I-RISK

Integrating management and technical systems

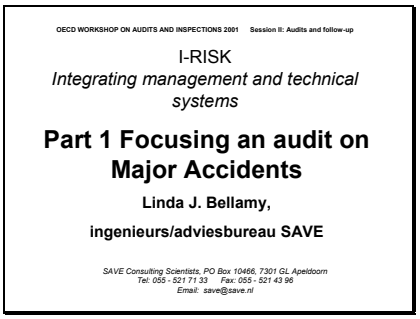
Part 1 Focusing an audit on Major Accidents

Linda J. Bellamy,

ingenieurs/adviesbureau SAVE

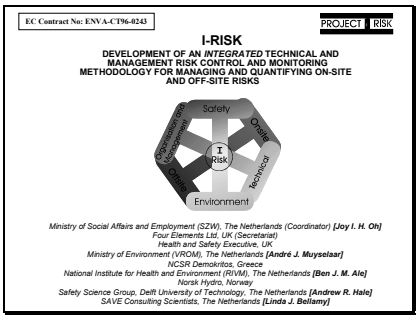
SAVE Consulting Scientists, PO Box 10466, 7301 GL Apeldoorn
Tel: 055 - 521 71 33 Fax: 055 - 521 43 96
Email: save@save.nl

Slide 1



This is the first part of a two part presentation. Part 2 is presented in session VI: Management Monitors.

Slide 2



The I-Risk project was an ambitious programme of research for integrating Quantitative Risk Assessment and Management System auditing. For this reason the partners came from a variety of organisations with a variety of interests and expertise, but a common goal – to develop an integrated model.

The authors of the final I-RISK report were:
Linda J. Bellamy (SAVE) , Netherlands
Ioannis A. Papazoglou and Olga N. Aneziris (Demokritos), Greece
Andrew R. Hale and Frank Guldenmund (TU Delft), Netherlands
Ben J. M. Ale (RIVM), Netherlands
Mark I. Morris (Four Elements), UK
Joy I. H. Oh (SZW), Netherlands

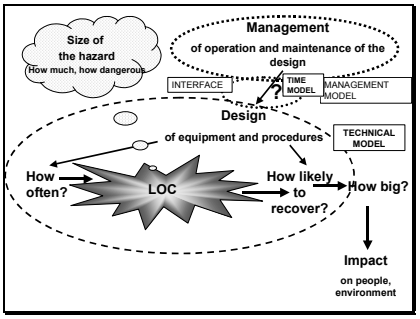
Slide 3

Focus

- Chemical production and storage
- Major hazards = dangerous substances
- Major accident = Sudden **Loss Of Containment (LOC)**
- The risk of major accidents

The focus was on major hazards and the risks of major accidents in the chemical industry. This was especially important in the light of the Seveso II Directive in Europe.

Slide 4



The basic modelling concepts involved linking the model of the Loss Of Containment (LOC) risks in the design of a chemical installation to the way those risks are managed in the operation and maintenance of the system. This required building models of the technical and management systems in a way which could be interfaced. In addition, the question was to be tackled as to how the risks might change over time as a result of changes in the management system. The questions to be answered were how to focus the evaluation of the management system on the site specific risks of LOC, how to determine the sensitivity of the risks to the management system and to determine what is important in the management system for managing those site specific risks.

Slide 5

I-Risk Components

- Technical Model for Risk Assessment
- Management Model
- Technical-Management Interface
- Time model

Our primary interest is major accident frequency

The technical and management models that were developed required constant coordination between the parties with a need to understand each others models and concepts. Building an interface between the two models was crucial to linking the two. Modelling how management quality might change over time was especially difficult. However, the basis for having a management simulator exists and the areas where data are needed are identified.

Slide 6

Technical Model

- Master Logic Diagram:failure tree model of the design (equipment + humans)
- Parameters of failure and unavailability
  - ***probability, frequency, duration***

The technical model began with QRA concepts taken from chemical and nuclear risk assessment. The model contained a generic Master Logic Diagram which effectively represented all containment system failures, and mathematical equations of failure and unavailability of technical components. The model can include onsite risks.

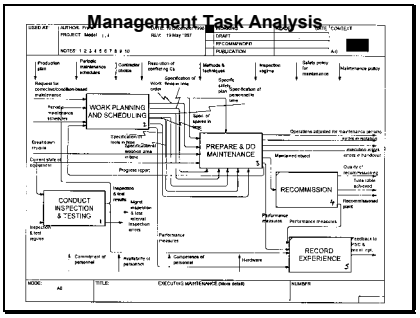
Slide 7

Parameters of the technical model

Q_{O1}	Probability of not performing an action
Q_{O2}	Probability of not detecting and recovering an error
Q_{M1}	Error in test and repair
Q_{M2}	Failure to detect a previous error
f_I	Frequency of an initiating event
λ	Failure rate of monitored or non monitored components
T	Period of inspecton/testing
f_m	Frequency of routine maintenance
T_R	Duration of repair
T_M	Duration of maintenance

The technical model is the technical description of the ways the installation can fail. The parameters in the model are a mix of human factors parameters and the classical parameters of component failure. It was these parameters that ultimately formed the basis for interfacing the technical and management models. For example, what is required in the management of the test/inspection interval?

Slide 8



The management model began life as complex form of task analysis involving the breakdown of the management system into all its processes, their inputs and outputs and the criteria and resouces needed to deliver the output.

Slide 9

Management Model

- 8 management subsystems: "Delivery systems"
  - ***delivering criteria and resources for control of major hazards***
- Management system model structure
  - ***Control and Monitoring (feedback and learning) cycles***

Ultimately these criteria and resources were collapsed into 8 subsystems which we called the delivery systems. The complexity of the original model could not be used for auditing or for integrating with the technical model. For these purposes we developed a management control and monitoring loop with feedback and learning cycles.

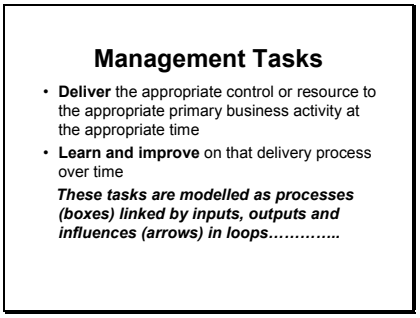
Slide 10

Delivery Systems

- **Availability** of personnel
- **Competence** of personnel
- **Commitment** and motivation
- **Resolution of conflicts** of goals/demands
- **Communications** and coordination
- **Procedures**, rules and methods
- **Man Machine Interface**: Ergonomics
- Equipment **Spares and Tools** for tasks

From the task analyses, these were the 8 delivery systems identified as the controls and resouces needed for carrying out the management tasks for major hazards.

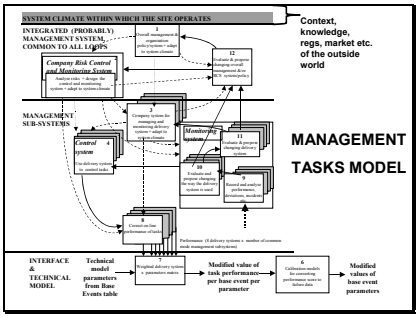
Slide 11



The management tasks are to deliver the appropriate control or resources to the operations or maintenance activity involved, The tasks are modelled as processes with inputs and outputs which are linked together in learning cycles. The ultimate goal of the task relates to the management of the people who affect the parameters of the technical system. For example, for the test/inspection interval this can involve:

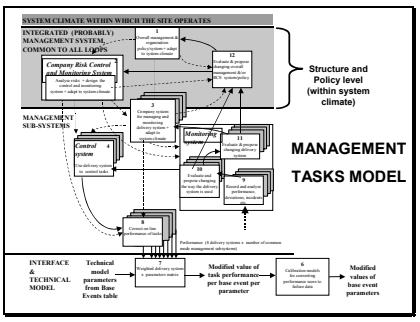
Interface *Design for ease of inspection, testing*
Rules and Procedures (Performance Criteria) Specification of requirements for equipment inspection and testing, Scheduling of inspection and test procedures, Learning system for re-scheduling, Inspection rounds
Availability of personnel Ensuring availability of (competent) people for testing and inspection
Commitment of personnel Emphasis on safety priorities, Keeping to schedules (alert, motivated), Penalising not following safe rules and procedures, Rewards, Alertness to failed states, equipment readings (e.g. in inspection rounds)
Communications and co-ordination Communication of schedules, Communication of priorities, Unambiguous instructions on scheduling
Spares and tools Availability for inspection and testing
Conflict Resolution Ensuring major hazard safety related inspection and testing tasks and other tasks do not conflict, Task planning and co-ordination to avoid conflicting demands/goals, Emphasising safety as a priority, Allocation of priorities to major hazard related tasks, Handling production pressure conflicts with inspection and testing, Ensuring that inspection and testing action requirements do not potentially expose the personnel to the major hazard source

Slide 12



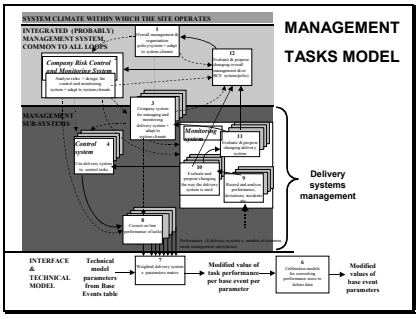
This is the management system model and the interface which have a total of 12 processes (boxes). At the highest level in the diagram is represented all the factors which the management system has to reckon with and which exist in the 'outside world'. The solid lines represent inputs and outputs of the processes. The dotted lines indicate influences that one process can have on the quality of another in transforming input to output.

Slide 13



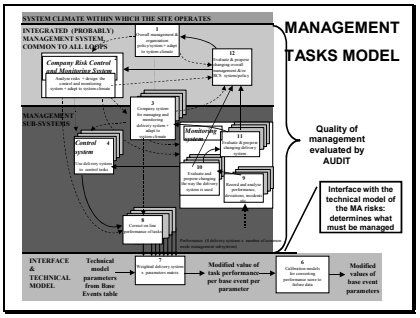
At the next level are the processes of the system at the organisation and policy level. One of the tasks at this level is to set up and run the risk control monitoring system. Another is to provide feedback on how the system is working.

Slide 14



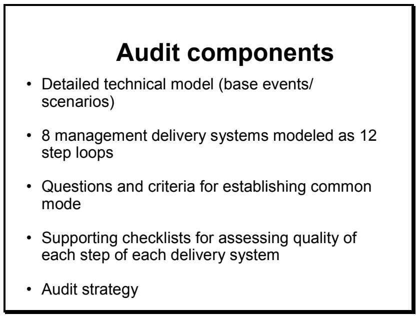
At the next level all the management processes involved in the delivering the appropriate controls and resources, the 8 delivery systems, are represented. Here the control and feedback loops can be seen between the control and monitoring system. Box 8 is the only process whose outputs directly affect the technical system.

Slide 15



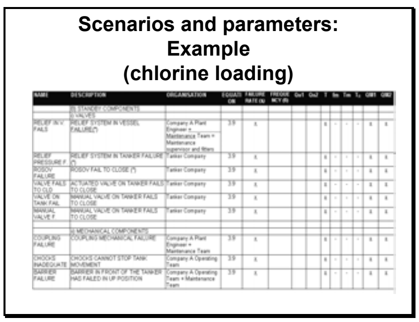
The technical system interfaces with the management system at the point at which the management system delivers an output which directly affects a particular parameter of the technical system. The quality of the output is used to modify the value of the parameter. For example by how much the test interval might be greater than the installation's stated values. This is done using a weighting system and a data calibration model for converting the score to failure data. This is not detailed further here. Only the information of interest in the technical system needs to be generated from assessment of the management system. This assessment is done by audit, evaluating the quality of the management system by auditing the management processes (the boxes). For the management sub systems each box will be evaluated 8 times at a minimum for the 8 delivery systems, multiplied by the number of times that a separate quality management system exists (there is not one common mode management system influencing human error, for example). This might be the case where a technical parameter can be influenced by different (quality) management systems (which might be the case for a decentralised management system, for example). In principle, the audit results are applicable across the whole of a common mode management system which means that the technical model which is used to support the audit can be built for, say, just one small unit on the installation.

Slide 16



In summary, the components of the audit included the failure scenarios identified from the technical model, the loop model, a set of checklists for supporting the auditor and a strategy.

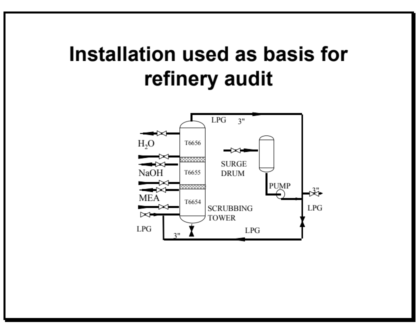
Slide 17



NAME	DESCRIPTION	ORGANISATION	EQUATION	FAILURE RATE (λ)	FREQUENCY (f)	Qu1	Qu2	T	θm	Tm	Tr	QB1	QB2
	(B) STANDBY COMPONENTS												
	i) VALVES												
RELIEF IN V. FAILS	RELIEF SYSTEM IN VESSEL FAILURE(*)	Company A Plant Engineer + Maintenance Team + Maintenance supervisor and fitters	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
RELIEF PRESSURE F.	RELIEF SYSTEM IN TANKER FAILURE (*)	Tanker Company	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
ROSOV FAILURE	ROSOV FAIL TO CLOSE (*)	Tanker Company	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
VALVE FAILS TO CLO	ACTUATED VALVE ON TANKER FAILS TO CLOSE	Tanker Company	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
VALVE ON TANK FAIL	MANUAL VALVE ON TANKER FAILS TO CLOSE	Tanker Company	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
MANUAL VALVE F.	MANUAL VALVE ON TANKER FAILS TO CLOSE	Tanker Company	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
	ii) MECHANICAL COMPONENTS												
COUPLING FAILURE	COUPLING MECHANICAL FAILURE	Company A Plant Engineer + Maintenance Team	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
CHOCKS INADEQUATE	CHOCKS CANNOT STOP TANK MOVEMENT	Company A Operating Team	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]
BARRIER FAILURE	BARRIER IN FRONT OF THE TANKER HAS FAILED IN UP POSITION	Company A Operating Team + Maintenance Team	3.9	[illegible]				[illegible]	-	-	-	[illegible]	[illegible]

Here, for example, is part of the base events table used in assessing a chloring loading system.

Slide 18



The technical basis for an I-rRsk audit can be a very small part of the total.

Slide 19

Audit Results: example

- High scores on all delivery systems
- Strong fast feedback loops
- Weakest delivery system was 'ergonomics'
- Major hazards could be made a more explicit aspect of the safety management system

For one of the test site companies, a refinery, the results produced very high scores on all delivery systems, but the major hazards aspects of management were not an explicit part of the overall safety management system. At that time the company was considering losing a part of its management system related to 'communications' but this system was considered an important part of the strength of the fast feedback loops.

Slide 20

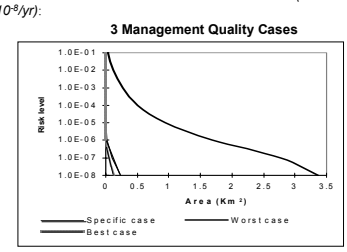
Recommendations from audit included:

- Developing a Major Hazards Management Manual
- LOC-specific category of incidents and near misses
- Treating human reliability on major hazard tasks in the same way as equipment reliability
- Developing a systematic review and improvement procedure for Man-Machine Interface (MMI) design

Specific recommendations were made to fill in the gaps.

Slide 21

Sensitivity of the risks to management:
Area inside risk contours above certain risk levels (10^{-1}-10^{-8}/yr):



When the results of the audit were fed into the technical model the test site was found to be very close to the best possible case. As can be seen a poor quality management system for the same installation, in this case an LPG scrubbing tower, was evaluated to produce a much higher risk.

Slide 22

Sensitivities derived from the integrated model

Key management deliveries:

- Producing right type of spares on time for maintenance
- Existence of appropriate procedures for various tasks
- Providing the right incentives for personnel commitment
- Provisions for resolving conflicts between safety and production tasks *(could provide largest effect on risk)*

When looked at from the technical perspective, the important delivery systems could be identified.

Slide 23

Sensitivities derived from the integrated model

General conclusion

- More important to maintain current quality of the management system than trying to improve it.

The general conclusion was that it was more important to maintain the quality of the current system than to attempt making improvements.

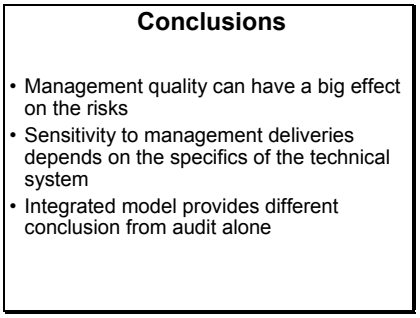
Slide 24

Problems

- I-Risk audit very detailed and time consuming
- More detailed due to elaboration of the aspect systems of the total SMS

The main problems identified with this kind of audit is its complex and time consuming nature.

Slide 25



On the other hand, such as audit homes in on the management systems related to the major hazards and, when integrated with the technical system, indicates how sensitive that system is to management influences.