Accident Analysis using Storybuilder:

Illustrated with overfilling accidents including Buncefield, UK

Ir. Hans Baksteen, RIVM
Ir. Martijn L. Mud, RPS
Dr. Linda J. Bellamy, White Queen BV

4 September 2007

Prepared for:
Ministerie Sociale Zaken en Werkgelegenheid
Postbus 90801, 2509 LV Den Haag

This page left blank

Acknowledgements

ΜΕΤΑΜΌΡΦΩΣΗ

Models and data provided by the WORM and WORM Metamorphosis teams formed the background to this work. The core team members comprised:

Joy Oh, Ministry of Social Affairs and Employment (SZW), Health & Safety Directorate, NL (Client)
Jos Post, Netherlands Institue of Physical Safety (NIFV,) NL (Project manager WORM Metamorphosis)
Ben Ale, TU Delft, NL (Project manager WORM)
Olga Anezeris , National Centre for Scientific Research “Demokritos”, GR
Erik de Baedts EDBC, NL (Technical Secretary WORM Metamorphosis)
Hans Baksteen, National Institute for Public Health and the Environment (RIVM), NL
Linda Bellamy , White Queen BV, NL (Deputy Project manager)
Anneke Bloemhoff, Consumer Safety Institute, NL
Martin Damen, RIGO Research and Consultancy, NL
Andrew Hale, TU Delft, NL
Kirsten Jørgenson, Technical University of Denmark, DK
Judith Kuiper, Consumer Safety Institute, NL
Kees Leidelmeijer, RIGO Research and Consultancy, NL
Tom Maddison, Health and Safety Executive, HID, UK
Martijn Mud, RPS Advies, NL
Saakje Mulder, Consumer Safety Institute, NL
Ioannis Papazoglou, National Centre for Scientific Research “Demokritos”, GR
Vera Sol, Ministry of Social Affairs and Employment (SZW), Health & Safety Directorate, NL
Paul Uijt de Haag National Institute for Public Health and Environment (RIVM), NL
Jeroen Versteegen, AT Osborne, NL (Technical Secretary WORM)
Julius Whiston, Whiston Computers Ltd, UK
Richard Whitehouse, HCRM Ltd, UK
Petra Zahradnik, National Institute for Public Health and the Environment (RIVM), NL

This page left blank

Contents

This page left blank

1 Introduction

1.1 Background

In the Netherlands there are about 7.000.000 workers in 500.000 companies. In 2004 there were 87.000 occupational accidents (about 50 injured workers every working hour). 83 persons died (about 2 workers die of an accident every working week). The bulk of these were in 36 industry branches with 3.000.000 workers. The main causes were

Falling from height
Contact with machines
Hit by vehicles
Falling objects

These injuries and deaths cause suffering and distress to the victims and to their relatives. They also cost the Netherlands' society a sizable amount of money in the form of sick leave payments, medical treatment and labour replacement costs.

The traditional approach to reducing these numbers is based on observations by inspectors of what causes accidents and the making of rules and regulations to prevent further occurrence. Also much effort has been spent in attempts to communicate the importance of working safely. These efforts by nature are aimed at preventing accident causes from the past. However, there are not many instruments to assess potential underlying causes of accidents that could form the basis for policies aimed at preventing future accidents.

The Ministry of Social Affairs and Employment (SZW) embarked on a project called WORM - Workgroup Occupational Risk Model- to identify as far as possible these underlying causes and quantify the contribution (Ale *et al*, 2006). The results of this and other safety improvement projects of the Ministry are used to underpin a nation wide campaign - Strengthening Labour Safety - aimed at improving occupational safety. The WORM project has developed a comprehensive set of scenarios to cover the full range of occupational accidents. One objective is to support companies in their risk analysis and prioritisation of prevention. Its aim is to introduce risk-based thinking to the full range of accident prevention. This work has also influenced the Dutch causal modelling for air transport safety - CATS. The modelling of accidents for prioritising prevention is discussed by Hale *et al*, 2006.

1.2 ORM

The Occupational Risk Model (ORM) developed in WORM will allow companies, government or industry representatives to assess the occupational risks for individual workers and for sections of the workforce and identify cost effective risk reduction strategies.

The development of the modelling was assembling and analysing accident data, generalisation of these data into a logical risk model, deriving improvement measures and their costs and assessing cost effective risk reduction. The project builds on previous work executed with support from SZW and the European Union, such as the AVRIM and IRISK projects. The experiences and knowledge developed in these projects have been combined and enhanced to achieve ORM.

The ORM model consists of the following steps:

- the analysis of accidents to get the numerator data for the risk model
- the building of logical bow-tie models
- the selection or identification of potential barriers against accidents and their probability influencing entities (PIEs)
- Surveying bowtie and PIE exposures to obtain denominator data for the risk model
- The identification of measures (which influence PIEs), their effectiveness and their costs
- The identification of jobs and activities and the selection of the appropriate hazards or bow-tie concerns
- The determination of the 'efficient frontier' for given costs and risk reduction.

This is illustrated in Figure 1

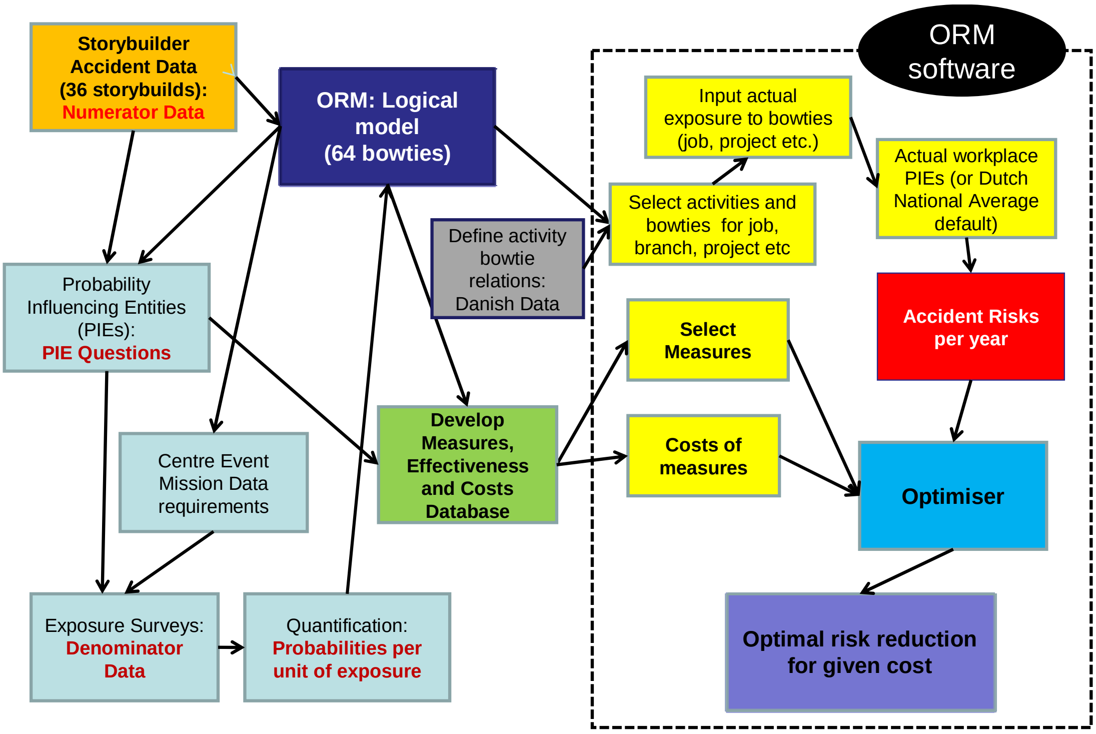

Storybuilder Accident Data (36 storybuilds): Numerator Data
ORM: Logical model (64 bowties)
ORM software
Input actual exposure to bowties (job, project etc.)
Actual workplace PIEs (or Dutch National Average default)
Select activities and bowties for job, branch, project etc
Define activity bowtie relations: Danish Data
Probability Influencing Entities (PIEs): PIE Questions
Select Measures
Accident Risks per year
Develop Measures, Effectiveness and Costs Database
Costs of measures
Optimiser
Centre Event Mission Data requirements
Exposure Surveys: Denominator Data
Quantification: Probabilities per unit of exposure
Optimal risk reduction for given cost

Figure 1 Data flow for the ORM model

1.3 Storybuilder

1.3.1 Starting point

The starting point of analysis of accidents was a bowtie and barrier structure (Hale *et al* 2004). The analysis was achieved using a tailor made software tool called Storybuilder (Bellamy 2006, 2007; Ale 2007) and uses a set of building rules developed in the WORM project. The tool was used to model the "horrible stories" and is the first step in the development of ORM.

1.3.2 The analysis

In 2004-2006 a team was formed for the sole purpose of analysing occupational accident investigation reports made available by the Dutch Labour Inspectorate. In this period the software StoryBuilder was developed to support the development of an events structure and a quantification of the accidents represented in that structure. Horrible stories (accidents) were analysed in order to build structures according to strict building rules.

This went through a process of first and second pass development and checking. At the end of the first pass the event structure was frozen. In the second pass it was filled with all the available data from the specified time period.

A storybuild is a graphical structure representing failure events in accidents. The centre event of this structure is the event in the structure through which all scenarios (accident paths) pass and which represents the release of the hazard agent e.g. in *Figure 2 Section of a storybuild showing centre event* the centre event is Contact with Hazardous Substance.

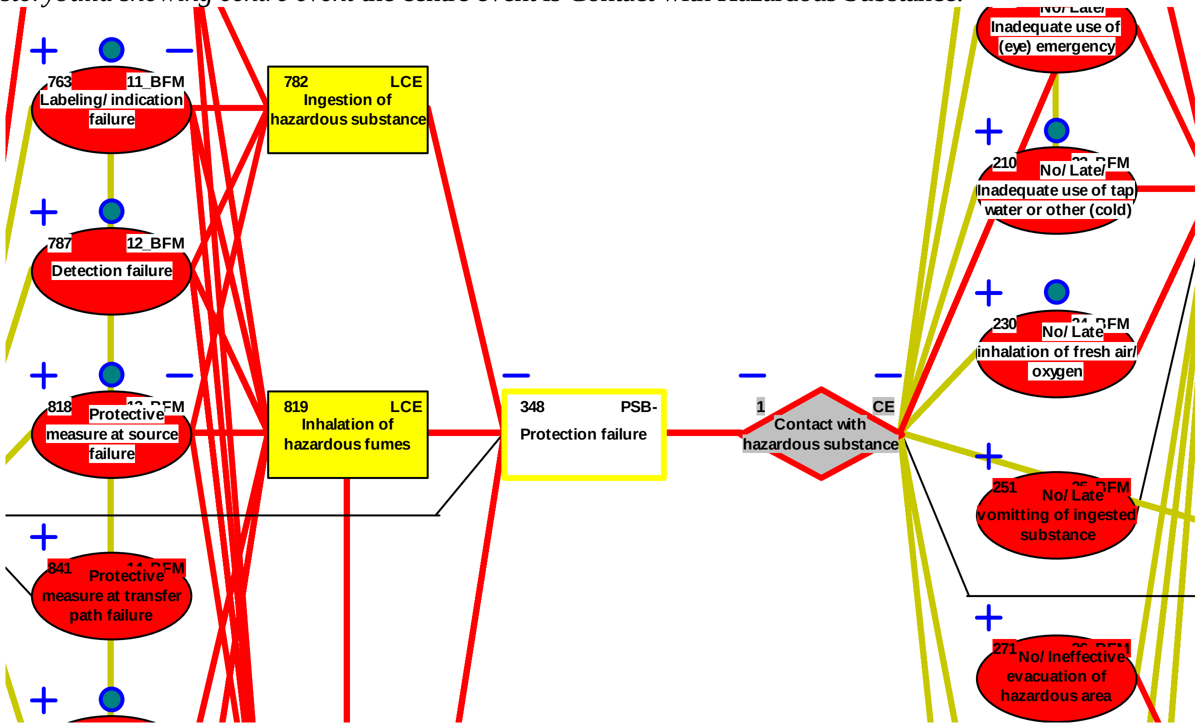

763
11_BFM
Labeling/ indication failure
787
12_BFM
Detection failure
818
Protective measure at source failure
841
Protective measure at transfer path failure
782
LCE
Ingestion of hazardous substance
819
LCE
Inhalation of hazardous fumes
348
PSB-
Protection failure
1
CE
Contact with hazardous substance
Inadequate use of (eye) emergency
210
No/ Late/ Inadequate use of tap water or other (cold)
230
No/ Late inhalation of fresh air/ oxygen
251
No/ Late vomitting of ingested substance
271
No/ Ineffective evacuation of hazardous area

Figure 2 Section of a storybuild showing centre event

In the storybuilds (graphical structures containing accident pathways) a barrier is a physical entity (object, state, or condition) that acts as an obstacle in an accident path.

Typical Barrier Functions are:

- Prevent presence, build-up, or release of the hazardous agent/ energy
- Separates hazardous agent/ energy in space (safe distance) or time (safe moment)
- Prevents the undesired transmission of energy/ hazardous agents
- Prevents incompatibility of materials

- Prevents unsafe process conditions (pertains to sequence, temperature, pressure, composition)

- Prevents unsafe physical conditions (pertains to structural integrity, strength, stability)

A barrier failure mode (BFM) is one way in which the barrier failed in an accident scenario e.g. a structure not being strong enough for the exerted load

Barriers are supported by tasks. The tasks, particularly the use and maintain tasks, are operable on a lower level in the overall system: i.e. at the barrier level where operators/workers and maintenance fitters are working. The provide task is, on the other hand often a management task.

The tasks fail as follows:

- **Provide-[barrier] failure**
  = It does not exist, has not been well designed, or it is not provided and / or sufficiently/easily available when you want to use it. Such a barrier can be hardware or a specific method (sequence, composition, or other parameter(s) with safe limits).
- **Use-[barrier] failure**
  = the correct barrier is provided, but the way in which the provided barrier is used is incorrect, it is only partially used, or it is not used at all. A ‘use’ failure is also the case, when somebody chooses to use a barrier other than the correct one, despite the correct one being available.
- **Maintain-[barrier] failure**
  = the barrier is not kept available according to its designed function; i.e. in an adequate state. This does not only cover the maintenance aspect but also the management of change aspect of a barrier, i.e. a barrier is modified without ensuring that it maintains its barrier function.
- **Monitor-[barrier] failure**
  = the barrier condition is not checked/ measured/observed/inspected. This task relates directly to the state of the barrier, or to the supervision of the use of the barrier.

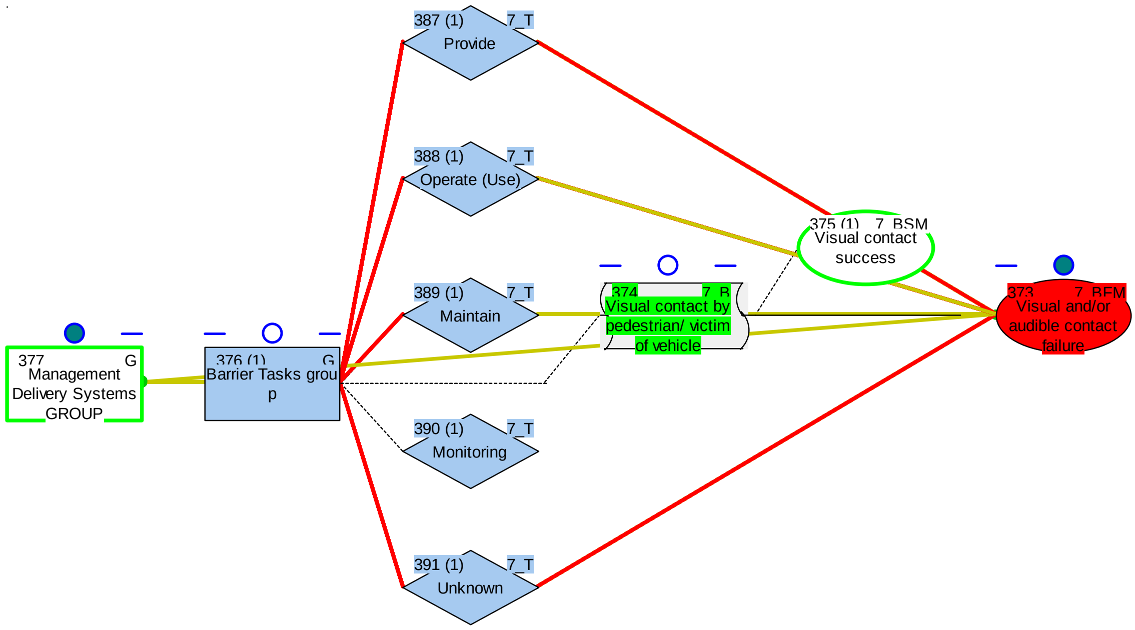
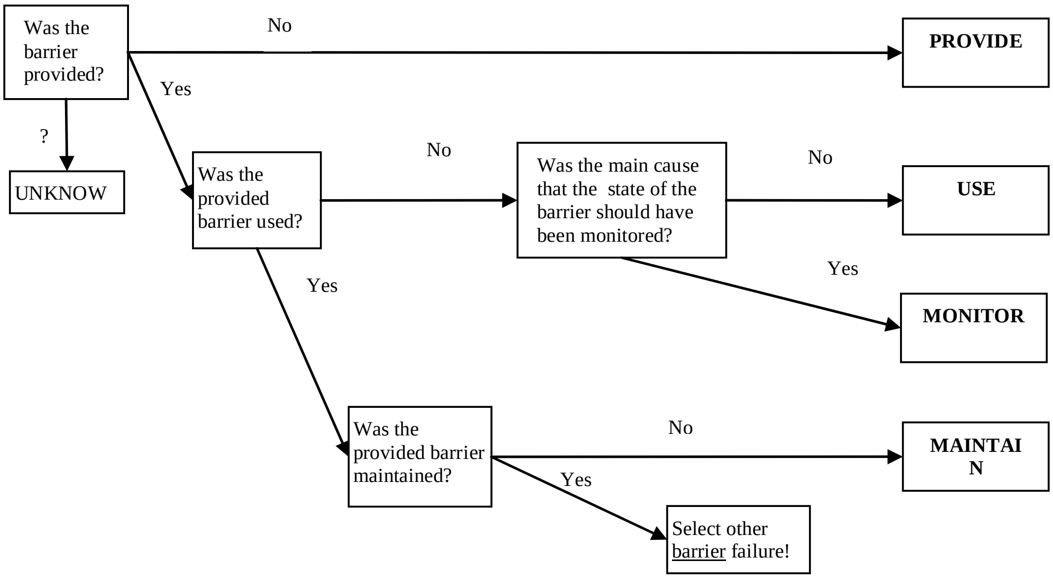


Figure 3 Part of storybuild showing the "PUMM" tasks which support a barrier

The most relevant failing task per barrier is identified by applying the following scheme:


Was the barrier provided?
No
PROVIDE
Yes
?
UNKNOW
Was the provided barrier used?
No
Was the main cause that the state of the barrier should have been monitored?
No
USE
Yes
MONITOR
Yes
Was the provided barrier maintained?
No
MAINTAIN
Yes
Select other barrier failure!

Management delivery system failures (DS) are modelled to show whether the criteria and resources failed to have been delivered to the technical system through the task.

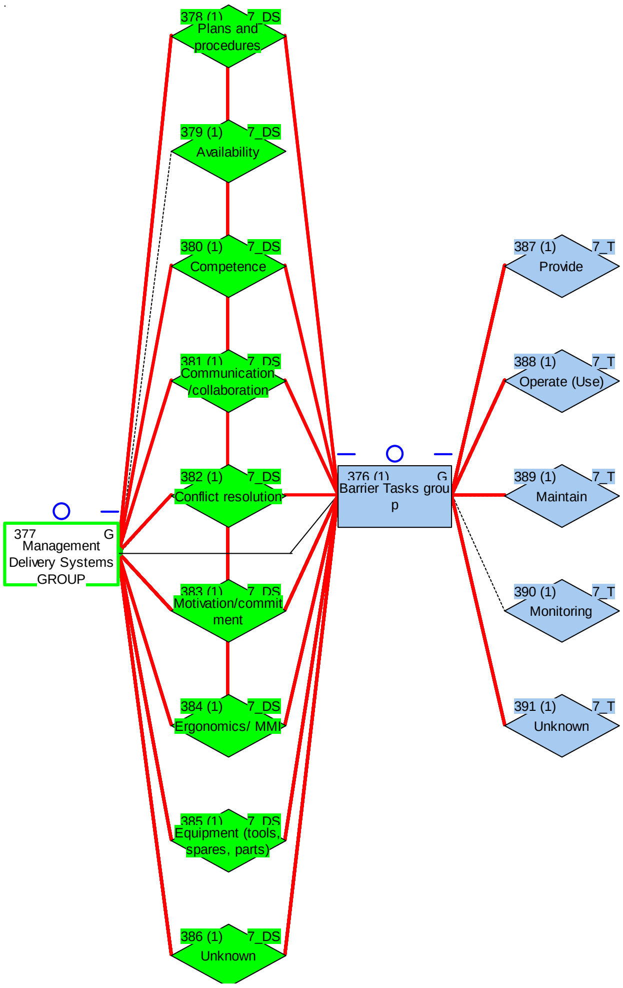

378 (1) 7_DS Plans and procedures
379 (1) 7_DS Availability
380 (1) 7_DS Competence
381 (1) 7_DS Communication /collaboration
382 (1) 7_DS Conflict resolution
383 (1) 7_DS Motivation/commitment
384 (1) 7_DS Ergonomics/ MMI
385 (1) 7_DS Equipment (tools, spares, parts)
386 (1) 7_DS Unknown
377 G Management Delivery Systems GROUP
376 (1) G Barrier Tasks group
387 (1) 7_T Provide
388 (1) 7_T Operate (Use)
389 (1) 7_T Maintain
390 (1) 7_T Monitoring
391 (1) 7_T Unknown

Figure 4 Example of delivery systems connected to barrier tasks

Delivery System (What's delivered)	Description
Plans & procedures [NL: Plannen & Procedures]	Procedures refer to specific performance criteria which specify in detail, usually in written form, a formalised 'normative' behaviour or method for carrying out tasks, such as: checklist, task list, action steps, plan, instruction manual, fault-finding heuristic, form to be completed, etc. Plans refer to explicit planning of activities in time: either how frequently tasks should be done, or when and by whom they will be done within a particular time period (month, shutdown period, etc.). It includes: maintenance regime, maintenance scheduling (including shutdown planning), and testing and inspection activities. This delivery system also refers to rules, permits, programs and risk assessments.
Availability [NL: Beschikbaarheid (van mankracht)]	Availability refers to allocating the necessary time (or numbers) of competent and suitable (incl. anthropometrics and biomechanics) people to the tasks to be carried out. It emphasizes time-criticality, i.e. people available at the moment (or within the time frame) when the tasks should be carried out. This delivery system includes the availability of staff for repair work on critical equipment outside normal work hours, incl. coverage for absence and holidays.
Competence [NL: Deskundigheid]	Competence refers to the knowledge, skills and abilities of the people selected for the execution of tasks. It also covers the selection and training function of a company to deliver sufficient staff for overall manpower planning. This delivery system also refers to 'right person for the job', i.e. with the proper knowledge to provide, use, maintain or monitor the barrier effectively.
Communication, collaboration [NL: Communicatie, samenwerking]	Communication/ Collaboration refers to internal communication and coordination. Internal communications are those communications which occur implicitly or explicitly, within any primary business activity, i.e. within one task or activity in order to ensure that the tasks are coordinated and carried out according to relevant criteria. This delivery system also refers to task instructions and communication channels and means (such as meetings, logs, phones, radio). Note: this delivery system is only relevant if the activity is carried out by more than one person (or group), who have to coordinate or plan joint activities.
Motivation/ Commitment [NL: Motivatie/ Instelling]	Motivation/ Commitment refers to incentives and motivation with which people have to carry out their tasks and activities, i.e. with suitable care and alertness and according to the appropriate safety criteria and procedures specified for the activities by the organisation. This delivery system also includes the aspect of alertness, care & attention, concern for safety of self and others, risk avoidance and willingness to learn & improve. Note - This delivery system is fairly closely related to Conflict resolution, in that it deals with the incentives of individuals carrying out tasks not to choose other criteria above safety, such as ease of working, time saving, social approval, etc. - Organizational aspects of conflicts are covered by Conflict resolution. - More personal aspects, such as violation of procedures, are covered by Motivation/ Commitment.

Delivery System (What's delivered)	**Description**
Conflict resolution [NL: Prioriteitstelling (het stellen van de juiste prioriteiten)]	Conflict resolution deals with conflicts between safety and other goals within the performance of tasks. It deals with the mechanisms (such as supervision, monitoring, procedures, learning, group discussion) by which potential and actual conflicts between safety and other criteria in the allocation and use of personnel, hardware and other resources, are recognised, avoided or resolved. Note: - This delivery system is closely related to Motivation/ Commitment. - Issues of violations within tasks at an individual level are covered by Motivation/ Commitment. - Conflict resolution covers the organisational mechanisms for resolving conflicts across tasks, between people at operational level and at management level.
Ergonomics [NL: Ergonomie]	Ergonomics/ MMI deals with the fit between the man and the task. It refers to the ergonomics of all equipment used/ operated by operations, inspection or maintenance to provide, use, maintain or monitor the barriers. This delivery system covers both the appropriateness of the interface for the task and the user-friendliness to carry out tasks. It includes: - appropriate equipment, tools and software, - robust/ appropriate/ good interface and labelling, and - operability and maintainability. Ergonomics/ MMI also covers: - design and layout of control rooms and manually operated equipment, - location and design of inspection and test facilities, - the maintenance-friendliness of equipment, and - ergonomics of the tools used to maintain it. Note: MMI stands for Man - Machine Interface
Equipment (tools, spares, parts) [NL: Equipement (gereedschap, materieel, (reserve) onderdelen]	Equipment refers to the hardware needed for provision, maintenance and monitoring of barriers. This delivery system covers both the correctness of the equipment for their use (compatibility, suitability, quality), and the availability of equipment where and when needed to carry out the activities. It includes: spares & parts (incl. those needed for maintenance) and adequate & correct stocks.

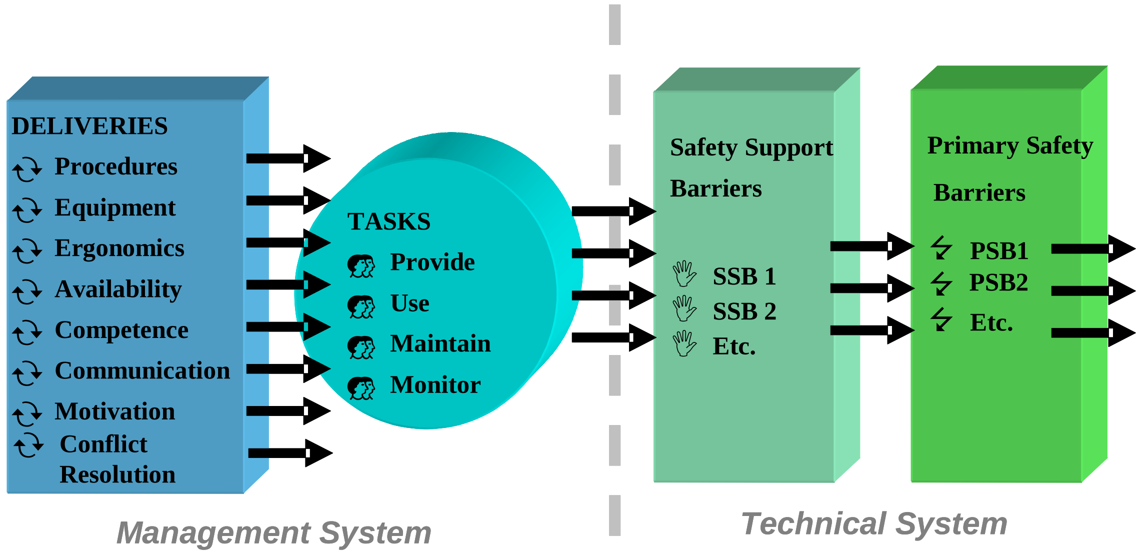


Figure 5 Management Deliveries and Tasks which support Barriers

1.3.3 The accidents analysed

The accidents analysed (9142 in total) are reportable occupational accidents . Employers are obliged to report serious occupational accidents to the Dutch Labour Inspectorate (Arbeidsinspectie). Sometimes this does not happen and the accident is either not notified at all or brought to the attention of the Labour Inspectorate by police, insurance companies or victims. Accidents are reportable according to article 9 of the Dutch Working Conditions Act (Arbowet 1998) if they are occupational accidents resulting in serious physical or mental injury or death within one year. A physical injury is considered to be serious if the victim is hospitalised within 24 hours and for at least 24 hours or the injury is permanent whether or not the victim is hospitalised. A reportable accident has to be reported within 24 hours. Then there are also criteria concerning whether an injury is permanent or not (physically or mentally).

GISAI (Geïntegreerd InformatieSysteem ArbeidsInspectie) is the Dutch Labour Inspectorate management system for occupational accidents. The Dutch Labour Inspectorate stores all correspondence about occupational accidents in GISAI. Data was available on 22,892 occupational accidents that were reported between 1 January 1998 and end February 2004. 10,237 of these had no offence or investigation report and were not analysed. The main reason why there was no report was that they were not reportable (82% of the accidents without report). The other cases were waiting to be investigated or were under investigation or too sensitive to be made available.

Only accidents with reports could be used for detailed analysis of causes. There are different kinds of reports and only if a breach has been found is the report complete with respect to witness statements and injury classes. If there is no breach report then there is a summary of the investigation findings and the reason why it is not a breach. The latter were also analysed but contain less information. If the conclusion is that the accident was not an occupational accident e.g. natural death or suicide then these were not included in the analysis.
There are also limitations on which occupations appear in GISAI e.g. self employed are excluded unless they are working under the authority of another company. Also excluded are occupational accidents occurring in air transport for flying aircraft, for cabin personnel

on stationery aircraft. Loading/unloading and other non-cabin staffs are included as are cabin personnel outside the aircraft. Oil and gas exploration is also excluded. All other drilling for scientific research, geothermal energy, groundwater accidents are covered by the Labour Inspectorate. Shipping – all accidents while building, repairing, maintaining or cleaning ships are included, and loading and unloading is only in the Labour Inspectorate database if the crew is not involved. Railway accidents are in principle incuded, but really serious incidents with collision and electrocution are done together with another inspectorate which means the investigation is not in the GISAI database… If a pupil of any school/university has an accident it is considered a labour accident where the teacher or school can be held responsible after the investigation. Military is included other than in wartime. Passers by or trespassers on worksites during working hours are included. Accidents to illegal workers, foreigners etc working on Dutch soil are included – the company is obliged to report them.
An accident is an occupational accident if it occurs at the workplace working during work. Underreporting for serious occupational accidents is considered to reach 50%. The underreporting % cannot be distributed evenly across the 3 categories of consequences (death, permanent injury, recoverable injury).

The 9142 reported investigated accidents of the Dutch Labour Inspectorate that have been analysed are distributed across 36 Storybuilds. Storybuilds are graphical structures in the software StoryBuilder each representing a type of occupational accident, characterised and named in each case by the release of the hazard agent or centre event of a bowtie of causes and effects. Annex I gives the number of accidents per Storybuild centre event from most to least frequent accident type.

The analysed accidents occurred between 1998 and end February 2004 inclusive, except for Storybuilds *Contact with falling objects* and *Contact with moving parts of machine*, where only accidents between 2002 to 2003 were analysed due to the large proportion of accidents in these cases and the limited resources available to analyse them.

1.3.4 Facts and Figures

The accident analysis provides facts and figures for each hazard type. Examples are given in Annex 2. The facts and figures sheets are intended to communicate the main information from the Storybuilds that can assist in accident prevention. These sheets are limited to 3 pages of information giving:
Numbers of deaths, permanent and recoverable injuries
Activites and equipment involved at the time of the accident
The barriers which failed.
The barrier support tasks which failed and the underlying management failures in terms of failed control or resource deliveries

1.3.5 The current work

The ministry of SZW asked for a small team of Storybuilder and Major Hazard experts to illustrate the use of Storybuilder by analysing in more detail one class of accidents. Major hazard accidents with hazardous substances was chosen due to special interests of members of WORM:
- SZW: Major hazards is one of the tasks of SZWs policy unit within the Directorate of Health and Safety
- EU Major Accidents hazards Bureau: to whom chemical major accidents in Europe are reported

- UK HSE Hazardous Installations Directorate: Policy in relation to control of major accident hazards (COMAH regulation)

It was chosen to focus on accidents which could throw light on the possible causes of the Buncefield accident which occurred at Hemel Hempstead in the UK on 11 December 2005. Loss of containment (LOC) accidents, and more specifically overfilling accidents were chosen. Due to availability of data it was possible to analyse reported overfilling accidents from UK HSE's database and from the MARS database.

The aim of the analysis was to investigate the usefulness of the present Storybuilds for the analysis of major hazard accidents with hazardous substances. The Storybuilds available were built on the basis of loss of containment accidents and fire and/or explosion accidents which are recorded in the GISAI system as described in section 1.3.3. Most of these GISAI-accidents are non-major hazard accidents.

Using the Storybuilder software tool, a number of major hazard accidents with hazardous substances which occurred in the UK in the recent past were analysed. One of those accidents was the Buncefield accident in Hemel Hempstead in 2005 where a loss of containment occurred followed by an explosion and fires. This accident was analysed in as much detail as possible from published reports (HSE, 2006)

Questions to be answered were:

- Are the current Storybuild models (Loss of Containment-model, Fire-model, Explosion-model) applicable for the analysis of the causes of major hazard loss-of-containment (LOC) accidents?

- Can specific patterns be identified in the causal chain of events which have led to the central loss of control events (LOC, Fire, Explosion)?

- How valuable is the presentation in Storybuilder of the analysed major hazard accidents? What are the advantages and what are the disadvantages?

The results of the work, and the wider context of the WORM metamorphosis project were presented at a workshop at Health and Safety Executive in the UK on 27 June 2007 with the following agenda

Meeting HSE- Ministry of Social Affairs (The Netherlands)

On 27th june 2007, 14.00-16.00
Venue: Auditorium Redgrave Court, Bootle UK

14.00	Opening: Tom Maddison, HSE
14.10	General introduction to the Program Improvement Occupational Safety: Joy Oh, Ministry of Social Affairs
14.30	Example Storybuilder: Overfilling accidents Hans Baksteen, RIVM
14.50	Example Storybuilder: Big scaffold accident Martijn Mud, RPS
15.10	Some thoughts on the Occupational Risk Model Linda Bellamy, White Queen
15.30	Use and developments in Denmark Kirsten Jörgenson, BYG-DTU
15.50	Closure: Tom Maddison , HSE

2 Storybuild model for all kinds of LOC-accidents

In the WORM project a number of accidents were analysed were hazardous substances were involved. The accidents were categorized in three types:

1. Accidents where workers were exposed to hazardous substances which were accidentally released from an open containment
2. Accidents were workers were exposed to hazardous substances which were accidentally released from a closed containment
3. Accidents where workers were exposed to hazardous substances without the occurrence of a accidentally release from a containment

The second model contains all sorts of accidents resulting in a release of a hazardous substance from a *closed* containment. The analysed LOC-accidents were caused by:

- Mistakenly opening of containments by operators
- Working on containment parts which were not well isolated from containment parts with hazardous substances in it
- Opening a closed containment which was not secured (hazardous substances were there while they should have been removed)
- Overfilling
- Overpressurisation
- Overheating
- Substandard containments (erosion, corrosion, etc)
- Mechanical impact

These 8 main causes are modelled in the storybuild model as Loss of Control Events (LCE) graphically represented as yellow squares . Every LCE is preceded by at least one barrier failure which is represented in the Storybuild model by a red ellipse.

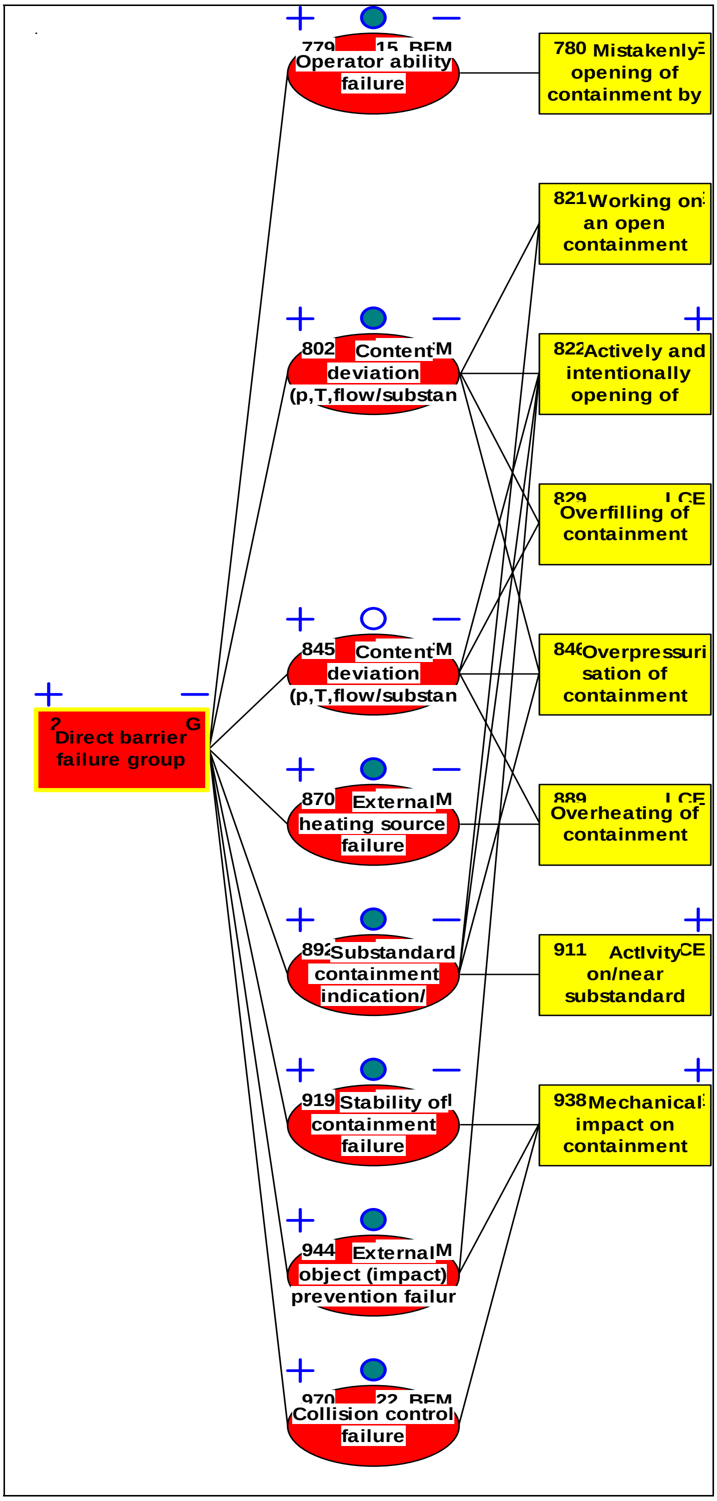

779 15 BFM
Operator ability failure
780 Mistakenly opening of containment by
821 Working on an open containment
802 Content M deviation (p,T,flow/substan
822 Actively and intentionally opening of
829 LCE Overfilling of containment
845 Content M deviation (p,T,flow/substan
846 Overpressurisation of containment
? G Direct barrier failure group
870 External M heating source failure
889 LCE Overheating of containment
892 Substandard containment indication/
911 Activity CE on/near substandard
919 Stability of containment failure
938 Mechanical impact on containment
944 External M object (impact) prevention failur
970 22 BFM
Collision control failure

Figure 6 Loss of control events directly preceding the LOC (from the closed containment model of the WORM-project)

This is shown in Figure 6. When we focus on the LCE “Overfilling” we can see in the model that this LCE is preceded by two types of barrier failures (blocks 802 and 845):

- Indication/detection failure
- Diagnosis/response failure

These failures are related to a preceding LCE which is a deviation in the level (a higher level than normal). See Figure 7. The relationship is seen by the lines of the accident pathways (green and red) which go link the boxes.

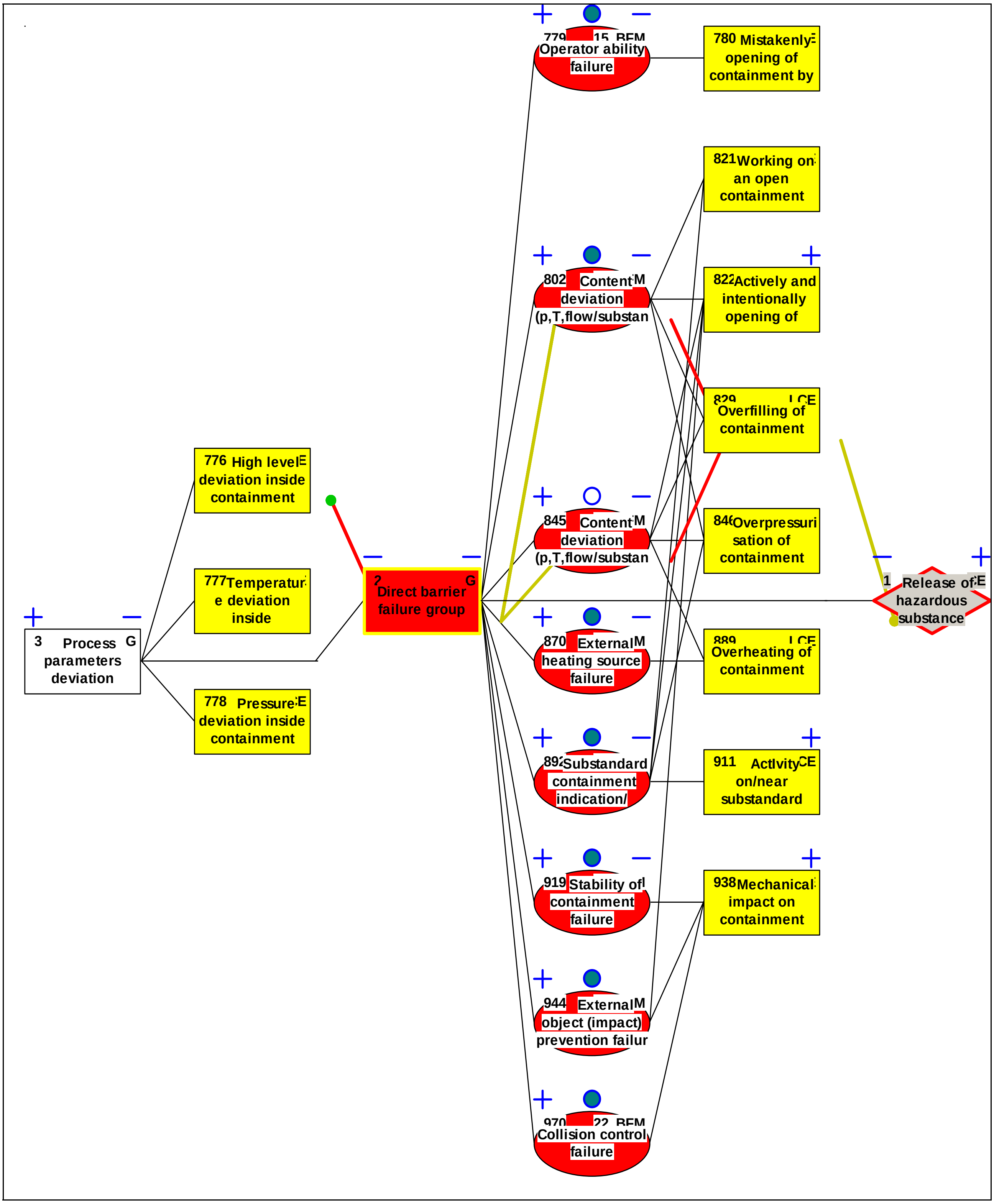

779 15 BFM Operator ability failure
780 Mistakenly opening of containment by
821 Working on an open containment
802 Content M deviation (p,T,flow/substan
822 Actively and intentionally opening of
829 LCE Overfilling of containment
776 High level E deviation inside containment
845 Content M deviation (p,T,flow/substan
846 Overpressurisation of containment
777 Temperature deviation inside
2 Direct barrier G failure group
1 Release of E hazardous substance
3 Process G parameters deviation
870 External M heating source failure
889 LCE Overheating of containment
778 Pressure E deviation inside containment
892 Substandard containment indication/
911 Activity CE on/near substandard
919 Stability of containment failure
938 Mechanical impact on containment
944 External M object (impact) prevention failur
970 22 BFM Collision control failure

Figure 7 Typical pathways of overfilling accidents in the Storybuild model of WORM.

If the event of a high level deviation occurs the two barriers should be a success in order to prevent the containment from overfilling:

- the high level should be indicated and detected

- after a well indicated and detected high level a corrective action should be taken, which prevents the high level to continue and to result in overfilling; therefore two things are needed:
  - a right diagnosis is made
  - the right corrective action (response) is made

The above described structure was the basis for a separate overfilling model which was built within this small project.

Of course there are also barriers which have to prevent the high level in a containment but these barriers will be described in the next section where we will elaborate on this separate overfilling model.

This page left blank

3 Storybuild model for overfilling accidents

The overfilling Storybuild model contains two sets of barriers:

1. Barriers preventing a deviation in liquid level
   - Batch Size Preparation
   - Connection
   - Flow feed control
   - Flow discharge control

2. Barriers preventing (given a deviation in the liquid level) an overfilling of the vessel/storage tank
   - Indication
   - Detection
   - Diagnosis
   - Response

This second set was briefly discussed in the previous section the only difference being that the two barriers are now split into 4.

In Figure 8 the Left hand side (LHS)-overfilling barriers and loss of control events are presented.

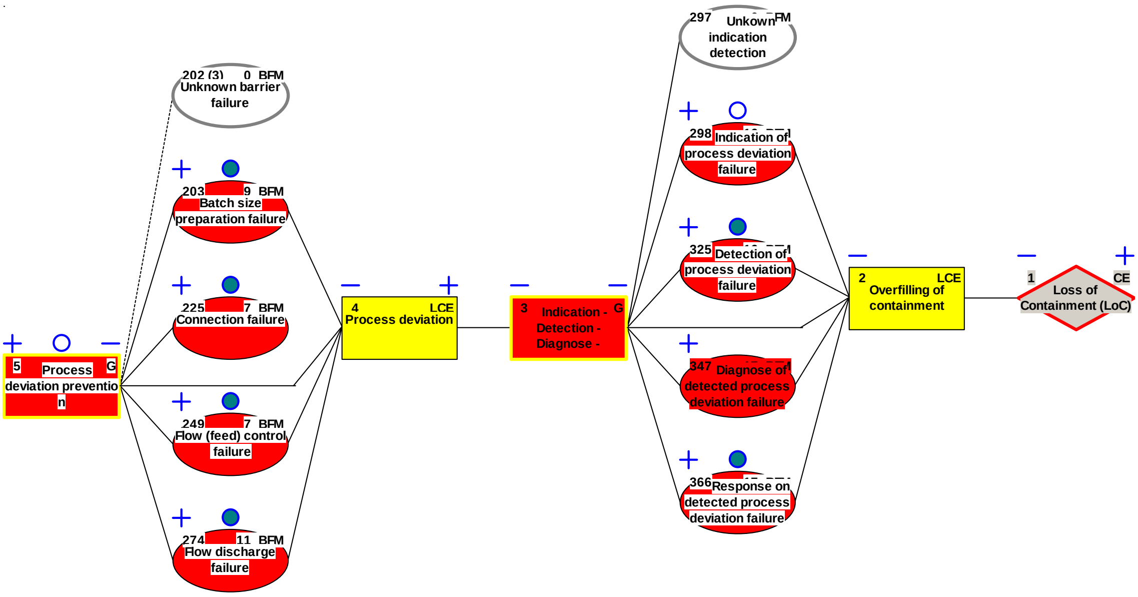

202 (3) 0 BFM
Unknown barrier failure
203 9 BFM
Batch size preparation failure
225 7 BFM
Connection failure
249 7 BFM
Flow (feed) control failure
274 11 BFM
Flow discharge failure
5 Process deviation preventio n G
4 LCE
Process deviation
3 Indication - Detection - Diagnose - G
297 Unkown indication detection FM
298 Indication of process deviation failure
325 Detection of process deviation failure
347 Diagnose of detected process deviation failure
366 Response on detected process deviation failure
2 LCE
Overfilling of containment
1 CE
Loss of Containment (LoC)

Figure 8 Left (of centre event) side of overfilling model

The first set of barriers has to prevent the occurrence of a high level deviation.

Based upon the analysis of 86 overfilling accidents 4 main barriers were distinguished:

1. Batch size preparation
   Before the start of the transfer of a batch of liquids it should be clear whether batch size fits into the remaining space of the receiving storage tank. Also the expected transfer time should be calculated which is the batch size (in m3) divided by the flow rate (m3/hr))

2. Connection
   Failure takes place when wrong containments are connected

3. Flow feed control
   Failure can take place by:
   - flow too high
   - flow duration too long

4. Flow discharge control
   Failure can take place by:
   - flow too low
   - flow duration too short
   - reverse flow: feeding instead of discharging

To every barrier two sets of blocks are connected which are there for the recording of the management factors which played a role in the failure of the barrier. In Figure 9 the blocks sets connected to the batch size preparation barrier are presented.

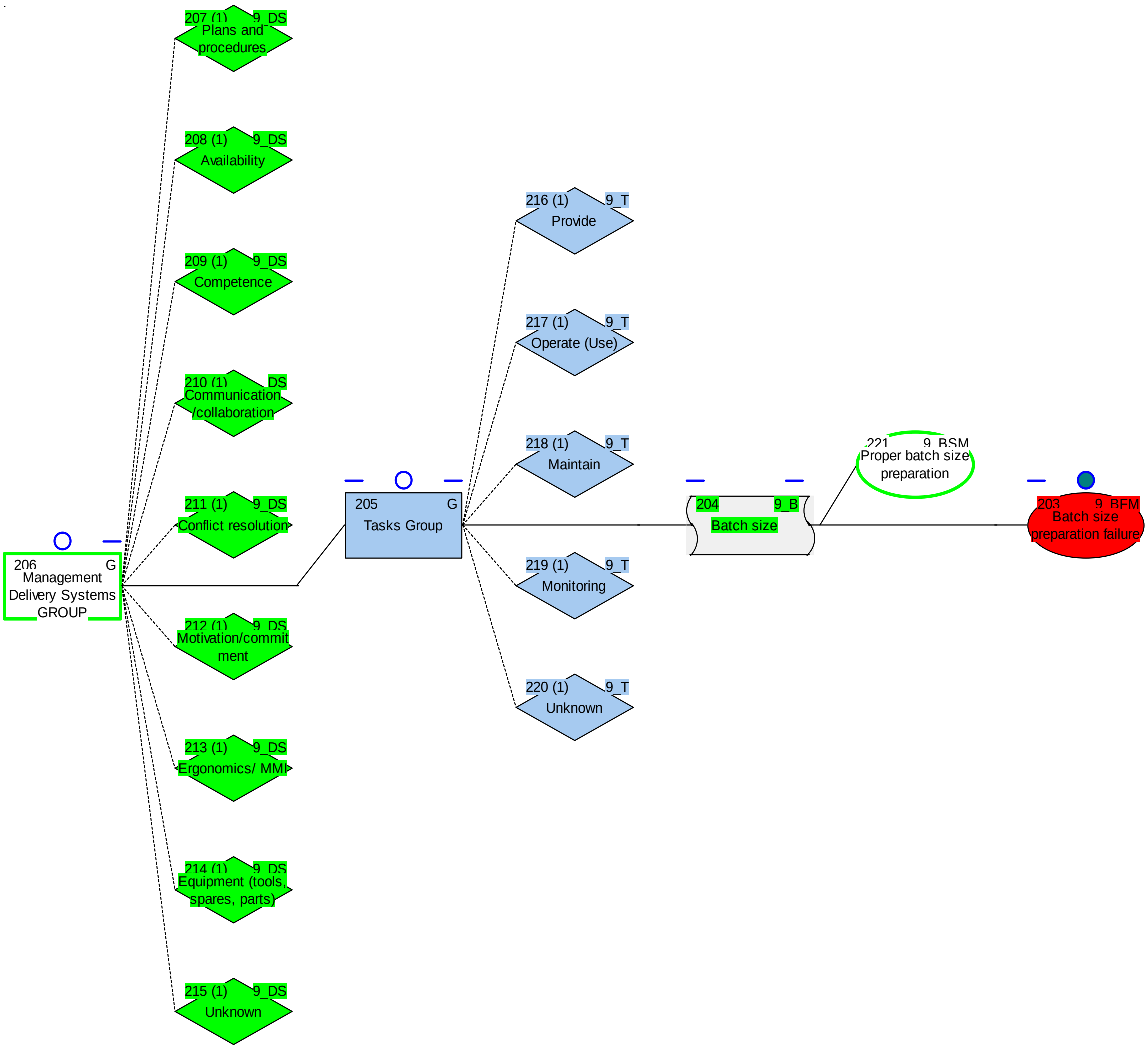


Figure 9 Management delivery systems and tasks connected to the batch size preparation barrier

The first block is called “Task group” and contains sub blocks with additional information about the barrier failure:

1. Provide: the barrier was not there at all
2. Use: the barrier was there but not or wrongly used
3. Maintain: the barrier was there but its function was not there
4. Monitor: the state of the barrier was not well monitored.

The second group is called “Management delivery systems”. This block contains sub blocks with additional information about what part of the management system failed in order to guarantee the presence of a barrier, the right use of it and the maintenance and/or monitoring of the barrier.

A more extensive description about these Tasks and Management Delivery Systems was given in section 1.3.2.

4 Results of analysing 86 overfilling accidents

4.1 Percentages of barrier failures

86 overfilling accidents have been modelled. These comprise 77 UK accidents supplemented with 5 accidents in The Netherlands, 1 in the US and 1 in Thailand (accident references and descriptions are available in the Storybuild model). In the model each accident has a multiple failure of barriers: at least one of barrier set 1 and at least one of barrier set 2 have failed resulting in an overfilling of a vessel/storage tank. In table 1 the percentages of all barrier failures are presented.

Table 1 Percentage of all barrier failures for overfilling

Barrier set 1	Failure %	Barrier set 2	Failure %
Batch Size Preparation failure	34%	Indication failure	56%
Connection failure	20%	Detection failure	16%
Flow feed control failure	33%	Diagnosis failure	1%
Flow discharge control failure	8%	Response failure	21%
Unknown	9%	Unknown	15%

4.2 Analysis of Barrier Tasks

Batch Size Preparation failures:

- Provide: Batch Size Preparation was not performed (no calculation was performed to ensure that the batch which had to be transferred fits into the empty space of the receiving vessel) (20%)
- Use: Batch Size Preparation was performed but was not used (75%)
- Maintain/monitor: 10%
- Unknown: 10%

Connection failures:

- Provide: a wrong connection was made or the right connection was not provided (18%)
- Use: the right connection was there but not used (75%)
- Maintain/monitor: 6%
- Unknown: 12%

Flow feed control failures:

- Provide: flow feed control was not provided (results: flow remained too long, flow too high, or reverse flow) (11%)
- Use: flow feed control was there but not well used (e.g. because of communication problems) (43%)
- Maintain: flow feed control was provided and well used but control equipment did not maintain its function (25)
- Monitor: flow feed control was provided, used and control equipment was maintained but not monitored (25%)
- Unknown: 7%

Flow discharge control failures:

- Provide: flow discharge control was not provided (results: flow remained too short, flow too low, or reverse flow) (14%)
- Use: flow discharge control was there but not well used (e.g. because of communication problems) (28%)
- Maintain/monitor: flow feed control was provided and well used but control equipment did not maintain its function or was not well monitored (42%)
- Unknown: 28%

Indication failures:

- Provide: absence of indicators (60%)
- Use: Indication was there but not used (5%)
- Maintain/monitor: HL-Alarms or HL-Trip-functions failed to work (not well maintained) or was not well monitored (30%)
- Unknown: 5%

Detection failures:

- Provide: level indication was there but not connected to an alarm (29%)
- Use: indication was there but not used (e.g. sight glass was there but operator did not use it) (64%)
- Maintain/monitor: detection instrumentation not well maintained or monitored (14%)
- Unknown: 1%

Diagnosis failures (only 1%):

- Use: wrong diagnosis was made (alarm was accepted)

Response failures:

- Provide: no response was performed (35%)
- Use: response was done but not correctly (41%)
- Maintain/monitor: wrong response caused instruments which did not maintain their function or which were not well monitored (24%)
- Unknown: 6%

5 Modelling the Buncefield accident in the overfilling Storybuild model

Publicly available information has been used to analyse the information needed for a modelling of the barriers preventing the overfilling part of the Buncefield accident.

Based upon this information it could be concluded that 4 barriers have failed before the overfilling started:

1) Barrier failure : Batch size preparation failure

See recommendation HSE (http://www.hse.gov.uk/comah/buncefield/bstg1.htm):
Pipeline transfers
7. The safe management of product transfer will be improved by receiving site operators positively confirming that they can safely receive the product package before transfer starts and are able to initiate emergency shutdown if necessary. This will be achieved through the use of a standardised consignment transfer agreement.

Three possible use failures:

- batch size/ filling time was not calculated at all
- calculations were done but the results not communicated (shift-handover?)
- calculations communicated but not responded to

Second option is considered most likely (see HSE recommendation above*).*

Failed delivery systems:
communication/ collaboration, plans& procedures

Note: we lack information to be sure about this.

2) Barrier failure : Flow (feed) control failure

See Third Progress Report page 8 (HSE 2006)
24. The evidence to date is consistent with continued filling of Tank 912 after 03.00, despite the ATG system showing a static level reading.

See Initial Report p.7 (HSE 2006)
From approximately 03.00, the level gauge for Tank 912 recorded an unchanged reading.

Failing barrier tasks:

- Maintain (designed function of pressure not maintained)
- Monitor (deviation of intended process of filling tank was not monitored properly)

Failed delivery systems:

- Equipment (to maintain the control of flow)
- Alertness (to monitor the barrier state) or Communications/ collaboration (to monitor the barrier state)

Note: we lack information on the failed delivery systems for monitor

3) Barrier failure : Indication of process deviation failure

From the public available information, it cannot be concluded why there was no high level alarm signal, however the high level indication was designed to provide an alarm signal, although seemingly, in this case, the indication was not functional (i.e. maintain failure).

See Initial Report para.22 (HSE 2006)
22 The ultimate high level switch should, if triggered, cause an alarm to sound and shut down the supply of fuel to the tank.

4) Barrier failure : Response failure
The automatic trip function of the (ultimate) high level instrument was not functional at the moment of the accident. There are indications that this barrier maintain failure might be caused due to de-activation during testing (HSE Safety Alert to operators of "COMAH" oil/fuel storage sites & others storing hazardous substances in large tanks, SA0106, see quote see below).

"The switches are tested by using a lever or plate fitted to the head of the switch, which can be raised to simulate a high level of liquid in the tank. If the switch is working, then alarms and trips connected to the switch should operate.
However, it is critical that after carrying out this test that the lever or plate is returned to the correct position and locked into place, using a special padlock supplied by the manufacture [3], and in accordance with the manufacturers instructions. Failure to do this can lead to the switch being inoperative in normal operating mode even though it gives the appearance of functioning normally when tested".

6 Conclusions

1. Even a relatively simple model, containing 8 barriers to the left of the Loss of Containment event, is sufficient for the modelling of all sorts of complex overfilling accidents

2. High level failures (barrier failure set 1)
   - The failures of the barriers ‘Batch size preparation’ and ‘Flow feed control’ are the main causes for high level deviations in process vessels or storage tanks
   - In 75% of all ‘Batch size failures’ the batch size preparation was performed but not used
   - At least 85% of the ‘Flow feed control failures’ were not caused by absence of control (equipment) but because the control was not used or flow control equipment was not maintained or monitored
   - Overall conclusion:

     1. barriers for preventing high level deviations are mostly in place
     2. the main reason for failing are a wrong use of barriers or badly maintained or monitored barriers

3. Overfilling failures (barrier failure set 2)
   - The main barrier which failure causes an overfilling is the indication barrier. In almost 60% of all cases this barrier was the direct cause for the overfilling.
   - Most of the indication failures was caused because of the absence of indicators (60%).
   - Overall conclusion:

     In almost 40% of all overfilling cases there were no indicators present to indicate a deviation in the level.

4. Buncefield accident
   - Barrier failures are easily to recognize when reading publicly available information (HSE 2006)
   - The identification of the failing tasks and failing delivery systems is hard when only publicly available information can be used
   - The model is a useful tool to record in detail all possible causes and root causes. When detailed information about the underlying causes of an accident is not available, Storybuilder can be used to generate focused questions to support the investigation .

This page left blank

7 References

Ale, B.J.M., Bellamy, L.J., Papazoglou I.A., Hale A.R., Goossens L.H.J., Post J., Baksteen, H., Mud M.L., Oh J.I.H., Bloemhoff A., Whiston, J.Y. (2006) ORM: Development of an integrated method to assess occupational risk, International Conference on Probabilistic Safety Assessment and Management, May 13-19, 2006, New Orleans, ASME, New York, 2006, ISBN 0-7918-0244

Ale, B.J.M, Bellamy, L.J., Baksteen, Damen, M., Goossens L.H.J., Hale A.R., Mud, M, Oh, J., Papazoglou, I. A., Whiston, J.Y. (2007) Using Storybuilder to analyse accident reports for causes and cures. Risk, Reliability and Societal Safety – Aven & Vinnem (eds) 2007 Taylor & Francis Group, London, ISBN 978-0-415-44786-7

Bellamy, L.J. Oh, J., Ale B.J.M., Whiston J.Y., Mud, M.L, Baksteen H. Hale, A.R., Papazoglou, I.A. (2006) Storybuilder: The new interface for accident analysis, International Conference on Probabilistic Safety Assessment and Management, May 13-19, 2006, New Orleans, ASME, New York, 2006, ISBN 0-7918-0244

Bellamy, L.J., Ale B.J.M., Geyer T.A.W., Goossens L.H.J., Hale A.R., Oh J., Mud, M., Bloemhof A, Papazoglou I.A., Whiston J.Y. (2007) Storybuilder—A tool for the analysis of accident reports, Reliability Engineering and System Safety 92 (2007) 735–744

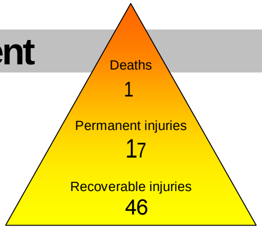
Hale, A.R., Goossens, L.H.J., Ale, B.J.M., Bellamy, L.J., Post, J., Oh, J.I.H. & Papazoglou, I. A. (2004). "Managing safety barriers and controls at the workplace". in Probabilistic Safety Assessment & Management. Pp 608 - 613. Springer Verlag. Berlin.

Hale, A.R., Ale, B.J.M., Goossens, L.H.J., Bellamy, L.J., Mud, M.L., Roelen, A., Baksteen, B., Post, Bloemhoff, A., Papazoglou, I. A., Oh, J.I.H. (2006) Modeling accidents for prioritising prevention. Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, May 14-18, 2006, New Orleans, Louisiana, USA. PSAM-0102

Health and Safety Executive (2006) Investigation reports Buncefield Major Incident Investigation: Progress Report, published 21 February 2006; Second Progress Report, published 11 April 2006; Third Progress Report, published 9 May 2006; Initial report, published July 2006 . Available from www.buncefieldinvestigation.gov.uk

This page left blank

15 Loss of containment from a closed containment



1

Based on: 244 GISAI ACCIDENTS FROM 1998 - FEB 2004

Table 2 Accident consequence frequencies

STORYBUILD	AVERAGE NUMBER OF GISAI ACCIDENTS PER YEAR				RATIOS		
	Deaths	Permanent injuries	Recoverable injuries	Unknown injury type	Deaths	Permanent injuries	Recoverable injuries
15 LOC closed containment	<1	8	22	3	1	17	46

Table 3 Type of activity (process state)

Activity	**Description**	**% of accidents**	**Nr. Accidents 1998-feb 2004**	**Nr. Accidents per year**
Normal operation	Start up/shutdown of a reactor operation according to procedures or within specification. Normal operation of equipment functioning as a containment.	37.7%	92	15
Maintenance on containment	replacement/reinstallation, changing of filters, maintenance of equipment functioning as a containment.	30.3%	74	12
Not-normal operation	Troubleshooting, operating outside specifications, start up or shut down of (part of) plant or of a whole utility system	23.8%	58	9
Cleaning of containment	Cleaning in place (CIP). Cleaning of the containment.	7.8%	19	3

Table 4 Barrier failure modes and how often they occur (not necessarily mutually exclusive)

BARRIER FAILURE MODE (Only LOC related Left Hand Side Barriers) [1]	Description	% of accidents	Nr. Accidents 1998-feb 2004	Nr. Per Year
Prevention of loss of containment				
Content deviation (p,T,flow/substance) indication/ detection failure	The indication of the content of the containment (p, T, flow) was absent/inadequate OR The indication was present and adequate but not (adequately) noticed/detected.	29.1%	71	12
Substandard containment indication/ detection/ diagnose/ response failure	It was not detected that the containment was in a substandard condition	23.0%	56	9
Content deviation (p,T,flow/substance) diagnose/ response failure	The indication of the content of the containment (p, T, flow) was present and adequate AND The indication was adequately noticed/ detected BUT a wrong diagnosis/response was made.	11.9%	29	5
Protection against external influences failure	Dropping or collisions	9.4%	23	4
Operator ability failure	Opening wrong valves or doors or wrong timing or sequence of events	3.7%	9	1
Stability of containment failure	Not stable causing containment to fall	3.7%	9	1
Collision control failure	Refers to an activity with a moving containment	1.2%	3	<1
External heating source failure	From nearby heat source (welding, fire)	0.8%	2	<1

[1] In total there are 23 Left Hand Side Barriers in two groups, 15 of these barriers deal with the containment, the other 8 with the loss of containment, these 8are listed in this table. There are 15 Right Hand Side Barriers in two groups not listed here.

Table 5 Dominant underlying barrier tasks and management delivery system failures (not necessarily mutually exclusive)

Underlying failure	**Description**	**% of accidents**	**Nr. Accidents 1998-Feb 2004**	**Nr. Per year**
Barrier task failure (LOC LHS only)	**Description**			
Provision of means (human and hardware) to detect deviations in containment	Failure to provide (or not present) the means to detect deviations from normal in the containment	14.8%	36	6
Provision of means to detect substandard container	Failure to provide means to detect substandard container	11.9%	29	5
Provision of an adequate response (human or automated) to the diagnose of an deviation	Failure to provide the adequate response to a change in the containment	9.0%	22	4
Use of means (human and hardware) to detect deviations in containment	Failure to use the means to detect deviations from normal in the containment	8.2%	20	3
Delivery system failure[2] (LOC LHS only)	**Description (and % of accidents per barrier support task)**			
Motivation to ensure the detection of deviations from normal in a containment	No motivation delivered to ensure the provision of means of detection (1.6%), the use of these means (5.2%) or the monitoring of the use (1.2%)	8.6%	21	3
Plans and Procedures to ensure the detection of deviations from normal in a containment	No Plans and Procedures present or fail to ensure/guide the provide means of detection (4.5%), use them (1.6%), maintain them (0.8%) and monitor the use (1.2%)	8.2%	20	3
Plans and Procedures to ensure the detection of a substandard container	No Plans and Procedures present or fail to ensure/guide the provide means of detection (4.9%) and use them (1.2%)	6.6	16	3
Motivation to ensure the detection of a substandard container	No motivation delivered to ensure the provision of means of detection (3.3%) and the use of these means (2.5%)	6.1	15	2

[2] Of 3 accidents per year (average) where a substandard container was not detected it is Unknown what Delivery System did not deliver

Table 9 Dominant underlying barrier tasks and management delivery system failures (not necessarily mutually exclusive)

Underlying failure	**Description**	**% of accidents**	**Nr. Accidents 1998-Feb 2004**	**Nr. Per year**
Barrier task failure	**Description**			
Provide edge protection	Failure to provide sufficient Edge Protection (edge protection completely absent 18.9%)	25.7%	136	22
Use ability to keep balance	Failure to use ability to keep balance on a scaffold (situation beyond normal ability like climbing scaffold from the outside: 6.6%)	24.5%	130	21
Provide anchoring and/or fixation	Failure by provide anchoring or fixation of scaffold (no stabilisers: 5.7%)	9.8%	52	8
Provide ability to keep balance	Working on a scaffold without the ability (unwell, sick or circumstances not compatible with normal human ability) to keep balance	8.5%	45	7
Provide proper scaffold floor	Failure to provide a proper intact/strong floor	8.5%	45	7
Delivery system failure[4]	**Description (and % of accidents per barrier support task)**			
Motivation to ensure user ability to keep balance	Insufficient motivation or commitment to be aware of the need to provide ability (4.2%), use ability (12.1%) or monitor that ability (1.7%)	17.9%	95	15
Equipment to ensure edge protection	No equipment to provide scaffold with edge protection	12.6%	67	11
Motivation to ensure edge protection	Insufficient motivation or commitment to be aware of the need to provide edge protection (8.7%) or use edge protection (1.3%)	10.2%	54	9
Motivation to ensure anchoring and/or fixation of scaffold	Insufficient motivation or commitment to be aware of the need to provide anchoring (3.2%), use anchoring (4.0%), keep anchoring in place (0.6%) or check presence of anchoring (0.9%)	8.1%	43	7

[4] Excluding unknown delivery system failures