BOW TIE METHODOLOGY: A TOOL TO ENHANCE THE VISIBILITY AND UNDERSTANDING OF NUCLEAR SAFETY CASES

Marc Vannerem
Office for Nuclear Regulation, UK

Abstract – There is much common ground between the nuclear industry and other major hazard industries such as those subject to the Seveso II regulations, e.g. oil, gas & chemicals.

They are all subject to legal requirements to identify and control hazards, and to demonstrate that all necessary measures have been taken to minimise risks posed by the site with regard to people and the environment.

This places a requirement on the Operators of major hazard installations, whether nuclear or conventional, to understand and identify the hazards of their operations, the initiating events, the consequences, the prevention and mitigation measures.

However, in the UK, nuclear and "Seveso" type facilities seem to adopt a different approach to the presentation of their safety cases.

Given the magnitude of the hazards, safety cases developed for nuclear fuel cycle facilities are rigorous, detailed and complex, which can have the effect of reducing the visibility of the key hazards and corresponding protective measures.

In contrast, on installations in the oil & gas and chemical industries, a real attempt has been made over recent years to improve the visibility and accessibility of the safety case to all operating personnel, through the use of visual aids / diagrams.

In particular, many Operators are choosing to use "bow tie methodology", in which very simple overview diagrams are produced to illustrate, in a form understandable by all:

- what the key hazards are;
- the initiating events;
- the consequences of an incident;
- the barriers or "Layers of Protection" which prevent an initiating event from developing into an incident;
- the barriers or "Layers of Defence" which mitigate the consequences of an incident, i.e. which prevent the incident from escalating into major consequences.

The bow tie method is one of a number of methodologies that can be used to make safety cases more accessible. It is used in this paper to illustrate ways to improve the visibility and accessibility of complex

safety cases. The bow tie method is a purely qualitative technique, which could be successfully introduced (or similar methodologies) to the nuclear industry as an additional tool to improve the visibility and understanding of the safety case, and thus complement (not substitute) the more rigorous safety analysis techniques which are the norm in this industry.

By making the diagrams readily accessible in the control room, the operators of nuclear facilities could further improve their understanding of the safety significance of their role in preventing major accidents and mitigating consequences.

1. Introduction

The nuclear industry is by no means unique in its legal obligation to demonstrate that hazards associated with its operations are properly managed.

In Europe for example, various high profile accidents in the chemical industry have resulted in legislation (Council Directive 96/82/EC [9], also known as the Seveso II Directive) aimed at the prevention of major accident hazards, but also aimed at limiting the consequences of such accidents to people and the environment.

One of the objectives of the Directive is to prevent or reduce accidents caused by management factors, or safety management systems, which have proved to be a significant cause of accidents. [9]

The Directive, implemented via national legislation, places a general duty on the operators of hazardous installations to prepare a safety report demonstrating that “major accident hazards have been identified, and that the necessary measures have been taken to prevent such accidents and to limit their consequences for persons and the environment.” [1] “The complexity of the demonstration presented in the safety report is expected to increase with the complexity of the facility concerned.” [1]

Similarly, the nuclear industry operates in an extremely highly regulated environment, where national legislation requires the operators of nuclear facilities to ensure that “all practical efforts [are] made to prevent and mitigate nuclear or radiation accidents.” [12] “The fundamental safety objective is to protect people and the environment from [the] harmful effects of ionising radiation.” [12]

Therefore, in general terms, national and international legislation requires the operators of major hazard installations (chemicals, oil & gas, nuclear, etc …) to understand and identify:

- The hazards of their operations;
- The initiating events which could result in an accident;
- The consequences of such accidents;
- The prevention measures which they have in place to prevent an initiating event developing into an accident;
- The protective measures which are in place to limit the effects of an accident.

This report considers to what extent methodologies such as bow tie could be applied to the nuclear industry, in order to enhance the communication, visibility and understanding of the safety case. Bow tie methodology has been selected for examination in this report over other similar techniques, due to its increasing popularity and widespread use throughout the world by the operators of major hazard installations.

2. Risk Analysis and Safety Critical Events

There are numerous ways in which risk analyses may be conducted, from simple qualitative approaches to a fully quantitative risk analysis. In order to select the most appropriate technique, UK guidance to the "Major Hazard Industries" indicates that "the depth and sophistication of the analysis should be proportionate to the hazard and risk present." [10]

CONSEQUENCE					INCREASING PROBABILITY				
Severity Rating	People	Assets	Environ-ment	Reputation	A Rarely occurred in E&P industry	B Happened several times per year in industry	C Has occurred in operating company	D Happened several times per year in operating company	E Happened several times per year in location
0	Zero injury	Zero damage	Zero effect	Zero impact	Manage for continued improvement				
1	Slight injury	Slight damage	Slight effect	Slight impact					
2	Minor injury	Minor damage	Minor effect	Limited impact					
3	Major injury	Local damage	Local effect	Considerable impact					
4	Single fatality	Major damage	Major effect	Major national impact	Incorporate risk reducing measures				
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact				Intolerable	

Figure 1 – risk matrix

UK guidance [13] also provides a useful definition of safety critical events, i.e.: "Safety critical events are those that dominate the contribution to risk, so they should be identified by your risk analysis."

The risk matrix [fig 1] is an easy and effective way to qualitatively assess and represent the risks to people, assets, environment and reputation. [2]

A qualitative assessment is made of the probability and the severity of the consequences of each event without taking credit for protective measures. A more detailed analysis is then carried out for all safety critical events.

3. Prevention and protective measures

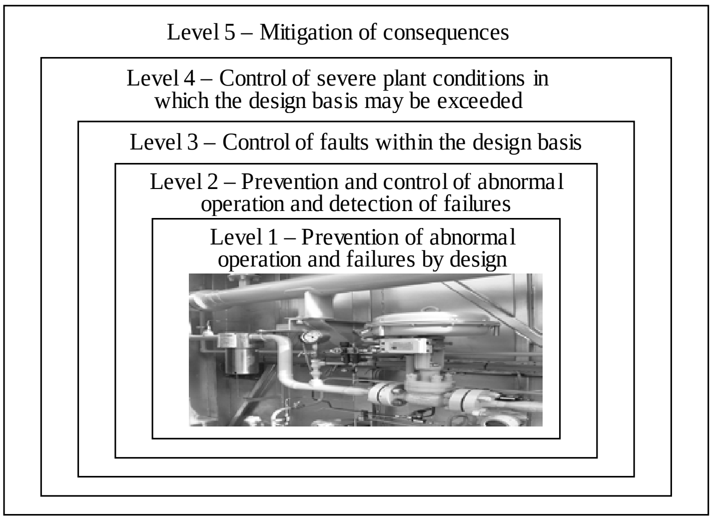


Figure 2 – The 5 general levels of defence in depth

The principle of defence in depth is described in detail in the IAEA's Safety Standard NS-R-1 [14], the UK nuclear regulator's safety assessment principles [11], and research papers commissioned by the UK regulator for the Major Hazard Industries [8]. The various protective measures are illustrated as concentric "lines of defence" (LODs) or "layers of protection" (LOPs) around the basic process. [8, 11, 14, fig 2] The function of the inner layers is to prevent the process from deviating from its normal design parameters. The severity of the deviation from normal operation increases as the internal layers of protection are progressively breached and challenges are placed on outer layers.

The “Bow Tie” model [fig 3] provides an effective illustration of the different functions of the layers of protection, by placing them into two separate categories: [7]

- those which provide primary barriers to prevent hazards from arising;
- those which mitigate the consequences of hazards which arise if prevention measures identified in (a) are breached.

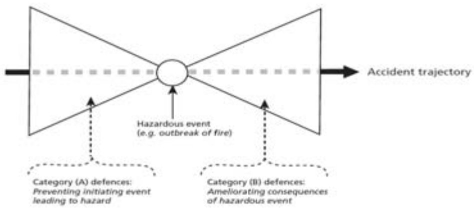


Figure 3 – the bow tie model

The name given to the resulting diagram [fig 3] comes from its very obvious resemblance to the bow tie, i.e. the short knot tie worn by gentlemen on formal occasions.

4. Safety cases in the nuclear industry

The principle of proportionality, described in previous paragraphs for major hazard installations, also applies to nuclear facilities, i.e. “*the depth and sophistication of the analysis should be proportionate to the hazard and risk present.*” [1] Nuclear installations fall into the “high hazard” category, and should therefore use “the most developed and sophisticated techniques.” [11]

In accordance with this principle, the safety cases developed for nuclear facilities are detailed and can appear complex to non-specialists.

Safety inspections of nuclear fuel cycle facilities routinely identify that the necessary rigour and depth of analysis of nuclear safety cases can reduce the clarity with which key hazards and safety measures are communicated to the operators of those facilities. There is scope for improving plant operators’ understanding of the safety significance of the operations and checks which they routinely carry out.

The typical hierarchy [fig 4] of safety case documents on nuclear fuel cycle facilities in the UK shows three generic categories of documents, i.e.:

- At the highest level, the detailed safety case documents which are normally reserved for safety case specialists and plant management.
- An intermediate level, which translates the detailed safety case requirements into rules and instructions for the controlled operation and management of the

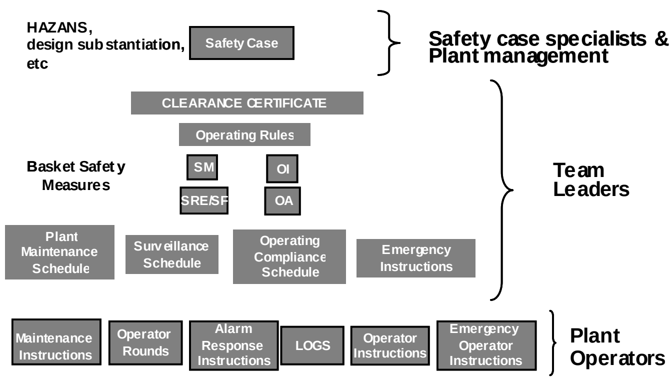


Figure 4 - Typical hierarchy of safety related documents

plant. This level of documentation is typically accessed by team leaders.

- Finally, detailed instructions are provided for plant operators and maintainers, to ensure that the nuclear facility remains within a tightly controlled operating envelope, and that nuclear emergencies are adequately managed.

This hierarchy of safety documentation has evolved over a number of years, and has been successful in managing and controlling hazards on nuclear fuel cycle facilities.

However, this approach leads to limited visibility of the overall safety case, and further efforts need to be made by nuclear licensees to ensure plant operators understand why it is important to perform the specific tasks which they routinely carry out.

What seems to be missing is a simple overview diagram, which illustrates in simple terms:

- What the key hazards are;
- What could initiate those hazards (the initiating events);
- The consequences of an incident, once it has occurred;
- The barriers or “Layers of Protection” which prevent an initiating event from developing into an incident;
- The barriers or “Layers of Defence” which mitigate the consequences of an incident, i.e. which prevent the incident from escalating into major consequences.

5. Bow tie methodology

Bow tie methodology has been increasingly used throughout different areas of business and industry since the early 1980s, principally to provide corporate assurance that major risks are adequately identified and controlled. [4]

Bow tie diagrams [fig 5] combine into a single diagram the possible causes and consequences of a potential accident. The left hand side represents the fault tree, which links the accident to possible causes, whilst the right hand side represents the event tree, linking the accident with possible consequences. [6]

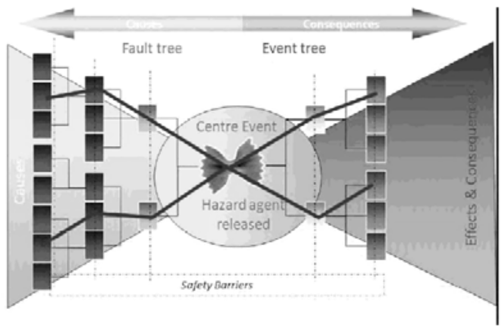


Figure 5 - The bow tie diagram

The development of the diagram [fig 6] starts with the identification of all potential threats which could lead to an event, i.e. the realisation of the hazard. The next step is to identify, for each threat, the barriers which prevent those threats from developing into the event. The right hand side of the diagram is then developed in a similar manner. All consequences are identified, and, for each one, the barriers which prevent the escalation of the event are identified and included. [5]

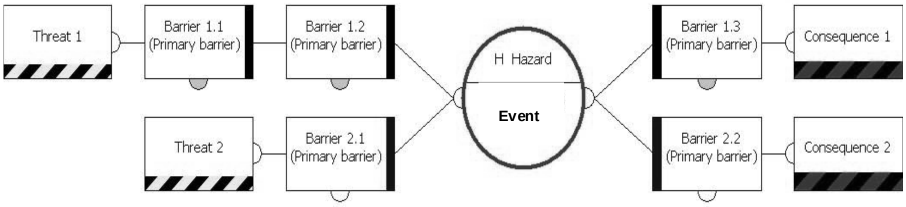


Figure 6 – Construction of bow tie diagram

This systematic step by step approach results in the construction of a complete bow tie diagram, which includes all protective measures or barriers.

6. Types of barriers

Barriers are variously classified into different categories:

- Primary and secondary barriers [5]
  Primary barriers prevent or reduce the development of threats into accidents, and mitigate or prevent the accident from escalating into major consequences. Secondary barriers prevent or reduce the erosion (referred to as "decay") of the effectiveness of the primary barriers. Primary barriers are the primary means of preventing and controlling hazards, whilst secondary barriers are put in place to ensure that the effectiveness of the primary barriers is maintained.

Typical examples of primary and secondary barriers are listed below: [5]

- Primary barriers:
  - ~ Active barriers: shut-down valves, deluge system;
  - ~ Passive barriers: fire wall, blast wall, containment, separation;
  - ~ Control barriers: fire and gas detection, alarms;
  - ~ Organisational / procedural barriers: inspection and monitoring;
  - ~ Human / operator barriers: process control operator.
- Secondary barriers:
  - ~ Human / operator barriers: supervision;
  - ~ Procedural barriers: design reviews, operational reviews, competenceassurance;

- Passive, active and behavioural barriers [6].
  Passive barriers prevent or reduce the transmission of threats, or mitigate the consequences of accidents without any requirement for automatic or human intervention. Retention bunds are a typical example of passive barriers.

  Active barriers require human intervention or are activated automatically. An automatic shut down system is a typical example of active barriers.
  Finally, behavioural barriers require human judgement and intervention. A typical example would be the requirement for a plant operator to base his decision to shut down a piece of equipment on instrument readings.

- Full or partial barriers [8]

A full barrier is designed to completely stop a cause from developing into a consequence, unless it fails to operate. A partial barrier offers a degree of protection, but does not fully prevent a cause from generating a consequence. An alarm is a typical example of partial barrier.

7. Barrier decay – barrier failure modes

There are many reasons why the integrity of protective barriers may be lower than originally intended, such as inadequate design or maintenance, poor procedures and communication, insufficient training, etc… [5]

In bow tie methodology, barrier decay modes, i.e. the underlying causes of barrier failure, are identified and included on the diagram. [fig 7] The secondary barriers, i.e. those which prevent the degradation or decay of the primary barriers, are also identified and included on the same diagram. As illustrated [fig 7], there could be several possible decay modes for each primary barrier, which need to be protected by corresponding secondary barriers. [5]

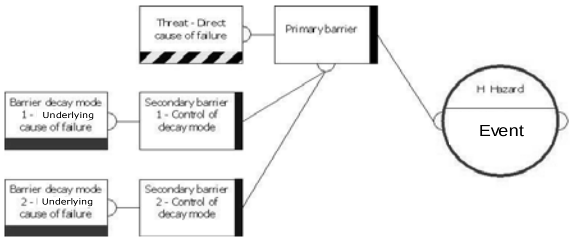


Figure 7 – Barrier decay modes

This approach brings together in a single diagram all relevant protective barriers, their modes of degradation, and all measures taken (secondary barriers) to prevent the decay of those barriers. [5]

Reference 6 proposes a hierarchy for the implementation of barriers, and suggests useful questions for the investigation of incidents and accidents, i.e.:

- Provide barrier (question: “Was the barrier provided?”);
- Use barrier (question: “Was the provided barrier used?”);
- Maintain barrier (question: “Was the provided barrier maintained?”);
- Monitor barrier (question: “Was the state of the barrier monitored?”);

“For an operating plant, the key controls are in making sure that the installed equipment keeps working properly” [5], and “that barriers are operational at all times.” [3]

Reference 5 proposes a “barrier rating scheme” to rate the effectiveness and complexity of barriers.

8. Compatibility of the bow tie method with fault analysis techniques commonly used in the nuclear industry

This section examines the compatibility of bow tie methodology with fault analysis techniques routinely used in the nuclear industry, i.e. Design Basis Analysis (DBA), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA).

“Design basis analysis is a robust demonstration of the fault tolerance of the facility, and of the effectiveness of its safety measures.” [11] DBA uses appropriate conservatism to assess the suitability and sufficiency of the safety measures. [11] Risks are not quantified in this approach. However, “DBA should provide a clear auditable link between initiating faults, fault sequences and safety measures.” [11] The bow tie method, which is also qualitative, could act as a useful complement (but not a substitute) to the more rigorous DBA approach, by providing a diagrammatic illustration of fault progression and protective measures.

Probabilistic Safety Analysis is a quantitative approach, which addresses the overall risk presented by facilities. It "enables complex interactions to be identified and examined, and provides a logical basis for identifying any relative weaknesses." [11] This aspect of safety analysis is recognised as one of the principal limitations of the bow tie technique. (see paragraph 10)

Severe Accident Analysis addresses severe but very unlikely faults. Indeed, "DBA should ensure that severe accidents are highly unlikely. Nevertheless, the principle of defence in depth requires that fault sequences leading to severe accidents are analysed and provision made to address their consequences." [11] Severe Accident Analysis is designed to identify protective measures required for severe accident scenarios. Also, "severe accident analysis may also identify that providing further plant and equipment for accident management is reasonably practicable." [11] As outlined in para 0, the bow tie method could be used as a purely qualitative diagrammatic aid to help identify additional measures of protection.

9. The benefits of bow tie diagrams

a. Communication: visualisation and improved understanding of major hazards

"A picture paints a thousand words." Bow tie diagrams are an extremely user-friendly tool for providing a readily understandable visualisation of the main hazards, their causes and consequences, and the prevention and protective measures. Bow ties could be introduced in addition to the more rigorous safety analysis techniques currently used in the nuclear industry to improve visibility and understanding. Ideally, the bow tie diagrams should be displayed on posters in the control room to allow plant personnel at all levels to understand the importance of their role in preventing accidents, and where their work fits in the overall picture.

"Understanding why and how something has to be done on the barrier facilitates appreciation of the barrier function and its failure." [5]

Removing a barrier or a set of barriers for the purpose of maintenance immediately highlights the resulting weakening of the system, and the importance of making a risk informed decision whether to shut down the facility and / or to put in place additional protection. [5]

b. Workforce involvement and ownership

The benefits of bow tie are from applying the approach and involving the workforce in the development of the diagrams. [3] Operational personnel typically have limited knowledge of the safety case, but a high level of experience of its practical implementation and of any related incidents. [3]

When people feel involved and action is taken based on what they say, they tend to "buy in" to the process and take ownership. [3]

c. Focus on Critical Systems

Bow ties are an extremely effective tool for keeping sight of the big picture, i.e. top level safety critical events and corresponding control measures. They clearly illustrate, to plant personnel and stakeholders such as regulators, how hazards are managed and controlled. "What is important is that critical tasks have been identified, and that people know they need to do them and why." [4]

Bow ties pull together into one single diagram not only the hardware, but also the actions and controls conducted by real people on the plant. A visual examination of the diagrams provides a useful overview of the protective measures, and allows users to qualitatively identify weak areas where there appear to be gaps or insufficient protection.

d. Continuous Improvement and demonstration of ALARP

The bow tie approach fits well with the legal requirement to demonstrate that all reasonably practicable controls have been identified and implemented in order to ensure that risks are As Low As Reasonably Practicable (ALARP). [5]

However, it must be recognised that bow tie is a purely qualitative method, which cannot be used to quantitatively estimate the improvement afforded by an additional Independent Protective Layer.

The following questions must always be asked in order to achieve sustained and continuous improvements in safety standards: "What additional, practical controls can we implement?" or "Is there anything more we can reasonably do?" [3]

10. Limitations of bow tie diagrams

Bow tie diagrams provide a clear qualitative graphical representation of system failure logic and the role of the various layers of protection (barriers) in place. [8] "However, the method avoids any explicit calculation of risk. Therefore, barrier diagrams could be used in circumstances where a qualitative approach was justified, but would not be appropriate in situations where the use of a semi-quantitative or quantitative approach was demanded." [8]

Bow tie methodology also has a tendency to over-simplify the real underlying safety challenges of complex facilities. For example, it tends to hide dependencies and is not able to adequately model complex inter-relationships between various risk controls.

Also, in common with most other hazard management techniques, the successful application of the bow tie approach depends on the experience of personnel involved.

11. Conclusions

In accordance with the "high hazard" categorisation of the nuclear industry, safety cases developed for nuclear facilities are rigorous and detailed, which can reduce the clarity with which key hazards and safety measures are communicated to the operators of those facilities. There is scope for improving plant operators' understanding of the safety significance of the operations and checks which they routinely carry out.

The bow tie method is one of several methods which has been successfully used in numerous areas of business and industry to enhance the visibility of the safety case. It successfully illustrates in a single user-friendly diagram the hazards, the initiating faults, the consequences, and the prevention and mitigation barriers.

The bow tie method is a purely qualitative technique, which could be successfully introduced to the nuclear industry as an additional tool to improve the visibility and understanding of the safety case, and thus complement (not substitute) the more rigorous safety analysis techniques which are the norm in this industry. By making the diagrams readily accessible in the control room, the operators of nuclear facilities could further improve their understanding of the safety significance of their role in preventing major accidents and mitigating consequences.

References:

[1] Application of QRA in operational safety issues, Andrew Franks, Richard Whitehead, Phil Crossthwaite and Louise Smail, Det Norske Veritas, 2002, http://www.hse.gov.uk/research/rrpdf/rr025.pdf

[2] Marine risk assessment, Det Norske Veritas, 2002, http://www.hse.gov.uk/research/otopdf/2001/oto01063.pdf

[3] Lessons Learned from Real World Application of the Bow tie Method, Steve Lewis and Kris Smith, Risktec Solutions, March 2010, http://www.risktec.co.uk/knowledge-bank/publications.aspx

[4] Bow tie: an Elegant Solution?, Steve Lewis and Sheryl Hurst, Risktec Solutions Ltd, November 2005. http://www.risktec.co.uk/knowledge-bank/publications.aspx

[5] Optimising Hazard Management by Workforce Engagement and Supervision, Vladimir M Trbojevic, prepared by Risk Support Ltd for the Health and Safety Executive, Research Report 637, 2008, http://www.hse.gov.uk/research/rrpdf/rr637.pdf

[6] Feasibility of Storybuilder Software Tool for Major Hazards Intelligence, prepared by the Health and Safety Laboratory for the Health and Safety Executive, Diego Lisbona & Mike Wardman, Research Report 778, 2010, http://www.hse.gov.uk/research/rrpdf/rr778.pdf

[7] The Nimrod Review, An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, Charles Haddon-Cave QC, 28th October 2009, London: The Stationery Office, ISBN: 9780102962659

[8] Lines of Defence / Layers of Protection Analysis in the COMAH Context, Andrew Franks, prepared by Amey VECTRA Ltd for the health and Safety Executive, http://www.hse.gov.uk/research/misc/vectra300-2017-r02.pdf

[9] Council Directive 96/82/EC on the control of major-accident hazards (also known as the Seveso II Directive), http://ec.europa.eu/environment/seveso/index.htm

[10] Health & Safety Executive (HSE 1999a). A Guide to the Control of Major Accident Hazard Regulations 1999. L111, HSE Books.

[11] Safety Assessment Principles for Nuclear Facilities, Health and Safety Executive, 2006 Edition, Revision 1, http://www.hse.gov.uk/nuclear/saps

[12] Fundamental Safety Principles, International Atomic Energy Agency, Vienna, 2006, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf

[13] Health & Safety Executive (HSE 1999c). Preparing Safety Reports: Control of Major Accident Hazard Regulations 1999. HSG 190, HSE Books.

[14] IAEA Safety Standards Series, Safety of Nuclear Power Plants: Design, Safety Requirements, No. NS-R-1, International Atomic Energy Agency, Vienna, 2000, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1099_scr.pdf

Bow Tie Methodology

A tool to enhance the visibility and understanding of nuclear safety cases

Workshop on the Safety Assessment of Fuel Cycle Facilities – Sep 2011

Marc Vannerem
UK - Principal Nuclear Inspector

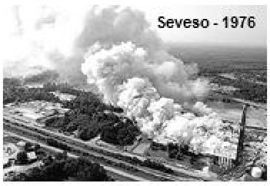
Office for Nuclear Regulation
An agency of HSE

Structure of presentation

- **Safety cases nuclear industry:** rigorous, in-depth, complex
- **Reduce visibility / understanding** (workforce)
- **Bow tie method: widespread use in the oil & gas and chemical industries**
- **Comparison / common ground: nuclear and other major hazard industries**
- **Incl. legislative framework (high level)**
- **Introduction to the bow tie method**
- **Simple example for nuclear fuel cycle facilities**
- **Finally, conclusions as to how it could be applied to nuclear fuel cycle facilities**

Office for Nuclear Regulation
An agency of HSE

Nuclear: not unique in managing hazards



Major hazard industries: oil & gas, chemicals

- E.g. Seveso 1976, Bophal 1984
- Europe: Seveso II directive (1996): control of major-accident hazards involving dangerous substances
- Implemented via national legislation
- UK: COMAH Regs 1999

Seveso Directive: safety report demonstrating

- major accident hazards have been identified
- all necessary measures have been taken to prevent such accidents and to limit their consequences for persons and the environment

The complexity of the demonstration presented in the safety report is expected to increase with the complexity of the facility concerned

Office for Nuclear Regulation
An agency of HSE

Similarly - Nuclear industry:
highly regulated environment

IAEA's Fundamental Safety Principles
(implemented via national legislation)

require the operators of nuclear facilities to:

- ensure that "all practical efforts are made to prevent and mitigate nuclear or radiation accidents."
- "The fundamental safety objective is to protect people and the environment from the harmful effects of ionising radiation."

Office for Nuclear Regulation
An agency of HSE

Nuclear / major hazard: much common ground

Nuclear industry Major Hazard Industries (oil & gas, chemicals)	Legal requirement to: •identify & control hazards •minimise consequences to persons & environment

Legislation requires the operators of nuclear and other major hazard installations (oil & gas, chemicals) to understand and to have identified:

- The hazards of their operations
- The initiating events which could result in an accident
- The consequences of such accidents
- The barriers which they have in place to prevent an initiating event becoming an event
- The various layers of protection which are in place to limit the effects of an accident

Office for Nuclear Regulation
An agency of HSE

What are the Regulators' expectations?
•depth and detail of the 'safety analysis' by the Operators of hazardous facilities

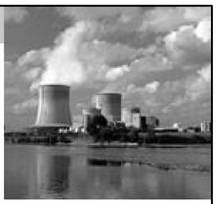
<u>Principle of proportionality</u>

Nuclear: IAEA's 'Fundamental Safety Principles'
(applied by UK's ONR)
Conventional: UK guidance to Major Hazard Industries

The depth and sophistication of the safety analysis should be proportionate to the hazard and risk present.

Office for Nuclear Regulation
An agency of HSE

Depth and rigour of safety cases in the nuclear industry



Nuclear installations: high hazard category

Proportionality principle: safety analysis should use "the most developed and sophisticated techniques"

- Nuclear safety cases:
  - Typically detailed, rigorous, in-depth analysis
  - Complex and lengthy (100s / 1000s pages)
- This can reduce: clarity, visibility, communication
  - key hazards and safety measures
- UK's ONR is always favourable to improvements:
  - visibility of safety case to plant personnel.
  - understanding of safety significance of operations and controls

Office for Nuclear Regulation
An agency of HSE

Typical hierarchy of safety case documents – UK NFC facilities

Highest Level: Detailed Safety Case Documents } Safety case specialists & plant management

Intermediate Level: converts "detailed safety case requirements" into "rules and instructions". Controlled operation / management of plant. } Team Leaders

Detailed instructions: Operation, Maintenance and Emergencies } Plant Operators and Maintainers

•Evolved / refined over many years

•Successful in managing and controlling hazards on nuclear fuel cycle facilities

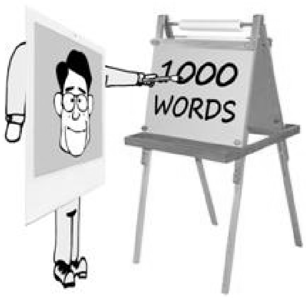
This approach: scope for improving visibility of the overall safety case.
UK's ONR encourages nuclear operators to further improve:
- visibility of safety case to all plant personnel.
- understanding of safety significance of operations and checks carried out.

Office for Nuclear Regulation
An agency of HSE

Simple overview diagram

illustrate in simple terms

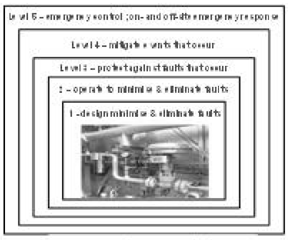
- Key hazards
- Faults: initiate events
- Consequences of events
- Prevention measures: barriers which prevent faults developing into events
- Mitigation measures: Barriers which mitigate / reduce the consequences of events



Office for Nuclear Regulation
An agency of HSE

Principle of 'defence in depth'

- **Nuclear industry:**
  - IAEA's safety standards
  - UK nuclear regulator's 'Safety Assessment Principles'
- **Conventional:**
  - UK regulator guidance for Major Hazard industries



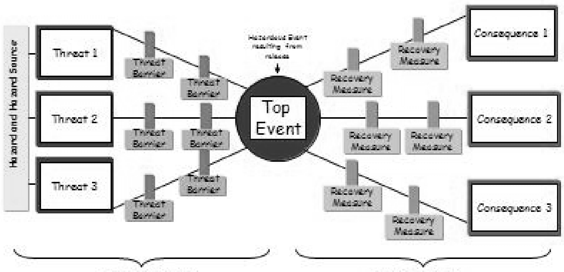
Defence in depth – IAEA safety standard

Protective measures = concentric 'layers of protection' or 'lines of defence'

Office for Nuclear Regulation
An agency of HSE

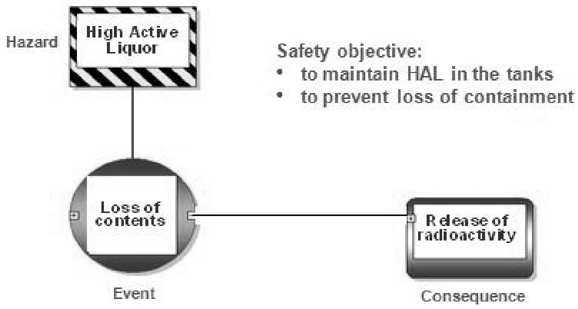
The bow tie model

Effective illustration of the different functions of the layers of protection: 2 separate categories



Office for Nuclear Regulation
An agency of HSE

Example: Nuclear Fuel Cycle Facilities
Loss of containment – High Active Liquor



Safety objective:
- to maintain HAL in the tanks
- to prevent loss of containment

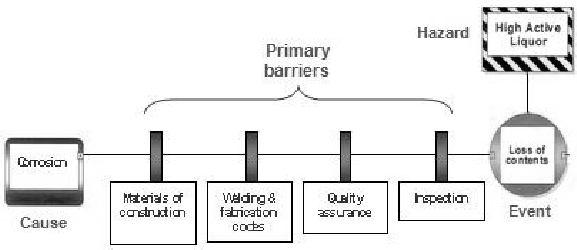
Office for Nuclear Regulation
An agency of HSE

Loss of containment (2)

Corrosion: potential cause of 'loss of containment'

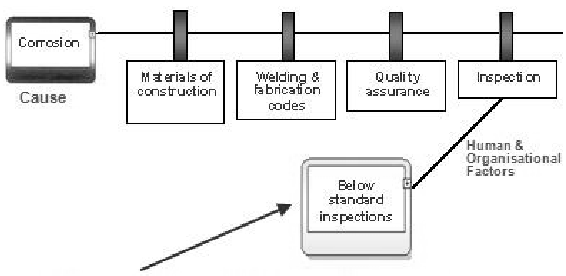
Office for Nuclear Regulation
An agency of HSE

Loss of containment (3)



Office for Nuclear Regulation
An agency of HSE

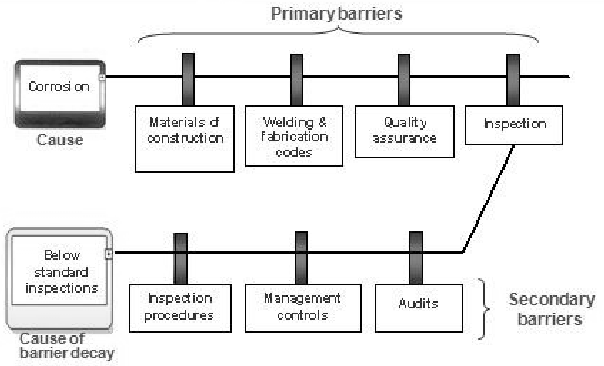
Loss of containment (4)



How could a barrier be weakened? (escalation)

Office for Nuclear Regulation
An agency of HSE

Loss of containment (5)



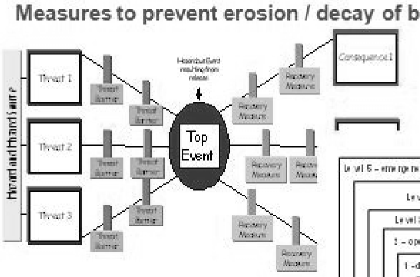
What barriers to prevent weakening of barriers?

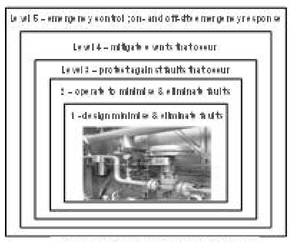
Office for Nuclear Regulation
An agency of HSE

Bow-tie diagram: step by step

All layers of protection: hard (physical equip) **& soft** (management, training, Human and Organisational Factors)

Measures to prevent erosion / decay of barriers

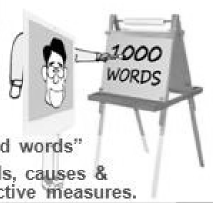




Defence in depth – IAEA safety standard

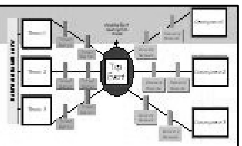
Can include layers of information as required:
- Roles and responsibilities
- Links to operating / maintenance instructions

Benefits of bow-tie method



- Communication – "a picture paints a thousand words"
- User-friendly visualisation of the main hazards, causes & consequences, and the prevention and protective measures.
- Benefits are from applying the approach and involving workforce.
  - Ownership. Buy-in.
  - Understanding the importance of their role in preventing accidents, and where their work fits in the overall picture.
- Focus on critical systems – big picture
  - Illustrate how top level safety critical events are managed and controlled
  - Enable qualitative assessment of areas of weakness
- International application – overcomes language difficulties

Office for Nuclear Regulation
An agency of HSE



Limitations of bow-tie

- Purely qualitative graphical representation
- Tends to over-simplify
  - –Underlying safety challenges of complex facilities
  - –Inter-dependencies / inter-relationships between various risk controls

  Hence:
  Bow ties: in addition (not substitute) / complement
  - –the more rigorous safety analysis techniques currently used in the nuclear industry (DBA, PSA, SAA)
  - –to improve visibility and understanding.

Office for Nuclear Regulation
An agency of HSE

Conclusions

Nuclear Fuel Cycle Facilities: 'high hazard'
Safety cases: rigorous, in-depth, complex

- Can reduce: visibility & understanding of key hazards and safety measures
- Bow-tie method:
  - successful in other 'Major Hazard' industries (oil & gas, chemicals)
  - could be introduced to the nuclear industry as an additional tool
    - diagrams readily accessible in the control room
    - provides purely "qualitative illustration"
    - improve visibility and understanding of the safety case
    - \+ role of operators in preventing major accidents and mitigating consequences
- Not a substitute, but a complement to the more rigorous safety analysis techniques currently used in the nuclear industry
- Purpose of presentation: awareness - a tool amongst others in the tool box

Office for Nuclear Regulation
An agency of HSE

Questions

Office for Nuclear Regulation
An agency of HSE