure (Hartnett *et al.* 2003).

2.2.2. Stocktake of use of risk analysis principles and techniques in DAFF

The stocktake of the use of risk analysis principles and techniques, carried out by Hennessey and Barry from BRS (2006), formed a starting point for reviewing techniques used at DAFF. For the stocktake, a contact from each division was asked to fill in a questionnaire that aimed to identify whether risk analysis was used in the area, what activities used risk analysis techniques, what the techniques were and where they originated. The scope of the stocktake was, 'activities that directly relate to achievement of the output objectives where the activity is being performed'. Project risks were not part of the scope. The questionnaire followed the Codex Alimentarius framework and terminology rather than that of IPPC or OIE, so the initial step of identifying hazards, which is separated in the IPPC framework, was not isolated from the consideration of the magnitude of consequences and likelihood.

In spite of the definition of risk assessment provided to participants, it appears that risk assessment was interpreted to mean 'finding a level of risk', since identifying hazards and pathways (which also forms part of risk assessment) is necessarily qualitative. The term 'risk assessment' appeared to be interpreted quite narrowly. For example, the International Division (IFAS) considered that risk assessments were not part of their function. The output objectives of that Division are to make Australia's agricultural, food, fisheries and forestry industries more sustainable, competitive, and profitable. It would appear that identifying and understanding what might happen to affect the sustainability, competitiveness, and profitability of these industries is part of their role. This is not, however, seen to be part of 'risk assessment'.

DAFF also participates in the risk assessment exercise overseen by Animal Health Australia (AHA) in which risks associated with agreed National Animal Health Performance Standards are identified and assessed by DAFF, the relevant state agencies and animal industry associations, and recorded in a central database (see Section 2.5). This risk assessment activity was not mentioned in the stocktake, although several of the Divisions included in the stocktake did participate directly in the AHA exercise.

2.3. Discussions with DAFF personnel

2.3.1. AQIS

To AQIS Border Programs staff, 'risk identification' involves identifying which shipments or other importation routes present the greatest risk so that inspection can be targeted. This is done through profiling and analysis of surveillance data, including recording both the number of problems found during normal inspections and an estimate of the number of problems missed, which are identified through follow-up sampling.

The study intended originally to explore how AQIS activities might fail — for particular pests and diseases, or in particular circumstances. However, when this topic was discussed in 2007, some AQIS staff indicated concern that this might be seen as being critical of AQIS. The interviews when this was expressed took place in 2007. Instead, the subsequent outbreak of EI in Australia was used to create a hypothetical case study, which was used to illustrate potential strengths and weaknesses of a range of hazard identification techniques.

2.3.2. Biosecurity Australia

Biosecurity Australia (BA) follows techniques of hazard and risk identification that are consistent with international guidelines. Identification of pests and diseases associated with a particular import is a matter of reviewing literature, data, and intelligence from overseas. Pests and diseases are identified in this way without undue difficulty and there was no perceived need for the increased structure and imaginative thinking of formal identification techniques.

BA follows the methods and terminology of OIE and IPCC codes and guidelines, and considers the identification of pests, diseases, and other sources of risk to be the hazard identification step. Analysing potential pathways of how pests and diseases might get from a shipment into a situation where they might cause a problem to Australian plants, animals, or environment in this terminology is part of risk assessment. Some foresight activities are carried out by members of BA to identify new

and emerging animal diseases, but there was no departmental commitment to support these activities more widely.

2.3.3. Office of the Chief Plant Protection Officer and Office of the Chief Veterinary Officer

The discussion with representatives of the Office of the Chief Plant Protection Officer (OCPPO) was more wide-ranging. Unlike AQIS and BA, OCPPO has a major role in post-border quarantine issues. They need to identify issues that may become a problem in order to direct their limited resources appropriately. Because part of its role includes coordinating the national response to plant pest incursions, it needs to identify how and where to plan a response. However, the group does not use formal risk identification tools to anticipate threats or to set priorities, in contrast to Animal Biosecurity Branch of Biosecurity Australia and the Office of the Chief Veterinary Officer (OCVO), which deploy structured animal foresight activities.

Ecological and environmental issues are complex and changing. It was recognised that external factors such as climate change could change the level of risks of existing exotic species as well as allow pests and diseases that have entered but not become established to start causing problems. Some foresight (see Section 9.2) is undertaken in AQIS and the group also sees its informal links nationally and internationally as an important source of information that enable risks to be identified.

2.4. Visits to overseas departments

Overseas travel was not funded within this project. Brief meetings were held with representatives of the Department of Environment Food and Rural Affairs (DEFRA) in the UK, and with the Ministry of Agriculture and Forestry (MAF) and the Environmental Risk Management Authority (ERMA) in NZ, in the course of travel for other purposes.

2.4.1. Department of Environment Food and Rural Affairs, UK

Government in the UK, as in Australia, has over the past few years adopted a risk management approach in departments at both policy and operational levels. As a consequence, DEFRA is actively working to embed risk management throughout the department. DEFRA's overall risk coordinator at a policy level was interviewed to explain the department's uptake of risk management principles and methods. The term 'risk management' was used in the interview with him in the sense of all activities undertaken to identify, understand, and manage risks.

In the UK, there was growth in interest in formal risk management in the 1990s. During the same period, there were several important biosecurity events including outbreaks of BSE and FMD. Since biosecurity and animal health issues were drivers for business and strategic risk management within government in the UK, biosecurity risk analysis and strategic and operational risk management are more closely linked in the UK than in Australia. A major push to enhance risk management in the UK public sector was initiated. A report on progress issued in 2004 by the National Audit Office (NAO) illustrated the approach taken (NAO 2004). The BSE and FMD outbreaks led the UK Government to establish a significant number of high-level cross-departmental groups and initiatives concerning risk and its management.

There has been significant UK Government funding for horizon scanning and foresight exercises across government, with a is *Foresight Horizon Scanning Centre*, a part of the Government Office for Science within the Department for Business, Innovation and Skills (see: www.bis.gov.uk/foresight). One of the early projects concerned detection and identification of infectious diseases in plants, animals, and humans in a 10–25 year horizon. Other relevant major foresight activities internationally include that of the European Foresight team of the Knowledge for Growth (KfG) Unit (see http://foresight.jrc.ec.europa.eu/index.html).

From the viewpoint of coordination in DEFRA, risk management is a governance issue as well as something carried out at an operational level to manage the risks to environment, food, and rural affairs. Significant disease outbreaks such as FMD and BSE were of wide strategic importance to the organisation, and the organisation does not separate strategic risk management from specific risk analysis exercises. Activities at the strategic level include:

identifying the organisation's top 12 risks and ensuring each had a champion at board level;

linking risk management to the balanced score-card management approach, and

applying risk management within all major projects.

To earn a place on the top threats register, the risk had to meet one of several criteria including:

posing a major problem for the department's budget;

high-profile policy where headline criticism needs to be avoided; and

strong public concern.

There were no specific guidelines on how the potentials for headline criticism or strong public concern are assessed. Top-level threats are assigned to a board-level champion (the Board comprises directors of the groups within DEFRA plus three external non-executive directors). The champion is responsible for ensuring a robust action plan is implemented. Progress towards reducing risk is monitored. The list of top risks changes from time to time and includes biosecurity issues.

In addition to cross-government initiatives on horizon scanning and foresight, DEFRA has undertaken its own 'specific future' studies activities. The Department undertook a baseline scan of key political, economic, social scientific, and technological trends and drivers that were brought together in a database. A series of projects on horizon scanning and futures was carried out covering various themes. Results have been used to provide an evidence base for policy change including changes to DEFRA's farm regulation and charging strategy, and to setting priorities for natural resource protection. There has also been a 'blue skies' thinking workshop on non-food crops.

Risk management is also seen as opportunity management; the foresight and futures work actively identifies long-term potential opportunities, and shorter-term activities capture bright ideas suggested by staff. These form the topic of one of the cases studied in the Risk: Good Practice *G*uide published by the Government (HM Treasury 2006).

DEFRA contributed five case studies to the two volumes of the Risk: Good Practice Guide issued by HM Treasury (2006). These illustrate the way thinking about strategic and specific operational risks are linked, and the breadth of activities that DEFRA sees as risk analysis/management. The five case studies comprise:

Spotting emerging risks

This is the Department's horizon-scanning and futures program, which aims to: '*identify the key trends and drivers that could shape DEFRA's external environment over the next 50 years, and give the Department a head start in predicting – and preventing – the biggest problems*.'

Rising to the challenge

This project challenges staff to think more creatively, and to look at how they could improve the way they work.

Top threats and the Board

DEFRA believes that it is important for the Board to know and understand its weaknesses and to focus its attention on them. This case study describes their systems to ensure that staff anticipate risks, and that the right risks are being identified and escalated up through management to the Board. Improvements in managing animal health emergencies that have been achieved are cited as examples of the success of this approach.

Engaging stakeholders

A series of all-day meetings was held, designed to enable a wide range of interested and affected parties to discuss and inform key policy issues relating to nanotechnology.

Partnership delivery

Directors wanted to improve the way risks were being managed between the department's business/policy areas and non-departmental public bodies and other partners. A series of half-day, externally facilitated workshops was held with partners to develop a shared understanding of the threats and opportunities on both sides of the partnership. The workshops also provided both sides with an opportunity to discuss their current relationship, and to highlight what was working well, and what prevented progress. The workshops were found to defuse problems, and promote working together to minimise risk.

Risk perception is an important element of many of the above issues, although as noted above, it is beyond the scope of this report. Import risk assessment is carried out according to international convention in the same way as in Australia and New Zealand. The UK manages additional difficulties including the lack of border controls between countries in the European Union (EU). For example, in discussing import risk analysis, one participant commented that although DEFRA has overall responsibility for plant health controls (other than forestry) and for live animals, HM Revenue and Customs (HMRC) has responsibility for enforcement at the border. In 1993, Customs ceased to enforce border health controls on plant and forestry materials and on live animals from other EU member states other than for the purpose of rabies control. The UK was therefore reliant on the policies, procedures, and risk assessments of other member countries for its border protection.

The priorities of HMRC with respect to risks necessarily differ from those of DEFRA. HMRC web pages were searched for information on the top risks reported to senior management. These do not appear to be published as a list, but references to several of the top 16 risks appear in management committee minutes. Those shown relate to processes rather than outcomes, and are causes rather than risks. For example, one risk identified in Government documents was not having the right number of people, with the right skills, in the right places to deliver business outcomes. The priority given to animal and plant health risks by HMRC is therefore unclear.

The DEFRA website indicates one specific risk assessment relating to disease that enters the UK via the EU: that of equine infectious anemia, which is present in Russia and in neighbouring EU countries. This report uses a scenario tree to help identify pathways. Surveillance methods are also

used involving a range of different data sources (DEFRA 2006b). In addition to assessing risks to biosecurity, DEFRA also applies formal risk analysis/management at a project level (e.g. identifying risks of project delay) and it has a database for project risk management called RAID.

2.4.2. New Zealand

Biosecurity New Zealand, a division of the Ministry of Agriculture and Forestry (MAF), is responsible for 'facilitating international trade, protecting the health of New Zealanders and ensuring the welfare of our environment, flora and fauna, marine life and Maori resources' (www.maf.govt.nz). In addition to MAF, the Environmental Risk Management Authority (ERMA) was set up under the Hazardous Substances and New Organisms (HASNO) Act 1996 to make decisions on applications to introduce new organisms or hazardous substances to New Zealand. A new organism is defined as:

> any life form coming into New Zealand for the first time - this means anything capable of reproducing including micro-organisms, seeds, plants, fish and animals, and/or
>
> any genetically modified organism (GMO) - this means any plant, animal or micro-organism developed through genetic modification.

Under the HASNO Act, the responsibility for identifying risks and potential pathways by which harm might occur rests with the proponent of the introduction of the new organism. The ERMA website provides general guidance on how this must be done, but no specific tools or techniques of identification are discussed. These risk assessments are then reviewed and a decision is made by ERMA. ERMA also specifies risk controls required. A representative from ERMA indicated that staff often needed significant help in producing an adequate risk assessment.

MAF's scope of activities differs from that of DAFF because of the interaction with ERMA and because some state responsibilities lie with MAF. Methods used in New Zealand for identifying hazards, pathways and the nature of harm are similar to those used in Australia. A meeting with representatives of MAF did not bring to light any specific methods. Some time was spent discussing why New Zealand did not use a semi-quantitative analysis of the level of risk and why it preferred providing general qualitative and quantitative information to allow a decision to be made.

2.5. Animal Health Australia Project

2.5.1. Background

Simultaneously with this ACERA project, a project has been carried out for Animal Health Australia advising on the risk management system it has established for member organisations. The aim of the AHA risk management system is 'to assist government and industry identify and assess risks to the animal health system, including risks faced by individual governments, by industry and nationally' (AHA 2005).

The framework developed for Animal Health Australia by consultants is based on AS/NZS4360 and uses the National Animal Health Performance Standards (NAHPS) as a checklist to help identify risks. The NAHPS are management system requirements that have been developed as a result of considerable stakeholder consultation, and are based round six core functions, each of which may be combined with any of nine capabilities. The functions are

consumer protection;

trade and market access;

disease surveillance;

endemic disease management;

emergency preparedness and response; and

livestock welfare.

The capabilities are

policy development;

management;

service capability/capacity;

information management;

livestock tracing;

training;

communication;

research and development; and

legislation and development.

A set of required national outcomes and performance measures has been developed for each capability/function pair, and each organisation has committed to achieving each performance measure.

For example, one of the national outcomes for the capability 'policy development' for the function of 'consumer protection' is 'a quality assurance system for production and processing'. The industry performance measure is to 'develop and promote policy relating to quality assurance for production and processing', and the government performance measure is 'to contribute to the development and promotion of policy relating to quality assurance for production and processing'.

Members of AHA were asked to identify risks using the 214 performance standards as a checklist. The objectives of AHA in requesting this were to identify risks to the animal health system and to assess compliance with the NAHPS. This produced a database of risks, identified by all the organisations associated with animal health including DAFF and all state jurisdictions. Risks were rated by the organisations using a consequence-likelihood matrix system supplied by AHA. The original concept was that high risks would provide a basis for participants and for AHA to set priorities and plan future actions, and would also demonstrate areas where compliance with NAHPS could be improved. Low risk was believed to imply compliance with the NAHPS, and high risk, to imply non-compliance.

The aim of the project was to audit the management system using risk registers. The risk register was analysed and three organisations (including DAFF) were visited to discuss their entries. The information on risks that was recorded in the register was viewed to see the extent to which it could be used to highlight any gaps in existing defences, and to assist AHA define its future programs. Levels of risk that were recorded were reviewed to see the extent to which they were capable of use by AHA to set priorities and measure compliance.

2.5.2. Findings relating to risk identification

2.5.2.1 Overview

Analysis of the statements recorded under the headings of 'risk' revealed three different types of risk entered on the risk register.

1. A statement of how a hazard might cause harm, e.g. a new insect-borne disease enters Australia on illegally imported goods, resulting in cattle disease. This is the classic description of a risk.
2. A statement of a failure of a control, e.g. surveillance may fail to find the illegally imported goods, or a vet might fail to diagnose the new insect-borne disease quickly resulting in spread of disease.
3. A statement of a management systems failure, e.g. a failure in the accreditation system for private vets or lack of a state government business plan for disease surveillance.

The use of the performance standards, which are required management system components, as a checklist to identify risks predominantly produced the third category of issues. Most organisations identified no classic risks.

Risks were often recorded generically rather than specifically, so the meaning was unclear. For example, a risk identified by one industry under 'risks to policy in the trade and market access' function was that Australia's contribution to international trade agreements does not reflect industry views and needs. It emerged in discussion that this concern was in fact a specific European policy under discussion, which although apparently quite minor, could prevent the particular industry from exporting to the European Union, a significant trade partner. The way the risk was formulated did not communicate the issue clearly, so even though the issue was flagged as high priority (likely to occur and with very serious consequences to the industry), no action could be taken.

The level of detail recorded needs to be consistent between members to ensure that broad statements covering multiple problems are not rated against narrow definitions of a single problem resulting in inappropriate priorities. Further consultation is needed to consider the level of detail that needs to be recorded to strike a balance between providing an understanding of the problem but not producing an unmanageable list of risks. There is a very wide range of risk management understanding within government agencies and industry. This study indicated that tools must take into account the different expertise, experience, and needs of all potential users.

2.5.2.2 Risk rating

The use of the consequence likelihood matrix as a rating system for all three different types of risk has fundamental problems. The rating matrix requires a single consequence and its likelihood to be defined. For most classic risk events, there will be a range of different consequences of varying severity to different stakeholders. The variation of the severity of consequence that might arise from a single event is dealt with either by rating each consequence level as a separate risk, or by selecting the highest consequence and its likelihood. Either approach is an approximation to the level of risk that should represent a probability distribution of all the different consequences.

In addition, a particular consequence may have a different value to different stakeholders and stakeholders are likely to have different perceptions of risk depending on their context. The

consequence likelihood tool gives a subjective assessment of level of risk, hence different stakeholders may give quite different ratings.

Risks that derive from exposure to hazards (as in example 1 above) can be assigned a risk rating using a consequence likelihood matrix because, subject to an understanding of hazards, pathways, and targets, a consequence and likelihood can be defined. But different ratings will be given depending on the extent to which different hazards and pathways are disaggregated.

Control failures usually apply to more than one hazard, and the level of risk associated with a control failure depends on the severity of all the underlying hazards and their probability of occurrence rather than on the probability of failure of the control and its possible consequence. The level of risk also depends on the extent to which other controls are present and effective. Priorities for improving controls are not set by rating risk using a consequence/likelihood matrix, because the range of possible consequences is too large, and the likelihood of the consequences occurring depends on factors other than the probability of failure of one particular control.

Management systems' failures are not risks in the strict sense, but are weaknesses, deficiencies or changes that increase the level of risk overall. These also are not amenable to analysis using a matrix of 'likelihood' and 'consequence'. For example, even though institutional factors may influence risk management, it is not possible to estimate a level of risk associated with a state government not having a business plan for surveillance, if only because there is not necessarily a direct relationship between having a business plan and good surveillance. This issue is elaborated in the following section.

Some of the items on the NAHPS checklist related directly to setting priorities within the organisations on the basis of risk assessment. Although no organisation indicated this performance standard to be a problem, the extent to which organisations actually had risk-based decision processes appeared to be extremely mixed, and in many cases, decisions were not based on an assessment of risk at all.

2.5.3 Current status

The main finding of this project was that in order to use a register of risks to set priorities, and as part of a management information system, risks need to be recorded in a way that separates consequences that arise from exposure to a hazard, or source of risk from control failures and management systems failures.

A revised system for producing a risk register is to be trialled. To clarify the distinction between risks control failures and possible management system weaknesses, it is proposed to structure the risk register around the bow tie model of risk. (Figure 2 and Section 8.1)

2.6. Summary

Formal identification techniques were used where required by agencies and industry, in some circumstances where international standards and guidelines require them, but were not applied more generally to biosecurity issues in any of the three countries reviewed. Interviewees generally felt that the methods that they currently used were appropriate and sufficient for their purpose. This context provided the platform for the remainder of this report, which was to outline formal methods that may play a role in some part of the biosecurity domain. This work will provide an opportunity for analysts

to reassess the potential costs, benefits, strengths and weaknesses of these tools in their operational areas. The focus of the project therefore was to assess the potential for increased application of formal techniques to identify risk across areas of relevance to DAFF.

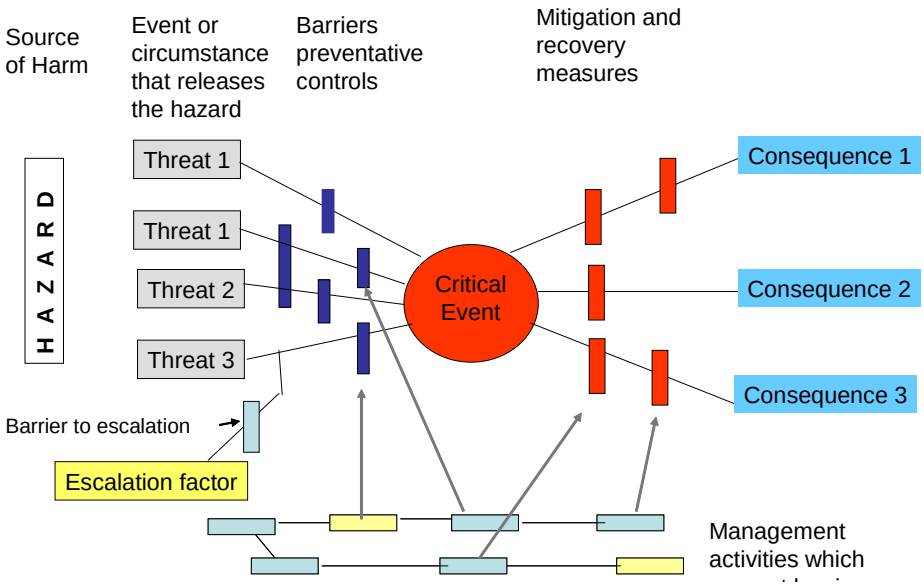

Figure 2 Illustration of a bow tie diagram

Part B TOOLS AND TECHNIQUES

3. Introduction

The purpose of this section of the report is to explore the extent to which hazard and risk identification tools originally developed for reliability or process engineering can be usefully applied in the biosecurity context. Tools are described and the literature is reviewed to explore the range of applications to which tools have been applied. The way in which they could be used to anticipate issues that might affect the ability of Australia's agriculture, fisheries, food and forestry industries to remain competitive, profitable, and sustainable is discussed.

The techniques reviewed below are relevant to one or more of the elements of risk identified in the bow tie model of Figure 2 above. These are:

the nature of the hazard or source of harm;

the nature, vulnerability, susceptibility, and resilience of the target(s);

the types of outcome relevant to the target(s);

the pathways by which the hazard may reach the target;

the mechanisms by which the hazard causes harm when it reaches the target;

the barriers or controls that should prevent exposure to the hazard or protect the target, and

the factors that could exist to make the level of risk higher or lower.

Problems that might adversely affect the ability of an industry to remain profitable, competitive, and sustainable, or a government organisation to remain effective and efficient, are not necessarily directly caused by hazards, such as pests and diseases. Such risks can arise from political, economic, organisational and social factors from both inside and outside the organisation. This also applies to organisations in chemical and process industries that are increasingly applying formal techniques to identify these more generic issues.

The ISO 31010, Risk Management – Risk Assessment Techniques, lists many methods of risk assessment. Some techniques concentrate on seeking events that might occur, some on hazards that might cause harm, some on controls that might fail, and some on targets that might be affected. All techniques are applied within a logical structure that attempts to identify weaknesses in each aspect of a timeline or each step in a process. More than 20 can be applied to the identification phase of risk assessment, but only a few are commonly used in environmental or agricultural-related areas. This report focuses on tools that can be used for identifying hazards, pathways, and outcomes, and does not include those used only for considering the magnitude of risk.

Formal risk identification and assessment methods described in this report have been developed over the past 50 years. Many were first developed as a result of a major incident, or recognition that a past failure has resulted in major harm. Structured ways to identify potential adverse events and outcomes were developed when it became clear that unstructured approaches, and reliance on historical procedures, have not been effective in preventing failure. Risk assessment tools are also applied to identify and analyse issues and uncertainties (both positive and negative) that might arise from change more generally; for example, from climate change or from changing perceptions and values in the community.

In both engineering and biosecurity applications, investigations of failure find that there were warning signs well before the incident that escalates to a disaster occurs. These may take the form of

minor incidents or recognised control failures that are not followed up. Systems to improve reporting or to follow up warning signs are also a useful means of identifying risks.

In essence, formal tools of risk identification are ways of structuring the problem and applying imagination to think about what might happen in the future. Structure provides some assurance that a problem or situation has been explored comprehensively, but imagination is necessary to identify what might happen, (particularly if it has not happened in the past), and to anticipate how different people will perceive and react to a risk. The different formal tools offer different ways of structuring problems and applying imagination to the different elements that make up risk. Historically, they were developed as separate tools for a particular industry sector, and were given a specific acronym. As applications of the tools have widened, they have evolved and the distinctions between some of them have become blurred. Tools are thus reviewed in sections that group together similar or related methods. At the end of each section, the application of that range of methods is demonstrated by reference to case studies of failures. Different problems need different ways of thinking, hence different types of technique are effective in different circumstances. These are indicated in this report, in each relevant section.

3.1. Lessons from incident analysis

After a major failure or loss in any field of endeavour, investigations invariably report some obvious failures that should have been readily apparent before the loss. The ease with which these factors come to light with hindsight during a structured investigation suggests that it might be possible to identify at least some of them before a loss by following the same types of analytical processes that are carried out retrospectively (see Fennel 1988; Cullen 1990; Dawson and Brooks 1999).

Inquiries into failures generally start by establishing a timeline, working backwards from when the event was detected, and asking what occurred, then how and why. The timeline is then extended forward to consider whether detection could have occurred earlier, or whether impacts could have been reduced or better mitigated. This logical process of considering what happened, how it happened, why it happened, and what could have prevented it from happening, can equally be carried out in advance of loss, and it is the basis of many formal risk identification techniques.

In biosecurity failures, the timeline may be very long; for example, the establishment and spread of pests and diseases may take a decade or longer before the problem is manifest. The general process, however, of seeking how and why the problem was initiated and what could have been done to manage it better still applies.

In some cases, factors emerge during an inquiry that comprise essentially new information (or exist outside the knowledge of the people concerned). In an inquiry, these factors are found by seeking new hypotheses that fit observed facts and by modelling and research. Although it is less clear whether they could be identified in advance, the use of imaginative risk identification techniques and modelling can be used to attempt to identify new issues.

Inquiries into failures usually identify multiple controls that can be improved. Recommendations relate to both direct and indirect causes of failures, and often have a high focus on human, organisational, and sometimes social factors. In seeking to identify problems prior to a loss, the complexity of real failures and the role of organizational and human factors need to be included.

3.2. Case studies

Two recent incidents are used as the basis for case studies to illustrate the potential for application of tools. For those tools not applicable to these case studies, other potential applications are outlined.

3.2.1. Foot-and-mouth disease in Surrey

There was an outbreak of FMD in Surrey in the UK in 2007, caused by a laboratory strain of the virus not then found in the environment. It was believed to have originated from a site in Pirbright occupied by the Institute of Animal Health (IAH), run by the UK Government and two private companies, Merial Animal Health Ltd and Stabilitech Ltd. All three organisations were working on the strain in question.

The report of the UK Health and Safety Executive (HSE 2007) found that the release occurred from faulty effluent drainage pipes on-site, and was probably carried from the site and past the immediate area to farms that became infected on construction vehicles working in the vicinity of the failed drain pipes (HSE 2007). The drains were known to be faulty, but there was a contractual dispute about which of the organisations on-site should fix them. Two local premises were infected. Early estimates put the total cost of the incident at more than £100 million (Callaghan 2007). The outbreak was contained, with only eight cases confined to the local area, but failures within the government department contributed to the release, so there was also significant reputational and political harm.

3.2.2. Equine influenza in NSW

In August 2007, cases of EI were reported from a number of locations around NSW and in southern Queensland involving horses that had attended a one-day event near Maitland. By October 2007, there were 4500 infected premises in an area of about 278 000 square kilometres (km^2). The virus may have escaped from the Eastern Creek Quarantine Station in NSW via a contaminated person or on equipment leaving the quarantine station (Callinan 2008). This context was subsequently used to help develop hypothetical scenarios to illustrate potential applications of the methods outlined in this report.

4. Methods based on data analysis

4.1. Introduction

Managing biosecurity risks requires the identification of what might go wrong, what kinds of things may be affected if things do go wrong, and how the likelihood or the consequences may be mitigated to ensure the risk is acceptable. Data can be used to identify risks in three ways:

1. To detect losses or indicators of problems directly. For example, there is monitoring of medical outcomes to detect any increase in medical error.
2. To detect small failures that, given different circumstances, could escalate. For example, the petrochemical industry monitors all loss-of-containment incidents as indicators of the potential for a major fire or explosion.
3. To detect changes in conditions that may introduce new risks or affect the magnitude of known risks. For example, monitoring parameters of climate change that may affect the viability of agriculture or the spread of pests and diseases.

Surveillance activities and methods are the subject of other ACERA reports, but a brief indication of the use of surveillance techniques in risk identification is provided here. Some of the data routinely collected for biosecurity, public health, or environmental surveillance can give information on changes in levels of risk or about new and emerging risks. It would be helpful to consider how additional data might usefully and cost-effectively be collected, specifically for the purpose of identifying early warning signs of known risks, for identifying changes that might lead to risk, or identifying new and emerging issues.

4.2. Statistical control charts for identifying change

Once suitable data sets are identified, the analysis needed to identify risks is often the identification of changes in:

- conditions and factors that may result in new risks;
- the level of risk, or
- risk outcome measures.

Control charts provide a useful way of identifying whether a change is real, or simply a random fluctuation. Control charts were originally devised in the 1930s for quality control in manufacturing (Shewhart 1931). Shewhart control charts are a means of easily seeing when a change is unlikely to be a random fluctuation. Variations in manufacturing dimensions or quality, especially the averages of subsamples, are expected to follow a normal distribution. If an adjustment is made to the manufacturing machinery whenever a component varies in size from its mean value, unnecessary adjustments will be made for what is purely random fluctuation. This will result in a bigger spread of sizes than if the machine had been left unadjusted. The machinery should only be adjusted when the variation in size is such that it is unlikely to have occurred by chance alone.

Time series data are plotted on a graph that shows the mean value and control limits (conventionally, plus and minus three standard deviations from the mean). There is a 99.73% chance a measurement will lie between the mean and plus or minus three standard deviations, i.e. approximately 0.3% chance that such a deviation would occur by chance alone. Significant deviations or out-of-control situations can be identified using several tests. Assuming a stationary normal process that is ‘in

control', the following all have about a 0.27% chance of occurring and therefore can be considered as unlikely to be due to chance alone:

One data point falling outside the three standard deviation control limit;

Six or more points in a row steadily increasing or decreasing;

Eight or more points in a row on one side of the centerline, or

14 or more points alternating up and down.

Operators look for any of these conditions before adjusting the machine.

Control limits can be set at any appropriate level, depending on the application. Broader limits (i.e. higher confidence that an event cannot occur by chance alone) means later warning of a potential problem; narrower limits tend to lead to more false alarms. In risk applications where the information is used to trigger further investigation, false positives may not be a problem so lower limits tend to be set than those in manufacturing. Polonecki (1998) applied control charts to detect poor practice in surgery, and suggested that using limits that represent a 0.01 chance that the event could occur by chance alone is acceptable and appropriate.

Discrete failures and losses are expected to follow a Poisson rather than normal distribution, and to be one-sided (one is seldom interested in a reduction of failures). Control limits for the appropriate confidence levels can be selected for the Poisson distributions. In fact, changing to the Poisson distribution makes little difference to the control limits unless the mean value is low.

An alternative method of detecting change is a CUSUM control chart. CUSUM takes the cumulative sums of differences between the values and the mean. If fluctuations are random, then the cumulative sum will be zero; however, if a set of values are disproportionately above average, the cumulative sum will start to increase and similarly a segment with a downward slope shows that a set of values are below the mean. Some regularly increasing or decreasing values could occur by chance alone. Control limits are therefore set by the rate of increase of the cumulative sum. CUSUM shows small but continuing changes from a mean value more clearly than the traditional Shewhart control chart, so this method is more suitable for detecting small but sustained changes. CUSUM control charts are now commonly used in medical applications to detect changes in performance; for example, in surgery or infection control.

Other methods of plotting and interpreting control charts give additional weight to recent values. Weighting algorithms vary. A common choice is the EWMA (exponentially weighted moving average). This is used in to detect small changes in accuracy or precision.
The reason these methods may be useful for biosecurity applications is because they were invented for application in areas where data are collected routinely and where the staff interpreting the data may have no specialist training. They have proven to be highly successful in a wide range of operational circumstances for many decades (see below). The tools can be tuned to specific operational conditions and their performance will improve over time. The operational conditions in some aspects of border and post-border biosecurity may be suited to such tools. For example, data are collected routinely on failures and non-conformities, and on the prevalence and abundance of pests and diseases during routine surveillance. Correct decisions depend on distinguishing trends and unusual occurrences from background natural variation and sampling variation. The ability to improve the use of these tools, reducing the number of false positives and false negatives, by tuning the decision thresholds, makes them particularly potentially useful.

4.2.1. Syndromic surveillance

Following the terrorist attacks in New York on September 11 2001, there was considerable research activity on statistical analysis of data for early detection of bioterrorism events. The term 'syndromic surveillance' is used and defined as, 'surveillance using health related data that precede diagnosis and signals a sufficient probability of a case or an outbreak to warrant public health response' (CDC 2006). A wide range of statistical techniques is used to detect change, including those discussed above. There is no clear distinction between conventional biosurveillance or medical surveillance techniques and 'syndromic surveillance', but bioterrorism fears following September 11 have resulted in renewed interest in biosurveillance techniques. The recent papers that fall under the category of 'syndromic surveillance' look specifically at:

the nature of data sources that could be used as early warnings of disease;

statistical analysis techniques;

automated statistical 'out of control' detection system, and

the way sets of data can be grouped to categorise 'syndromes'.

The literature suggests that the techniques are of limited use for early detection of bioterrorism, both for cost-benefit reasons and because false positives have a serious negative effect on public confidence. The consensus, however, is that applications for early detection of natural animal diseases are more useful. Here false positives are less of a problem and the methods provide an alert for further investigation (Stoto *et al.* 2004). Both false positives and false negatives in a biosecurity context may have significant social and political costs. The arguments for deployment of syndromic surveillance tools are much the same as those for process control techniques. If the tools are tuned appropriately to the local operational context, they will improve over time, eventually reducing both false positive and false negative decisions. The track record for syndromic surveillance is, however, shorter and the tools are more complex than statistical process control techniques, demanding greater technical skill and more extensive data to develop and implement them.

4.2.2. Applications of control charting and syndromic surveillance

There are a large number of papers looking at the use of control charts in medical applications including their use for the detection of poor quality medical or surgical procedures, for quality in laboratory testing, and for measuring physician productivity (see Polonecki 1998; Lee and McGreevey 2002; Rogers *et al.* 2003; Benneyan 2003; Thor *et al.* 2007). There are also many publications in environmental, security, and veterinary literature on different applications of control charting techniques (see Morrison 2008; Yih *et al.* 2004). Control charts have had wide application in agriculture and farming for quality control, for early detection of emerging trends and to assist with decisions on herd or farm management (see Reneau and Lukas 2006). In animal production, control charts are be used in a number of applications to detect early signals of health problems through monitoring production such as egg sizes, milk yield, pregnancy rates or the number of piglets in a litter (e.g. Thrusfield 2005). Control charts have been used to monitor water conditions in fish farms and soil conditions in agriculture. They can also be used in conjunction with the monitoring carried out in the HACCP process (see Section 5.4; and DAFF 2002); however, this application relates to risk management rather than risk assessment.

Two recent PhD studies of relevance to biosecurity are by Shepherd (2006) and Shaffer (2007). In his PhD thesis from the University of Sydney, Shepherd considers control charting methods for early detection of disease in remote-area cattle stations in Australia. Shaffer (2007), in a PhD thesis for

Ohio State University, demonstrates improved detection of emerging zoonotic diseases from syndromic surveillance of data from veterinary diagnostic laboratories.

Most of the published work relates to surveillance of direct consequences of a threat, or of immediate indicators of problems, and hence is reactive in nature. Generally a change in outcome is measured, and changes in risk factors are then sought to identify the cause. For example, Altekreuse *et al.* (1997) identified an increase in food-borne diseases in the US, then explored the changes that could have caused the observed increases.

It is also feasible to use data more proactively to seek changes in risk factors and to try to anticipate the problems. For example, climate changes may increase (or decrease) the risk of establishment and spread of some pests or weeds. Changes in demographics of visitors to Australia could change the nature of pests and diseases that might enter. To some, extent data is used in this way in some types of scenario analysis discussed below; however, there is room for a more explicit consideration of risk indicators and factors that might be expected to increase risk when data collection protocols are designed.

4.3. Expert data analysis techniques

Expert systems use information and knowledge from a range of different sources, including human experts, to solve problems. The understanding and reasoning processes of experts are stored as data or decision rules within the computer. These rules and data can be called upon to solve problems. The decision rules for problem solving can be acquired by 'machine learning' techniques, or entered explicitly as rules.

4.3.1. Applications of expert data analysis systems

Expert systems have been used for many years for medical diagnosis in remote situations where there is no doctor present. The Dutch Ministry of Agriculture Nature and Food Quality (NLV) funded a research project, which ran from 2004 to 2009, into developing an information management system to identify emerging risks to food safety. The research project focuses on the fish food chain (particularly salmon) as a case study. To demonstrate the capabilities of the technique, Hulzebos and Broekstra (2007) quote an example where, in late-2006, pets in the US became ill and died after consuming a brand of pet food containing wheat sourced from China that was contaminated with Melamine. On 30 March, the FDA blocked the import of products from the Chinese company.

In May 2007, Melamine was found in hatched salmon in Canada. Hulzebos and Broekstra point out that all the information that could have warned salmon producers of the risk was in the public domain within the food safety-related area by the end of March that year. Such information, however, needs to be brought together and sifted and risk alerts provided. The expert system (Emerging Risk Detection System, ERDS) aims to do this. In the Melamine example, the information that the system would locate and highlight would be:

the detection of melamine in wheat from China;

the banned products list from the FAO that showed that the Chinese company supplied wheat as fish meal, and

the fact that salmon are fed fish meal containing wheat.

The project adopts a holistic approach, taking signals and indicators from a wide variety of sources including government, information from experts, and news media. ERDS software processes this information to identify and draw attention to emerging risks. The way that this is done is explained more fully in the 2007 project report (Hulzebos and Broekstra 2007). The project is still at an early stage of development with a prototype ERDS and relatively small data set. It is, however, showing interesting possibilities.

Foresight of the kind that is supported by ERDS is also the provenance of a range of software tools dedicated to the early detection of emerging diseases, pests, and pathogens, some of which include ProMed and GPHIN. These and related tools and platforms are developing rapidly, as are the statistical data mining tools that they employ to find and synthesise relevant information. It is difficult to know which of these tools would be best suited to Australia's biosecurity environment, without some form of empirical evaluation.

4.4. Checklists

Checklists are used universally in risk assessment. They are collated from a combination of experience, data from past losses, and expert opinion to help ensure all important areas are considered when risks are being identified. Checklists may be linear or hierarchical. They are used as an aid to both brainstorming and interview techniques for eliciting information on risks.

In general, checklists used in risk assessment may relate to hazards (or hazard categories) or to events that may occur, or to the types of consequence of interest. For example, Biosecurity Australia (BA) considers risk to each of seven standardised direct and indirect impact criteria in preparing import risk assessments. It also uses a wide range of published information and data sets, including the Australian Plant Pest Database and the Australian National Insect Collection database, to create lists of potential plant pests for new commodities or commodities from new regions. These checklists are then evaluated, species by species, to assess whether each of the pests represents a credible quarantine risk.

4.4.1. Application of check lists

A checklist-based process known as HAZID is used in the chemical and processing industries after the conceptual design stage and before the detailed design stage. A set of guide words are put together, usually based on existing checklists, to use in a workshop to identify the safety problems that must be taken account of in the design. A HAZID workshop for the proposed Gunns pulp mill in Tasmania can be found at http://www.gunnspulpmill.com.au/IIS/V15/V15_A48.pdf. Some of the techniques reviewed later in this paper have a checklist approach to identification within them, such as the key words in a hazard and operability study (HAZOP) (Section 5.3).

Checklists have the advantage of uniformity of approach and they help to ensure common problems are not missed when similar risk assessments need to be carried out (as in the case of BA). Since they are based on past experience, they do not identify new and emerging issues. Checklists need to be regularly reviewed using information from research, expert opinion, or more imaginative identification methods to ensure that they continue to be useful. Checklists of pests of potential quarantine concern are clearly a sensible protocol for evaluating what might cause damage to a country's environment or economy, provided they are relatively complete and up to date. If pest risk assessments, for instance, were to be extended beyond a single commodity and region, to include all

potential pathways of entry, then more creative methods for considering exposure pathways may be warranted.

4.5. Summary of data analysis techniques

To analyse data effectively using conventional statistical means such as control charting, one needs to know what one is looking for in order to select the right data set and analyse it in the right way. Conventional data analysis methods therefore provide a good way of obtaining an early warning that a risk that has been identified is in fact occurring, or that conditions likely to increase the level of risk are arising. Control chart techniques require a string of data points before loss of control can be detected. Thus they often cannot detect a rapid onset risk before it has already escalated. Many outbreaks, such as the FMD and EI examples used to develop hypotheticals in the case studies used in this report, are sudden.

Modern data-mining techniques can automate alerts to loss of control, and could be applied across a wide range of existing data sets to identify changes. Data from public health and environmental areas could be of relevance, as well as data collected through the biosecurity and agricultural systems. The alerts could then be reviewed for possible indicators of new and emerging issues. This is not commonly practised at present, and the majority of applications for data analysis techniques aim to provide early warning of the appearance of known risks. Expert data analysis systems such as that being explored by in the Netherlands also show significant promise as a means of identifying and communicating risks. So far, only a specific biosecurity example has been tested and the utility for biosecurity and quarantine operational conditions would need to be evaluated further.

This section has provided only a very brief introduction to the use of data to identify risks and emerging issues. Burgman (2005) gives a more detailed review of control charting techniques, and discusses their application for environmental risk. More information on the statistics of the techniques can also be found in the ACERA report 0605 by Fox (2007).

5. Process-based methods

5.1. Introduction

Process-based methods take as their starting point a process or procedure and work through it to consider problems that might arise at each step. Methods considered here include Failure Mode and Effect Analysis, (FMEA), Hazard and Operability Studies (HAZOP), and Hazard and Critical Control Point analysis (HACCP). They were developed for different industries and purposes, but all consider each step of a process or procedure and analyse what can go wrong and how to prevent this happening. Each has been adapted for application outside the original purpose for which it was originally designed, and each has been extended to cover processes and procedures as well as equipment. In some adaptations, the distinctions between the techniques have become blurred.

5.2. FMEA

Failure Mode and Effects Analysis (FMEA) was originally developed to identify possible failure modes of equipment to improve equipment reliability in military and aviation applications (MIL STD1629A 1949). It was adopted by NASA in the 1960s, and by the automotive industry in the 1970s. It has been extended to apply to processes and procedures and to include human as well as equipment reliability.

A failure mode is a description of an undesired cause-effect chain of events (MIL-STD-1629A, 1994). It is a statement of what is observed to go wrong (e.g. the car stops).

The effect is the adverse outcome of the observed failure. This may be a chain of consequences (e.g. late for work and miss important meeting and consequently lose contract).

The mechanism is how the failure occurs (e.g. ran out of petrol).

There is a further level of analysis that is not usually part of FMEA that is the causal analysis of the mechanism (e.g. why the car had no petrol). This is investigated by one of the root cause analysis techniques described in the next section. FMEA is carried out by a team of experts who understand the process or equipment, its functions, and how it might fail. The team considers each element of a process or item of equipment in turn and considers its function, its failure modes and mechanisms, the effect of failure, and how failure would be detected before it was too late. Current controls for each failure mechanism are also reviewed. Table 1 shows an example of how information for an FMEA for pumping water might be recorded.

Table 1. Example of FMEA report.

Item	Pump	
Function	What it should do	Pump water at 10^{0C}
Failure mode	What is observed to go wrong	Pump stops (bearing seizes)
Mechanisms	Physical chemical or engineering cause	Contamination in bearing
Failure effect	What is the observed outcome	Overheated process
Detection	How to detect before it is too late	Temperature gauges
Current controls	Provisions in the design for prevention and protection	Sealed bearings, preventative maintenance

The FMEA process can be carried out at different levels. For example, the system as a whole can be considered where the pump is one component. Alternatively, the pump could be taken as the system under review, with the bearing and seal, etc., acting as the components considered. If applied with a high level of detail, the process may miss some system-wide failure modes (Bednarz and Marriott 1988). If applied at a system level, it may miss the opportunity for detailed design improvements. Ideally, FMEA for new equipment would be performed several times from the early design stage to implementation.

FMEA is used to identify potential failures in processes or procedures in a similar way, but instead of considering each component of equipment, each step of a procedure is analysed. Process FMEA usually involves some steps where the failure mode is a human error. As with FMEA based on equipment, the error mode and mechanism must be identified rather than possible causes. The error mode is what is observed to be done wrong and the mechanism is how it occurs. Causes of error modes (such as distraction or lack of training) are not identified in FMEA. In general, FMEA is a time-consuming process and not often practicable to implement on a routine basis. Its main application is to test newly developed equipment and procedures, especially those for which there are very significant costs of failure and exposure pathways may be complex. Biosecurity includes many such contexts.

5.2.1.FMECA

When a large number of failure modes are identified, a criticality rating may be added. The technique is then known as Failure Mode and Effect and Criticality Analysis (FMECA). The criticality analysis rates the different failure modes according to their importance, so the most important failure modes are addressed first. It may be qualitative, semi-quantitative, or quantitative.

There are a number of different ways criticality can be defined. Common methods are:

mode criticality;

risk level, and

risk priority number.

The mode criticality index relates the criticality to the probability that the particular failure mode will result in failure of the system. The same end-point (failure of the system as a whole) applies to

each mode so consequence is not taken into account in this method of defining criticality. Mode criticality is defined as:

Failure Effect Probability * Mode Failure Rate * Operating Time of the System

This method of defining criticality is most often applied to equipment failures where each of these terms can be defined quantitatively.

The risk level is obtained by combining the consequences if a failure mode occurs with the probability of the failure. It is used when consequences of different failure modes differ. Risk level can be expressed qualitatively, semi-quantitatively, or quantitatively.

Quantitative analysis uses measured failure rates and a measure of the failure consequences (often in dollars). In semi-quantitative analysis, a criticality matrix is used that has the scales defined in numerical terms that represent orders of magnitude for severity of consequence and probability of failure. Figure 3 shows a typical criticality matrix. The horizontal axis may be defined in dollars (with each scale point increasing by an order of magnitude), or on a qualitative scale defining importance to a mission or injury and death. The vertical axis defines probability or frequency of failure.

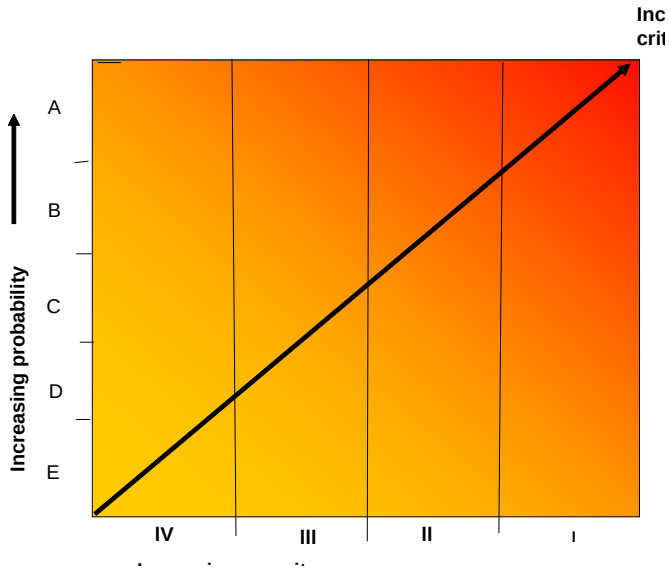

Figure 3. Example of a criticality matrix (Mil std 1629A 1980).

The third method of criticality analysis allocates a **Risk Priority Number (RPN)** to each failure mode. This is obtained by multiplying numbers from rating scales between one and 10 for consequence of failure, likelihood of failure, and ability to detect the problem. A failure is given a higher priority if it is difficult to detect. This method is used most often in quality assurance applications, and was used by Hayes (2002c) looking at infection failure modes from ballast water.

5.2.2. Applications of FMEA

FMEA can be applied to functions and systems, component or subcomponents, processes, and the provision of services and software. In addition to its use in reliability, it is commonly applied to quality control (particularly in the automotive industry), and for identifying and preventing adverse events in medicine.

An example of FMEA applied to a process relevant to biosecurity is given in Table 2, which considers a step in the National Livestock Identification System (NLIS) tracing process. The example shows one mode and mechanism where the tracing system could fail. The details are taken from an actual failure reported on the NSW Department of Primary Industry website (DPI NSW 2008).

Table 2. Example of process FMEA applied to animal tracing system.

Process step	**Description of step**	**Attach tag to ear of cattle**
Function	What it should do	Identify cattle place of origin year and tag manufacturer
Failure mode	What is observed to go wrong	Tag from wrong property fitted
Mechanisms	Direct cause	Left over tags from interstate property
Failure effect	What is the observed outcome	Potential for diseased animal not to be traced
Detection method	How you could you detect it before it is too late	Automatic check in database for Property Identification Code versus stated origin
Current controls	What provisions are there in the design for prevention and protection	

Another step of a tracing process is entering data in a computer: some error modes here may include data missed or incorrect numbers entered. The error mechanisms may be losing place in a list or a typing error. There are many possible causes for these mechanisms occurring and superficial causal analysis may be counterproductive. Therefore causes are normally not included in FMEA, and a root cause analysis or other causal analysis technique is carried out for those failures that are identified by a criticality analysis to be either high impact, high probability, or high risk. Causes of error such as lack of experience or distraction should not be entered in an FMEA table. A taxonomy of error modes and mechanisms that can be used as a checklist is discussed in Section 7.3.

5.2.3. HFMEA –application of FMEA in healthcare

Traditionally, the healthcare industry has taken a quality control approach to patient safety assuming that procedures can be defined to prevent adverse events, and quality control systems can assure that procedures are followed. A number of highly publicised failures demonstrate that this approach is not working well, and healthcare managers are increasingly using formal risk assessment techniques to identify potential failure modes and to define controls that are not so heavily reliant on people following correct procedures.

The Joint Commission for the Accreditation of Healthcare Organizations (JCAHO) in the US requires hospitals to carry out a proactive risk assessment on at least one high-risk activity each year for each accredited program. Healthcare FMEA (HFMEA) was pioneered by the US Department of Veteran

Affairs as a suitable technique for fulfilling this requirement (McDonough 2002; Derosier *et al.* 2002; Stalhandske *et al.* 2003). Details and training materials are available on the department's website (Department of Veterans Affairs 2008).

Some of the healthcare examples demonstrate clear applicability to animal as well as human health issues. For example, FMEA was used at a Rhode Island hospital to improve surveillance in the process of admission screening of high-risk patients. Only an abstract has been published thus far, but the authors concluded that not only was the process useful for gaining a better understanding of possible failures of a complex screening process, but it also facilitated communication among the various departments and resulted in creative and sustainable solutions (Monti *et al.* 2005).

There is now a large number of published practical applications of HFMEA internationally, particularly in the US where it is a legislated requirement, but also in other countries, because it has been found to be useful in prevention of adverse events. Many of the applications in healthcare relate to processes and procedures and to quality assurance of processes. Table 3 provides a few examples from different countries.

In Australia, HFMEA is mentioned on clinical risk websites of health departments in a number of states, but there is no legislated requirement for formal risk assessment for accreditation and there do not appear to be any published practical examples of its application in Australian hospitals.

5.2.4. Application of FMEA in biosecurity

FMEA has not been widely applied in the agriculture or biosecurity fields. Hayes (2002c) applied the basic FMEA technique to investigate the potential spread of marine organisms from small boats. The study started by identifying all the components of boats that could be infected, then identified the infection modes. These were then given a risk priority number by combining environmental suitability, likelihood of occurrence of infection, and likelihood of detection. Each was allocated points on a 10-point scale that were then multiplied to give a risk priority number. This technique was called Infection Mode and Effect Analysis.

DEFRA and the Environmental Agency in the UK used FMEA to assess the reliability of flood and coastal defences in the UK. This area falls under DEFRA's environmental rather than biosecurity responsibilities (Buijs 2007).

5.2.5. Strengths and limitations of FMEA

Strengths
The method is reasonably intuitive and can be applied with little training. It can therefore provide a useful format for brainstorming and stakeholder involvement in identifying how equipment, procedures, or controls for risk can fail. It can be applied at a systems level or a detailed level as appropriate. It is very thorough and identifies a large number of possible failure modes. The format demonstrates the thoroughness of the technique, providing evidence for audit or other purposes. It considers explicitly where monitoring is critical for early detection of failure.

Limitations
FMEA can be costly in person-hours unless the number of components or process steps it is necessary to analyse, or the number of failure modes of each step, is relatively limited in number. It can thus become impractical for analysing a process with a large number of steps where human

failure modes and mechanisms are involved, unless the magnitude of the potential consequences justifies the expenditure.

It is useful for analysing failure modes of equipment, of current controls for known risks, and for processes that are relatively simple.

Successful FMEA depends on the knowledge of failure modes of the experts in the team. The method does not seek to identify new modes and mechanisms of failure; instead it draws attention to weaknesses and the susceptibility to known failure modes (Leveson 1995).

FMEA identifies single point failures. It will not identify failures that require multiple coexisting faults, or where system failure is due to the poor quality of a number of elements rather than failure of any single one. In biosecurity contexts, its main utility may lie in reassessing existing operational procedures, to identify weaknesses, and anticipate faults. It may also be useful to improve understanding of the relative importance of various steps in complex exposure pathways for pest risk assessments.

5.3. HAZOP

A Hazard and Operability study (HAZOP) aims to identify pathways by which failures in a process can occur resulting in either physical harm or inefficiencies. HAZOP was developed by ICI with the first comprehensive guides to its use published in the mid-1970s (Chemical Industries Association 1977). HAZOP is usually carried out at the detailed design stage of a process plant or a change to process plant with the aim of improving process design. HAZOP starts with the flow and control diagrams that represent the intention for the construction and operation of the plant or process. The following steps are then carried out:

Each section of the diagram representing the plant or process is considered to define the intention of the section and any specified conditions needed to achieve it.

Key words are applied to each intent and condition to seek possible deviations from design intentions.

The deviations are considered to decide whether they are important and if so, possible mechanisms and actions are recorded.

Table 3. Examples of HFMEA published in the scientific literature.

Wetterneck TB, Skibinski K, Schroederx M, Roberts TL and Carayon P	US	Human Factors and Ergonomics Society Annual Meeting Proceedings, Medical Systems and Rehabilitation, pp. 1708-1712 (5).	Challenges with the Performance of Failure Mode and Effects Analysis in Healthcare Organizations: An IV Medication Administration HFMEA.
Kimchi-Woods J and Shultz JP	2006 US	Joint Commission Journal on Quality and Patient Safety **32** (7), 373-381.	Using HFMEA to assess potential for patient harm from tubing misconnections.
Linkin DR, Sausman C, Lilly S, Lyons C, Fox, Aumiller L, Esterhai J, Pittman B and Lautenbach E	2005 US	Clinical Infectious Diseases **41,** 1014–1019.	Applicability of Healthcare Failure Mode and Effects Analysis to Healthcare Epidemiology: Evaluation of the Sterilisation and Use of Surgical Instruments.
Esmail, Cummings, Dersch, Duchscherer, Glowewr, Ligett, Hulme	2005 Canada	Health Care Quarterly **8,** 73-80.	Using HFMEA Tool to review the process of ordering and administering potassium chloride and potassium phosphate.
Ouellette-Piazzo K, Asfaw B and Cowen J	US 2007	Radiology Management **29**(1) 36-44.	Healthcare failure mode effect analysis (HFMEA): the misadministration of IV contrast in outpatients.
Greenall J, Walsh D and Wichman K	2007 Canada	Canadian Pharmacists Journal **140**(3) http://www.pharmacists.ca/content/cpjpdfs/may_jun07/SafetyFirst.pdf	Failure mode and effects analysis: a tool for identifying risk in community pharmacies.
Gilchrist M, Franklin B, Patel D and Jignesh P	UK 2008	Journal of Antimicrobial Chemotherapy **62**(1),177-183.	An outpatient parenteral antibiotic therapy (OPAT) map to identify risks associated with an OPAT service.
Day S, Dalto J, Ox J, Allen A and Listrup S	US 2007	Quality Management in Health Care **16**(4), 342-348.	Use of failure mode effects analysis in trauma patient registration.
Federici A, Consolante CA, Barca A, Baiocchi D, Borgia P, Marzolini L and Guasticchi G.	Italy 2006	Annale di Igiene **18**(6), 467-79.	Risk management in a regional screening program for breast cancer in Lazio, Italy.

Key words seek to prompt thinking through recall of experience and intuitions among participants. Words may be varied to suit the circumstances, but are generic words for deviations such as ‘none’, ‘too little’, ‘too much’, ‘reverse of’, ‘other than’, etc.

The HAZOP process can be illustrated by considering an example in the processing of carcasses in an abattoir. One step in the process is washing the carcasses. The design intent is to decontaminate the carcass. The conditions for successful cleaning are a certain flow of water and temperature of water. Applying HAZOP, each key word is applied to each condition. For example, what if the temperature was too hot? The team considers whether this would matter, what would cause it, and how it would be detected, then moves on to the next condition. What if there was no water flow, or too much, or too little? What if something other than water flows? The questions asked are: how could this happen? What would be the effect? Would it matter, and how would we know?

The essential distinguishing feature of HAZOP is that it looks at possible deviations in design intent and operating conditions, and works back to identify failure mechanisms. In contrast, FMEA starts from failure modes and mechanisms and works forward to identify effects. HAZOP identifies where problems could enter the system as a result of a failure in the internal process. It suggests where monitoring is required to recognise these problems, and it looks at failures that could result in decreased efficiency as well as safety issues.

HAZOP does not specifically address the nature of the hazard being controlled or how it might enter the system. Continuing with the example of carcass washing, HAZOP does not attempt to identify the range of pathogens that might arrive with the animal, or consider the design of the abattoir’s system to control them. The HAZOP process assumes that this had been identified in a process of Preliminary Hazard Analysis (PHA), and that the process design had been intended to address these hazards. It would then seek to identify how the design could fail.

5.3.1. Application of HAZOP

HAZOP was originally developed to identify potential safety and operational problems in the design of processing plant and equipment where this form of design verification provides considerable cost savings in the commissioning phase. It is used both for initial design review, and when changes need to be made to operating process plant. HAZOP can also be applied to equipment where FMEA would be the more conventional technique. For example, the IEC standard on HAZOP provides an example of an application to an automatic train protection system (IEC 2001). HAZOP has been applied to computer software where the process is known as CHAZOP (Kletz *et al.* 1995), and is increasingly applied to procedures as well as equipment. SCHAZOP, an application of HAZOP to management systems and safety culture, is discussed under human error analysis methods in Section 7.2.

5.3.2. Applications of HAZOP in biosecurity, farming, and food safety applications

HAZOP was developed for processes in the chemical and processing industries but applies to anything that can be divided into elements for each of which a functional output or design intent can be defined.

Some of the applications published as HAZOP differ significantly from the original intent of the process. Mayers and Kilby (1988), looking at a food safety application, started by identifying hazards rather than the outcomes of failure. The process they followed would be known in the chemical industry as HAZID rather than HAZOP, as it starts with a generic checklist of hazards rather than deviation words to prompt 'what if' thinking about design intent.

Table 4 shows the factors considered at each step of the process by Mayers and Kilby (1988). The approach is quite different from the keyword approach of HAZOP, where simple deviation key words are applied to required conditions and outcomes.

Table 4. HAZOP analysis property words (Mayers and Kilby 1988).

Microbiological hazards

- Factors affecting change in microbial numbers: raw materials and product formulation and composition, time, temperature.
- Factors affecting contamination: people, process equipment, environment, packaging materials.
- Compliance with legislation and standards: international, national, trading standards, in-house standards.

Foreign body hazards

- Factors affecting contamination: origin, pre-treatment, processing and storage of raw materials and product, people, process equipment, environment.
- Compliance with legislation and standards.

Chemical hazards

- Factors affecting contamination: origin, pre-treatment processing, and storage of raw materials and product; non food-grade materials, processing.
- Compliance with legislation and standards.

Product quality hazards

- Factors affecting product taste, odour, texture and appearance: product formulation, structure, storage, processing; microbial and chemical contamination; chemical reactivity.

Some of the literature describing applications of HAZOP uses the key word approach but misses the other main distinguishing feature of HAZOP; i.e. that it starts with the observed deviation from what is intended and then moves on to consider cause. For example, Hayes (1998) applied HAZOP guide words to a review of controls for ecological risks of ballast water. The starting point was a list of ballast water and sediment management control options from Carlton *et al.* (1995). The deviation guide words were applied to each control. For example, one control is biocide addition. The analysis explores the cause and effect of too much biocide, too little, addition too slow, addition too fast, and other than biocide, then moves on to the next control.

The way guide words are used in this application differs from conventional HAZOP in that they are used to identify failure modes of controls rather than failures in the intended outcome and conditions. A conventional HAZOP would identify the intention of the addition (i.e. kill biological organisms), then consider more organisms killed, not all organisms killed, other than the intended organisms killed, and so on. The Hayes example (which is probably more useful than traditional HAZOP in the context) is more accurately considered to be a guide word FMEA. As with any method based on analysis of control failures, it is presupposed that the controls are appropriate to the risks. When applied to controls, it will identify the result of a control failure but does not identify new issues requiring new controls.

5.3.3. Application of HAZOP to genetically modified organisms

An attempt to adapt HAZOP to identify risks associated with the introduction of genetically modified organisms (GMOs) was made in the UK in the early 1990s. The Royal Commission into Environmental Pollution set up a high-level working party of experts in genetic modification and in the use of HAZOP to see if HAZOP could be adapted to assess risks of development and introduction of GMOs. It was intended that the method would be used by those required to assess applications to release GMOs.

A report was published in 1991 describing the adaptation, called GENHAZ (HMSO 1991). The efficacy of the method was demonstrated in an application to a hypothetical modification of a potato by insertion of a gene coding for an imaginary protein TP in leaves of the plant, which was toxic to a specific caterpillar pest.

In chemical applications, HAZOP starts with the line diagram of the process plant and first identifies the intention of each component. The working group found no obvious equivalent to a process plant line diagram that could be used as the basis of identifying intentions and conditions. They recommended instead considering each step of the process of modification and release, and also the components of a GMO (components being the construct, the recipient or host, and the product).

In the case of GMOs, the intentions of the steps and the components of a GMO are rather more complex than their chemical plant equivalents. Therefore a questionnaire was developed to help users identify the intentions to which guide words would be applied. For example, one question in the construct section of the questionnaire is, ‘what is the source of nucleic acid to be modified?’ The answer will identify the donor. Application of keywords leads to discussion of the possibility of transferring none, part of, more of, or the wrong part of the donor’s nucleic acid. As with HAZOP, in the GENHAZ method, consequences, causes, and actions needed are recorded before proceeding to the next question in the questionnaire.

The Commission recommended that the Government, with the assistance of the Advisory Committee on Releases to the Environment (ACRE), should arrange for full trials on real rather than hypothetical examples, then consider whether to integrate GENHAZ into procedures for the assessment of GMO releases. Full trials were carried out, and in 1994 DEFRA published a research report entitled, ‘An Evaluation of GENHAZ as a Risk Assessment System for Proposals to Release Genetically Modified Organisms into the Environment’.

Before its release at the end of 1993, the Royal Commission received a draft report and commented:

> *We are concerned that the essential purpose of GENHAZ, and the Commission's views about it, may not have been fully appreciated. It appears from this response that the method was criticized on the grounds of not being quantitative. This may have arisen because the analogy with the HAZOP system used in the chemical industry has been pushed too far. The Commission is very well aware of the complexities of the natural environment, and the purpose of GENHAZ was not (as the Government's response implies) to produce quantified results of the kind produced by HAZOP. We agree that appraisal of proposals to release genetically modified organisms into the environment requires a qualitative approach. In view of the difficulty and unfamiliarity of problems*

> *raised in many cases, the aim of our recommendation was to create a structure which will make those responsible for appraisal approach such problems in an interdisciplinary way and employ lateral thinking to identify unfamiliar interactions (RCEP 1993).*

HAZOP is not in fact a quantitative technique and neither is there any suggestion of quantification in the 1991 report, so it appears that the intent of GENHAZ was misunderstood by those reviewing it. GENHAZ appears in more recent UK Government documents only to be noted as a report that sold very few copies. It therefore appears that in spite of a strong recommendation from an expert panel, the method was not adopted. In Australia there is reference in Hansard in answer to a Parliamentary Question to GENHAZ as one possible risk assessment technique for the introduction of GMOs, but no reference to its actual use in Australia could be found.

Like HAZOP, GENHAZ requires a substantial amount of work involving multiple half-day workshops of a team of people. Like HAZOP, it provides a great deal of detail on possible failures and a long list of actions to minimise them. There are, however, a number of major differences between HAZOP, as it is applied in the chemical and process industries, and GENHAZ that might account for the apparently low uptake of the method.

- The checklist-of-questions approach to identifying intentions as the starting point in GENHAZ is a much more complex starting point than a line diagram of a process plant that will exist for other purposes. A questionnaire is likely to be necessary for other biological applications and would have to be designed differently to suit each application. This would require significant work from a team that includes experts in the biological application and in HAZOP.
- HAZOP is demonstrably cost effective in the chemical industry because it identifies problems at the design drawing stage prior to the process plant being built. Changes made at this stage are very substantially cheaper than changes made when a hazard or an operability problem is found during commissioning or operation. There is no obviously equivalent operational cost saving from carrying out GENHAZ.
- HAZOP has become regarded as essential good practice for management of change in chemical and process plant. Failure to undertake HAZOP is considered to be a failure in management in the event of an incident and inquiry; i.e. HAZOP has become an expectation of the Courts (Dawson and Brooks 1999). There is no regulatory driver of GENHAZ.
- The state of knowledge on GMO is such that when consideration of a key word raises a question, the answer may not be known. Many of the actions in the case study example in the 1991 report were in fact questions requiring further research. This is not useful at the stage of the project where approval is being sought, which is generally after the research phase.
- HAZOP is applied in the chemical industry when there is a reasonable expectation that failure would bring significant harm to the community. Application of HAZOP is a demonstration that everything reasonably practicable has been done to prevent this. This scenario has not clearly arisen in the context of GMOs.

GENHAZ was intended to be a tool for those who must assess applications for release of GMO, and was apparently rejected for that application. It might still find application in other contexts, however. The only successful application of GENHAZ that could be found in the literature was that reported by Williams (2000) in Australia to consider the risks of introducing genetically modified organisms to control mice. Although GENHAZ and HAZOP have not found application

in practice, the guide word approach to considering deviations from the expected is a useful concept that can be applied outside the full HAZOP process as demonstrated by Hayes. The GENHAZ experience is an important lesson in the sensitivity of adoption of a method to the local nuances of a decision problem. Many biosecurity questions would have much in common with the GENHAZ context (different opinions regarding consequences, poor understanding of cause and effect, lack of regulatory motivation). Some routine operations in the biosecurity continuum may fit the 'chemical plant' model closely, and may benefit from its application.

5.3.4. Strengths and limitations of HAZOP

HAZOP and FMEA produce basically the same type of information; however, whereas FMEA can be applied equally at a system, block diagram or component level, HAZOP applies to a detailed design where the design intent of each element or component can be defined. HAZOP is less intuitive than FMEA because it starts from the unwanted outcome and works backwards, rather than starting from known failure modes. This direction of thinking does, however, allow unwanted outcomes due to multiple component failures, or interfaces between components, to be identified (which is a weakness of FMEA). The requirement to seek failure modes for all possible deviations to the design intent may identify new failure modes not within the direct experience of the team.

HAZOP, like FMEA, is thorough and detailed but very time-consuming. When it is applied at the design stage of processing equipment, it has proved to be cost-effective because it identifies design problems before the plant is built and change becomes expensive. Making changes to procedures is less costly than redesigning plant, so the cost-benefit of HAZOP in this application is less clear. HAZOP is therefore likely to be of most value in identifying risks in processing plant or in computer software systems and for procedures where consequences of failure are extremely high warranting a detailed understanding of what failures can occur.

HAZOP has two defining features. One is diagnosing failure modes by first thinking about unwanted outcomes (rather than the other way round), and the use of guide words for deviations. These two features can also be used independently of each other. For example, deviation guide words are useful for identifying human error modes for Human Reliability Analysis or in FMEA. Causal analysis techniques, such as Fault Tree Analysis (Section 6.2) essentially start with a failure and work back to failure modes.

HAZOP is applicable when a line diagram can be drawn through elements of a process to provide the structure for identifying problems. This diagram may represent a physical process or a procedure. Adaptation to applications where simple elements cannot be identified (such as demonstrated in GENHAZ) is complex.

5.4. HACCP

The Hazard Analysis and Critical Control Point (HACCP) method was first proposed at the 1971 National Conference on Food Protection (APHA 1972). It was initially designed as a quality assurance tool by NASA for food to be used in spacecraft. It was applied to minimise food safety risks in food processing plants, and its application rapidly extended to catering establishments (see Bryan *et al.* 1980). In 1993 HACCP was adopted by the FAO/WHO Codex Alimentarius Commission.

HACCP is mandated in many countries, usually commencing when the farm output begins to be processed into food. For example, in the US the Department of Agriculture established HACCP requirements for meat and poultry establishments in 1996. Similar HACCP requirements for seafood were required in 1997 and for juice in 2002 (USDA 2008). In the US, HACCP is not required on- farm, and the regulation begins at the point of processing,

The EU and some other countries also mandate HACCP for animal feed production. The EU requires that food and feed business operators must monitor the safety of products and processes under their responsibility, follow general hygiene provisions for primary production, develop HACCP principles, and register establishments with the appropriate competent authorities. Again, HACCP is not required for primary producers. Australia also has mandated requirements for HACCP for food processing but not for on-farm processes except for industries such as dairy, where a level of food processing occurs on farm.

The HACCP process consists of five preliminary steps and seven principles (WHO 1997). The preliminary steps are:

assemble HACCP team;

describe the food and its distribution;

describe the intended use and consumers of the food;

develop a flow diagram that describes the process; and

verify the flow diagram.

The main HACCP procedure is defined in seven principles.

Principle 1: Conduct a hazard analysis.

In the food context, this involves identifying relevant physical, chemical, and biological contaminants of the food. Guidelines vary in the amount of detail they give for how the hazard analysis is done. In some cases, brainstorming with a checklist is advised. Others recommend a detailed consideration of each input to the process at each step of the process, and the movement of people to identify what hazards could enter the process (Canadian Food Inspection Agency 2008).

Principle 2: Determine the critical control points (CCPs).

This involves reviewing each step of the process to see if it is a CCP. A point in the process will be a CCP if:

it is associated with the hazard being considered;

reduction and control of the hazard is possible at this step;

measurement (of the condition or the hazard) is possible, and

control at this step is necessary to reduce risks to the consumer.

Figure 4 shows a decision tree for identifying CCPs.

Principle 3: Establish critical limit(s) for measurable parameters at the CCP.

Principle 4: Establish a system to monitor control of parameters at the CCP.

Principle 5: Establish the corrective action to be taken when monitoring indicates that a particular CCP is not under control.

Principle 6: Establish procedures for verification to confirm that the HACCP system is working effectively.

Principle 7: Establish documentation concerning all procedures and records appropriate to these principles and their application.

HACCP is a technique for controlling hazards and identifying early warning signs that indicate deviations from the operating conditions required to maintain food quality and safety. Hazards are identified as one step of HACCP, but the focus is on control monitoring and quality assurance.

HACCP does not necessarily consider in detail how hazards (physical, chemical, or microbiological) can enter the process, but rather where hazards can be detected and controlled. HACCP also does not consider specifically the effect of deviations in the process, or human and equipment failures although these may be recognised during the hazard analysis stage. Often in food processing, the presence of a pathogen may be beyond the direct control of the organisation. For example, it may be present in the raw ingredient or in the air or water. The food processing company's role is to detect it in the process and remove it. In order to undertake a HACCP study,

there must be a clearly defined process;

hazards or sources of harm must be able to be readily identified;

it must be possible to apply means of destroying the hazard. (e.g. it must be possible to destroy bacteria without damaging meat), and

success of the control must be able to be monitored.

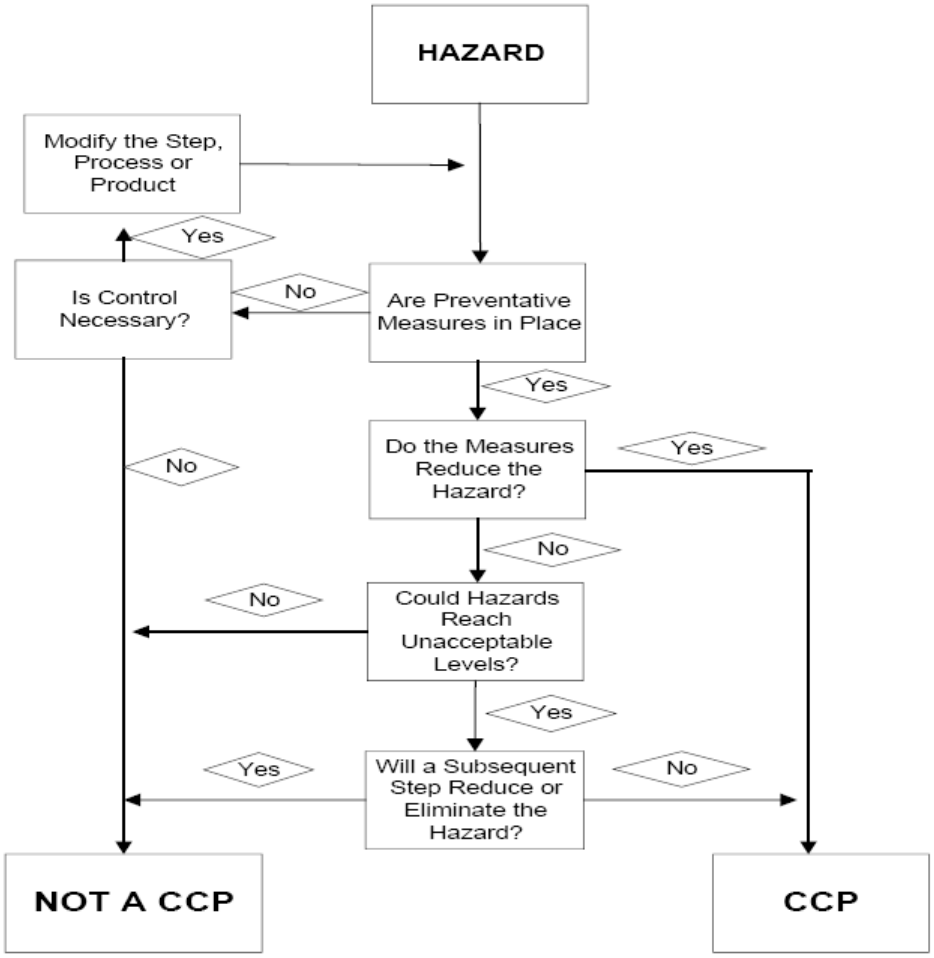

Figure 4. Critical Control Point Decision Tree.

5.4.1. Applications of HACCP

HACCP is generally applied in the food industry where the food can be described as a product being processed. Some products (e.g. minimally processed vegetables) do not lend themselves to a HACCP approach.

Over the past few years, there has been discussion of the application of HACCP throughout the process 'from farm to table'. The Food Safety Inspection Service of the US Department of Agriculture was urging the use of HACCP at farm level in 1997. Since that time, there has been considerable discussion on its practicality. For farms where the on-farm procedures can be considered a food process, such as dairy, HACCP is clearly applicable. All dairy companies in Australia require their suppliers to implement on-farm HACCP-based quality assurance programs (Dairy Australia 2008).

For industries that are less process based, it is less clear that it is the most effective approach. Sperber (2005) suggests that HACCP does not work at farm level because there is a lack of definitive CCPs. He suggests that Salmonella outbreaks and other food-borne diseases still occur, often through poor hygiene or control practices, and that HACCP must be supplemented with good agricultural practice (GAP) and management awareness of sources of risk and controls. Horchner *et al.* (2006), from the Australian Meat Industry, suggest HACCP works, but is complex and difficult for farmers to apply. They also argue that codes such as GAP are as effective at maintaining quality as application of HACCP. On the other hand, Baines *et al.* (2004) evaluated the extent to which farm-level quality assurance programs addressed on-farm microbiological risks and concluded that there was a missing link in managing food safety risks in the supply chain that could be bridged by applying HACCP on the farm.

The decision rules for identifying CCPs suggest that a step is not a CCP if a subsequent step in the production process is able to eliminate the hazard, or reduce its likely occurrence to an acceptable level. This has been interpreted as implying that a hazard should be controlled at one control point only, and hence if it can be controlled at the food processing stages, control points within a farm are not CCPs. Heggum (2004) argues for HACCP on the farm and points out that if the farm output is taken as the end-point of the process, rather than the food for human consumption, then on-farm control points can be CCPs.

Heggum (2004) recognises the difficulties of applying traditional HACCP at the farm level, but suggests that the HACCP principles can be applied in the development of practical codes of good practices (where the authors of the code act as the 'HACCP team'). The outcomes of the HACCP study are then a list of practical measures and routines similar to traditional codes of practice. He also provides a detailed demonstration of HACCP to the production of animal feed. This is shown in Table 5.

An early attempt was made to apply HACCP at farm level to reduce salmonellosis in pigs (Simonsen *et al.* 1987). Their method has a simplified diagram of pig production, considers external inputs and interactions at each stage, and identifies where the pathogen can enter the system and how to prevent its entry. A more detailed study that used HACCP to develop codes of practice for biosecurity in the Australian egg industry was carried out by Grimes and Jackson (2001). This application is interesting in that the hazards are not food safety hazards but pests and diseases that might affect poultry health. The HACCP analysis starts with a flow chart of the procedures carried out in egg production, starting from shed set-up and chick placement to the end of laying, hen removal and shed clean-up. The central steps of pullet growing and egg laying involve a number of activities that will be carried out routinely, rather than sequentially as in most food processing applications. These are listed as sub-steps.

The inputs at the steps that could have the potential to introduce hazards (such as chicks, feed, water, wild birds, etc.) are listed. This flow-charting step is more complex than in traditional applications of HACCP. Hazards (i.e. pests and diseases) are identified, together with how they are controlled. Hazards are mostly identified by research and knowledge, as is common practice in biosecurity risk assessments. The list of inputs is then reviewed to identify how hazards might enter the system.

Table 5. Application of HACCP to industrial feed (Heggum 2004).

Step	Title of step	Specific considerations
1	Assemble HACCP team	Must be multidisciplinary, including expertise in practical farming and animal physiology, and veterinary matters (including veterinary medicine).
2	Describe feed	Description must include sufficient data and information to identify and evaluate occurrence of any potential hazards; e.g. chemical, physical and biological characteristics of the feed, ingredients used, their source(s), end-product composition and physical/chemical structure, any treatments used that affect hazard levels (e.g. heat treatment), packaging, durability and storage conditions and method of distribution.
3	Identify intended use	Expected use for the end user (farmer), natural variation in transfer rates between species, individual animals, intended/typical amount (doses).
4	Construct flow diagram	Should cover all steps in the operation for a specific product, including interactions, rework and recycling, and should cover detail to a degree that enables the identification of where additional hazards may occur or increase in level, and show the sequence of steps.
5	Confirm flow diagram on site	Check whether the flow diagram is constructed in conformity with practical operation during all stages and hours.
6a	List all potential hazards	Those relevant for food safety that may be expected to occur during the whole feed chain, using the information gathered in Steps 2–4.
6b	Conduct a hazard analysis	Identify for the HACCP plan which of the hazards need be eliminated or reduced to acceptable levels to meet end-product requirements and targets that will enable the production of a safe food derived from the animal to which the feed will be administered.
6c	Consideration of control measures	To determine those that are available and can control each hazard to the level required.
7	Determine CCPs	To be done at processing steps that have a significant impact on the presence of the hazard, taking into account the performance needed to achieve the required outcome.
8	Critical limits for each CCP	To define when a CCP is functioning correctly.
9	Monitoring system	Determination of the scheduled measurements or observations of the CCPs required, relative to critical limits, needed to evaluate the correct functioning of the CCPs.
10	Corrective actions	Predetermination of actions, when critical limits are exceeded; i.e. actions that bring CCPs back into control, and actions that ensure the proper disposition of affected feed.
11	Verification procedures	Methods, procedures and tests to determine if HACCP is working correctly (includes audits and sampling/ testing, but also other means).
12	Documentation and record keeping	The information needed to demonstrate that the HACCP controls are in place and are being maintained. Includes the rationales for excluding any potentially significant hazards from control, how CCPs and critical limits have been determined, and validation of results. Records include the monitoring results, the corrective actions taken, and the verification of results.

The critical control-point decision tree is then applied to each step of the process outlined in the flow chart define where the controls should be applied and monitored. This process is used to define the required controls. Grimes and Jackson (2001) list good management practices derived from the application of HACCP to egg production.

This procedure could be followed for biosecurity in other industries, and the model produced by the egg industry provides a useful template, illustrating the difficulties of turning the less structured activities of general farming into a flow chart of processes with defined inputs. However, may mean that it may be more suitably applied at an industry level to produce generic guidelines rather than being applied at the individual farm level.

In summary, it appears that the literature indicates that where on-farm activities are structured and can be considered a process (such as in the dairy or seafood industry), HACCP is useful at the individual farm level. In less structured farming such as in the meat industry, HACCP appears to be of most use once processing starts (i.e. at the abattoirs) and on-farm practices may be controlled by an established set of quality control procedures such as GAP. These quality control procedures and risk controls may be defined by a generic HACCP applied at industry level.

5.4.2 Strengths and weaknesses of HACCP

HACCP is primarily a quality control technique. Whereas HAZOP and FMEA aim to identify in advance the many different ways the process might fail, HACCP concentrates on identifying and monitoring parameters that demonstrate the process is working correctly. Hazards are identified as part of the process of defining the control points that will be monitored and the critical safe levels, but the technique does not aim to provide detail of how the process might fail. HACCP can be applied both to processing plant and to procedures. In the former case, the parameters monitored at CCPs are physical parameters such as temperature. In the latter, the CCPs identify points in a set of procedures where controls must exist and be monitored, but the controls may themselves be procedures.

HACCP monitors systems that are already operating rather than being a design check as are FMEA and HAZOP. HACCP may be useful in areas of biosecurity concerned with systems management. For example, when assessing the possibility of substituting one management system (or set of quarantine measures) for another, HACCP may provide a useful framework for evaluating system equivalence and the potential for failures in the candidate system.

5.5. Application of process techniques to biosecurity case studies

Importation can clearly be defined as a process. At a generic level, the process involves removal of animals from aircraft, transportation to the quarantine station, and care at the station. Care at the station may involve separate steps such as visits by veterinary officers, grooming and cleaning out, etc.

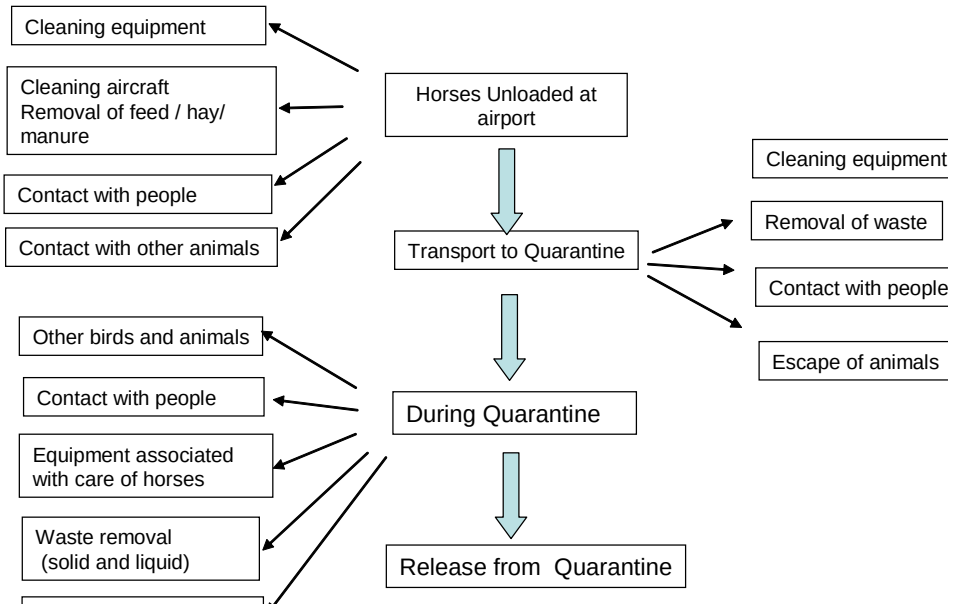

Figure 5. Possible process steps and outputs for horse imports.

If process techniques are detailed and time-consuming, the most appropriate and practical approach to reviewing the importation process for weaknesses would be to look initially at the system generically (i.e. without specifying particular diseases or animals). This would identify potential weaknesses of the system as a whole. Subsequent studies could be applied to selected animals or animal groups regarded as high risk or that present different challenges. Application of process-based identification techniques to the example of quarantine demonstrates how techniques often need to be combined and adapted to particular circumstances. This following section outlines such a hypothetical application.

5.5.1 Application of HACCP to hypothetical EI case study

Application of HACCP to quarantine is similar to the egg producers' demonstration of HACCP in that there are some time-sequenced steps, but other activities are ongoing routine occurrences., However, in quarantine the concern is with a hazard escaping from the process rather than being generated from within the process or entering from outside. Thus rather than identifying inputs at each step, one needs to identify outputs; that is, those people and things that leave the process.

Figure 5 illustrates some steps in the import process and related outputs. The central set of boxes represents steps followed in processing horses on entry to the country. The arrows point to the things that are removed at each step that could be potential pathways of disease. In practice, the 'during quarantine' step would be divided into sub-steps that could result in more exit pathways being identified.

Controls can then be defined to prevent pest and disease movement through the identified pathways. This will produce a list of physical controls and procedures against which current procedures could be checked, both for whether they exist and whether they are applied. It may also identify existing procedures that are no longer useful.

There is no need to separate critical from non-CCPs on the basis of the CCP decision tree, because all potential pathways that could allow the hazard to escape need to be controlled. However, the principle of identifying which controls are the most important to monitor, and what should be monitored, still applies. Many of the controls will be procedures, and failures will not be immediately identifiable by monitoring physical process parameters (as in the case of conventional HACCP). The choice of what should be monitored will depend on practicalities, the importance of a particular pathway, and the importance of a particular control in that pathway. In considering whether a particular pathway is relevant and important, different animals and diseases may need to be explicitly considered.

A detailed review of all pathways by which disease may escape by a method such as this is likely to produce more detailed prevention procedures than those built up in the absence of a structured technique such as HACCP. The analysis confirms that current control procedures match the detail of current risks and provides assurance that procedures cover all risks. Analysis of pathways of escape might be carried out without being specifically related to HACCP procedures; however, HACCP adds the step of analysing what should be monitored at each step and what constitutes acceptable deviations.

Racing Victoria uses a HACCP-based quarantine program for the Sandown station. A hazard analysis is carried out for each step of the quarantine management program. CCPs are identified where hazards may occur, and control monitoring, corrective action and verification procedures are proposed.

5.5.2. Application of HAZOP to the hypothetical EI case study

HAZOP applies guide words for deviations to the intent of each step of a process. It checks how that step might fail to achieve the intent. It does not identify that a step might be missing and does not identify that a step that does formally exist in written procedures is not being carried out well. Application of HAZOP to error and management systems failures is discussed in Section 7.2.

5.5.3 Application of FMEA to the hypothetical EI case study

FMEA would require an additional level of detail within the process steps shown in Figure 5, particularly in the step involving care of animals in quarantine. Different care activities would need to be identified, and the function and failure modes and effects of that step identified. One function of many quarantine activities is to contain any viruses, hence the failure modes associated with escape should be identified. The processes also have other functions, so a much broader range of potential failures would be identified. Some issues identified in the HACCP process above would be identified in a different way. For example, the function of a veterinarian's visit may be to diagnose ill health. Failure to diagnose correctly would be identified and the reasons why this might occur could be explored. The possibility of infection escaping quarantine via a released infected animal is thus identified through the process of considering functions of activities rather than directly as an exit pathway.

FMEA would be inefficient and overly time-consuming if the specific issue is to look for modes of escape of infection. It would need to be applied to all procedures carried out within quarantine to find those where infection escape is an effect. In addition, FMEA would only consider

activities that are currently carried out and how they might fail. It would not identify additional activities that would improve control but are not currently carried out. FMEA would be useful if specific procedures need to be reviewed to look for weaknesses.

The rationale behind FMEA and FMECA could also add an additional layer of detail to other methods for identifying pathways of infection and controls. The potential pathways out of the quarantine system are the failure modes of FMEA. In some cases, controls can be defined once the mode is known. In others, a further level of analysis considering mechanisms is relevant and useful. For example, in considering the failure pathway whereby disease may be transferred via veterinarians, mechanisms such as on the clothing, on the hands, or on equipment may be usefully identified.

A criticality analysis such as that in FMECA may be added, but the conventional criticality analysis methods are problematic when applied to control failures rather than component failures. There is often redundancy in controls (several may be applied in series), so the criticality of a control depends not only on the probability of failure of the particular control but the probability that a particular failure will in fact lead to the specified adverse consequences. This in turn depends on the probability of failure of other controls, and how the controls act together to control the risk. The criticality of a control also depends on the number of other risks that the failed control protects.

5.5.4 Application of process-based techniques to the FMD case study

A simple HACCP-style process analysis of activities at the Pirbright site that looked at hazards on-site and all exit routes would have clearly identified the potential for liquid waste to carry infectious virus. In fact, this had been identified and procedures were in place that were part of the DEFRA licensing requirements for the site. The failure of containment had also been identified, and complaints on the state of drains had been made, but there was a contractual dispute between the Government owners of the site and one of the commercial laboratories on the site about whose responsibility it was to fix them.

Although a site HACCP would have identified the wastewater system as a possible exit route and the drainage system as a control, there is not normally an easy way to monitor conditions of the drains. So according to decision rules, there is unlikely to be a relevant CCP associated with the drains. There appears to be a failure to recognise that the drains were a critical control for the site by the people involved in discussions on responsibility for repair such that the contractual issues were seen as more important than the biosecurity issues. The problem lay within the communication path to decision makers or the decision makers' criteria about what constitutes a priority issue that requires swift action, rather than with identification of the problem.

FMECA would probably identify wastewater escape as a failure mode and leaking drains as a mechanism, but in the absence of past problems with drains, this might not have been seen as a high probability failure mode. There are also several steps between the virus leaking from a drain on-site and the virus reaching a farm. FMEA tends to identify only direct effects; in this case, soil contamination. Similarly, the possibility of escape of a virus leaving the site on vehicles might be identified as a failure mechanism but would, under normal circumstances, not be seen as critical because vehicles would not be expected to come into contact with a laboratory virus.

In this case study, there are two failure modes that had to operate together for infectious virus to leave the site, and the particular combination of failures is unlikely to have been envisaged in a

proactive risk analysis using FMECA. In any situation where two events must arise together for failure to occur, the likelihood of this happening is perceived in advance to be very low. The problem lies in the very large number of conceivable combinations of events, each of extremely low probability.

Once the drains were known to be leaking, someone needed to make the connection from drains to contaminated soil and recognise the likelihood that soil would leave the site by some mechanism, given that the possible survival time of the virus in soil is several months (GAO 2002). Unless a risk assessment exercise was carried out when drains were known to be a problem, it seems unlikely that the process-based tools would help.

5.6. Summary of process-based techniques and their applications

All three techniques start with a process flow diagram and consider each step of the process but ask different questions. The difference can be illustrated by returning to the example of washing a carcass in an abattoir.

FMEA asks how that step (or component) might fail. Therefore it would identify the function of the washing equipment as producing a flow of water at a controlled temperature, and would ask what failure modes exist in each component of the washing equipment so that this is not achieved. For example, if a thermostat is one of the components, it would identify the different modes a thermostat might fail, causing high or low temperature or blocking flow. If a person uses the machine to wash the carcasses, the person would also be considered as a component and questions would be asked on what they could do wrong. (FMEA in human error analysis is discussed more fully in Section 6).

HAZOP would identify that the purpose of the step was to produce a carcass cleaned from specified contaminants, and would then describe the conditions of water flow needed to achieve this. Guide words would then be applied to the conditions to identify what deviations could occur and how. For example, HAZOP would identify that the water could have too much flow or too little flow and then ask what failure or combination of failures could cause this, and what would be the effect.

HAZOP looks at failure to achieve defined outcomes and FMEA looks at failure modes. The same questions are asked about how the failure might occur, its effect and detection, but the difference in thought processes can lead to different failures being identified. When applied to procedures, the two ways of thinking come closer together because both start with the functions of a procedure step. HAZOP differs from FMEA in applying key words to assist in identifying the failures that can occur. FMEA and HAZOP often identify the same problems, but HAZOP may also identify problems that arise from multiple failures occurring simultaneously or from failures at interfaces that FMEA might miss.

In the same example of carcass washing, HACCP would identify what hazards could enter the meat production system on the carcass and would identify that washing the carcass is a control point for removing the pathogen. The CCP decision tree would be applied to see if washing was a CCP, or whether the hazard could be removed elsewhere. If it was a CCP, water temperature and flow would be defined and monitored to ensure they remain within the specified limits for effective removal of the hazard. HACCP would not seek why the flow or temperature might fail

but would make sure that it was detected immediately if there was a deviation beyond defined limits. There is no specific structure within HACCP to aid the identification of hazards. HAZOP and FMEA and HACCP could be applied to any processing application within the food chain in a similar way to the abattoir example above.

In reviewing procedures for infection control, a combination of techniques could be considered. The review of hazards and input and output pathways from a HACCP approach can be used to identify (or confirm) where controls are needed. FMEA can be used to identify how controls might fail. The guide words from HAZOP can be useful in thinking through ways controls might fail. This can form the basis of inspection and audit. The techniques can identify what controls might fail and how, but do not identify why controls that are believed to be in place fail. Causal analysis techniques, including Human Reliability Analysis and organisational analysis methods, are needed. FMEA could also find application in identifying ways procedures in other areas of biosecurity might fail; for example, in laboratory testing or animal tracing. The results could be used to improve procedures.

6. Causal analysis techniques

Causal analysis techniques are applied typically after a failure of any kind causes harm, as a tool of investigation, and as a logical way to explore potential causes of failures identified through techniques such as FMEA and HAZOP. Causal analysis provides a detailed consideration of why failures occur that focuses on underlying problems.

6.1. Root cause analysis

Root cause analysis techniques seek to explore the underlying causes of failure. The methods are often displayed in a tree structure that breaks down underlying causes in increasing detail. Figure 6 shows a generalised diagram for root cause analysis for a technologically based environmental risk, and demonstrates how underlying problems are identified.

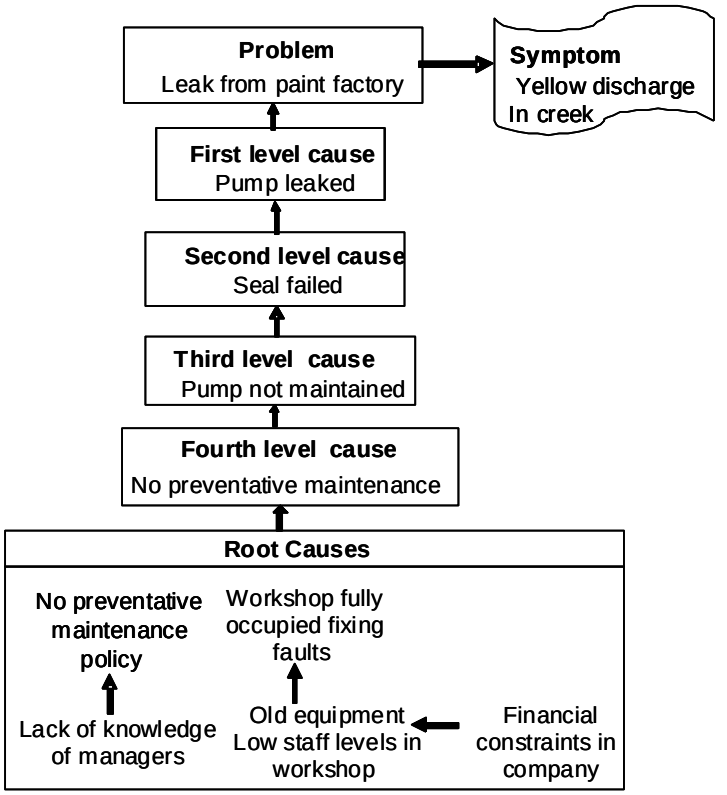

Figure 6. Root cause analysis for environmental spill.

The analysis starts by stating the problem; usually the observed 'loss' event. The symptom is what is observed to indicate the problem has occurred. It is often something that can be monitored to make sure the problem has been removed. There are then a series of levels of analysis that answer the questions 'why' and 'why was that' until the questions become redundant or their answers self-evident. The definition of what is a 'root' cause may vary, but generally this refers to system constraints that apply generically across different incidents. Causes at any level may be addressed, and the important part of root cause analysis is to identify all the main contributory

factors. In the example shown, a recommendation to introduce a preventive maintenance program will not be able to be implemented if the financial constraints are not recognised.

A similar diagram can be drawn for causation of an increase in Lyme disease in the US (information from Patz *et al*. 2004), as shown in Figure 7. The most important aspect of root cause analysis is not to jump to conclusions about cause, but to explore all potential causes logically, using an understanding of human and systems factors. When applied retrospectively to analyse an incident, all identified contributory factors should be based on evidence and not perception. Fault tree analysis and Ishikawa diagrams discussed below may be viewed as special cases of root cause analysis.

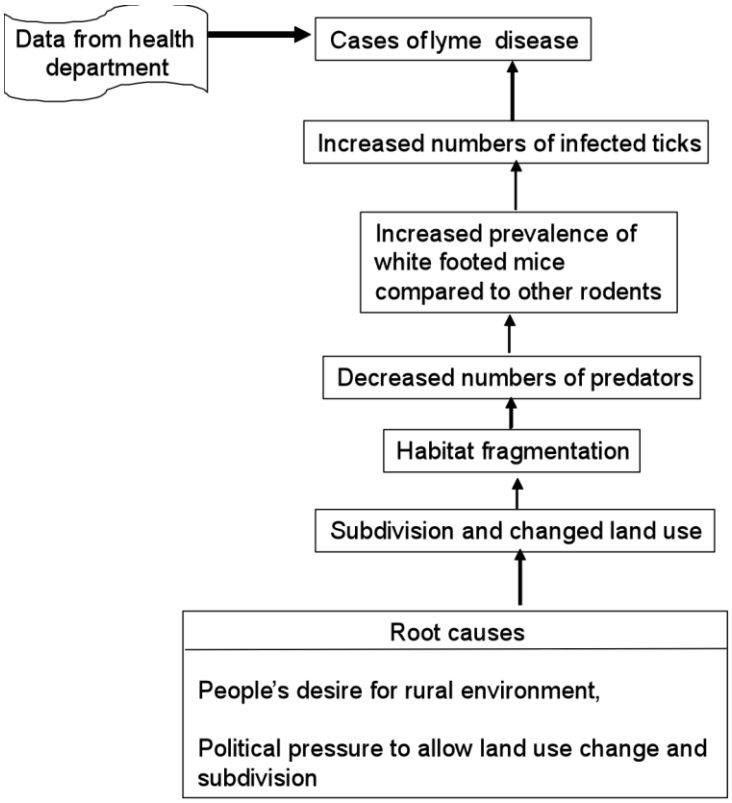

Figure 7. Root cause analysis for increase in Lyme disease in the US (Adapted from Patz *et al.* 2004).

6.2. Fault tree analysis

The analysis outlined in Figures 6 and 7 is linear, with each potential contributing factor identified separately and explored to its root cause. A broader picture can be obtained using a fault tree that allows analysis of failures where two problems may need to occur simultaneously. For example, for a disease to occur, a pathogen must be present, there must be a means of transmission, and a susceptible population (Figure 8). Each of these required components can then be explored for cause.

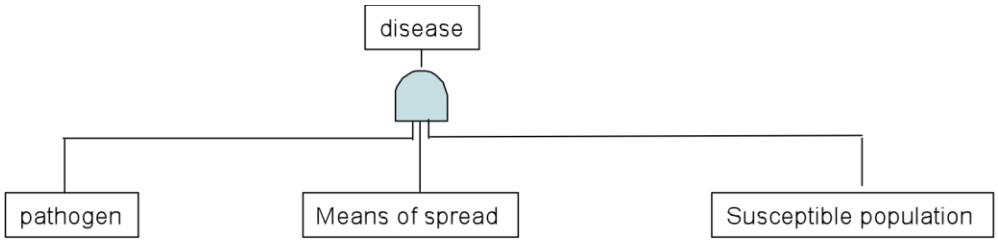

Figure 8. First line of a fault tree showing an AND gate.

Fault trees were initially developed by Bell Laboratories in 1962 to analyse the reliability of the Minuteman missile system. The method was further developed by Boeing to analyse aircraft reliability (Ericson 1999). In this application, data on failure rates of components of these complex systems were used to calculate the failure rate of the system as a whole and to check that the probability of overall failure was acceptable. Following the disasters at Flixborough in the UK[1] and Seveso in Italy[2] in the 1970s, the chemical and processing industries needed a method to reassure the public and regulators that the likelihood of a major chemical disaster was very low, and also to demonstrate that experts understood the causes of risks. The applicability of fault tree analysis was tested for the proposal to build a refinery at Canvey Island at the mouth of the Thames River. The method proved effective, and subsequently became an important tool used in planning major hazards facilities.

The fault tree notation is now widely used in risk management both as a qualitative method of analysing the causes or potential causes of major loss events, and as a quantitative tool calculating the probability of major failures and the probabilities of the different paths that might lead to it. To draw a fault tree the following steps are taken:

1. determine undesirable event that is to be the head event (also called the top event);
2. determine all faults and direct causes or necessary conditions that could *immediately* cause the head event. It is important here not to skip to sub-causes;
3. determine the relationship between the first level of causal events and the head event in terms of AND and OR gates (i.e. if all causal events must happen before the head event eventuates an AND gate is used and if any one of them alone leads to the head event an OR gate is used), and
4. determine whether any of the causal events need further analysis. If so, repeat Steps 2 and 3.

[1] http://www.hse.gov.uk/comah/sragtech/caseflixboroug74.htm
[2] http://www.unu.edu/unupress/unupbooks/uu21le/uu21le09.htm

In a true fault tree, each fault at the base of an OR gate is sufficient on its own to cause the fault above. Should any of the faults occur then the fault above will always follow. Similarly, if all faults at the AND gate occur, they are both sufficient and necessary to cause the fault above. Under these and only these circumstances, assuming the probabilities or frequencies of the base events are known, then the probability of the top event can be calculated.

A fault tree is drawn so that each fault is a cause either individually or in combination with the fault displayed above. The boxes in a fault tree do not represent classifications of failures. Groups of failure types, such as electrical and mechanical failure, or human and equipment failure, should not be separated into different parts of the tree because this loses important linkages.

A fault tree may be used with a positive top event, with the boxes representing the necessary conditions to achieve the desired top event. A success tree can also be used to identify risks by reviewing how the necessary conditions may not be achieved

6.2.1. Applications of fault tree analysis

A fault tree can be used proactively to explore the range of possible causes of potential top events, or retrospectively after failure to help define questions for investigation of an incident or to display a causal analysis (Ericson 2000). Hayes (2002b) demonstrated the use of a fault tree to explore the established introduction of an unwanted species from ballast water (Figure 9). The top event is introduction of a non-indigenous pest into a port where it can survive. In this application, the fault tree is used to display the necessary conditions for an organism to establish. The diagrammatic format can make it easier to demonstrate that failure pathways have been adequately considered. The tree continues through several further layers exploring how a viable pest can be entrained into the ballast tank (Box 11 in Figure 9).

To calculate the probability of the head event, the fault events in the tree must be ‘yes/no’ type failures for which the pass/fail probability can be estimated. In many environmental applications, the failure conditions represent a continuum rather than a specific pass/fail. For example, in the ballast water fault tree, environmental conditions may be marginal but particularly large numbers of pests might be released. The primary use of fault tree analysis in this situation is as a brainstorming or communication tool that demonstrates due diligence in analysis and becomes the basis for checking that controls cover the different pathways adequately.

Carey *et al.* (2005) used a fault tree to explore reasons for the failure of river gums to regenerate. The fault tree shown in Figure 10 was the outcome of a workshop in which facilitators started with a simple fault tree that was then expanded by workshop participants.

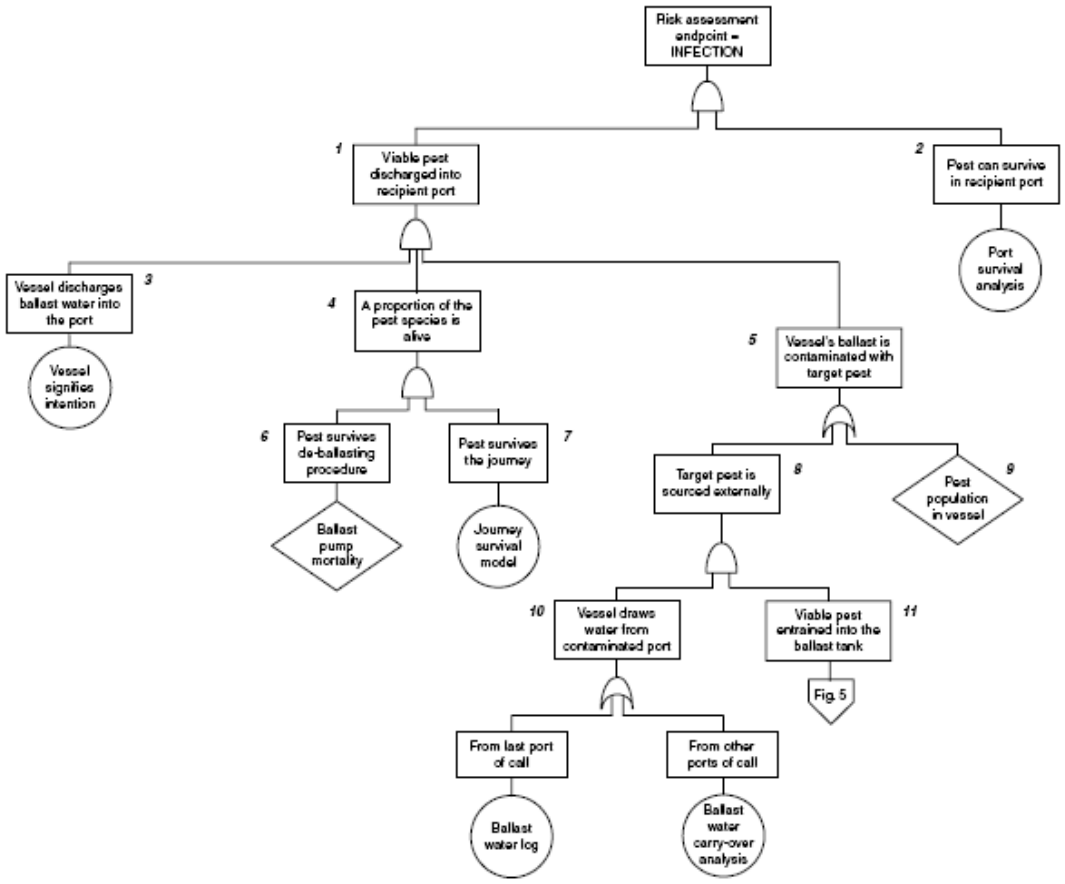

Figure 9. Part of a fault tree for introduction of a pest through ballast water (Hayes 2002b).

Carey *et al.* (2005) reported that fault tree analysis proved to be a useful tool for eliciting information in a workshop and resulted in identification of a significant number of additional elements. They found that the fault tree provided a useful record of the reasoning behind decisions to act on some issues and not on others, and was also useful in communication with stakeholders.

This fault tree could not be quantified, both because failures are not pass/fail events and because the events at an OR gate are not necessarily a complete set (for example, there may be other causes of flow blockage than those mentioned). Where a fault tree cannot be quantified, its value as a brainstorming and display technique for causal analysis may still be substantial.

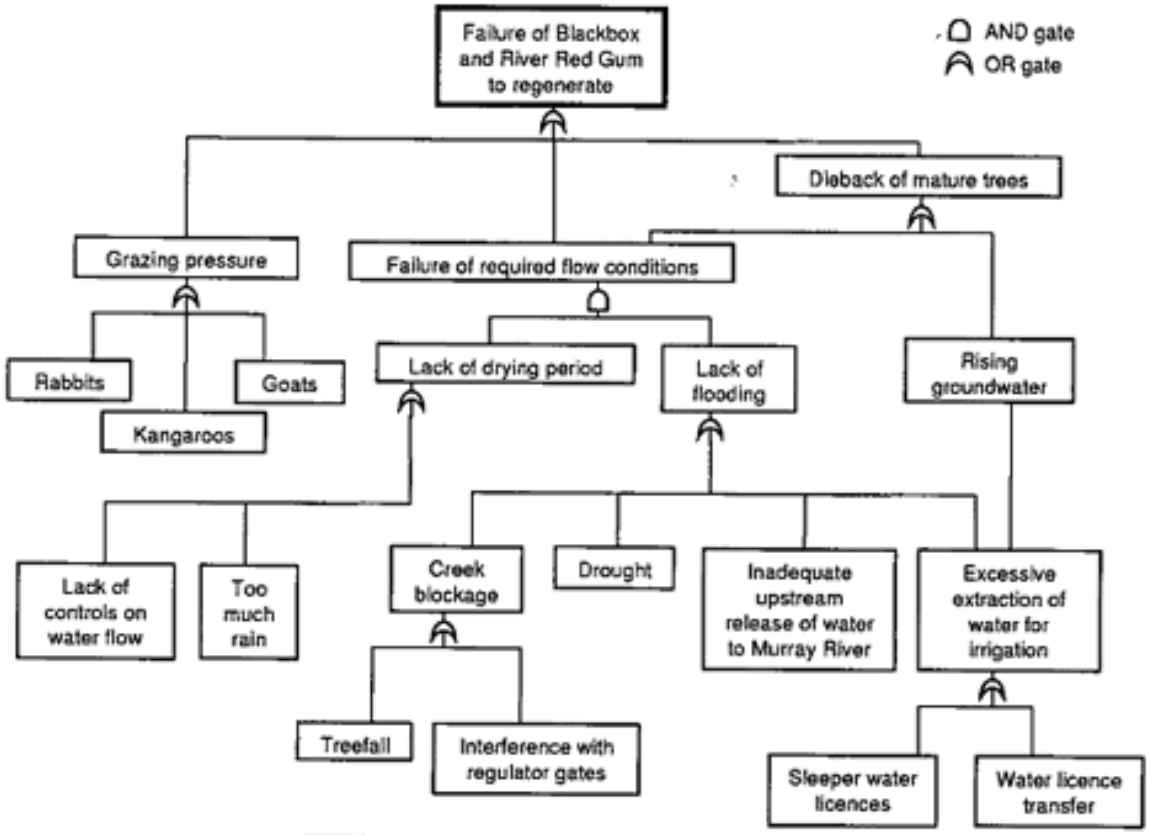

Figure 10. Fault tree analysis of failure of black box and river redgum to regenerate.

6.2.2. Strengths and limitations of fault tree analysis

Fault tree analysis provides a good display technique for describing complex failure scenarios, particularly where combinations of events must occur together. They can provide a useful communication aid in a workshop scenario when a group of people is exploring causes of a particular unwanted event.

The strict logic used in a true fault tree allows a fault tree to be analysed to calculate the probability of the top event, provided there is data for the probability of failure of the base events. It is also possible to identify cut sets. These are the separate combinations of events that can on their own result in failure. The ability to quantify allows the relative effectiveness of controls that change probabilities of base events to be analysed.

A fault tree models binary events: true or false, pass or fail (in the example illustrated in Figure 10, the creek is blocked or not). The fault tree cannot deal easily with situations that involve a combination of partial failures or a general degradation in quality. It also cannot deal with situations in which there are feedback loops or complex interactions. Equipment components normally have a relatively small number of failure modes that can be definitively identified. When used more broadly for analysis of potential incidents, the tree is more open-ended, and it can be difficult to ensure that all possible failure modes are included. For example, in a fault tree representing a fire, it would be difficult to ensure all possible ignition sources were included.

Fault trees do not deal well with root causes that involve human or organisational failures. Human fault modes (acts and omissions) arise in two ways. A person may be an intrinsic part of the system because of the actions he or she performs. For example, a person may fail to perform a procedure. This failure may be included directly in the tree as an error mode (what is observed to be done wrong). Error may also be involved indirectly as a root cause of some other failure. For example, a contributory cause to a machine failure may be insufficient maintenance. The fault tree formulation does not deal with this type of human performance failure well. Although the fault tree formulation could, in theory, be used to explore root causes of human error modes, there are usually multiple interconnected reasons why people fail, and forcing these into a simple fault tree logic leads to over-simplification.

6.3. Cause and effect diagrams

Cause and effect diagrams are structured and visual brainstorming tools designed to help a team identify all the possible causes and risk factors of a particular problem. One common format is the Ishikawa or fishbone diagram, originally developed in Japan as a total quality management tool (Ishikawa 1982). It is a means of achieving stakeholder input in identifying problems, and provides a structure to consider a range of potential problems that does not require the strict causal logic necessary for a fault tree. In an Ishikawa diagram, A may contribute to B, rather than A being an immediate cause of B. An Ishikawa analysis carried out proactively would encourage people to offer opinions about the adequacy of products, people, procedures, etc. (depending on the structure of the backbone categories), and would provide an opportunity for people to express concerns in an environment where this is acceptable and encouraged.

To construct a fishbone diagram, the problem to be solved is drawn as the fish head and a backbone is then drawn. The main bones of the fish represent the main categories under which problems might fall. Typically, these might be 'manpower', 'machines', 'materials', 'methods', or sometimes 'people' 'products', 'processes', 'procedures', and 'policies'. The team brainstorms each category to identify potential causes and sub-causes and factors that affect the risk. Figure 11 shows a generic diagram for a fishbone analysis.

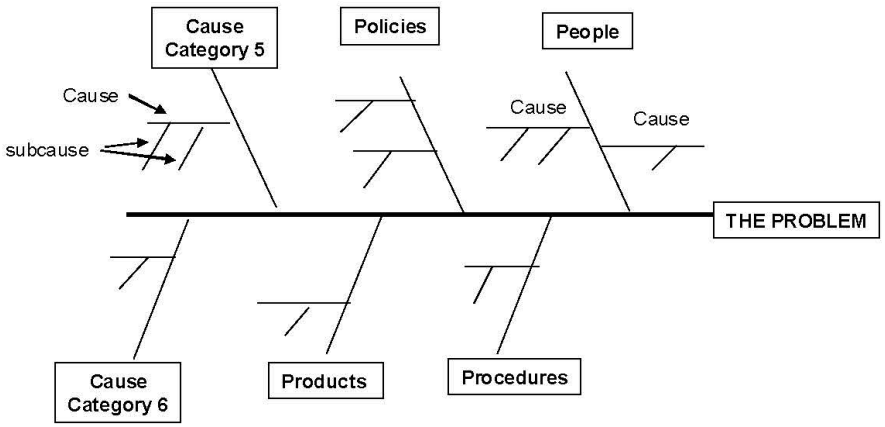

Figure 11. Ishikawa fishbone diagram.

To some extent, a cause and effect diagram is similar to a fault tree and could be drawn to look like a fault tree, but there is a fundamental difference in the logic of the two methods. Cause and effect analysis is a structured brainstorming exercise where different categories of problem are considered as separate thinking prompts. In a fault tree, the analysis must start from high level failures and work down to causes and sub-causes. To be displayed in a fault tree, a fault or failure must be a direct cause of the event in the box above, whereas the cause and effect diagrams such as the Ishikawa diagram can display general contributory causes and risk factors under each cause category. A cause and effect diagram divides potential problems into categories at the start of a diagram. This is poor practice in a fault tree because interactions between categories are lost.

An Ishikawa diagram is a qualitative tool. When the diagram is completed with all potential causes and risk factors listed, the team may further brainstorm to decide which causes are the most likely to occur and which need most immediate treatment.

The Ishikawa diagram can also be drawn with the desired outcome as the head event and brainstorming undertaken to identify the things needed to achieve the desired outcome.

6.3.1. Strengths and limitation of Ishikawa analysis

Ishikawa analysis is a brainstorming tool that encourages participation and allows imaginative consideration of potential causes of a specified problem. It provides a forum where people can discuss the problems that they perceive in a system. Unlike the fault tree, it is able to deal with partial failures and quality issues. The diagram is easy to interpret. The lack of structure offers the advantage of encouraging discussion and imagination, but also the disadvantage that discussions can be open-ended without the clear logic required to ensure all critical issues are included.

6.4. Applications of causal analysis techniques

Root cause analysis of various types is widely used for incident investigation in OHS and for major hazards accidents (e.g. Sklet 2004). The healthcare accreditation system in the US requires that a root cause analysis is carried out whenever there is an unanticipated fatality, and Ishikawa diagrams are widely used (see, for example, Carrico and Ramirez 2007). In healthcare, the analysis is carried out after loss rather than as a proactive identification tool following identification of a potential failure mode. Analysis of many failures does, however, result in an understanding of the common system failures in hospital systems. Root cause analysis has also been adopted by the National Patient Safety Agency in the UK (National Patient Safety Agency 2005) and by the states and territories in Australia.

Iedema *et al.* (2006) observed a root cause analysis exercise being carried out in a Sydney hospital. They found that the team discussed possible motivations for the acts and omissions that were retrospectively seen to be incorrect, but they had difficulty deriving generalisations and identifying systems problems from these. It was also found that in the hospital setting, it was difficult to derive rules and procedures for preventing the errors that were not going to get in the way of what clinicians were trying to do. In other words, formal rules could not account for every contingency in a clinical setting, and an attempt to introduce formal rules to solve all problems was found to be counterproductive.

The examples of root cause analysis published in the literature usually stop at the procedural level or, *'at the first point in a chain of events that can be eliminated by applying policy, practice, or procedure at the policy/management, supervisory, or individual level'* (Rzepnicki and Johnson 2005). Thus in practice, root cause analysis in healthcare does not identify problems with organisational culture or the drivers of poor practice, such as staff shortages or gaps in accountability, but only procedural errors and possible motivations.

Dhillon (2003; also cited in Lyons *et al.* 2004) proposes that fault tree analysis could be used for root cause analysis in healthcare, and that the tree could be quantified. The example he provides, however, does not support this view and illustrates some of the problems of transferring probabilistic fault trees to applications that are dominated by human error. The tree showing how the calculation would be done is presented in Figure 12. In this tree, rather than adding the probabilities of failure at the OR gates, they have taken the product of the probability of success. This is mathematically correct but has led to rounding errors that are confusing.

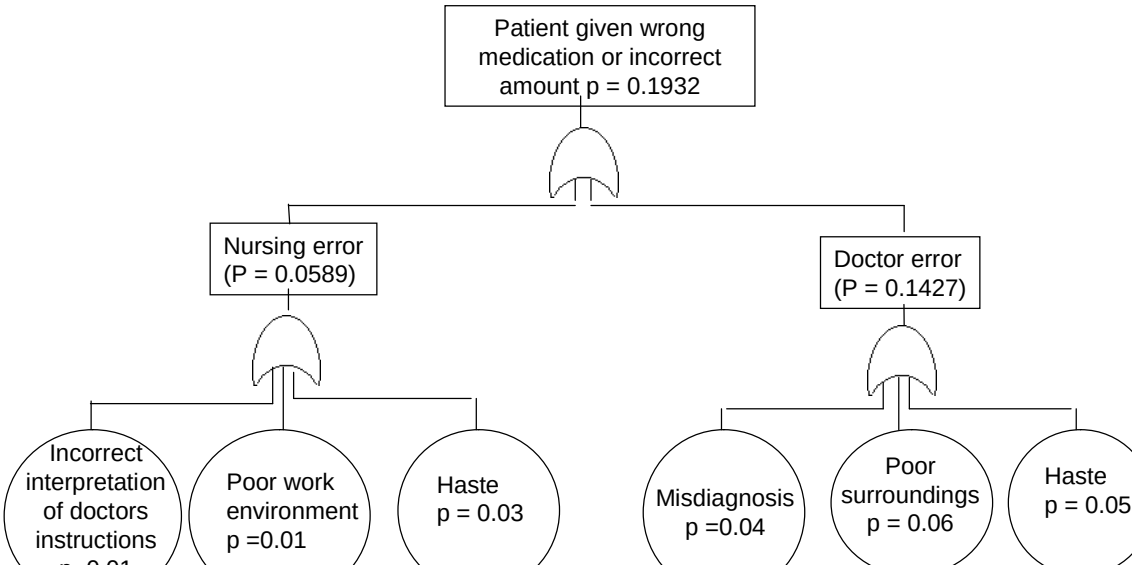

Figure 12. Fault tree taken from Lyons *et al.* (2004).

The tree has a number of flaws.

The fault tree should display the error mode (e.g. nurse gives too many pills) so that mechanisms and causes can be properly considered and attributed.

The example is clearly a subset. Unless all modes and mechanisms are included, quantification will not be valid.

A poor work environment is a potential cause of incorrect interpretation or misdiagnosis rather than an independent cause of nursing or doctor error.

A poor work environment or time pressures do not necessarily cause error but have the potential to be contributing factors; i.e. these faults will not on their own always cause error so the mathematical logic of the OR gate cannot be applied.

The fault tree method is not suitable for representing continuous variables (such as haste or poor surroundings), only binary ones (interpretation correct or incorrect).

The probability of misdiagnosis (or any other mode of doctor error not included in the tree) will depend on a range of factors associated with the task: the environment, any equipment used, and the person themselves. These so called performance-shaping factors and how they can be included in fault tree analysis are discussed in the Section 7.3 on Human Reliability Analysis.

That it is not uncommon to see incorrect quantification when fault trees are applied outside the reliability context does not lessen their value as qualitative aids to identification and causal analysis. The fact that specific error modes are identified and only causes for that particular error mode recorded at the next level helps avoid simplistic solutions to the causes of error.

An Ishikawa diagram might be more successful than fault tree analysis. Failure in quarantine is an obvious choice for the head of the fish, and it seems likely that if appropriate stakeholders had undertaken a detailed Ishikawa analysis in a favourable management climate, the problems with staffing and procedures could have been identified, which may have reduced the probability of the event if behaviours had changed or resources had been redirected. Ishikawa analysis will identify causes of breaches of procedures and human failings, provided that the correct procedure is known to at least some of the stakeholders undertaking the analysis, and that people are prepared to admit to error. It cannot identify causes not perceived to be a problem by stakeholders. For example, if people feel that they are coping adequately with their workload and doing everything necessary, staff shortages will not be identified as a problem. Supportive management is essential to the success of the Ishikawa method because people tend not to identify things that they believe will not be changed, or where they believe there will be negative consequences of admitting to error.

6.4.1. Application to FMD case study

The Pirbright incident had several faults that had to occur together, making it amenable to description via a fault tree (see Figure 13).

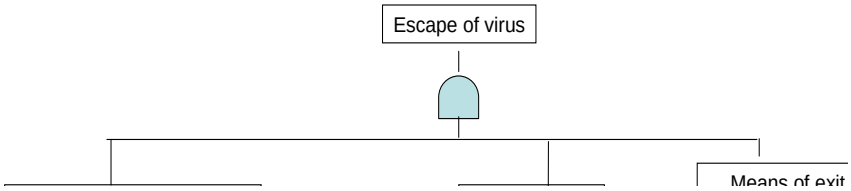

Figure 13. Fault tree for escape of virus.

There are many possible routes of loss of containment other than the drains, and many possible routes of exit from the site other than construction vehicles. Any list of mechanisms that may lead to loss of containment or means of exit would not be exhaustive or exclusive. Hence,

quantification is not possible. The fault tree formulation can be continued further as a qualitative investigative tool as shown in Figure 14.

An AND gate is shown joining old drains, nearby trees, and failure to fix drains. Trees do not necessarily cause a leakage in old drains, so use of the AND gate is not strictly accurate; however, where the fault tree is used for investigative purposes and as a display technique for possible contributory causes, this may not be important.

At the next level in the tree, causes for the failure to get the drains fixed can only be speculative. For example, was the decision maker for the site owner not aware of the importance of maintaining Level 4 containment, or were they not aware that the drains concerned were part of the containment system? By linking causes directly to observed failures, the analyst is limited to consider only why that particular error occurred rather than moving from identification of an error direct to generic causes (such as lack of training) that might or might not be relevant to the specific incident. For example, if the decision maker was not aware of the role of those particular drains in the biosecurity of the site, the solution lies in communication from the site to the contract manager rather than training.

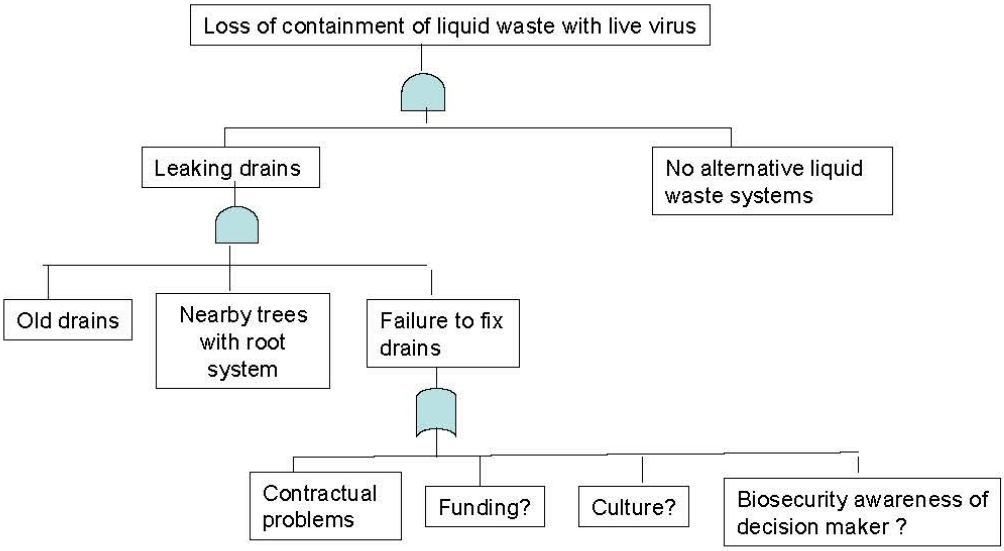

Figure 14. Continuation of fault tree for Figure 13.

The site owner was also a part of the Government department responsible for policing the containment. The body responsible for policing the containment was also one of the parties in the dispute about responsibility for drainage repairs. Such conflicts of interest would be difficult to display in the tree.

6.5. Summary of causal analysis techniques

As an investigation tool, the fault tree diagram suggests particular questions that focus on root causes rather than superficial ones. Not all these questions were asked (or at least reported) in the investigations explored here. As a proactive identification tool for a generic situation, such as escape of a virus from a laboratory or quarantine station, the size of a fault tree can become burdensome. Its strength lies in investigation or in fault finding in situations with relatively few binary failure modes.

The Ishikawa diagram is more open-ended than the fault tree, and seeks perceptions as well as evidence-based causes. For example, instead of asking why a particular person did not make a decision about drains, it will ask what are the problems associated with people that led (or in proactive mode, might lead) to the head problem. Since this method takes a holistic view, it tends to identify problems at a generic level and often to reinforce preconceptions of causes of problems rather than looking at evidence.

Theoretically, root cause analysis techniques could identify the problems that occurred in either case study above. They are used proactively in the chemical and processing industries for major hazards facilities to identify potential causes of failures, but these are largely equipment-based. There is insufficient evidence of the successful use of the techniques in a proactive way for problems involving human and organisational failures to be able to indicate how well they would work in these circumstances.

The root causes identified in most causal analyses of large failures relate to human or systems issues. These are usually the focus of investigations and inquiries, but are seldom adequately considered proactively in risk analyses. One difficulty in correctly identifying human and systems-based risks in advance of loss is the very large number of potential systems and human failures, any of which might occur at line and management levels, and the multiple and interacting possible causes for these failures. This tends to lead to grouping of human failure mechanisms under headings such as ‘training and supervision’ that are too broad to provide practical help for focused prevention. An understanding of human and organisational failures is needed to extend the root cause analysis into these areas, and to identify appropriate actions to minimise errors by people at all levels. This is the focus of the following section.

7. Human and organisational factors methods

'Human factors analysis' refers to the class of methods from behavioural science that aims to describe, predict, and manage human behaviour to achieve operational goals. Human factors methods are used in engineering to help design systems, procedures, and equipment to work efficiently and to minimise error. In some applications, particularly the nuclear industry, the probability of human error has been quantified and incorporated into fault trees or other safety analysis methods. In some European countries, acceptable risk to human life is defined quantitatively, and industry is required to demonstrate that it achieves relevant safety thresholds or criteria. Human factors methods are used proactively to demonstrate that risks are acceptable, and retrospectively as part of analysing root causes of failures involving human behaviour. Human factors analysis generally makes the assumption that in acting (or omitting to act) in a way that turns out to have an incorrect outcome, people are not acting maliciously.

7.1. James Reason's Swiss cheese model

A model frequently used in investigation of failures in complex technological systems is commonly known as the Swiss cheese model (Reason 1980). This model suggests that there are a number of protective layers between a hazard and a loss. Reason proposed that each of these barriers have potential failures, characterised as 'holes' (similar to those in slices of Swiss cheese) that change with time. If by chance the holes align, then the hazard can proceed to cause loss (Figure 15).

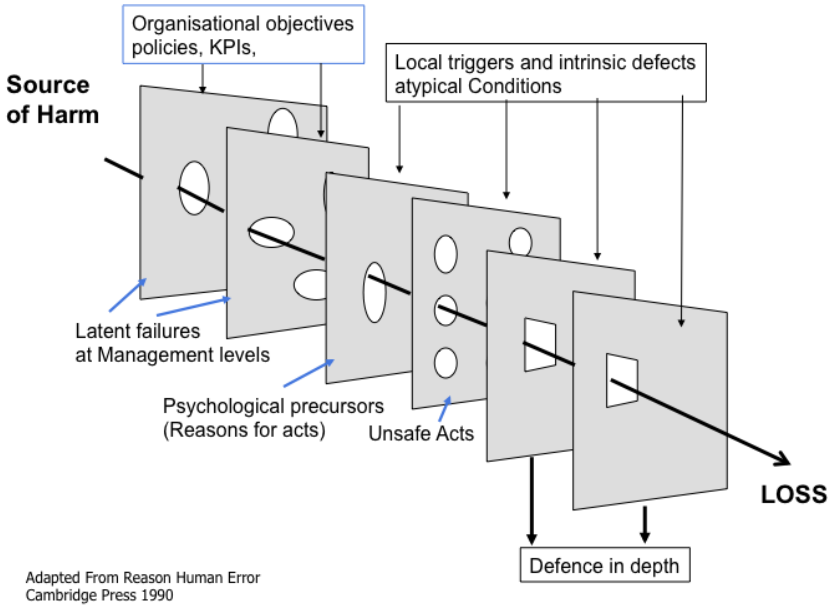

Figure 15. Reason's Swiss cheese model.

Investigation following a failure looks specifically at each layer and how it contributed to the failure. The layers considered are:

- physical barriers;
- procedural barriers;
- people's acts and omissions, and the motivations for them;
- local management acts, omissions, procedures, and activities that encourage or fail to prevent errors, and
- organisational and cultural issues.

The model can be used to help identify potential for human error, motivations for error, and how controls might fail. It encourages consideration of failures at all management levels, as well as failures of equipment, people and procedures at the front line.

To help analyse people's acts and omissions and the motivations for them, Reason classified human error into different types. These classifications help explain the underlying causes of human error and hence allow one to recognise situations with high potential for error and define more effective control measures.

Reason first separated human error into two categories, depending on whether what the person set out to do was what should have been done, or not. Actions where the intention was not correct may be mistakes or violations. The second group of errors is where the intention was correct but the action wrong. These can be divided into slips and lapses.

Mistakes occur when well-motivated people choose to act in a way that that leads to a failure or loss; for example, as a result of lack of knowledge or by following a poor procedure correctly.

Violations occur when people intentionally break rules. Usually this is a result of conflicting motivations such as a desire to save time and effort, or to help others, or to invent new ways of doing things. Most people violate some rules sometimes and seldom do so maliciously. Usually they are broken for what is perceived to be good reason. These motivations need to be identified if violations are to be minimised.

Slips are where a well-known and understood activity is performed incorrectly. Slips usually relate to the sort of activity that is performed automatically without conscious mental thought (e.g. making a typing error).

Lapses are errors that occur perhaps as a result of distraction when performing less automatic, skill-based tasks, such as mistakes in putting things in alphabetical order.

An important lesson from this classification is that training is an appropriate control for only a minority of errors. It is clearly not useful to train people when they already intended to do the correct thing, and it is probably not useful if there are conflicting motivations where the individual knows they are doing something incorrect but other factors override the decision on what to do. For example, if procedures are not followed because of lack of time to do the job properly, taking time out for training could be counterproductive.

In seeking causes of errors, one needs to seek error-producing conditions (such as distractions) and violation-producing conditions (such as shortage of time) (Reason 2001). Reason's model starts with 'active' errors; those of staff who are performing relatively routine actions. 'Latent errors' are the decisions of designers, procedure writers, and management at all levels that either translate into error-provoking conditions (such as staff shortages, fatigue, inadequate equipment, etc.), or lead to holes in the barriers (non-working alarms, poorly designed procedures, etc.).

Reason provides a basic model and assistance in defining error types, but does not give much guidance for people who are not human factors experts in thinking through causes of errors, at staff and manager level, or of organisational and system problems. This can be provided by SHAZOP and Human Reliability Analysis techniques, described below.

7.2. SCHAZOP

Kennedy and Kirwan (1998) developed a modification of HAZOP to identify failures in management systems and underlying cultural problems in organisations. Their intended application is to the management of hazardous facilities, but it is applicable more broadly. The process is called SCHAZOP (Safety Culture HAZOP). The SCHAZOP aims to identify:

- areas where the management process is `vulnerable' to failures;
- potential consequences of the management failure;
- the potential (safety culture) failure mechanisms, and
- management failure and the factors that influence their likelihood.

The steps are as follows.

- The management system is separated into components and an activity hierarchy list is defined.
- The function or intent of each activity and the conditions required in order to achieve it are defined.
- A set of guide words for deviations is applied to the required functions and conditions.

Table 6 shows guide words and properties proposed by Kennedy and Kirwan for study of a safety management system and culture. The method identifies the observed failures in management steps. They claim that consideration of mechanisms and causes of failure lead to identification of problems of culture.

Table 6. SCHAZOP guide words and properties.

Guide words	Property words	
Missing Skipped Mis-timed More Less Wrong As well as Other	Person Skill Knowledge Action Procedure Information Resources	Detail Protection Decision Control Communication

7.3. Human Reliability Analysis (HRA)

There were a large number of human error identification and analysis methods developed in the 1980s and 1990s (Kirwan 1994). They were mostly developed to try to include human error into

the fault trees, many required as part of official safety procedures prior to building and operating major hazards facilities. Some methods aim to identify potential for error and minimise it; others to quantify the probability of error for inclusion in fault trees or other risk assessment tools. HRA techniques recognise that humans cannot achieve continuous perfect performance, or error-free decisions and actions. The aim of the techniques is to understand factors that affect human performance so systems can be designed to improve performance and reduce errors.

Some common HRA methods are HEART (Human Error Assessment and Reduction Technique), SHERPA (Systematic Human Error Reduction and Prediction Approach), THERP (Technique for Human Error Rate Prediction), TRACEr (Technique for the Retrospective and Predictive Analysis of Cognitive Errors), and CREAM (Cognitive Reliability and Error Analysis Method). A brief description and review of methods is given in Stanton *et al.* (2005). A variety of techniques is used to estimate the probability of errors within these techniques, including expert opinion and error rate databases.

Most of the HRA techniques provide a taxonomy for considering error. These provide a set of checklists that can be used to predict the potential for error, or assist in exploring error in a root cause analysis. Kirwan (1998a; 1998b) reviewed 38 HRA methods existing at the time and constructed a framework from which people could select the relevant tools for error prediction and analysis. His work predated some of the so-called second generation techniques that took into account cognitive processes of decisions, but the framework he described is incorporated in most of those techniques.

Analysis of error usually starts by an analysis of the task to be performed. At its simplest, this is just a description of the steps that have to be performed with a hierarchical structure when steps of the task have sub-steps. More complex task analyses consider in addition

the goals of the task;

the plan for the task;

constraints (people and time equipment);

any adverse conditions;

the cognitive demands of the task;

availability of procedures, and

training and capability of people who perform the task.

Goals analysis involves checking that there are no goal-related errors inherent in the task. These can be classified as:

no goal;

wrong goal;

outside procedures;

goal conflict;

goal delayed;

too many goals, and

goal inadequate.

Errors may also stem from poor planning. Plan-related errors can be classified as:

no plan;

wrong plan;

incomplete plan;

plan communication failure;

plan coordination failure;

plan initiation failure;

plan execution failure;

plan sequence error;

inadequate plan, and

plan termination.

Assuming goals are clear and well-defined, and a plan to execute the goals is in place and communicated, the next phase of analysis is to consider human performance and the potential for error. Analysis of error starts by identifying the error mode. The error mode is the fault that is observed (this is the statement that would appear when human error is incorporated into a fault tree or FMEA). Error modes are classified in Table 7.

Some error analysis methods incorporate taxonomy for error mechanisms. The error mode is what is observed; the error mechanism is how it occurs. There are several different published tables of error mechanism. These were reviewed by Taylor-Adams (1994) who developed a taxonomy reducing some 58 error mechanisms to the list shown in Table 8.

Shorrock (2002) developed a system for analysing error in air traffic control. These are errors in decision making and are classified using a cognitive model of decisions. He called the error modes of Table 7 ‘external error modes’ (EEMs), and then differentiated between internal error modes and psychological error mechanisms. The internal error mode classification of Shorrock (2002) is illustrated in Figure 16. The psychological error mechanisms associated with the different cognitive domains are shown in Table 9. This mapping onto cognitive domains extends the analysis from operators to decision makers, illustrating the types of problems decision makers may experience and provides a more theoretical basis to the analysis.

Table 7. Taxonomy for error modes (Kirwan 1998b).

- Omissions
  - Omit task
  - Omit task step
- Timing
  - Action too late
  - Action too early
  - Accidental timing with another event
  - Action too short
  - Action too long
- Sequence
  - Wrong sequence
  - Action repeated
  - Latent error prevents execution
- Quality
  - Too much
  - Too little
  - Wrong direction
  - Misalignment
  - Other quality or precision error
- Selection Error
  - Right action, wrong object
  - Wrong action, right object
  - Wrong action, wrong object
  - Substitution error
- Information transmission error
  - Information not communicated
  - Wrong information communicated
  - Information unclear
- Rule violation
- Other

Table 8. Taxonomy of error mechanisms (Taylor-Adams 1994).

1. Action prevented
2. Attention failure
    - 2.1 intrusions
3. Cognitive overload
    - (a) identification prevented
    - (b) freeze
    - (c) hyperactivity
4. Concurrent plans
    - 4.1 indecision
5. Conscious versus subconscious
6. Encystment (withdrawal from perceived hostile environment)
7. Erratic response
    - 7.1 motor variability
        - 7.1.1 unintentional activation
8. Incorrect incomplete mental model
9. Memory failure
    - 9.1 mistake among alternatives
    - 9.2 place losing error
    - 9.3 mental blocks
    - 9.4 failure to consider special circumstances
10. Misdiagnosis
    - 10.1 signal discrimination failure
    - 10.2 misinterpretation
        - 10.2.1 miscuing
        - 10.2.2 wrong procedure/rule followed
11. Perception prevented
    - 11.1 out of sight bias
12. Procedure unfamiliarity
13. Risk recognition failure
    - 13.1 underestimate demand
    - 13.2 risk tolerance
    - 13.3 overconfidence
        - 13.3.1 oversimplification
    - 13.4 risk taking
14. Rule contravention
15. Shared schema properties
16. Short cut invoked signal/information unreliable / absent
    - 16.1 lack of or incorrect information
    - 16.2 lack of feedback on correctness of action
    - 16.3 need for information not prompted (including lack of feedback)
17. Stereotype takeover
    - 17.1 assumptions
    - 17.2 substitution
    - 17.3 mind set
18. Thematic vagabonding
    - 18.1 integration failure
    - 18.2 availability bias
    - 18.3 topographical or spatial misorientation

Table 9. Examples of the effect of source Psychological Error Mechanisms in different cognitive domains (Shorrock 2002).

Example 'source PEMs'	Example cognitive domain	Example PEMs
Complexity, understanding	Memory Judgment, planning and decision making	Insufficient learning Integration failure
Expectation, assumption	Perception and vigilance Judgment, planning and decision-making	Expectation bias False assumption
Association, confusion, interference, habit	Perception and vigilance Memory Action execution	Perceptual confusion Negative transfer, similarity interference Habit intrusion
Tunnelling, fixation	Perception and vigilance Memory Judgment, planning and decision-making	Perceptual tunnelling Memory block Cognitive fixation
Overload, underload	Perception and vigilance Memory Judgment, planning and decision-making	Vigilance failure Memory capacity overload Decision freeze
Internal distraction, preoccupation	Perception and vigilance Memory Action execution	Distraction/preoccupation Distraction/preoccupation Environmental intrusion

Cognitive Domain	Cognitive Function	Relevant Keywords	Example IEM
Perception	Vision – Detection	None, late, incorrect	Late detection
	Vision – Identification	None, late, incorrect	Misidentification
	Hearing – Recognition/ Comparison	None, late, incorrect	Hearback error
Memory	Recall perceptual information	None, incorrect	Forget temporary information
	Previous actions	None, incorrect	Forget previous actions
	Immediate/current action	None, incorrect	Forget to perform action
	Prospective memory	None, incorrect	Prospective memory failure
	Stored information (procedural and declarative knowledge)	None, incorrect	Misrecall stored information
Judgement, Planning and Decision Making	Judgement	Incorrect	Misprojection
	Planning	None, too little, incorrect	Underplan
	Decision Making	None, late, incorrect	Incorrect decision
Action Execution	Timing	Early, late, long, short	Action too early
	Positioning	Too much, too little, incorrect, wrong direction	Positioning error: overshoot
	Selection	Incorrect	Typing error
	Communication	None, unclear, incorrect	Unclear information transmitted

Figure 16. Internal Error Mode classification (Shorrock 2002).

When an error mode and mechanism have been identified, the person's performance in the task or their probability of error depends on performance shaping factors (PSFs), also called error-producing conditions (EPCs) or error-enhancing mechanisms. These are not causes of error but factors within the task, the environment, equipment, and the person that make errors more likely.

PSFs can be classed as internal and external; that is, they may be 'internal' characteristics of the person and 'external' characteristics of the task, equipment, and the physical and organisational environment. Internal PSFs include both those inherent to the person, such as height and gender, and those that can be changed (for example by training). Figure 17 shows a structure to help identify PSFs taken from Draft IEC standard Human Aspects of Design.

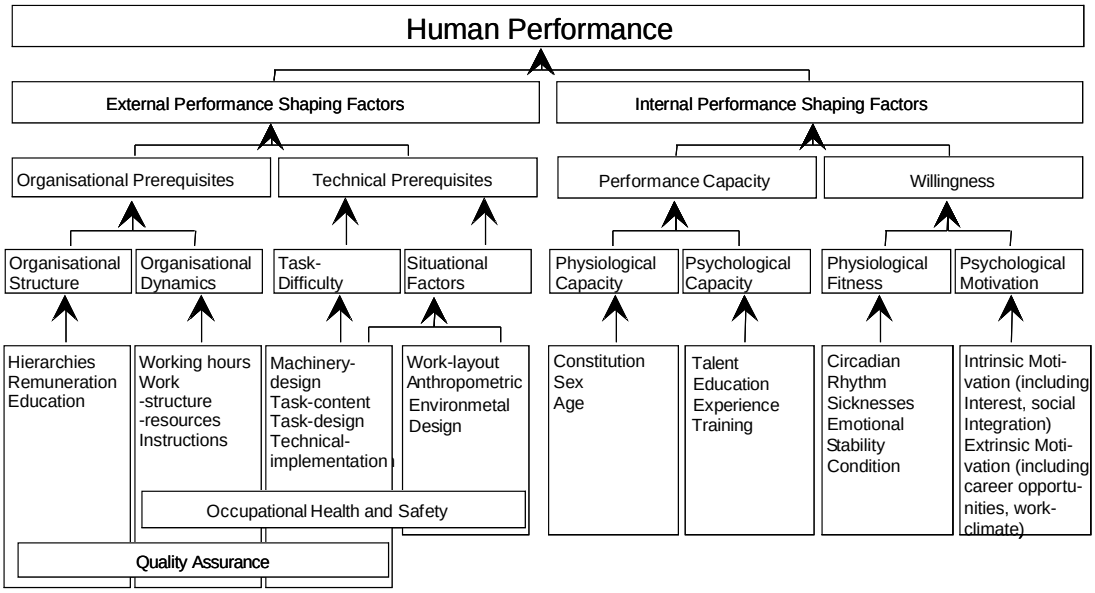

Figure 17. Performance shaping factors.

Since PSFs are possible contributory factors that increase the probability of error, rather than causes of error, they cannot be incorporated into a fault tree directly as faults. In quantitative Human Reliability Analysis, they are incorporated by multiplying the estimated probability of an error mode occurring by a factor to account for the negative influence of performance shaping factors.

7.4. Organisational factors

Hollnagel (1993, 1999) suggests that the decomposition into error modes, mechanisms, and performance-shaping factors is overly simplistic. He suggests that the probability of failure of a complex system is not related to the individual (Figure 18, left), but to the system as a whole and the level of control that people have in making decisions (Figure 18, right).

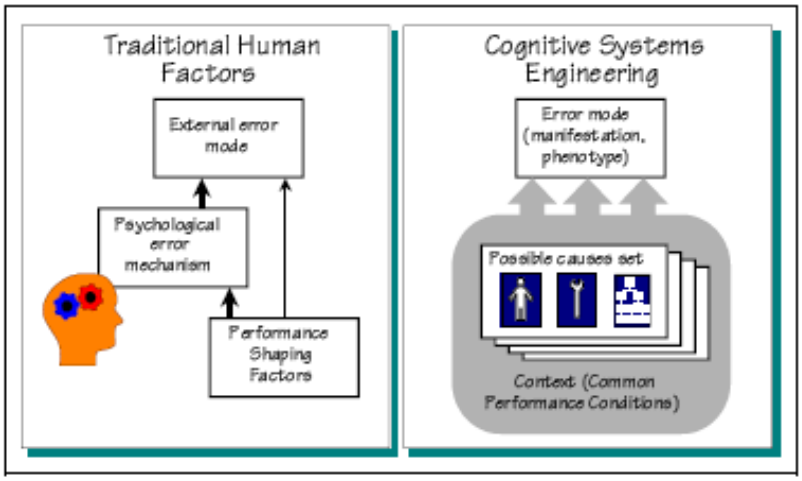

Figure 18. Two perspectives on failure causation (Hollnagal 1999).

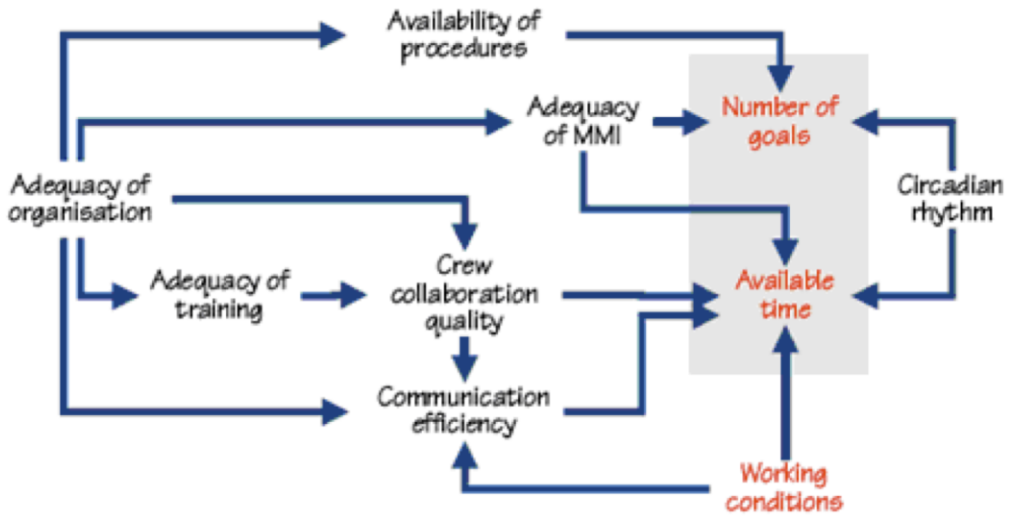

Figure 19. Common performance conditions (Hollnagal 1999).

According to Hollnagal (1999), error depends on the context that is formed by a set of interrelated common performance conditions (CPCs, Figure 19). Each of these is assumed to have a number of states. For example, the adequacy of organisation may be deemed to be very efficient, efficient, inefficient, or deficient.

In quantifying this model, Kim, Seong and Hollnagel (2006) use Bayesian belief networks to define the interlinked components of the context and each probability of being in a particular state. This is the basis of a quantitative HRA technique, CREAM, that, together with work of Weick and Rasmussen, has lead to the concept of resilience engineering.

Rasmussen (1997) suggests that models that seek to identify individual errors and their causes are useful for the design of work support systems for individual actors and decision makers, but do not adequately describe the risk management system for a complex system as a whole and why it fails. He suggests the model shown in Figure 20. Rasmussen divides the total system into a number of layers of control. These include Reason's organisational layers of control, but extend outside the organisation. Rasmussen's basic layers are government, regulators and associations (including unions), the company, management, staff, and the work itself. This list may be modified for particular situations when there may be other layers where control is possible.

In the classical command-and-control approach, each level is subject to laws, regulations, standards, and procedures, issued from the top down and based on task analysis. Each level is traditionally studied by its own academic discipline without detailed consideration of processes at other levels. Rasmussen argues that this is not appropriate for a modern, complex, and dynamic organisational system, where decisions made at higher levels need to be transmitted down the hierarchy, and information and feedback should propagate up the hierarchy.

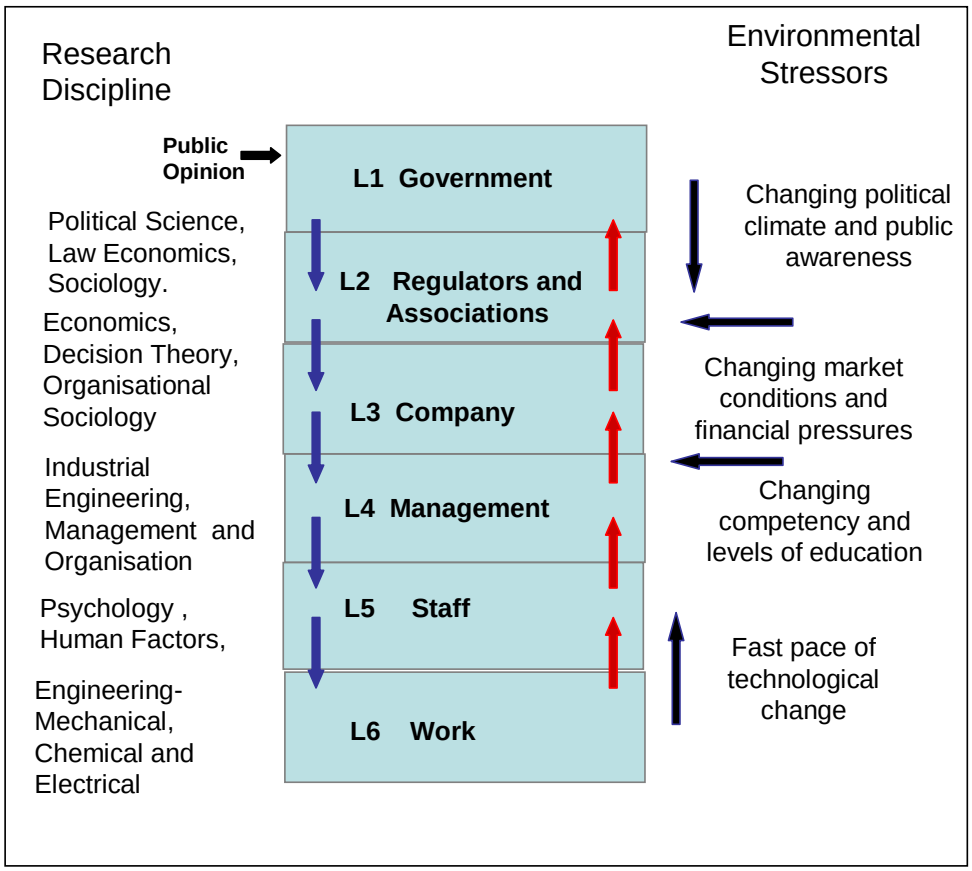

Figure 20. Hierarchical model of socio-technical factors involved in risk management (Rasmussen 1997).

Rasmussen points out that inquiries into failures frequently show that they are not caused by a coincidence of independent failures, such as described pictorially in a fault tree, but by, *'a systematic migration of organizational behaviour towards accident under the influence of pressure towards cost-effectiveness in an aggressive and competitive environment'*. Using a series of case studies, he demonstrates that failures often arise as a result of an interaction between the side effects of decisions made by several people in their normal work context. These decision makers cannot see the complete picture and are subject to the various competitive pressures of time and cost-cutting. The decisions and priorities are correct in the immediate context, but have side effects that increase risk. The general migration of performance towards the boundaries of acceptable risk is such that one variation in a person's behaviour, which might be quite normal, causes the failure. Had this particular error or variation been eliminated, an incident would most likely be caused by another trigger. The reasons for the degradation of the system are the internal and external pressures, such as the practicalities of getting the work done within a budget and time frame, and the fact that there is no negative feedback on poor or risk-increasing decisions.

Based on this model, an analysis technique that can be used reactively following an incident or proactively to identify a risk, can be defined for systems that depend on effective human behaviours (Svedung and Rasmussen 2002). The technique asks us to:

define the layers of control;

identify the relevant people who make decisions about control within each layer (the 'controllers');

for each controller, determine:

- their goals and work objectives,
- performance criteria and targets,
- their capability, and
- the information available.

These influence whether the controller is able to make the appropriate risk control decisions. For each controller, consider whether he or she is willing to make the appropriate risk control decision. This involves examination of priorities and communication that provide awareness of issues. Since most decisions made from day to day are spontaneous (Rasmussen 1997), it is also important to question whether there is anything to prompt a controller of a wrong decision or make a controller aware of outcomes.

Thus Rasmussen suggests that rather than analysing the tasks performed by individuals, an analysis of the requirements and constraints of the workspace is more useful. Although this is incorporated in Reason's model in the organisational slice of Swiss cheese, Reason provides no guidance for how organisational and cultural issues should be examined. The experience of root cause analysis in the healthcare industry demonstrated that in real applications, people have difficulty in going beyond procedural errors in their analysis without guidance (Iedema 2006).

Svedung and Rasmussen (2002) suggest that one role of an audit should be to analyse normal work conditions in the different organisations that may contribute to a failure path to reveal the potential for a connected set of side effects. Rasmussen's model has been extended by Leveson to a model of accident causation, Systems–Theoretic Accident Model and Process, or STAMP (Leveson 2004,) and to a proactive hazard and risk identification process (Leveson and Dulac 2005).

Woods (2000) suggests that a measure of success for a resilient organisation is the ability to 'foresight' changes that might herald a change in risk before failure and harm occur. This involves being aware of the way normal decision-making and change in complex systems can lead to problems. Woods' concept of 'foresight' is similar to the concept of 'mindfulness' (Weick 2001) that has grown out of sociological research into major safety failures, such as train crashes, mine disasters, or explosions. These are often attributed in part to an organisation's 'safety culture'. It is shown that rules, procedures, and management systems to enforce them are not sufficient to achieve a safe system. There needs to be also a set of common values and practices (Hopkins 2005). High reliability organisations 'organise themselves so they are better able to notice the unexpected and halt its development' (Weick 2001).

Weick and Sutcliff (2001) characterise a 'mindful' organisation by:

preoccupation with failure; mindful organisations understand that long periods of success breed complacency;

reluctance to simplify or discard information: mindful organisations socialise their workforce to notice and report, and employ more people for checking and double-checking;

sensitivity to operations: front-line staff and managers strive to understand and remain aware of the current state of operations;

resilience and flexibility in times of high workload or crisis, and

deference to expertise as being more important than organisational hierarchy.

From the work of Reason, Hollnagel, Rasmussen, Weick, Woods and others has grown the concept of resilient organisations and 'resilience engineering'. Resilience engineering looks for ways to enhance the ability of organisations to create processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or ongoing production and economic pressures (Hollnagel, Woods and Leveson 2006). Research in the area is very new and focuses on:

ways to measure organisational resilience (Mendonca 2004);

tools to help organisations recognise and make decisions where there are trade-offs between efficiency and risk, and

techniques to visualise and identify risks that are the side-effects of management decisions and of change (Hollnagel, Woods and Leveson 2006).

Resilience engineering removes the focus completely from identifying the potential for individual error and procedural failure, and looks at management decisions, organisational structures, communications, and foresight or mindfulness. The following section outlines several examples of the methods outlined above.

7.5. Applications

7.5.1. Reason's model

Research into human performance and reliability and the human causes of disasters was mostly initiated and applied to major hazards facilities, driven by a need to understand past disasters and by legislative requirements for a safety case that included quantitative risk assessment to be prepared at the planning stage of new facilities.

Many of the more recent publications on Human Reliability Analysis and human error relate to aviation, mostly in air traffic control, but also for maintenance where high reliability is required. Reason's Swiss cheese model is followed in incident investigation in aviation and rail both in Australia and overseas.

There are a number of papers in medical journals by Reason, Rasmussen and other human factors experts demonstrating application of their techniques to medical error and hospital systems (e.g. Rasmussen 1999; Reason 2001). Ferner and McDowell (2006) reviewed 85 cases of medical doctors charged with manslaughter and classified the errors according to Reason's classification of slips, lapses, mistakes, and violations. Even in this group of incidents that were considered sufficiently blameworthy to warrant prosecution, only four of the 75 cases could be classified as violations (i.e. intentionally not following a known rule).

In Holland, an incident classification system based on the Swiss cheese model has been developed and one version of this (PRISMA Medical) is designed for classifying medical error. Hebraken and Vander Shaaf (2005) reclassified errors recorded in a database in Holland, and found that that the number of root causes/incidents that had been recorded in the existing incident

database was too small and that, compared with the Reason-based classification, individual error was over-represented and organisational factors under-represented.

7.5.2. Application of HRA

Early methods that identified, and in some cases quantified, the probability of errors were mainly funded by, and directed towards the nuclear industry following the Three Mile Island accident. They mostly focused on errors of operators performing relatively routine tasks such as opening valves or switching power. Later methods attempt to address errors in decision making and are applied to error in air traffic control and other transport applications as well as to major hazards.

Tables 7 to 9 provide a set of checklists that can be used either retrospectively (to analyse failures) or proactively (to identify the potential for error in a task or decision). They help extend a root cause analysis to consider error at any level in an organisation in a logical way based on psychological theory. The error mode tables help identify errors that could occur at a future time. These can then be screened to identify which errors would be most critical to the operation of the system being considered so that error-reduction strategies or additional checking can be built into procedures.

The error mechanism table helps to define error reduction strategies and encourages strategies that go beyond training and increased supervision. Where lack of knowledge, skill or experience are identified as likely psychological error mechanisms for a particular error mode, the fact that the link to error mode is retained defines who needs to be trained about what, or gives information on the nature of the additional tasks a supervisor needs to perform. Shorrock's cognitive mapping of error mechanisms can be applied to the performance of managers and the way they make decisions, as well as to staff carrying out routine procedures. PSFs increase the probability of all types of error and a review of PSFs can be carried out to minimise the probability of error.

In addition to the original applications in energy generation and transport, the concepts are beginning to be used to analyse medical error, usually retrospectively, as part of a statistical analysis of the causes of incidents in a particular procedure. For example, Joice *et al.* (1998) used the external error modes classification of the SHERPA HRA technique (Embrey 1986) to classify errors that had occurred in endoscopic surgery. They were able to identify some of the common causes of adverse events in performing these surgical procedures, and hence recommend ways to reduce them.

Some medical applications that claim to be carrying out HRA are not using the techniques based on psychological research that are generally meant by that term. In some cases, the tools used are HAZOP, FMEA, fault tree analysis and root cause analysis with a rather superficial inclusion of error (Dhillon 2003). Inoue and Koizumi (2004) classify medical errors using first the skills, rules, and knowledge classification of error from Rasmussen and Jensen (1974). The next level of classification is according to two lists of direct and indirect threats. Direct threats classify according to whether people, machines, or the environment were involved. The indirect threats appear to be a rather arbitrary list of contributory factors identified from historical incidents. Some are to do with organisational culture, some with procedures, and some with management practices. There is no consideration of error modes, mechanisms or PSFs in this analysis.

There is no evidence of general uptake of formal human factors taxonomies in analysing root causes of individual medical error incidents, or in defining proactive prevention strategies for

medical procedures. Published root cause analyses do not generally indicate a good understanding of error mechanisms and organisational factors.

The concepts of error modes, mechanisms, and PSFs can be applied to identify and reduce the potential for unintentional errors, to improve performance in carrying out procedures, or to improve decisions made by individuals in basically good systems. For example, in biosecurity, they could be applied to surveillance activities where there may be errors in perception, memory, judgment, or action. Another potential application would be to examine human performance in data, collection, entry, and tracking in animal tracing systems, or to testing procedures in laboratories. The objective of this analysis would be to identify factors that decrease human performance or increase the probability of human errors so that procedures can be improved or checks implemented at critical points.

7.5.3. Application of organisational factors analysis

The concepts of Rasmussen's model and of resilience engineering are relatively new. Applications outside major industries and technical organisations to date appear mostly in the research literature. There is, for example, substantial literature on resilience engineering, and demonstration examples of its application can be found in areas ranging from medicine (Hollnagel, Nemeth and Dekker 2008) to analysis of the 2008 global international financial crisis (Sundstrom and Hollnagel 2008). Concepts of organisational mindfulness and strategies to achieve it are being used in healthcare (Issel 2007).

In theory, Rasmussen's model of complex organisations has promise in identifying proactively some of the drivers that send an organisation towards the boundaries of unacceptable risk, and to identify weaknesses in communication, information, and feedback systems that lead to poor decisions. Further research is needed, however, to develop the theory into a practical proactive tool to identify organisational and systemic problems. As measures of organisational resilience are developed further, they could be used as part of an auditing tool to identify where a more detailed analysis of organisational weaknesses would be beneficial.

7.6. Application of human factors methods to biosecurity case studies

7.6.1. Application of HRA methods

Task analysis is a starting point for most of the human factors analysis methods. The methods of Rasmussen and Hollnagel do not identify risks so much as riskiness, or lack of resilience to risk, built into organisations as a result of organisational structures, key performance indicators, and decision and communication pathways. These arise during strategic and operational planning and through organisational restructures. Taken too far, a demand for efficiency inevitably leads to decreasing resilience. Organizations in general do not consider factors that increase risk and decrease resilience when planning organizational change. Resilience engineering methods offer a possible means of doing so.

A key aspect of resilience is being sensitive to the possibility of failure (Hollnagel, Nemeth and Dekker 2008). To be resilient, key people in an organisation must recognise that complex systems

have complex communication paths that are prone to breakdown, and that there are many pressures on individuals at all levels that lead to decisions that retrospectively prove to be poor. Weaknesses must be expected and actively sought to prevent drift towards the boundaries of unacceptable risk. Current research is seeking to identify measures and indicators of organisational resilience that could be used as part of ongoing audits and reviews. Resilience analysis is not yet sufficiently mature, however, to be a practical tool (Hollnagel, Woods and Leveson 2006).

In the Pirbright incident outlined above, identification of a particular individual who made an error is difficult. The problem is clearly about priorities in decisions and information flow. The fundamental problem was in the priority given to fixing the drains, the failure by site personnel to recognise the level of risk posed by the drains, or communicate adequately. Although this is an example of the type of communication and feedback problem discussed by Rasmussen, it is difficult to see that formal methods would readily identify the problem.

7.7. Summary of human and organisational factors methods

Human factors and organisational analysis methods are commonly applied to investigate failure, and are also applied in design of complex technical systems with which people must interact. In spite of the fact that the majority of recommendations in any inquiry into an accident or failure relate to human factors or organisational issues, human factors and organisational analysis methods are seldom applied in practice as a means of identifying risks in advance of failure. The following show promise and are in need of further research, development, or demonstration:

- Applying the taxonomy of error modes, mechanisms, and performance-shaping factors to identifying underlying causes of individual human error in root cause analysis used as either a proactive or reactive tool.
- Applying an understanding of factors that affect individual and organisational performance to the design of procedures and organisational structures.
- Developing measures of organizational resilience to use as part of audit or review to identify where organisations (or subsets of organisations) may be prone to failure.

Further analysis of whether and how the Rasmussen model can be applied to identify organisational weaknesses in the biosecurity area could also be profitable. Barrier analysis techniques alluded to above also show some promise for complex operational circumstances. The following section outlines their use in biosecurity applications.

8. Barrier analysis techniques

Barrier analysis techniques are formal elaborations of the conceptual tools outlined above. The Reason model and Rasmussen's suggestions provide a useful conceptual template and qualitative system for analysing or anticipating failures. The following methods provide a more formal framework for implementing some of these ideas. They are not a complete representation of the systems outlined above, but rather provide a means for representing some of the ideas.

8.1. Bow tie analysis

The bow tie representation of risk revolves around a critical event that forms the knot of the bow tie. The critical event is equivalent to the top event in a fault tree. It is often taken to be the point at which control of the situation is lost, and one moves from prevention to mitigation and recovery. Figure 21 shows a generalised bow tie model. The left-hand side starts with the hazard or source of harm and the threat that is defined in the bow tie as the event of circumstances by which the hazard is released, and that leads to the critical event. Between the threat and the critical event are prevention controls. These are controls that directly prevent the critical event. Following the critical event, there may be ways of mitigating consequences. These are the protection and recovery controls that prevent the critical event leading to various specified consequences. Also included in the model are the management activities that maintain the controls.

Hale *et al.* (2007) discuss the use of the categories in a bow tie for recording and classification of incidents and their causes. In this application it is important to differentiate clearly between similar concepts such as hazard and threat, and the barriers and management support activities. Here the hazard is the source of harm. Shell, one of the earliest proponents of the model, uses the example of LPG gas (Zuijderduijn 1999). The threats are the means by which it is released (e.g. corrosion, valve failure, etc.). The outcome of the work of Hale *et al.* was to define the barriers/controls to be only those things operating in the primary sequence of events between exposure to the hazard, through the loss of control, to the injury. Thus the knowledge of the correct use of equipment or correct procedures to follow is a primary control, but training is a management activity that maintains this barrier and not a barrier in itself.

The bow tie can be regarded as a combination of a fault tree on the left-hand side analysing the causes of the critical event and an event tree on the right-hand side analysing the different possible consequences. Although multiple hazards and multiple threats from each hazard can be incorporated in the tree, the AND/OR logic is not included, and the pathways from hazard to event are assumed to be independent. This means that the model is more appropriate for qualitative use than quantitative. Unlike fault trees, the model draws attention to the controls and can be used to explore the adequacy of the controls. It draws attention to threats for which there are no controls, or only one control, or for which all controls are weak. It also draws attention to controls that are unsupported by management activities, such as monitoring.

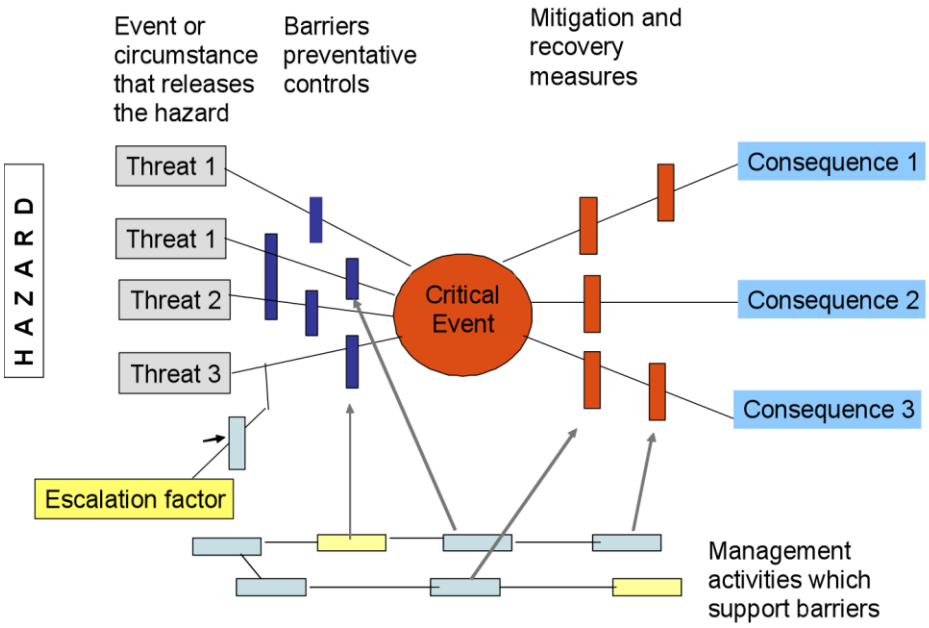

Figure 21. Bow tie analysis.

8.1.1. Applications of bow tie analysis

Bow tie analysis is used in safety applications where it is necessary to provide a documented demonstration that all risks have been reduced to as low as is reasonably practicable in order to comply with safety legislation. For example, bow tie analysis is used in the process industries as the basis for identifying major accident hazards for compliance with the Sveso II Directive and CIMAH regulations (Delvosalle *et al.* 2006, Zuijderduijn 1999). It is used in mining (Iannacchione *et al.* 2008) and in transport. In 2004, the US Federal Aviation Authority (FAA) mandated that its regulated entities employ a bow tie diagram as the main mechanism for safety analyses (FAST 2004). It is commonly used in rail to depict different paths to critical events such as derailment or collision, and to explore the efficacy of barriers to these events (Dabekaussen, Schaaf and Wright 2007; Lloyds Register 2006). It has been proposed for analysis of operational risk in financial institutions to comply with Basel II (McConnel and Davies 2006).

The bow tie diagram helps to display the different components of a risk pathway. Management information systems relating to risks, including incident-reporting databases and risk registers, are often confusing because the way terminology relating to hazards, risks events, consequences, and control failures is used is inconsistent. This becomes particularly problematic if priorities between problems formulated in different ways are set using a qualitative consequence-likelihood matrix. One example is the poor practice of recording the possibility that a barrier might fail as a risk, then ranking it against a risk expressed as the possibility that a threat might lead to a consequence. The priority to be given to a barrier failure depends on the importance of the threat it controls and the criticality of that particular barrier, and not on the probability of failure of the barrier and the consequence associated with that risk pathway.

The bow tie can also provide a unified structure for incident analysis (Hale *et al.* 2007). When used as a method of incident analysis, a bow tie focuses on barriers that failed and the management structures that should have supported them, rather than on the individual failures of personnel. The bow tie also helps inform audits by providing a checklist of barriers and asking whether barriers are actually in place and if the system provides the necessary support.

Hudson and Guchelaar (2003) have attempted to apply a bow tie to the analysis of the critical event of administering the wrong drug to a patient. The method falls down in this application because of the difficulty of identifying a specific hazard. The authors use error modes as the threats, and can produce the rest of the bow tie, but attempts to relate error causes or mechanisms to hazards fail because there are so many error causes that it is impractical to produce a complete diagram. Nevertheless the analysis can be used to review the controls for each threat. Bow tie analysis can also be applied in a medical context to infection control where the hazards are different infections, the threats are the pathways to infection, the knot is patient infected, and outcomes include patient sickness or death, litigation, reputation loss, or the infection becoming widespread.

Bow tie analysis was applied to GM crop hazards in the UK by Pidgeon *et al.* (2007). They demonstrate the technique by considering the risks associated with reduced weeds caused by additional use of chemicals with an herbicide-resistant sugar beet. The critical event analysed was ‘less weed seeds’, and consequences were less seed for granivorous birds, less seeds returned to seed bank, less nectar/pollen for pollinators, and less weeds to host insects for farmland birds. A significant advantage seen by the authors was the ability of a bow tie to illustrate risks and controls to stakeholders (in this case regulators and the public). It helped demonstrate compliance to the regulator and demonstrated to the public both that a detailed analysis had been undertaken and that all risks have controls. It is a simple enough concept to be used in consultation activities to brainstorm risks and controls.

Bow tie analysis is sufficiently commonly used that there are a range of commercial software packages available to assist in drawing a bow tie. Some packages attempt quantitative or semi-quantitative analysis of levels of risk, but since there is no Boolean logic in a bow tie and threats and barriers are not necessarily independent, this is likely to be invalid for most applications.

8.1.2. Application to biosecurity case studies

In the Pirbright FMD incident, it is less clear that the problem would be identified proactively using bow tie analysis, as a key issue is an escalation factor rather than failure of routine barrier. Escape of the virus required both failure of the drains and a means of escape. Bow tie analysis assumes a single threat.

Failure of the waste system may not have been seen as a likely occurrence prior to it happening. It assumed particular importance because of construction activities on-site that may not have been envisaged when a bow tie was drawn. The bow tie analysis (even without the escalation factor identified) is an effective means of communicating the importance of particular control measures from risk experts to lay people and could thus be a useful communication tool between those aware of the biosecurity importance of the drains and those more interested in the terms of the contract between the partners. In this application, the bow tie analysis provides a visual representation of the HACCP application described in Section 3.3. The separate pathways of escape are identified and the controls specified.

8.2. LOPA

Loss of Protection Analysis (LOPA) is a barrier analysis technique that helps organisations analyse, in a structured way, how many safeguards are necessary for a particular failure scenario (Dowell and Hendershot 2002). LOPA is a method for deciding whether there is sufficient control rather than how layers of control might fail. It is therefore not strictly an identification technique.

LOPA focuses on a particular cause-consequence pair (identified through other methods), identifies how many independent layers of protection are provided by existing or proposed safeguards, and decides whether these are sufficient. Unlike bow tie analysis, it focuses on one cause-consequence pair at a time, and only independent layers of protection are included, thus a level of quantification is possible. A layer of protection is defined to be an independent layer if:

- the control would be effective in preventing the cause from resulting in the consequence; i.e. the Independent Protection Layer (IPL) must be specifically designed to prevent or mitigate the consequences;
- the control is independent of the initiating event and the other IPL (i.e. there must be no failure that deactivates two IPLs);
- the safeguard is auditable; and
- the control produces a known change in the probability that the consequences will occur.

Figure 22 shows a flow chart of the process. For each cause-consequence pair, the probability of the cause or initiating event occurring is estimated. This is then reduced by the estimated probability that the IPL will prevent the consequence. It basically separates the probability of failure into two components: the probability of the initiating event, and the probability the controls will fail on demand. From this it is possible to estimate the probability that the consequences will occur and hence whether further safeguards are needed. It can also be used to demonstrate that a low enough probability has been achieved and further safeguards are either not needed or not cost-effective.

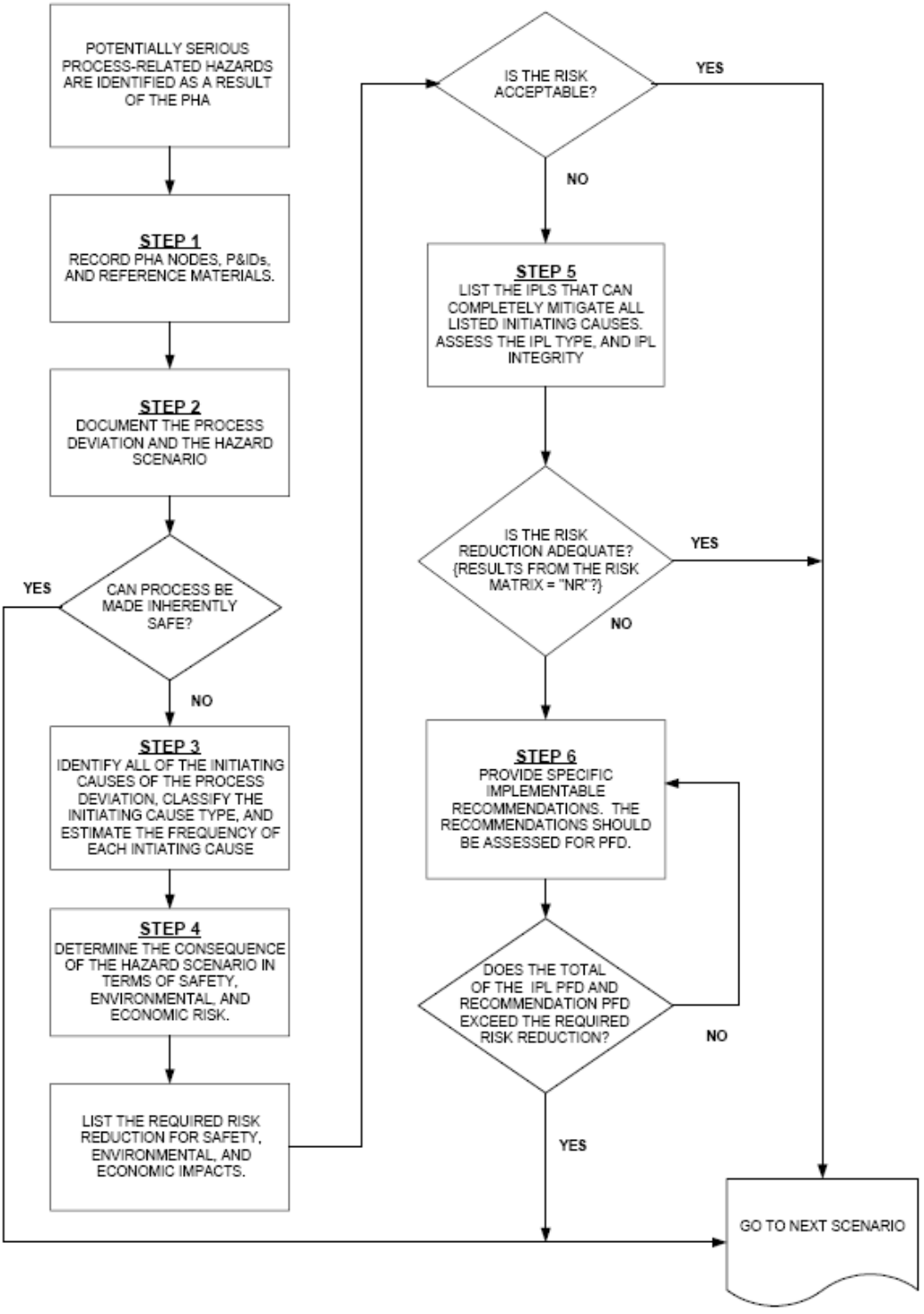

Figure 22. Flow chart of LOPA process.

8.2.1. Applications of LOPA

LOPA is used to design controls in highly reliable systems and to demonstrate that controls are adequate to achieve a desired Safety Integrity Level (SIL). It is primarily designed for Safety Instrumented Systems. The concept of the different layers of protection from design to recovery may be applicable in other areas where high reliability is required.

8.3. Summary of barrier analysis techniques

The bow tie is a structured way of visualising how hazards and risks are managed and consequences prevented. It can be used to demonstrate and communicate to regulators or other stakeholders that all threats are adequately controlled. It is both easy to communicate and an accessible way of thinking about the different components of risk that need to be analysed to understand the issues. It can be applied at several levels of detail (i.e. the threat from a high level bow tie analysis may be used as a critical event in a more detailed study). The bow tie assumes different threats are independent and that once a critical event has occurred, the consequences do not depend on the nature of the threat. This does not apply in all circumstances.

LOPA takes a single cause–consequence pair (which could be a path in a bow tie) and considers whether the controls in the pathway are sufficient. It is used primarily in applications where it is necessary to quantify that a design achieves predefined SIL but the concept of multiple barriers to achieve sufficient reliability is more generally applicable. Summers (2003) suggests that the advantage of LOPA are:

- the scenario-based focus of LOPA often reveals issues that were not identified in previous qualitative hazards analysis;
- hazards are directly connected to the barriers/controls providing clear identification of Safety Instrumented Systems and their associated SILs where these are specified, and
- it can be effective in resolving disagreements related to qualitative hazards analysis findings.

LOPA often identifies acceptable alternatives controls such as adding other layers of protection, modifying the process, or changing procedures, allowing the most cost-effective controls to be identified.

9. Scenario analysis methods

The term ‘scenario analysis’ is used to describe a range of techniques that explore different possible future outcomes, either qualitatively or quantitatively (Swart, Raskin and Robinson 2004; Grant 2004). The term covers techniques that explore possible futures either by extrapolation from the present or by imaginative storytelling and other techniques that consider how a system might behave in different circumstances.

Quantitative scenario analysis includes modelling with different choices for uncertain parameters (e.g. de Weger 2003), and extrapolating data from current trends using different models for how a trend might develop as for example in climate change modelling (Lechtenbömer 2008). In a qualitative scenario analysis, expert opinion and current information and data are used as inputs to an exploration of different hypothetical sequences of events that might follow a particular event or decision. These scenarios describe possible developments starting from what is known about the current situation, and different things that might be expected to happen. An essentially qualitative analysis can be quantified to some degree by estimating the probability of each particular scenario.

Scenario trees may be drawn to provide visual representations of different pathways that may occur. At the other end of the spectrum, scenario analysis is also used to describe foresight and futures analysis techniques where imaginative pictures of the future are developed to help identify new and emerging risks, or to suggest possible long-term effects of current policy decisions. Scenarios may relate to present circumstances or to short, medium or long future time frames. Generally the extrapolation techniques are appropriate for short-term analysis and the more imaginative of the qualitative techniques to long-term planning and strategic analysis.

9.1. Scenario trees

One method of scenario analysis is to build scenario trees. A scenario tree starts from an initiating event and demonstrates the different pathways that can be followed depending on other events or the way that controls are applied. Figure 23 illustrates the structure of a scenario tree. A tree such as the one illustrated, which explores the outcomes of success or failure of a series of controls, is also known as an event tree. The probability of each consequence can be calculated, provided the probability of success of each control is known, by multiplying the probabilities of each component of the pathway leading to that consequence.

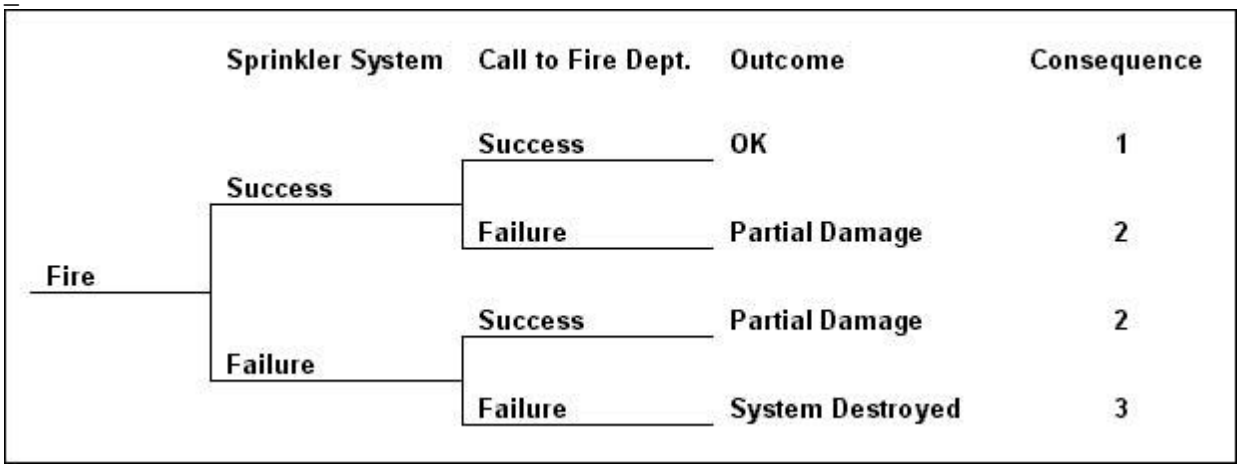

Figure 23. Scenario or event tree.

The term 'scenario tree' is also applied to trees where there are more than two options and the binary logic is not applicable. Scenario trees and event trees provide useful visual representations of risks that can be used to:

identify pathways and variables following an initiating event;

identify information requirements for analysis of outcomes;

ensure a logical chain of events in space and time;

provide a framework for the development of a mathematical model;

assist with communicating the model structure, and

clarify ideas and understanding of the problem (McDiarmid and Pharo 2003).

9.2. Futures, foresight, and integrated assessment

Qualitative scenario analysis involves story-building for imaginative but plausible futures. Within these scenarios, new risks and opportunities can be identified and known risks may be modelled in a different way. Generally, the aim of scenario analysis is not to predict the future but to develop plausible, challenging descriptions of what might happen so as to be better prepared to take advantage of opportunities and avoid potential threats. Scenario analysis can also be used to identify emerging risks and risks that might result in loss well into the future, but be the result of decisions made now (Swart, Raskin and Robinson 2003).

Techniques that combine modelling with social science techniques of scenario-building are sometimes called integrated assessment (IA). IA can be defined as an interdisciplinary process of combining, interpreting, and communicating (Van der Sluijs 2008). A subset of IA, known as participatory integrated assessment (PIA), includes techniques for involving stakeholders in scenario development and interpretation.

Detailed scenarios are often developed by thinking about changes that might occur or that are already occurring such as environmental changes, technical changes, political, or regulatory changes, etc. For example, one might develop a number of scenarios based on different predictions for future climate change and/or extrapolations of already occurring changes in world

demographics. Some characteristics of stakeholders within scenarios remain unchanged (such as their basic needs). Others, such as perceptions and values, may change. This information can be fed into the scenarios. Taking these basic ideas, the background for several possible futures is developed as if it were the background for a story. An important aspect of IA is that it can introduce potential discontinuities into the future that would be missed in modelling based on current knowledge or in long-term trends analysis.

Futures and foresight analysis is often based on regular horizon scanning. DEFRA defines horizon scanning as 'the systematic examination of potential threats, opportunities and likely future developments that are at the margins of current thinking and planning' (DEFRA 2008b). Rotmans *et al.* (2000) suggest that scenarios should focus on 'weak signals' that could come to dominate the future. They point out, however, that one clear lesson to be learned from scenario-based assessments made in the 1970s and 1980s is that dogmatic predictions regarding the future are unreliable and can be counterproductive.

Futures scenarios are only defined 'slices' of possible futures; it is usual therefore to take some account of the likelihood of a particular scenario occurring. For example, where best case, worst case, and expected case scenarios are used, some attempt should be made to qualify, or express the likelihood, of each scenario occurring.

9.3. Applications of scenario analysis

Scenarios can be used as a context to identify risks that would be relevant to the particular scenario should it occur or to look at the risks associated with scenarios that could be the outcome of different policy decisions. Scenarios can also be used to identify desirable over undesirable futures and hence to drive policy.

Scenario analysis is used across a wide range of disciplines. In engineering, it may be used to explore different design options by considering how they might perform under different scenarios. For example, de Weger applied a quantitative scenario analysis to optimising the design of road tunnels to cope with different accident scenarios. It is used in emergency planning and business continuity management often to check that generic plans will be appropriate for the range of disruptive events that might occur (e.g. Brown and Dunn 2005) Scenario analysis is used in financial planning and forecasting (e.g. Cavello and Tiulle 2006), and in business applications where different scenarios represent customer behaviours, the economic climate, or other key variables (e.g. Grant 2004). It is also used in strategic planning, both to imagine possible futures in which an enterprise operates, and to explore implications of a range of possible plans (Shoemaker 1993)

9.3.1. Application of scenario building, integrated analysis and foresight

Scenario building and analysis has been used by the Shell group of companies for more than 30 years as part of strategic planning. It is increasingly used by governments to support policy decisions on complex issues such as those related to the environment and sustainability (EEA 2001). The different scenarios considered may be expected changes in climate, demographics, or technology, or may be different policy decisions that are then followed through considering other likely social, technical, and economic changes. An example of using different policy choices to form the scenarios is presented by Tobara, Polo and Lemkov (2003) who explored implications

for three regulatory approaches to GMOs. These were full liberalisation, restricted liberalisation, and an indefinite moratorium.

Van Asselt *et al.* (2000) reviewed the Visions project set up by the Research and Development Unit of the European Commission. In their review, they provided a detailed description of scenario analysis and reviewed 40 European scenario analyses relating to sustainable development.

There are a large number of analyses of the effect of climate change and socioeconomic changes on agriculture (Fischeri *et al.* 2005; Berkhout 2002; Mohren 2003; Defra 2005). Some take a modelling approach, extrapolating from current data and incorporating different climate or other change models, and some take a sociological approach with discussions involving experts and stakeholders. The latter are better able to take into account factors that depend on perceptions and behaviours and to consider the 'so what' and 'what should be done' questions (Cohen 1997). For example, Pauly *et al.* (2003) used scenario analysis to consider the effect of various societal development choices on the future of fisheries and to suggest ways of turning round current negative trends.

The limitations of scenario analysis have been studied by Gleick (1999), who reviewed projections of water usage in 2000 from the 1960s, and demonstrated both the huge variability of predictions based on various assumptions made, and that extrapolating from the present without taking into account new developments and changes does not reliably predict the future. Estimates made 30 years earlier predicted nearly twice the water usage that actually occurred. This was partly due to failure of some parts of the world to keep up with the demand such that there were water shortages, and partly because improvements in water use efficiency were not predicted. This illustrates the problems of modelling, as extrapolation without imaginative consideration of the future once time lines become extended.

9.3.2. Applications of scenario analysis and scenario trees in biosecurity

Import risk assessments in Australia and overseas commonly commence their analysis by defining one or more scenarios of a potential outbreak. Scenario analysis is currently used in biosecurity as part of risk assessment by postulating exposure pathways from source to effect. In some cases this is shown pictorially, and in others demonstrated through the structure of the report. The BA scenarios include (Cooper and Beckett 2005):

- geographical distribution of the outbreak, and whether the outbreak is likely to be unifocal or multifocal;
- animal or plant species and industries that are directly involved;
- animal or plant species and industries that are indirectly involved; and
- duration of the outbreak, from the exposure of susceptible animal, plant, or human hosts to eradication or the establishment of an endemic state within Australia.

The scenario description is usually followed by qualitative or quantitative modelling of consequences of each pathway or of its level of risk. As well as defining a baseline scenario, the effect of different assumptions within the scenario can be modelled and compared with the base model. This is demonstrated by Adkins *et al.* (2005) in the assessment of the disease risk posed to the livestock population of Great Britain from the illegal importation of meat and meat products. Scenario trees have been drawn to represent the risk of BSE infectivity from disposal of sheep

(Figure 24), and to show the risk of exposing backyard chickens to avian influenza through imports of chicken or frozen chicken meat in New Zealand (McDiarmid and Pharo 2003) (Figure 25).

–

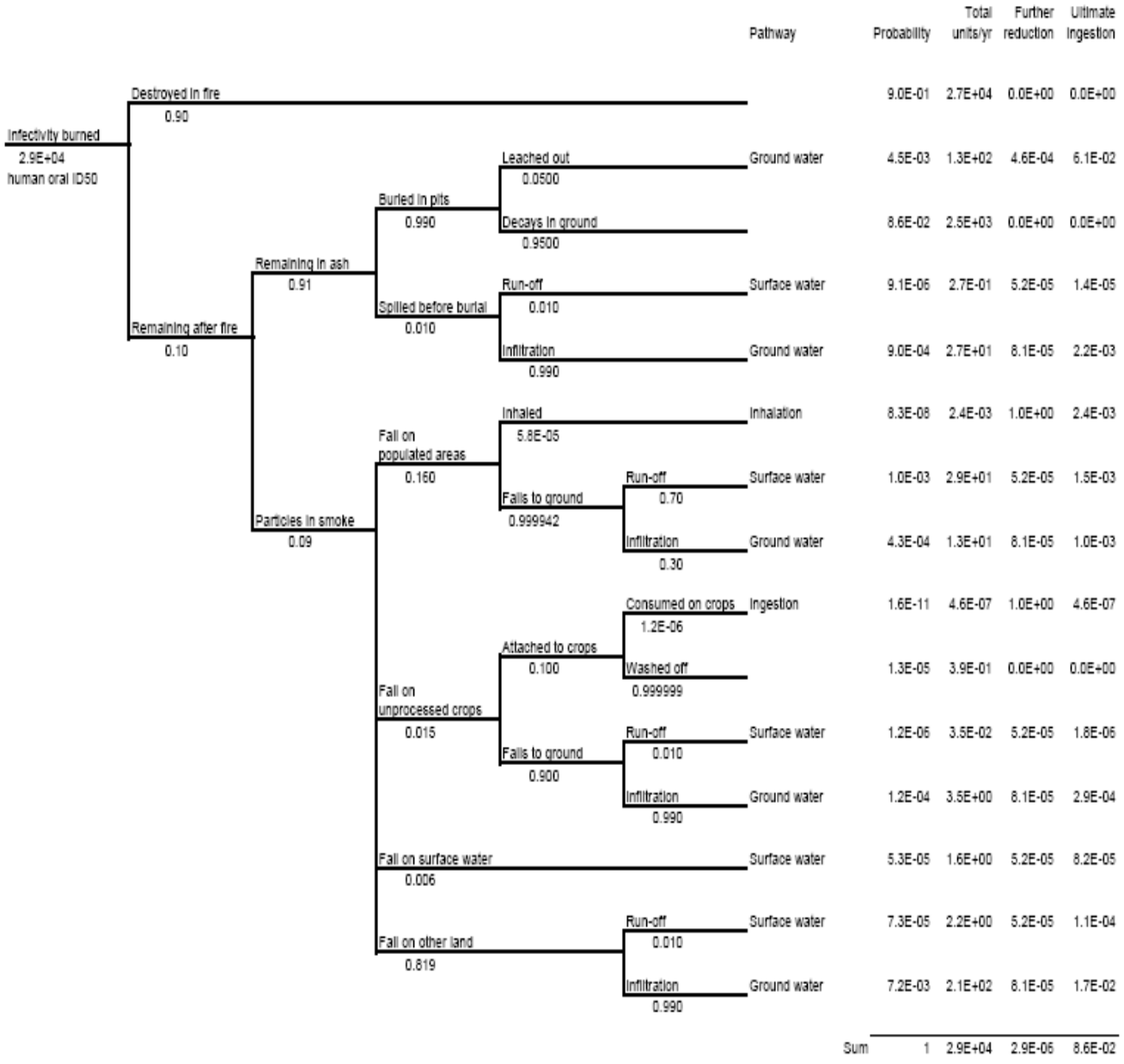

Figure 24. Scenario tree for infectivity from burning sheep.

–

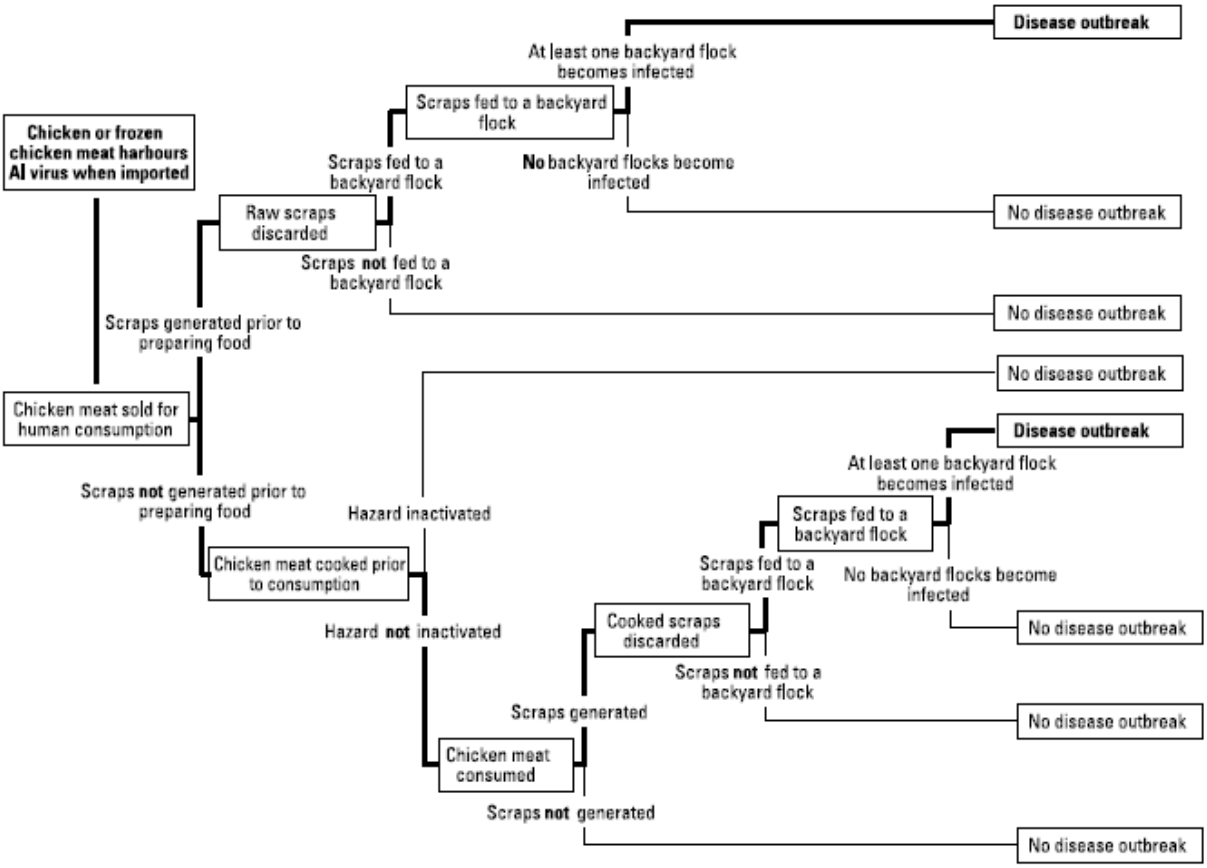

Figure 25. Scenario tree for avian influenza outbreak (McDiarmid and Pharo 2003).

There are many papers reporting the use of scenario analysis as part of policy analysis for agricultural planning. For example, the Food and Agricultural Policy Research Institute (FAPRI) in the US has used scenario analysis to provide economic analysis of agricultural policy options (FAPRI 2007). Aruofor (2000) used scenario analysis to predict possible future states of the forestry industry in Nigeria in 2020 to determine interventions that are needed.

Following the BSE outbreak in the UK, a new Policy and Corporate Strategy Unit was established in MAFF (Ministry for Agriculture, Fisheries and Food). This unit commissioned a scenario building exercise to assist in the Ministry's strategic planning. The work was conducted by the Henley Centre but was never published, as MAFF became involved in the FMD crisis and was replaced by DEFRA. The first phase of the work identified a series of drivers that was felt would shape the future environment. This phase of work and the scenarios that were developed from it are reported by Ward and Ray (2004). They stated that although these scenarios were not used directly by Government, they have informed subsequent (unspecified) 'work'. When DEFRA was established to replace MAFF, a new horizon-scanning program was commenced.

The initial program followed five themes:

> **Environmental constraints** is concerned with limitations on natural resources and effects of human intrusion into natural systems.

Coping with change aims to assess vulnerabilities to new threats and to improve society's capacity to adapt.

Future landscapes is concerned with urban and rural landscapes, broadly defined, with the forces that are likely to shape them in future.

Meeting people's future needs is concerned with people, communities, cultures, and lifestyles, and the ways in which the wants and needs of the general public and groups within it should influence DEFRA's policy agendas.

Re-thinking the food economy explores the options for creating food chains providing safe, nutritious food to the market at affordable prices.

In 2006 the program was reviewed. The outcomes of the review and future directions for the Horizon Scanning Unit in DEFRA are available on the DEFRA website (DEFRA 2008c).

9.4. Summary of scenario analysis methods

Scenario analysis methods explore what might happen and how in the future to inform decision making. They are quite widely used in biosecurity to explore possible pathways for entry and spread of pests and diseases and for both long and short-term policy development in agricultural areas. They are also useful as part of planning a response to an outbreak of disease or other emergency situations. There is a very wide spectrum of types of scenario analysis that have been described briefly here. There is potential for increased use of all of the different techniques in their different applications but particularly for incorporating greater consideration of hypothetical futures into long-term strategic planning.

10. Conclusions

A range of techniques used to identify issues in process and other engineering industries have been described. They are being applied increasingly outside engineering applications, particularly in healthcare. Some are already used in biosecurity-related applications and some have been demonstrated to be feasible. Different techniques are useful in different situations. Possible applications have been described for each technique.

Two case studies were chosen to demonstrate some of the techniques. In some instances, particularly in causal analysis, engineering tools are not ideal for biosecurity applications. Human factors are likely to be important in many biosecurity systems and appropriate tools will be required. Where techniques were clearly not relevant to these case studies, other applications are identified.

It is not possible to recommend any technique above all others because their use depends on the problem to be solved. For example, assessment of risk from particular hazards requires quite different thinking to assessment of risks that arise from organisational structures or human performance. This report has attempted to provide an overview that will suggest where analytical techniques that could identify issues and reduce the risk of loss might best be applied. It is possible to image useful results from the application of all of these techniques. The hypothetical examinations of FMD and EI indicate some possibilities, although any operational deployment of particular techniques would need to consider both the potential benefits and costs of their implementation.

11. References

ACERA Report 0608 (2006) Strategies for effective communication of probabilities. C Caponecchia. ACERA, University of Melbourne.

ACERA Report 0611 (2008) Eliciting expert judgements. M Burgman, F Fidler, L Flander, M McBride, T Walshe, B Wintle. ACERA, University of Melbourne.

ACERA Report 0801 (2009) Using stakeholder mapping and analysis with a mental models approach for biosecurity risk communication with peri-urban communities. J Gilmour, R Beilin, T Sysak. ACERA, University of Melbourne.

Adkins (2005) http://collections.europarchive.org/tna/20050301192907/http://www.defra.gov.uk/animalh/illegali/pdf/risk-assessment04.pdf

Animal Health Australia (2005) Risk Management User Manual, Version 11, http://www.animalhealthaustralia.com.au/wp-content/uploads/2011/04/risk_manual.pdf

Altekruse SF, Cohen ML and Swerdlow DL (1997) Emerging food borne diseases. *Emerging Infectious Diseases*, 3(3): 285–293.

APHA (1972) Proceedings of the 1971 National Conference on Food Protection. American Public Health Association, Washington DC.

Arvanitoyannis IS and Varzakas TH (2007) Application of failure mode and effect analysis (FMEA) and Pareto diagram in conjunction with HACCP to a potato chips manufacturing plant. *International Journal of Food Science and Technology* **42** (12): 1424–1442.

Aruofor R (2000) Forestry Outlook Studies in Africa, Food and Agricultural Organisation of the United Nations www.fao.org/docrep/004/AB592E/AB592E06.htm

Baines RN, Ryan PJ and Davies PW (2004) HACCP at the farm level – the missing link in food safety and security. International Food and Agribusiness Management Association Conference, Montreaux. http://www.ifama.org/tamu/iama/conferences/2004Conference/Papers/Baines1095.pdf

Benneyan JC, Lloyd RC and Plsek PE (2003) Statistical process control as a tool for research and healthcare improvement. *Quality and Safety in Health Care* **12**: 458–464.

Berkhout F, Hertin J and Jordan A (2002) Socio-economic futures in climate change impact assessment: using scenarios as learning. *Global Environmental Change* **12**(2): 83–95.

Brown D and Dunn WE (2005) Application of a quantitative risk assessment method to emergency response planning. *Computers and Operations Research* **34** (5): 1243–1265.

Bryan FL, Smith JD and Mckinley TW (1980) Hazard analysis of frozen dinners prepared at a catering establishment. *Journal of Food Protection* **43**: 512–513.

Buijs F, Simm J, Wallis M and Sayers P (2007) Performance and reliability of flood and coastal defences. R&D Technical Report FD2318/TR2, DEFRA, UK. http://sciencesearch.defra.gov.uk/Document.aspx?Document=FD2318_5926_TRP.pdf

Burgman M (2005) *Risks and decisions for conservation and environmental management.* Cambridge University Press, Cambridge, UK.

Callaghan (2007) *A review of the regulatory framework for handling animal pathogens*. Presented to the Secretary of State for Environment, Food and Rural Affairs 13 December 2007. DEFRA, HMSO, UK.

Callinan I (2008) *Equine Influenza. The August 2007 Outbreak in Australia*. Report of the Equine Influenza Inquiry, Commonwealth of Australia, http://www.equineinfluenzainquiry.gov.au/eiiexhibits/REP.0001.001.0001.pdf

Food Safety Enhancement Program Manual (2010), Canadian Food Inspection Agency http://www.inspection.gc.ca/english/fssa/polstrat/haccp/manue/tablee.shtml

Carey JM, Burgman MA, Miller C and CheeYE (2005) An application of qualitative risk assessment in park management. *Australasian Journal of Environmental Management* **12** 6–15.

Carrico R and Ramırez J (2007) A process for analysis of sentinel events due to health care-associated infection. *American Journal of Infection Control* **35** (8), 501–507.

Cavello M and Tille C (2006) Current account adjustment with high financial integration: A scenario analysis. *Economic Review.* Publication of the Federal Reserve Bank of San Francisco http://www.frbsf.org/publications/economics/review/2006/er2006.pdf#page=34

CDC (2006) Centre for Disease Control and Prevention USA. www.cdc.gov/biosense/publichealth.htm

Cohen S (1997) Scientist–stakeholder collaboration in integrated assessment of climate change: lessons from a case study of Northwest Canada. *Environmental Modelling and Assessment* **2** (4): 1420–2026.

Coles G, Fuller B, Nordquist K and Kongslie (2005) Using failure mode effects and criticality analysis for high-risk processes at three community hospitals. *Journal of Quality and Patient Safety* **31** (3) 132–140.

Cormier, SM and Suter, GW (2008), A framework for fully integrating environmental assessments, *Environmental Management* 42:543-556

Cullen (1990) *Public Inquiry into the Piper Alpha Disaster*. HMSO, UK.

Dabekaussen M, van der Schaaf T and Wright L (2007) Improving incident analysis in the Dutch railway sector, *Safety Science Monitor* 1: 1–10.

Dailey L,Watkins RE and Plant AJ (2007) Timeliness of data sources used for influenza surveillance. *Journal of the American Medical Informatics Association* **14** (5): 626–631.

Dairy Australia (2008) http://www.dairyaustralia.com.au/content/view/386/317/

Dawson DM and Brooks BJ (1999) *Esso Longford Gas Plant accident.* Report of the Longford Royal Commission. Government Printer for the State of Victoria.

DAFF 2002 Meat hygiene assessment: Objective methods for the monitoring of processes and product. http://www.daff.gov.au/__data/assets/pdf_file/0009/129285/meat_hygiene_assessment_2nd_ed.pdf.

DEFRA (2003a) *Delivering the evidence: Defra's Science and Innovation Strategy 2003–06*. Department for Environment, Food and Rural Affairs, HMSO, London.

DEFRA (2008a) Department for Environment, Food and Rural Affairs Impacts on Climate Change on Agriculture. A vision for our rural landscapes. http://www.defra.gov.uk/farm/environment/climate-change/pdf/seminar-report.pdf

DEFRA (2008b) Department for Environment, Food and Rural Affairs http://horizonscanning.defra.gov.uk/

DEFRA (2008c) Looking back at looking forwards, Next steps for Horizon Scanning and Futures. Department for Environmental Affairs, United Kingdom. http://horizonscanning.defra.gov.uk/ViewDocument_Image.aspx?Doc_ID=192

Delvosalle C, Fievez C, Pipart A and Debray B (2006) ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. *Journal of Hazardous Materials* **130,** 200–219.

Department of Veterans Affairs (2011) [online]: http://www.patientsafety.gov/SafetyTopics.html#HFMEA

DeRosier J, Stalhandske E and Bagian JP (2002) Using health care failure mode and effect analysis: the VA National Center for Patient Safety's prospective risk analysis system. *Journal of Quality Improvement* **28**: 248–67.

de Weger D (2003) *Scenario Analysis for Road Tunnels*. Safety and Reliability (Eds T Bedford, PHAJM van Gelder). Swets and Zeitlinger, Lisse.

DPI NSW (2008) http://www.dpi.nsw.gov.au/aboutus/news/recent-news/agriculture-news-releases/

Dhillon BS (2003) *Human reliability and error in medical systems*. Series on Industrial and systems engineering, Volume 2. World Scientific, New Jersey.

Dowell AM and Hendershot DC (2002) Simplified risk analysis: layer of Protection Analysis (LOPA) AIchE national meeting paper, 218a

EEA (2001) European Environmental Agency. Scenarios as tools for international environmental assessment. *Environmental Issue Report* **24**. EEA, Copenhagen.

Embry DE (1986) SHERPA a systematic Human error reduction and prediction approach. Paper presented at the International Topical Meeting on Advances in Human Factors in Nuclear Power Stations. Knoxville, Tennessee.

Ericson C (1999) Fault tree analysis – a history. Proceedings of the 17th International System Safety Conference, Washington, http://www.fault-tree.net/papers/ericson-fta-history.pdf

Ericson C (2000) Accident analysis using EEFTA. Proceedings of the 18th International System Safety Conference, Washington http://www.fault-tree.net/papers/ericson-evidence-tree.pdf

FAPRI (2007) http://www.reeis.usda.gov/web/crisprojectpages/203294.html

FAST (2004) Toolsets / System Safety Management Program- Section 4. Federal Aviation Authority Acquisition System Toolset; http://fast.faa.gov/docs/SRMGSA_1.5.pdf

Fennel D (1988) Investigation into the King's Cross fire. Department of Transport, HMSO, UK.

Ferner RE and McDowell SE (2006) Doctors charged with manslaughter in the course of medical practice: 1795–2005: a literature review. *Journal of the Royal Society of Medicine* **9**: 309–314.

Fischer G, Shah M, Tubiello FN and van Velhuizen H (2005) Socio-economic and climate change impacts on agriculture: an integrated assessment, 1990–2080. *Philosophical Transactions of the Royal Society B* **360**: 2067–2083.

Fox D (2007) Statistical methods for biosecurity monitoring and surveillance. I: Control charting. ACERA, Melbourne. www.acera.unimelb.edu.au/materials/endorsed/0605.pdf

Gilchrist IM, Bryony DF and Patel JP (2008) An outpatient parenteral antibiotic therapy (OPAT) map to risks associated with an OPAT service. *Journal of Antimicrobial Chemotherapy* **62**: 177–183.

Grant R (2004) *Contemporary Strategy Analysis*. Wiley, Chichester.

Grimes T and Jackson C (2001) Code of Practice for Biosecurity in the Egg industry. RIRDC Publication No. 01/102. http://www.rirdc.gov.au/reports/EGGS/01-109.pdf

Habraken M, van der Schaaf T (2005) Biases in a medical incident causation database: a quantitative evaluation using PRISMA-Medical. ACM International Conference Proceeding Series Volume 132. Proceedings of the 2005 annual conference on European association of cognitive ergonomics, pp. 175–181.

Hansson SO (2004) Philosophical perspectives on risk. *Techné Research in Philosophy and Technology* **8** (1): 10-35.

Hale A, Ale BJM, Goossens LH, Heijera JT, Bellamy LJ, Mud ML, Roele A, Baksteen H, Post J, Papazoglou IA and Bloemhoff A (2007) Modeling accidents for prioritizing prevention. *Reliability Engineering and System Safety* **92:** 1701–1715.

Hartnett E, Seaman M, Adkin A, Cooper J, Watson E, Cox T, and Wooldridge M (2003) Risk assessment for the import of meat and meat products contaminated with foot and mouth disease virus into Great Britain and the subsequent exposure of GB Livestock. Summary prepared for 35th General Session of the European Commission for the control of Foot-and-Mouth disease (Eu FMD).

Hayes K (1998) Ecological risk assessment for ballast water introductions. *ICES Journal of Marine Science* **55**: 201–212.

Hayes K (2002a) Robust methodologies for ecological risk assessment - Best practice and current practice in ecological risk assessment for Genetically Modified Organisms (CSIRO report is based on the proceedings of the workshop on best practice risk assessment for genetically modified organisms. CSIRO Division of Entomology, Canberra, 4–5 April 2002 (http://crimp.marine.csiro.au/ERAworkshop.htm).

Hayes K (2002b) Identifying hazards in complex ecological systems. Part 1: fault-tree analysis for biological invasions. *Biological Invasions* **4**: 235–249.

Hayes K (2002c) Identifying hazards in complex ecological systems. Part 2: Infection modes and effects analysis for biological invasions. *Biological Invasions* **4**, 251–261.

Heggum C (2006) Application of HACCP in the production handling and use of feed. IDF/FAO symposium on dairy safety and hygiene. A farm-to-table approach for emerging and developed dairy countries.
http://www.milkproduction.com/Library/article_series/idf_fao_symp/A+farm-to-table.htm

Hennessy R and Barry S (2006) DAFF Risk analysis stocktake. Australian Government Department of Agriculture, Fisheries and Forestry, Canberra.

Hill AB (1965) The environment and disease: association or causation? *Proceedings of the Royal Society of Medicine* **58**: 295–300.

Her Majesty's Revenue and Customs (2003) Departmental Management Committee Meeting, 21 October 2003, United Kingdom http://www.hmrc.gov.uk/management_committee/dmcm-21-10-03.htm

Her Majesty's Stationary Office (1991) GENHAZ - A System for the Critical Appraisal of Proposals to Release Genetically Modified Organisms into the Environment, 14th Report from the Royal Commission on Environmental Pollution, United Kingdom.

HM Treasury (2006) Risk: Good Practice in Government. HMSO, UK. http://www.hm-treasury.gov.uk/psr_governance_risk_good_practiceguide.htm

Hollnagel E (1999) Anticipating failures: What should predictions be about? NATO Research and Technology Organisation meeting proceedings **32,** Human Factors and Medicine panel, Italy.

Hollnagel E, Woods DD and Leveson N (ed) (2006) Resilience engineering: concepts and precepts. Ashgate Publishing, United Kingdom,

Hollnagel E, Nemeth PC and Dekker S (2008) Resilience engineering perspectives: Remaining sensitive to the possibility of failure. Volume 1. Ashgate Studies in Resilience Engineering.

Hopkins A (2005) *Safety Culture and Risk: the organisational causes of disaster*. CCH, Sydney.

Horchner PM, Brett D, Gormley B, Jenson I and Pointon A (2006) HACCP-based approach to the derivation of an on-farm food safety program for the Australian red meat industry. *Food Control* 17: 497–510.

Health and Safety Executive (2007) Final report on potential breaches of biosecurity at the Pirbright site 2007, Government of United Kingdom, http://www.hse.gov.uk/news/archive/07aug/finalreport.pdf

Hudson PTW and Guchelaar HJ (2003) Risk assessment in clinical pharmacy. *Pharmacy World and Science* **25** (3): 98–103.

Hulzebos L and Broekstra J (2007) ERDS Emerging Risks Detection Support Project Report,Agrotechnology and Food Innovations B.V, The Netherlands, http://www.wageningencns.wur.nl/NR/rdonlyres/2F05BDE6-371B-4D0D-A61E-BCA3800DDF74/63919/rapport.pdf

Iannacchione AT, Esterhuizen GS and Tadolini C (2008) Using Major Hazard Risk Assessment to Appraise and Manage Escapeway Instability Issues: A Case Study, The National Institute for Occupational Safety and Health (NIOSH), U.S.A, http://origin.cdc.gov/niosh/mining/pubs/pdfs/umhra.pdf

International Electortechnical Commission (2001) International Standard IEC 61882 Hazard and Operability Study, Geneva

Iedema RAM, Jorm C, Braithwaite J, Travaglia J and Lum M (2006) A root cause analysis of clinical error: Confronting the disjunction between formal rules and situated clinical activity. *Social Science and Medicine* **63**, 1201–1212.

IPPC 2004. ISPM 11 pest risk analysis for quarantine pests including analysis of environmental risks and living, modified organisms. FAO, Paris.

Inoue K and Koizumi A (2004) Application of human reliability analysis to nursing errors in hospitals. *Risk Analysis* **24** (6) 1459–1473.

Ishikawa K (1982) Guide to Quality Control, Quality Resources. White Plains, NY.

Issel LM and Narasimha KM (2007) Creating complex health improvement programs as mindful organizations: From theory to action. *Journal of Health Organisation and Management* **21** (2), 166–183.

Joice P, Hanna GB and Cuschieri A (1998) Errors enacted during endoscopic surgery--a human reliability analysis. *Applied Ergonomics* 29 (6), 409–414.

Kennedy B and Kirwan B (1998) Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high-risk systems. *Safety Science* **30**: 249–274.

Kim MC, Seong PY and Hollnagel EA (2004) Probabilistic approach for determining the control mode in CREAM. *Reliability Engineering and System Safety* **91**: 191–199.

Kimchi-Woods J and Shultz. JP (2006) Using HFMEA to assess potential for patient harm from tubing misconnections -Failure Mode and Effects Analysis. *Joint Commission Journal on Quality and Patient Safety* **32** (7): 373–381.

Kirwan B (1998a) Human error identification techniques for risk assessment of high risk systems; Part 1: Review and evaluation of techniques. *Applied Ergonomics* **29** (3): 157–177.

Kirwan B (1998b) Human error identification techniques for risk assessment of high risk systems; Part 2: towards a framework approach. *Applied Ergonomics* **29** (5): 299–318.

Kirwan B (1994) A Guide to Practical Human Reliability Assessment, Taylor and Francis, London.

Kletz TA, Chung P, Broomfield E and Shen-Orr C (1995) *Computer Control and Human Error*. Institution of Chemical Engineers.

Lechtenböhmer S (2008) Target 2020: a quantitative scenario on greenhouse gas emission reductions for the EU 25. European Foresight Monitoring Network www.foresight-network.eu/index.php?option=com_docman&task=doc_view&gid=337

Lee K and McGreevey C (2002) Using control charts to assess performance measurement data. *Journal of Quality Improvement* **28** (2), 90–101.

Leveson NG (1995) *Safeware: System Safety and Computers*. Addison-Wesley.

Leveson N (2004) A new accident model for engineering safer systems. *Safety Science* **42** (4): 237–270.

Leveson N and Dulac N (2005) Safety and risk driven design in complex systems of systems Ist NASA/AIAA Space Exploration Conference, Orlando. http://pdf.aiaa.org/preview/CDReadyMSEC05_1205/PV2005_2558.pdf

Lloyds Register (2006) Qualitative assessment of current defences of driver incapacitation. Report for the Independent Transport Risk and Reliability Regulator NSW, http://www.transportregulator.nsw.gov.au/rail/publications/presentations_papers/Qualitative%20_Assessment_Lloyds_Register.pdf, Sydney, Australia

Lyons M., Adams S, Woloshynowych M and Vincent C (2004) Human reliability analysis in health care – A review of techniques. *International Journal of Risk and Safety in Medicine* **16**: 223–237.

Makin AM and Winder C (2008) A new conceptual framework to improve the application of occupational health and safety management systems. *Safety Science* **46**: 935–948.

Mayes T and Kilsby DC (1989) The use of HAZOP hazard analysis to identify critical control points for the microbiological safety of food. *Food Quality and Preference* **1** (2), 53–57.

McConnel P, Davies M Safety First – Scenario Analysis under Basel II http://www.baselalert.com/data/basel_article_free/april06technical.pdf

MacDiarmid SC and Pharo HJ (2003) Risk analysis assessment management and communication. *Revue scientifique et technique de l'Office International des Épizooties* **22**(2): 39–408

McDonough JE (2002) Proactive hazard analysis and health care policy. http://www.milbank.org/reports/Proactive/020925Proactive.html

McInerney PAS (2005) Special Commission of Inquiry into the Waterfall Rail Accident-Final Report,Volume 1, NSW Government, NSW

Mendonca D (2009) Cognitive Underpinnings of Resilience: A Case Study of Group Decision in Emergency Response, *Resilience Engineering Perspectives Volume 1. Remaining Sensitive to the possibility of failure*. (Eds E Hollnagel, PC Nemeth and S Dekker). Ashgate, Aldershot.

Department of Defense (1949) Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis, United States of America

Department of Defense (1980) Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis, United States of America

Department of Defense (1994) Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis, United States of America

Mohren G (2003) Large-scale scenario analysis in forest ecology and forest management. *Forest Policy and Economics* 5 (2): 103–110.

Monti J, Jefferson L, Mermel S and Parenteau S (2005). Use of failure mode and effect analysis (FMEA) to improve active surveillance for methicillin-resistant Staphylococcus aureus (MRSA) at a university-affiliated medical center. *American Journal of Infection Control* **33**(5): 158.

Morrison LW (2008) The use of control charts to interpret environmental monitoring data. *Natural Areas Journal* **28** (1): 66–73. http://science.nature.nps.gov/im/units/htln/library/monitoring/JournalArticles/naar-28-1-66-73-e.pdf

NAO (2004). Managing risk to improve public services – Report by the Auditor and Controller General, National Audit Office, UK.
http://www.nao.org.uk/publications/0304/managing_risks_to_improve_publ.aspx

OIE (2011) *Terrestrial Animal Health Code*. World Organisation for Animal Health, Paris. http://www.oie.int/international-standard-setting/terrestrial-code/access-online/

Page E (1954) Continuous Inspection Scheme. *Biometrika* **41**: 100–115.

Patz J A, Daszak P, Tabor G M, Aguirre A A, Pearl M, Epstein J, Wolfe N D, Kilpatrick A M, Foufopoulos J, Moyneux D, Bradley D J, Members of the Working Group on Land Use Change, Disease Emergence, (2004) Unhealthy landscapes: policy recommendation on land use change and infectious disease emergence. *Environmental Health Perspectives* **112**:1092-1098

Pauly D, Alder J, Bennet E, Christensen V, Tyedmers P and Watson R The future for fisheries. *Science* **202**(5649) 1359–1361.

Pidgeon JD, May MJ, Perry JN and Poppy GM (2007) Mitigation of indirect environmental effects of GM crops. *The Royal Society Proceedings, Biological Sciences*. **274** (1617): 1475–1479.

Poloniecki J, Valencia O and Littlejohns P (1998) Cumulative risk adjusted mortality chart for detecting changes in death rate: observational study of heart surgery. *British Medical Journal* **316**:1697–1700.

Rasmussen J. (1997) Risk management in a dynamic society: a modeling problem. *Safety Science* **27** (2) 183–213.

Rasmussen J (1999) The concept of human error: Is it useful for the design of safe systems in health care? In *Risk and Safety in Medicine* (Eds C Vincent and B DeMoll), pp. 31–47. Elsevier, London.

RCEP (1993) News release September 1993. RCEP, London. http://tna.europarchive.org/20080610180247/http://www.rcep.org.uk/news/93-7.htm

Reason J (1980) *Human Error*. Cambridge University Press, Cambridge, UK.

Reason J (2001) Understanding adverse events: The human factor. In *Clinical Risk Management: Enhancing Patient Safety* (Ed. Charles Vincent). BMJ Books, London.

Reneau J and Lukas K (2006) Using statistical process control methods to improve herd performance. *Veterinary Clinics of North America: Food Animal Practice* **22** (1): 171–193.

Rogers CA, Reeves BC, Caputo M, Ganesh JS, Bonser RS and Angelini GD (2004) Control chart methods for monitoring cardiac surgical performance and their interpretation. *Journal of Thoracic and Cardiovascular Surgery* **128**(6): 811–819.

Rotmans J, van Asselt M, Anastasi C, Greeuw S, Mellors J, Peters S, Rothman D and Rijkens N (2000) Visions for a sustainable Europe. *Futures* **32:** 809–831.

Rzepnicki TL and Johnson P (2005) Examining decision errors in child protection: A new application of root cause analysis. *Children and Youth Services Review* **27** (4): 393–407.

Simonsen B, Bryan FL, Christian JHB, Roberts TA, Tompkin RB and Silliker JH (1987) Prevention and control of food-borne salmonellosis through application of HACCP. *International Journal of Food Microbiology* **4** (3): 227–247.

Shepherd WR (2006) The development of a surveillance system for the extensive beef cattle producing regions of Australia. PhD thesis, Faculty of Veterinary Science, University of Sydney, Sydney.

Shachak A, Ziv A and Reis S ILAIS 2006 conference http://ilais.openu.ac.il/wp/wp-content/uploads/2006/10/Shachak-Ziv-Reis-ILAIS2006.pdf

Shaffer LE (2007) Using pre-diagnostic data from veterinary laboratories to detect disease outbreaks in companion animals. PhD thesis, Ohio State University, Ames, Iowa.

Shewhart WA (1931) *Economic Control of Quality of Manufactured Product*. Van Nostrand Reinhold Co., Princeton, NJ. (Republished in 1981 by the American Society for Quality Control, Milwaukee, WI).

Schoemaker PJH (1993) Multiple scenario development: Its conceptual and behavioral foundation. *Strategic Management Journal* **14** (3): 193–213.

Sklet S (2004) Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials* **111:** 29–37.

Sperber WH (2005) HACCP does not work farm to table. *Food Control* **16:** 511–514.

Stalhandske E, DeRosier J, Patail B and Gosbee J (2003) How to make the most of failure mode and effect analysis. *Biomedical Instrumentation and Technology* **37** (2): 96–102.

Stoto MA, Schonlau M and Mariano LT (2004) Syndromic surveillance – is it worth the effort? *Chance* **17** (1): 19–24. (www.amstat.org/misc/stotoarticle.pdf)

Sundström, G. A. & Hollnagel, E. (2008). Modelling Risk in Financial Services Systems: A Functional Risk Modelling Perspective. Hollnagel, E., Rigaud, E. & Pieri, F. (Eds.) *Proceedings of the third resilience engineering symposium*. Paris, France: Collection Sciences Economiques, MINES ParisTech. (URL: http://www.resilience-engineering.org/RE3/papers/Sundstrom_Hollnagel_text.pdf)

Svedung I and Rasmussen J (2002) Graphic representation of accident scenarios mapping system structure and the causation of accidents. *Safety Science* **40:** 397–417.

Swart RJ, Raskin P and Robinson J (2004) The problem of the future: sustainability science and scenario analysis. *Global Environmental Change* **14:** 137–146.

Taylor-Adams SE (1994) Development of a human error taxonomy for use with a human error database. In *Contemporary Ergonomics. Proceedings of the 1994 Ergonomics Society Annual Conference* (Ed. Robertson) p. 329. Taylor and Francis, London.

Thor J, Lundberg J, Ask J, Olsson J, Carli C, Härenstam KP and Brommels M (2007) Application of statistical process control in healthcare improvement: systematic review. *Quality and Safety in Health Care* **16:** 387–399.

Thrusfield MV (2005) *Veterinary Epidemiology*. 3rd edn Blackwell Science, Oxford.

Tobara Polo D and Lemkov L (2003) Quality of life and management of living resources. Key Action 111-13. Socio-economic studies of life sciences project no. QLRT-2001-00034 http://technology.open.ac.uk/cts/peg/workshop%20report%20Spain.pdf

USDA (2008) Food Safety Research Information Office Sanitation and Quality Standards HACCP. http://fsrio.nal.usda.gov/document_fsheet.php?product_id=155

Van Asselt MBA, Storms CAHM(1998) Towards visions for a sustainable Europe: an overview and assessment of the last decade of European scenario studies. ICIS, Maastricht, The Netherlands.

Van der Sluijs JP (2002) *Encyclopedia of Global Environmental Change* (Ed. T Munn). Wiley, Chichester.

Van Tilburg CM, Leistikow IP, Rademaker CMA, Bierings MB, van Dijk ATH (2006) Health care failure mode and effect analysis: a useful proactive risk analysis in a pediatric oncology ward. *Quality and Safety in Health Care* **15:** 58–63.

Ward N and Ray C (2004) 'Futures analysis, public policy'. Centre for Rural Economy and Rural Studies. University of Newcastle-upon-Tyne Working Paper Series, Paper No.74. http://www.ncl.ac.uk/cre/publish/pdfs/wp74.pdf

Weick K and Sutcliffe K (2001) Managing the unexpected: assuring high performance in an age of complexity. University of Michigan business school management series, Jossey Bass, San Francisco.

WHO (1997) Annex Hazard Analysis and Critical Control Point (HACCP) System and Guidelines for its Application, WHO/FSF/FOS/97.2. World Health Organization, Geneva..

Williams CK 2002. Risk assessment for release of genetically modified organisms: A virus to reduce the fertility of introduced wild mice. *Mus domesticus. Reproduction Supplement* **60:** 81–88.

Woods DD (2000) Behind human error: Human factors research to improve patient safety. National summit on medical errors and patient safety research. Quality Inter-agency Coordination Task Force and

Agency for Heathcare Research and Quality, Washington, http://csel.eng.ohio-state.edu/woods/medicine/patientsafety/HFESinput_full_summit.pdf

Yih WK, Caldwell B, Harmon R, Kleinman K, Lazarus R, Nelson A, Nordin J, Rehm B, Richter B, Ritzwoller D, Sherwood E and Platt R (2004) National bioterrorism syndromic surveillance demonstration program. *Morbidity and Mortality Weekly Report* **53** (Suppl): 43–49. http://www.cdc.gov/MMWR/preview/mmwrhtml/su5301a10.htm

Zuijderduijn C (1999) Risk management by SHELL refinery/chemicals at PERNIS, The Netherlands. *European Conference on Risk Management in the EU of 2000: The challenge of implementing Council Directive Seveso II.* 10–12 November, Athens (Ed. GA Papadakis). EU Report EN European Commission, DG JRC, MAHB, Ispra, Italy. http://mahbsrv.jrc.it/proceedings/greece-nov-1999/B4-ZUIJDERDUIJN-SHELL-z.pdf