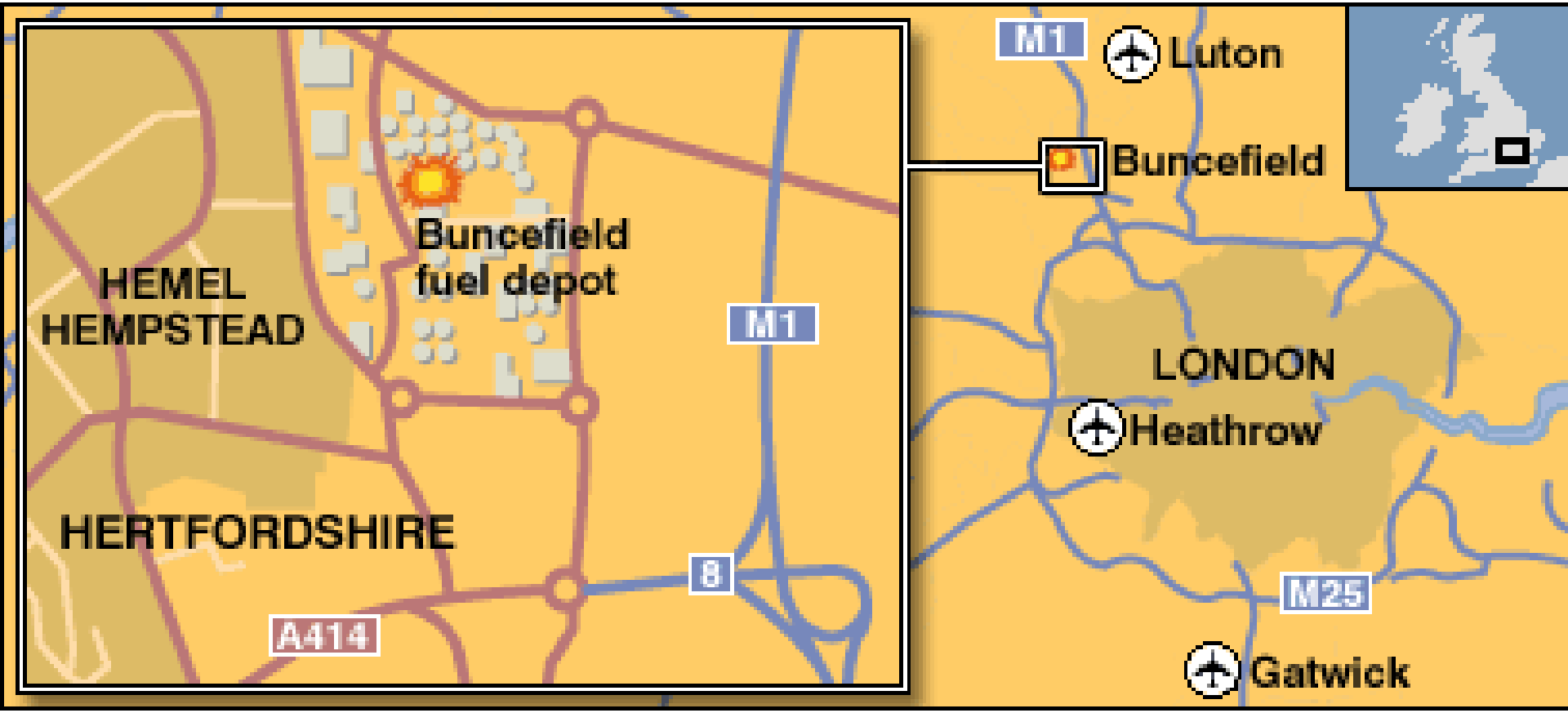
Layer of Protection Analysis – an aid to best practice for overfill protection of flammable liquid storage tanks.

Richard Gowland Technical Director EPSC

Timelines

- Layer of Protection Analysis emerged in late 1990s
- Aligned to IEC standard 61511 in early 2000s
  - Adopted by many companies and….
  - Some Competent Authorities as good practice
- My experience in Dow was as an implementer, practitioner and trainer in the method
- Institution of Chemical Engineers asked me to run a public training course ….then…

The Buncefield Fuel Storage facility

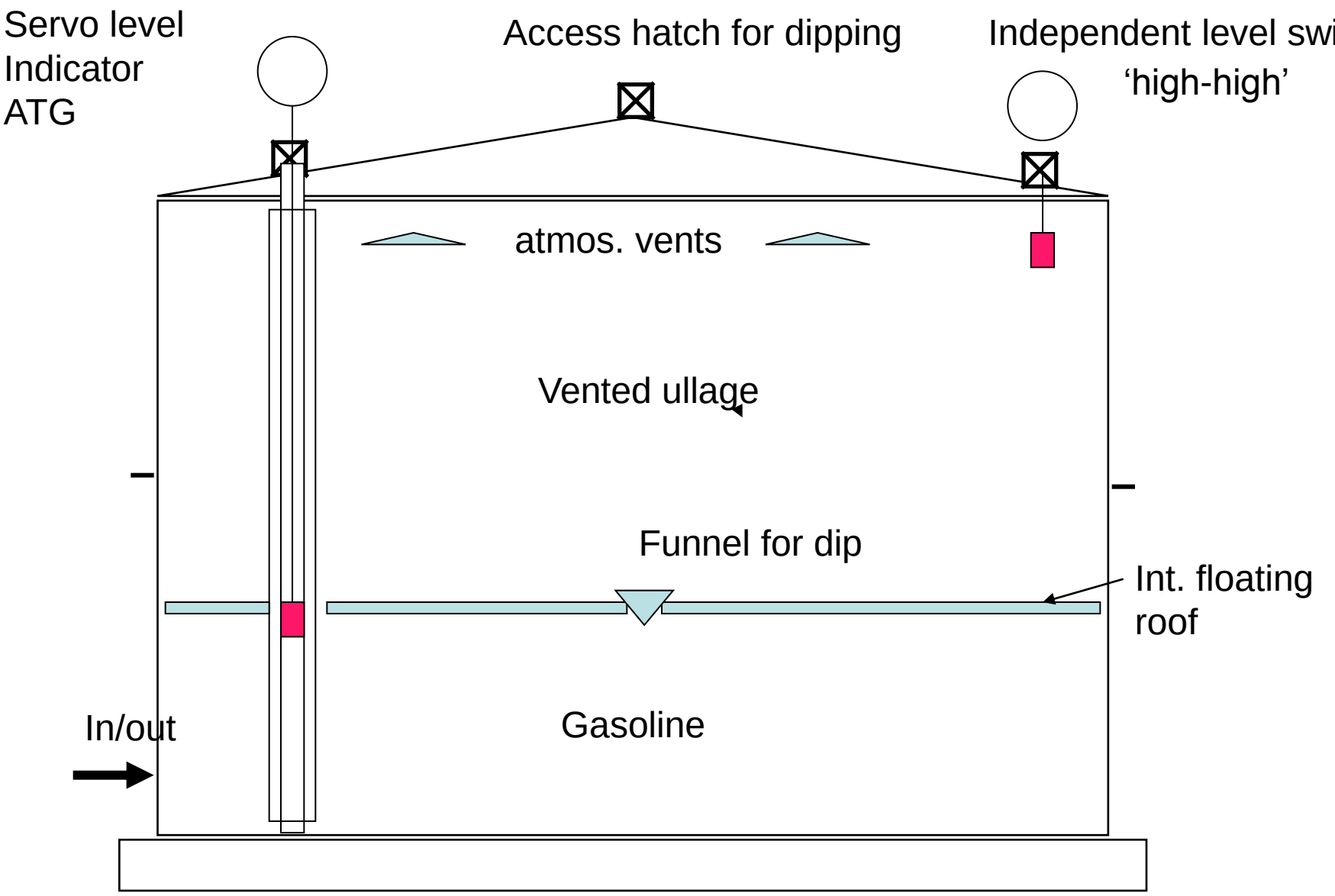


Fed by refinery pipelines from different locations.
Feeding users including Heathrow Airport via road
And distribution lines

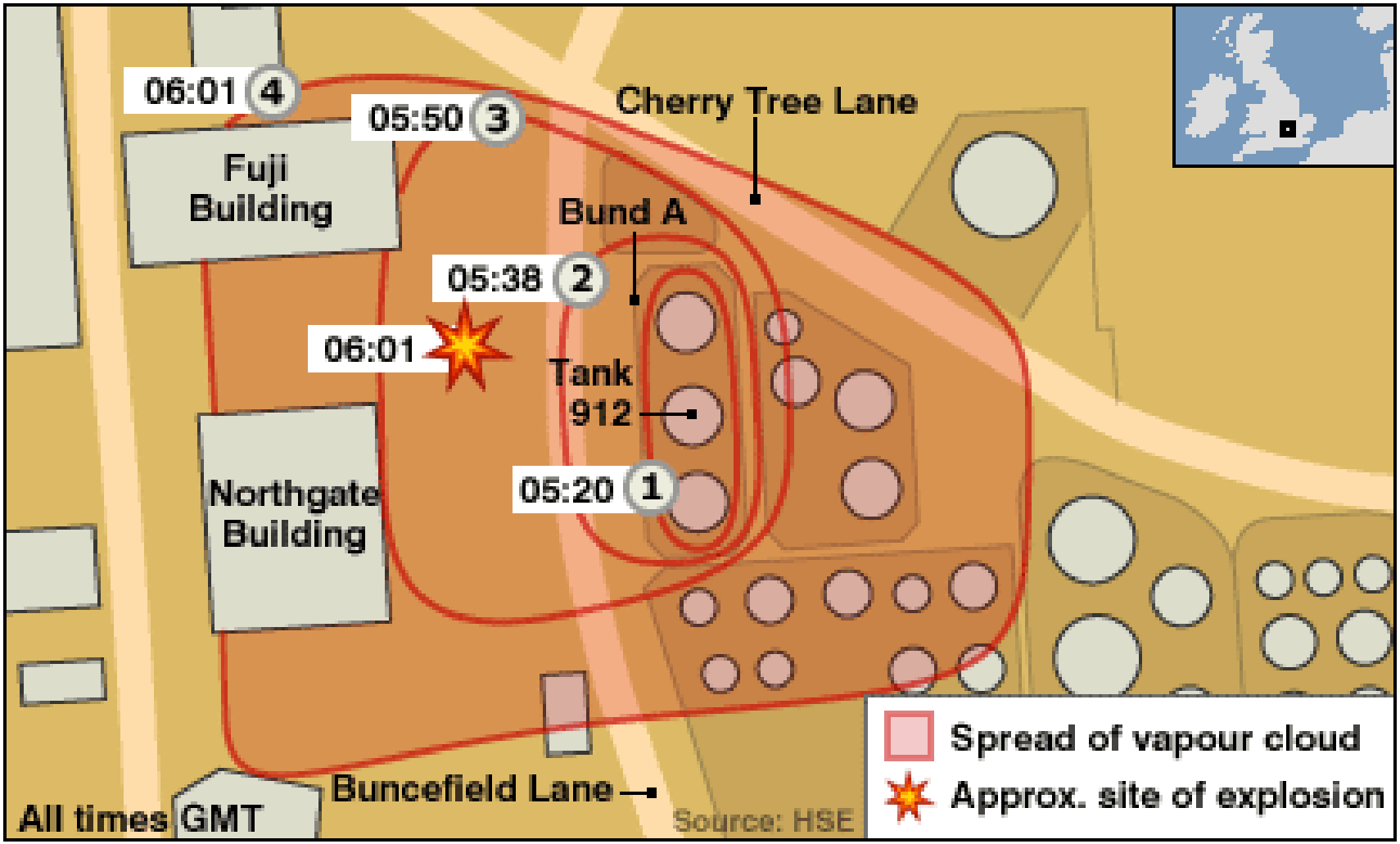
Disaster struck early in the morning of Sunday 11 December 2006 as unleaded motor fuel was being pumped into storage tank 912, in the north west corner of the site. Safeguards on the tank failed and none of the staff on duty realised its capacity had been reached.

By 0520 GMT, investigators believe, the tank was overflowing:

Overflow occurred at between 500 and 900 M3 for about 40 minutes


Servo level
Indicator
ATG
Access hatch for dipping
Independent level switch
'high-high'
atmos. vents
Vented ullage
Funnel for dip
Int. floating
roof
In/out
Gasoline

T912



1) Fuel cascaded down the tank and formed a rich fuel/air mix, which collected in dike A

2) CCTV footage showed vapour flowing out of dike A from 0538. The cloud was initially about 1m deep, but thickened to 2m.


11 12 2005 SUN
PLAY
Pause
11 12 2005
5:30:29 AM
1


11 12 2005 SUN
PLAY
Pause
11 12 2005
5:45:38 AM
1

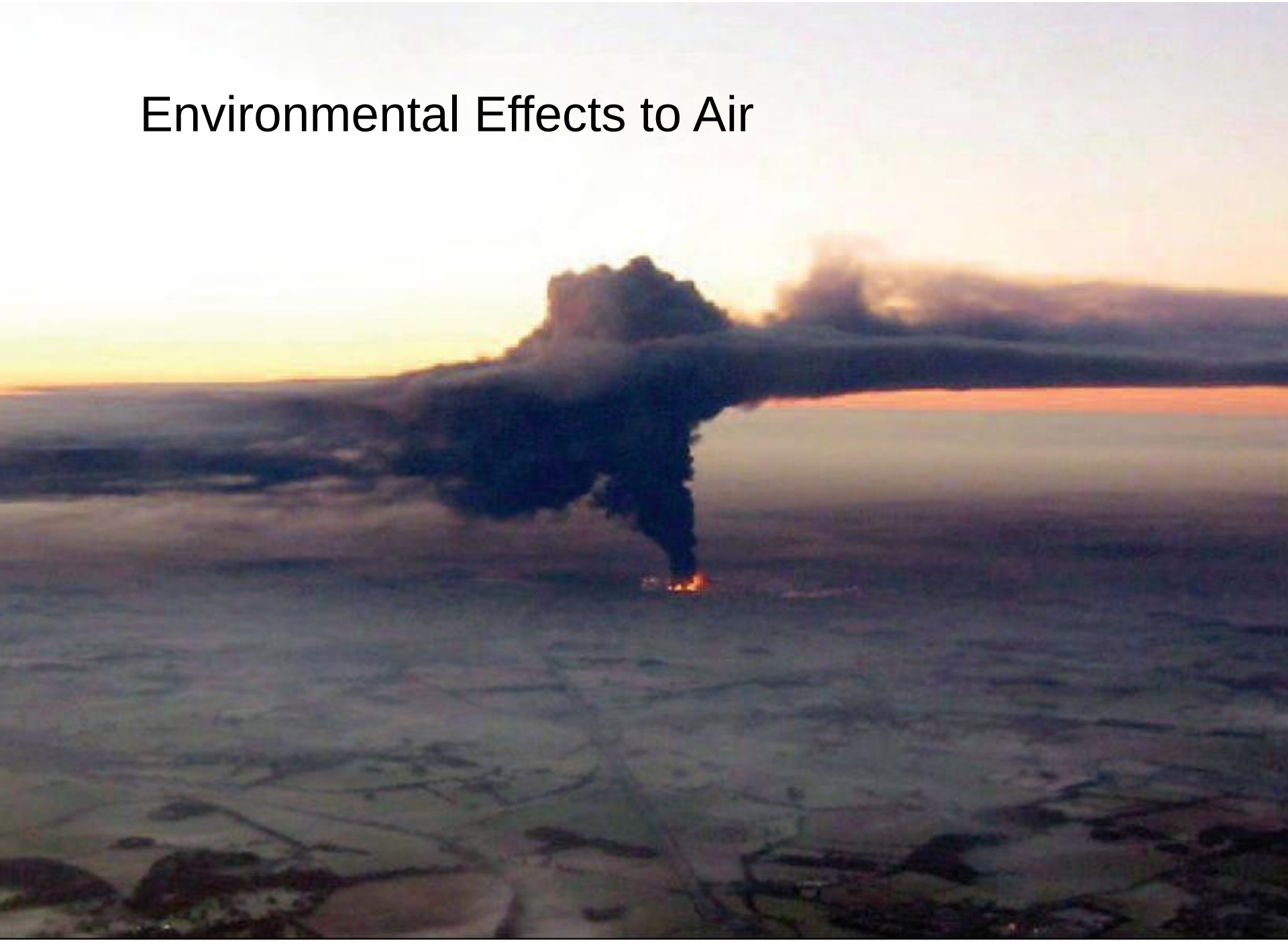

11 12 2005 SUN
PLAY
Pause
11 12 2005
5:53:43 AM
1


11 12 2005 SUN
PLAY
Pause
11 12 2005
5:36:00 AM
8
Tower 8


11 12 2005 SUN
PLAY
Pause
11 12 2005
5:51:00 AM
8
Tower 8

At 0601, with the vapour cloud cloaked over a large area and reaching buildings next to the site, the first explosion occurred.

Environmental Effects to Air



Explosion overpressure effects on neighbour buildings – Safety implications!

Environmental effects to ground

Some key issues

- Seveso 2 top tier site
- Risks previously modelled on:
  - Smaller releases
  - less severe effects
  - Assumptions on causes and protective measures
- Approximately 30 other terminals in U.K. and many more in Europe
- Lessons need to be applied here and to other sectors of our industries and to…
- Emergency Response
- Land Use Planning

The first reports (2007/8) from the Major Incident Investigation Board

LOPA introduced as a means of overflow risk assessment

- 2008 report LOPA example produced an answer that:
  - Introduced a concept of a ‘SIL 2 alarm’ and response
  - Suggested that LOPA could result in most installations avoiding the use of Safety Instrumented Systems (based on failure frequencies and Probability of Failure on demand of protective systems which are not allowed by the standard)
- There followed a technical challenge

Focusing on LOPA

- The Health and Safety Executive (HSE) as part of its regulatory duties requested 15 similar facilities to carry out LOPA (2007).
- The results showed inconsistency which caused concern for the regulator and for LOPA practitioners in the European Process Safety Centre (EPSC).
- Full report on errors and wild assumptions available from: www.hse.gov.uk/research/rrhtm/**rr716**.htm

Process Safety Leadership Group on LOPA

- EPSC (leader)
- Shell
- TOTAL
- P&I Design
- Petroplus
- INEOS
- Conoco Phillips
- U.K. Health and Safety Executive
- MHT Technology
- ABB
- SIMON Storage
- Environment

Final Report– Safety and Environmental Standards for Fuel Storage Sites - published 11 Dec 2009 (4th anniversary)
http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf

The final Report from the PSLG

- Part 1 Systematic assessment of safety integrity level requirements
- Part 2 Protecting against loss of primary containment using high integrity systems
- Part 3 Engineering against escalation of loss of primary containment
- Part 4 Engineering against loss of secondary and tertiary containment
- Part 5 Operating with high reliability organisations
- Part 6 Delivering high performance through culture and leadership

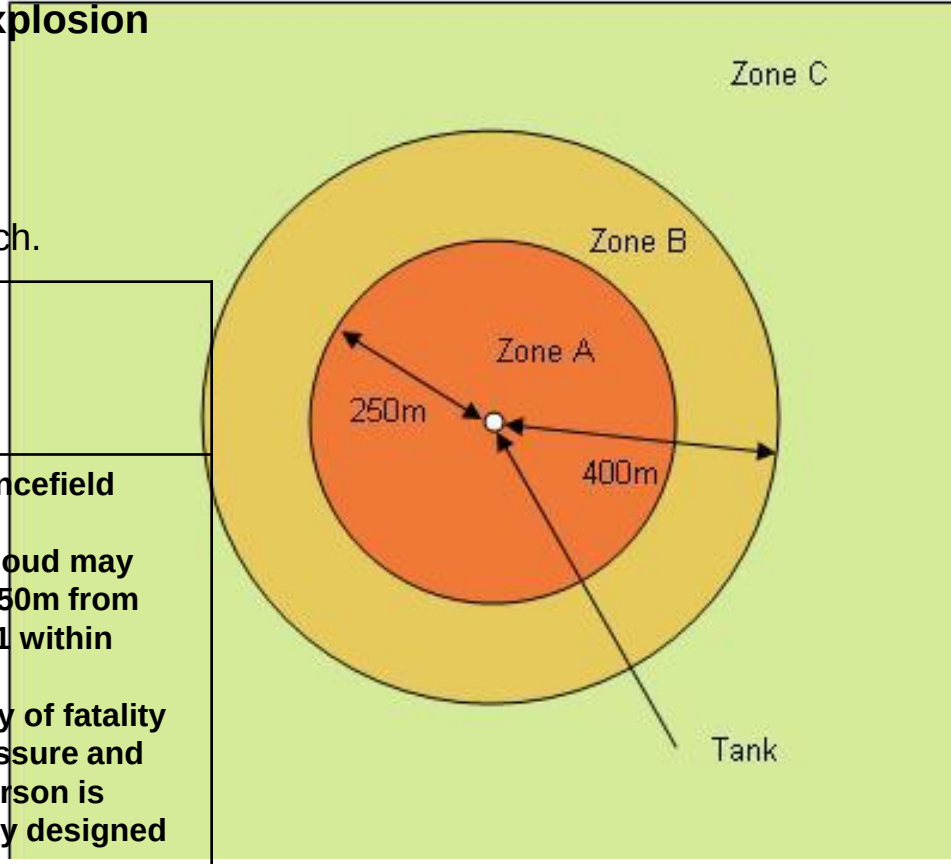
Results of the work

- What is in the Final Report
  - Annexes and Appendices are references to final report
  - IEC 61511 Rules!
  - This is Guidance only
  - We think it applies to more than just storage of gasoline.

Table 1: Hazardous Zones for a Buncefield-type explosion

Note: the distances are radii from the tank wall as this is the location of the overflow (see diagram below). Bund layouts can vary significantly, so measuring the distances from the bund wall would not provide a consistent approach.

Zone Name	Zone Size (measured from the tank wall)	Comment
A	**r < 250m**	**HSE research report RR718 on the Buncefield Explosion Mechanism indicates that overpressures within the flammable cloud may have exceeded 2 bar (200 kPa) up to 250m from the tank that overflowed (see Figure 11 within RR718). Therefore within Zone A the probability of fatality should be taken as 1.0 due to overpressure and thermal effects unless the exposed person is within a protective building specifically designed to withstand this kind of event.**
B	**250m < r < 400m**	**Within Zone B there is a low likelihood of fatality as the overpressure is assumed to decay rapidly at the edge of the cloud. The expected overpressures within Zone B are 5-25 kPa (see RR718 for further information on overpressures). Within Zone B occupants of buildings that are not designed for potential overpressures are more vulnerable than those in the open air.**
C	r > 400m	**Within Zone C the probability of fatality of a typical population can be assumed to be zero. The probability of fatality for members of a sensitive population can be assumed to be low.**



The HAZARD Zones for Buncefield type facilities

The steps in LOPA

A

1. Scenario definition
2. Assign severity and target frequency
3. Initiating events
4. Enabling events
5. Conditional Modifiers
6. Independent Layers of protection
7. Output result

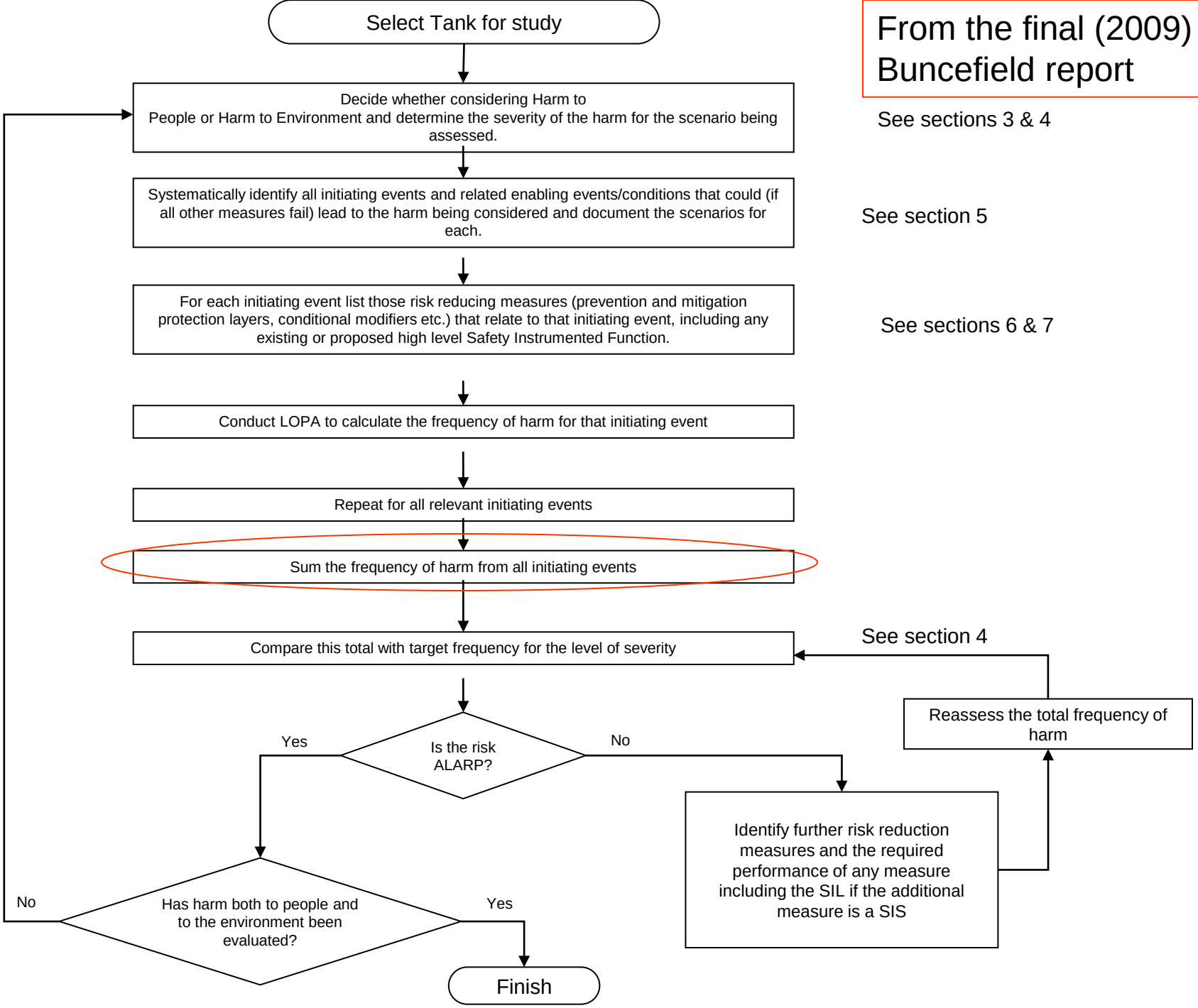
or

B

1. Scenario definition
2. Assign severity and target frequency
3. Initiating events
4. Enabling events
5. Independent Layers of protection
6. Conditional Modifiers
7. Output result

This is a choice where Conditional modifiers are used - may be left until last (B) or dealt with before IPLs (A).
Richard uses A because it seems ‘more honest’ - less temptation to massage CMs

From the final (2009) Buncefield report



See sections 3 & 4

See section 5

See sections 6 & 7

See section 4

Likelihood of 'n' fatalities from a tank explosion per tank per year	Risk Tolerability		
10^{-4}/yr - 10^{-5}/yr	Tolerable if ALARP	Tolerable if ALARP	Tolerable if ALARP
10^{-5}/yr - 10^{-6}/yr	Broadly acceptable	Tolerable if ALARP	Tolerable if ALARP
10^{-6}/yr - 10^{-7}/yr	Broadly acceptable	Broadly acceptable	Tolerable if ALARP
10^{-7}/yr - 10^{-8}/yr	Broadly acceptable	Broadly acceptable	Broadly acceptable
Fatalities (n)	**1**	**2-10**	**11-50**

Table 2 Risk matrix for scenario-based safety assessments

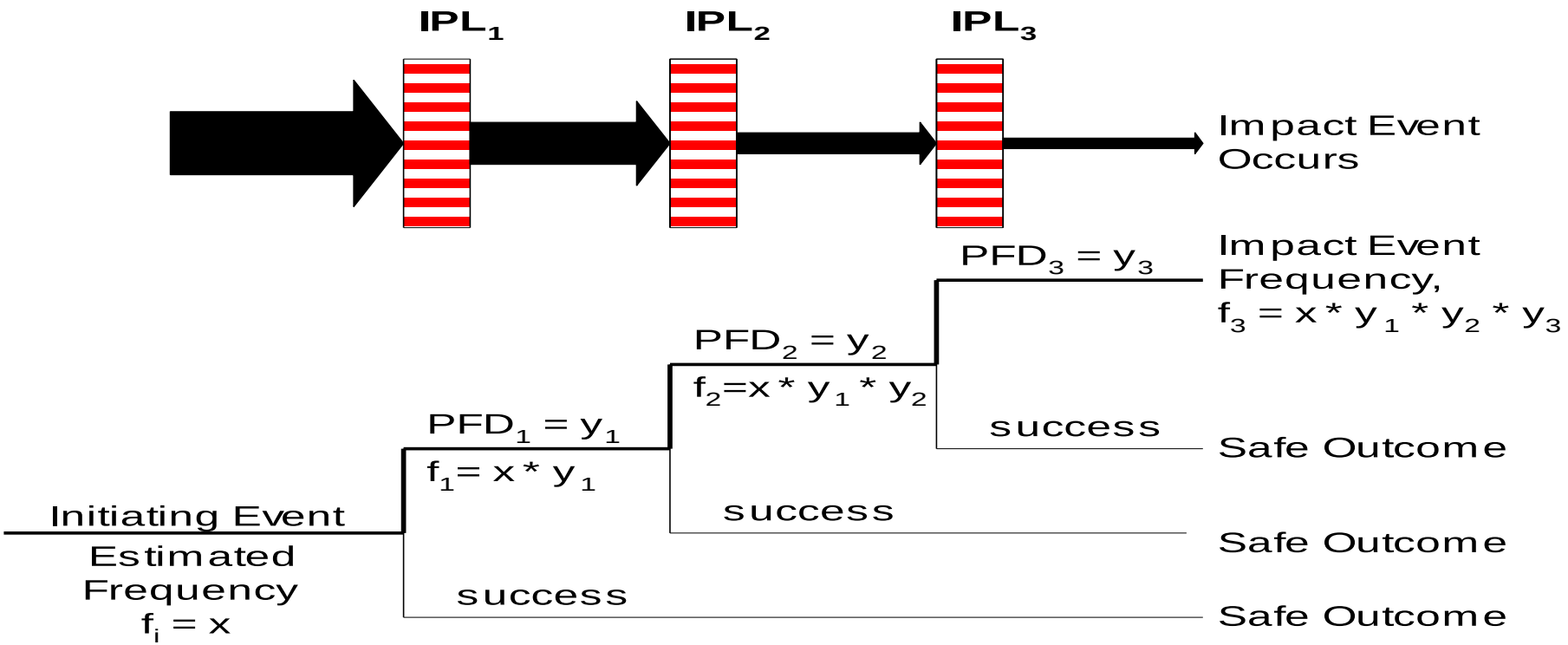
Extracted from the Buncefield Final Report

Environment

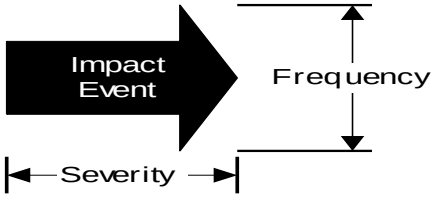
- U.K. Environment Agency was involved in the Buncefield PSLG final report and stated some target frequencies
  - Broadly Acceptable
  - Tolerable if ALARP

  But… these are now seen as obsolete
  - Negotiations have been gong on for 3 years and now Chemical and Downstream Oil Industries Forum (CDOIF) has issued guidance – available from Rtgowland@aol.com

Protection Layer Concept

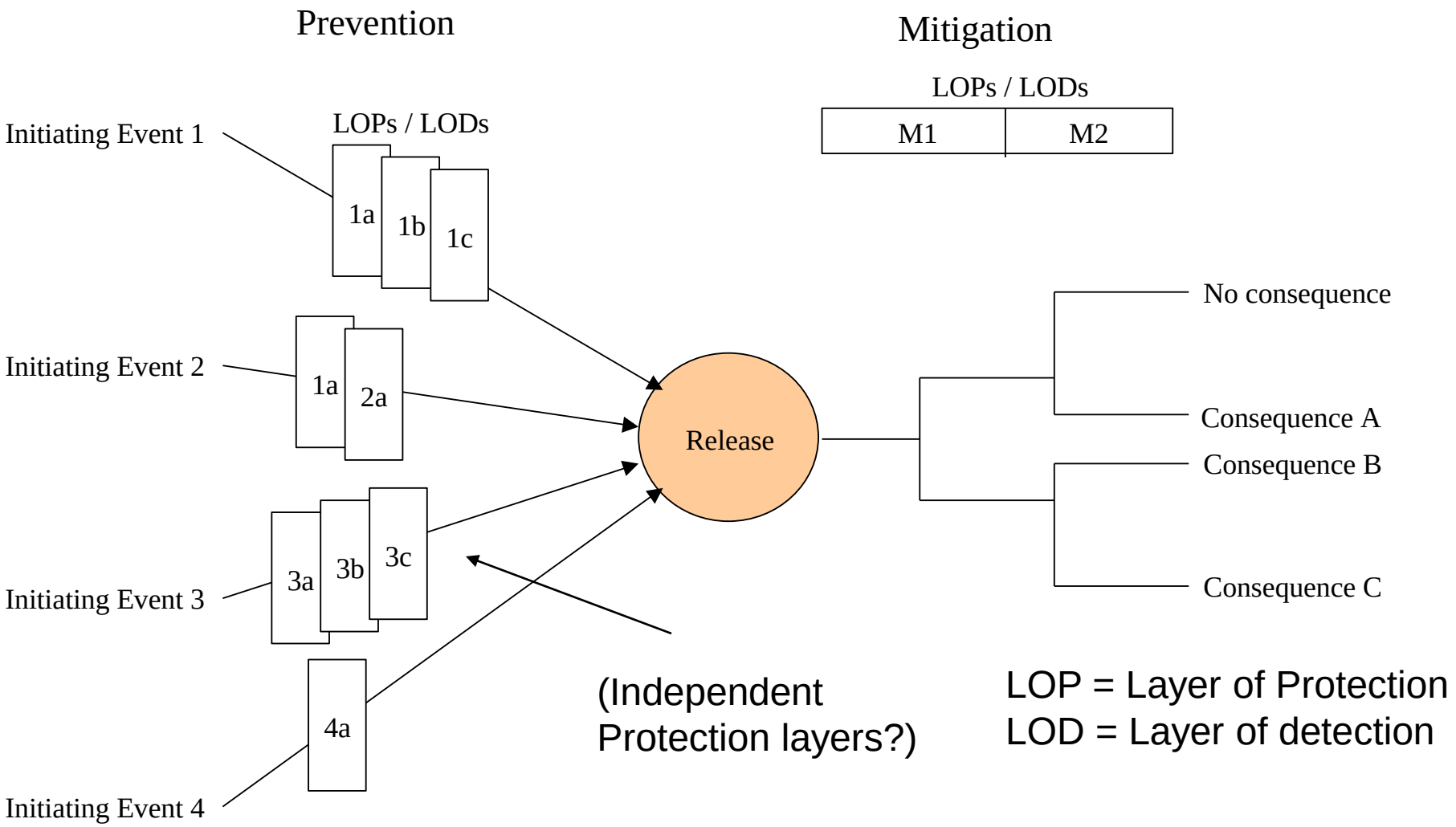


Key:
Arrow represents severity and frequency of the Impact Event if later IPLs are not successful



IPL - Independent Protection Layer
PFD - Probability of Failure on Demand
f - frequency, /yr

Applying LOPA – compatibility with…the ‘bow tie’ – yes it is compatible



Typical Initiating Events for tank overflow

- Failure of level measurement system:
  - (Buncefield Auto Tank Gauge ATG)
- Human Error:
  - Operator fails to observe level measurement
  - Wrong tank line up
  - Miscalculation of available space in receiving tank

Failure of level measurement system:

- Where the initiating event is caused by the failure of an item of equipment, the failure rate per year (in hours/year) may be derived from the failure-to-danger rate of the equipment item.
- Where the initiating event is taken to be the failure of a BPCS control loop (when it does not conform to BS EN 61511 as a SIS), the minimum frequency which can be claimed is 1E-05 dangerous failures per hour.

Human Error:

- Where the initiating event is caused by the failure of a person to carry out a task correctly and in a timely manner, the initiating event frequency is calculated as the product of the number of times the task is carried out in a year and the Human Error Probability (HEP) for the task. In this case, the time at risk is already included in the number of times the task is carried out in a year and no further factor should be applied.

Failures of the Basic Process Control System (BPCS) as initiating events

- The term “Basic Process Control Function” (BPCF) was developed to differentiate between the **functional** requirement for process control (what needs to be done) and the **delivery** of the functional requirement through the Basic Process Control System. The terminology is intentionally analogous to the terms “Safety Instrumented Function” and “Safety Instrumented System”.
- Although the definitions in IEC 61511 are not always explicit in this area, the sub - group considers that a BPCS can include either a fully automated control system or a system that relies on one or more people to carry out part of the BPCF. The BPCS is considered to comprise all the arrangements required to effect normal control of the working level in the storage tank, including operational controls, alarms through the BPCS and the associated operator response..

Enabling Events

- The number of tank-filling operations carried out in a year (which may change as commercial circumstances change); (avoid ‘double counting’)
- The proportion of tank fills which are carried out where the batch size is capable of causing the tank to overflow (it may be that the tank under review normally runs at a very low level and would not normally be able to be filled to the point of overflow by typical batch sizes);
- The tank operating mode (if the tank is on a fill-and-draw operating mode so that the level is more or less static);
- Role and effect of cross checks

Typical Conditional Modifiers (from Buncefield PSLG Final Report app.2)

- Probability of ignition
- Probability of calm and stable weather
- Probability of explosion after ignition
- Probability that a person is exposed in the hazard zone
- Probability that the exposed person will suffer the specified end result (e.g. fatality) – be careful

Protection Layers

A valid protection layer needs to be:

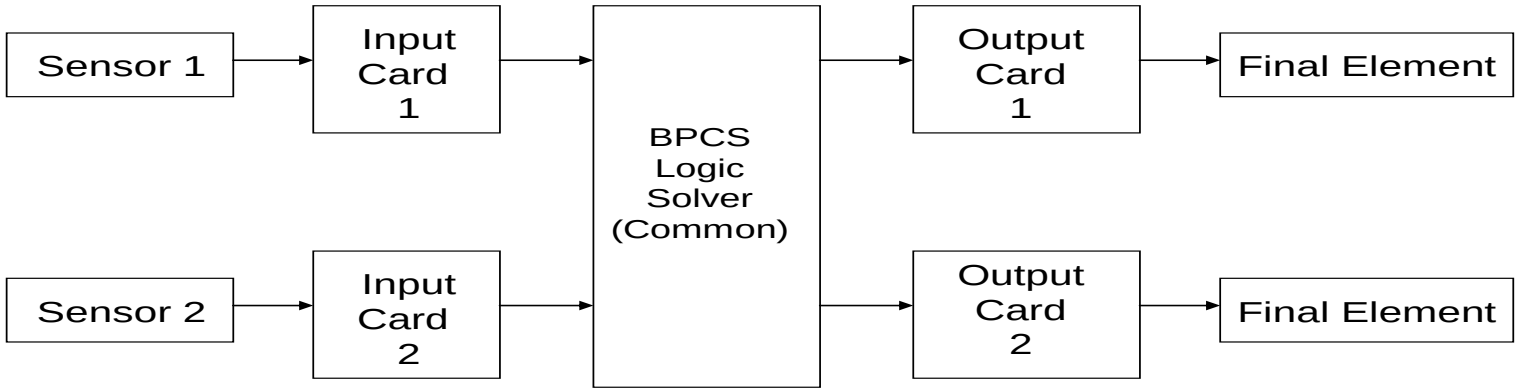
- effective in preventing the consequence; and
- independent of any other protection layer or initiating event; and
- auditable, which may include a requirement for a realistic functional test.

Protection Layers

- *The basic process control system as a protection layer*
  - It may be possible to take credit for the BPCS as a protection layer if sufficient independence can be demonstrated between the required functionality of the BPCS in the protection layer and any other protection layer and the initiating event.

Protection Layers

- ***The basic process control system as a protection layer***
  Claims for risk reduction achieved by the BPCS should meet the requirements of BS EN 61511-1 and 61511-2 (eg clauses 9.4, 9.5 and 11.2).
- Figure below illustrates what the application of these



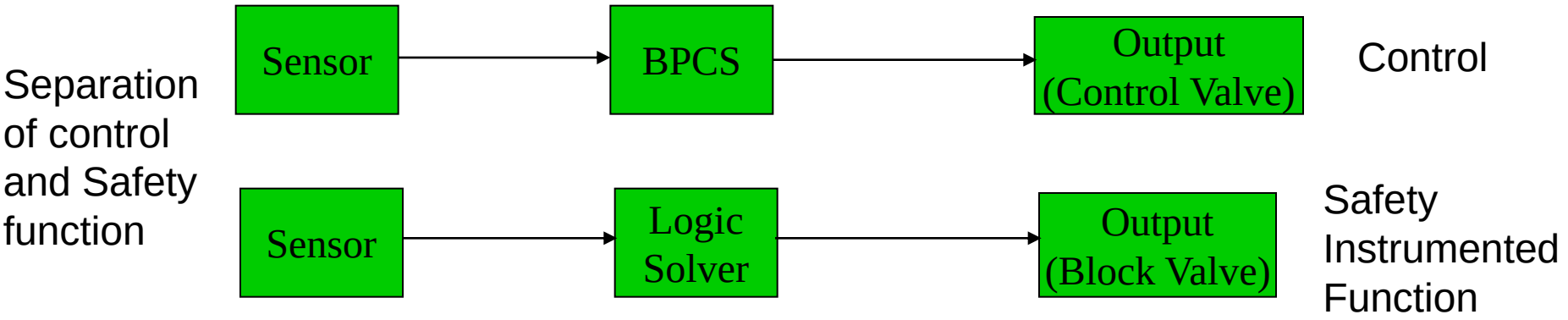
The role of the BPCS

- Question: If the BPCS acts as an independent layer of protection, what value (PFD) can it have?

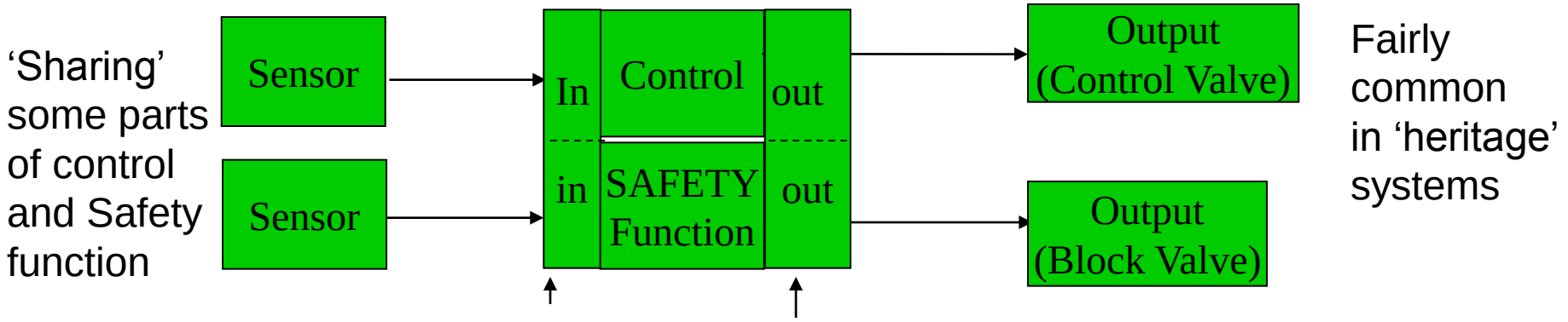
A) as an automated trip
   - refer to IEC 61511 9.4.2 (most interpret this to mean that the best PFD which can be claimed is 1E-01)

B) as an alarm … discussion follows

Conventional Control & Safety Systems designed to meet full independence in IEC61511



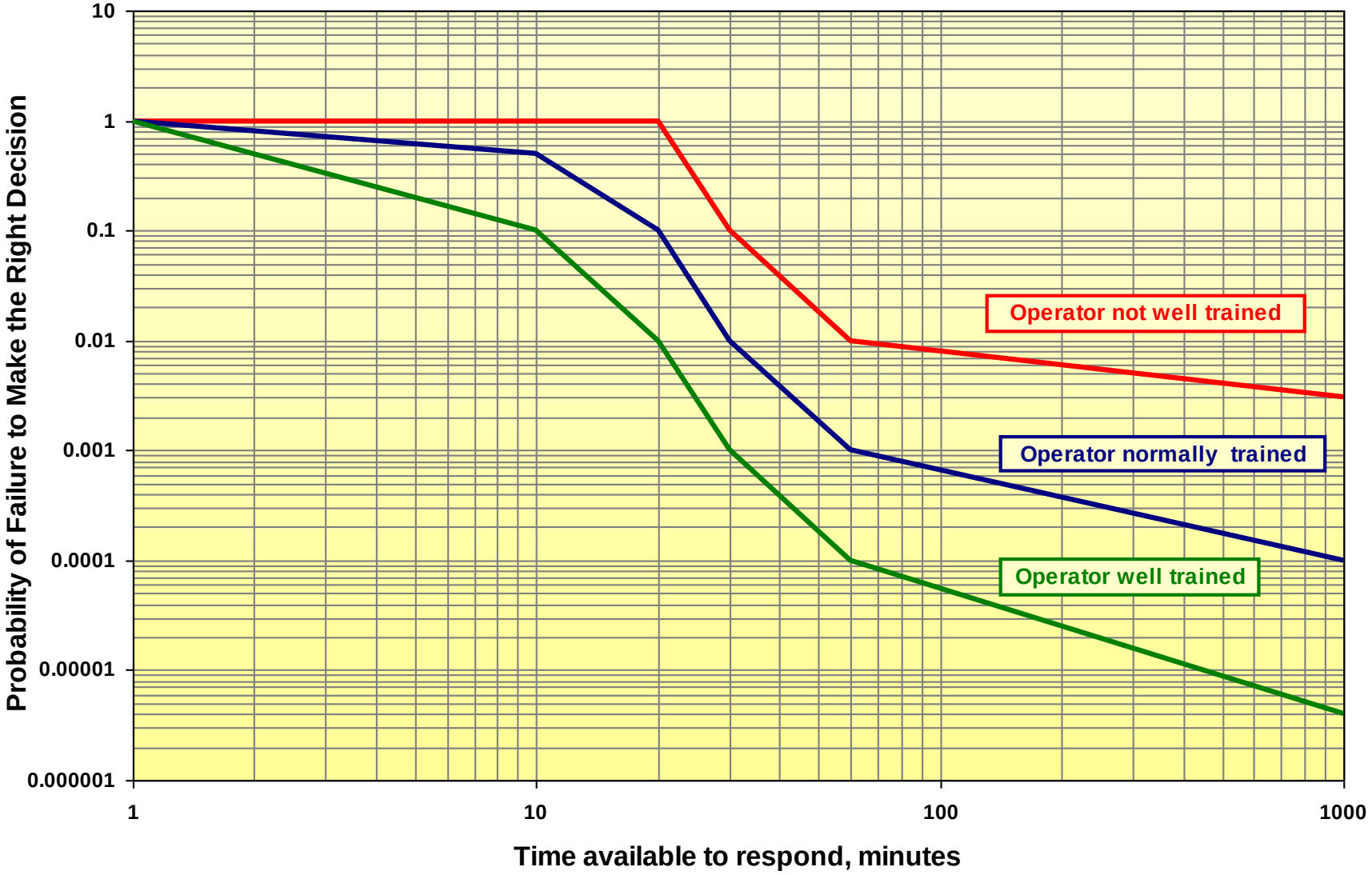
'Heritage' Control/Safety System in a BPCS



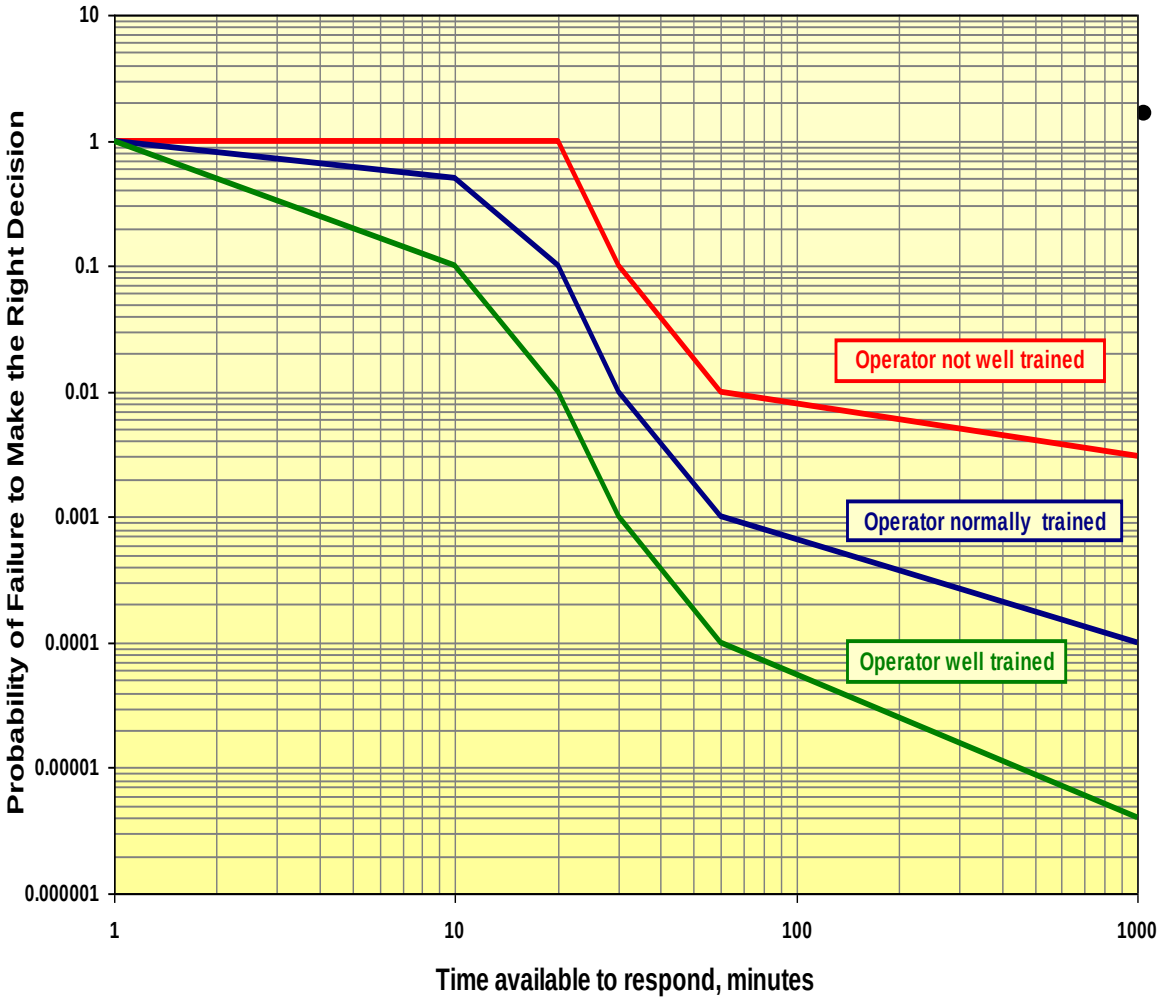
Alarms and Operator Intervention

- Must be independent of the BPCS if the BPCS already provides a trip (logic solver may be shared if it has proven reliability and separated channels)
- Different loops
- Different Power supplies (if UPS used for ‘active switching to safe state – mention this)
- Written procedure
- Accurate Fail Safe (power, signal etc) condition decided and implemented (look for it on P&ID)
- Operator must be trained
- Procedure must interrupt chain of events
- Operator must have time to respond
- Audited - tested - recorded

Operator Intervention – care needed – see PSLG Final Report App. 2



Take care



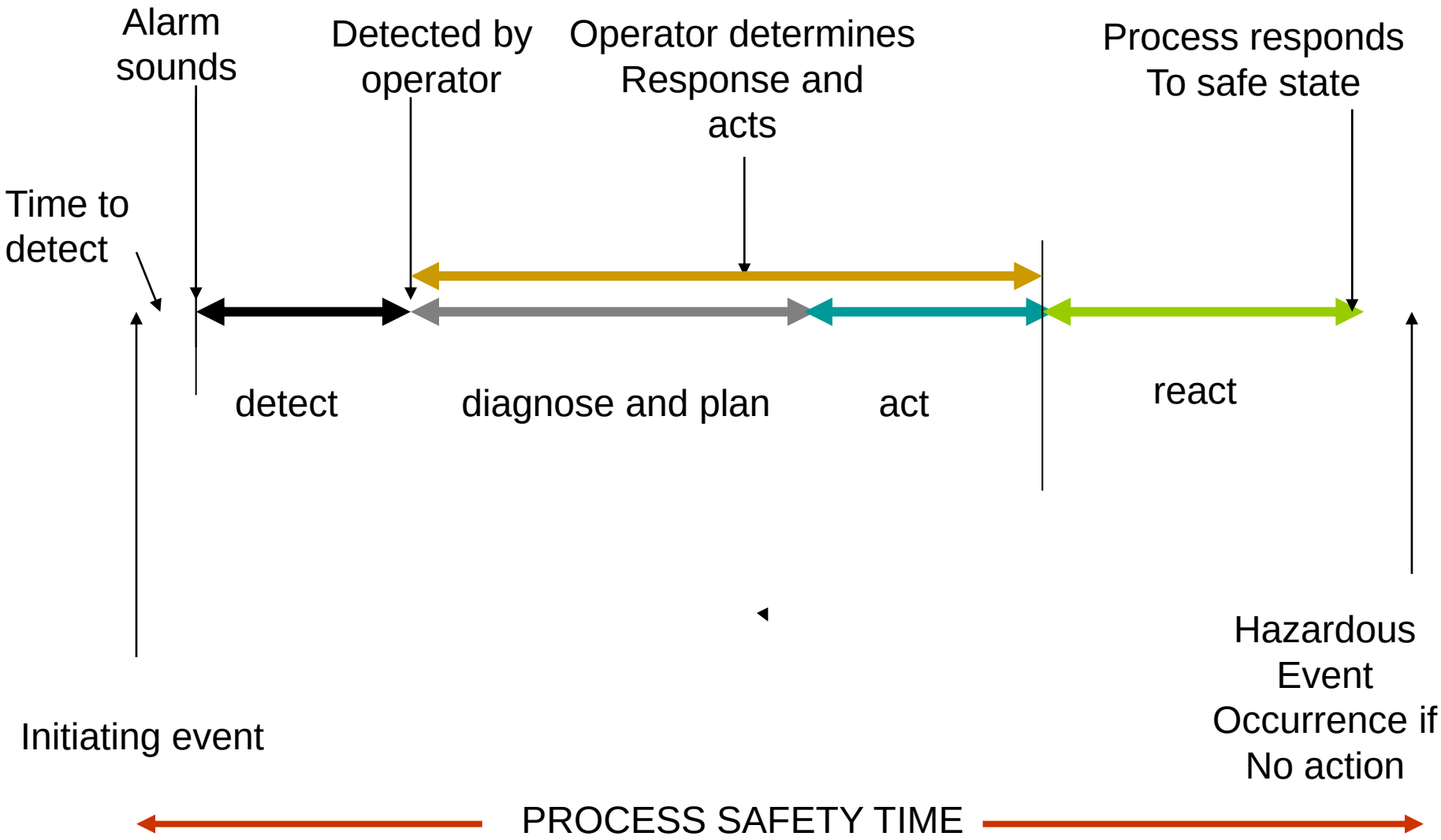
- The attached graph is from nuclear industry (Swain and Guttmann)
- The time scale is based on the time for the operator to be alerted, understand needed action and respond. The actual time you need to consider - for the complete protection to be effective may be longer – e.g. valve closing time may be a big factor

Recommendation – proper task analysis – look at EEMUA 191

Can an operator be part of a SIS?

- IEC 61511 says YES but does not specify how
- Recognising that most alarms come from the BPCS (non-SIS system, the limit for the PFD needs to be 1e-01) (some people talk about SIL2 alarms, but I don't believe it)
- If a SIS provides an alarm, the reliability of the operator is a weak link in the system Sensor-logic solver-final element and
  - Since the operator plays the role of Logic solver and (part) final element, it seems wise to assign an conservative PFD
  - Should be true for operator initiated ESDs

‘Process Safety Time’



Protection Layers

- *Safety instrumented systems*
- LOPA studies, the normal convention is that the need for SIS is determined when all other protection layers have been considered. If an existing SIS complies with IEC 61511 then a reliability performance consistent with the SIL-rating of the SIS and its design and operation can be claimed.
- If any ‘instrumented protection’ does not comply with IEC 61511 then a risk reduction factor of no greater than 10 can be claimed for it.

Mitigation – the right hand side of the bow tie….

- Can be:
  - Gas detectors
  - Fire Protection
  - Personal Protective Equipment
  - Secondary Containment
  - Emergency Plan
  - ……
- Usually appears on the right hand side of the ‘bow tie’
- Most LOPA (prevention) effort is on the left hand side of the ‘bow tie’

Mitigation

- Does not prevent the hazardous phenomenon at the centre of the ‘bow tie’

  Cannot be fully tested

  – E.g. fire protection is designed and tested to a standard based but there is a risk that it will not prevent the worst effect
- If effective, it does reduce the scale and severity of the scenario.

Example

- Occupied multi plant control room with up to 8 operators
- Adjacent reactor floor.
- Reactor containing Dimethyl Amine (Flammable/Toxic) and 2,4 – Dichlorophenoxyacetic acid - Exothermic reaction to Amine Salt
- Relief sizing not adequate for Fire exposure case (Exo. Runaway starts after 32 minutes exposure)
- Potential vessel rupture assumed to expose all 8 operators
- Is this credible?
- What is the mitigation effect of fire detection/protection and emergency evacuation?

Fire detection and response

- Automatic gas detection issues:
  - Where to place sensors?
  - How to determine response time?
    - Time of start of release
    - Time for vapour/gas to reach detector
    - Response time of automatic or manual response
      - Deluge , automatic block valves etc.etc.
    - Results in estimation of release quantity
  - Analysis of effect on scale of scenario – use in the case risk study e.g. Consequence severity in LOPA (day3)
  - Are these classed as Safety Instrumented Systems or Other Safety Related Protection Systems?

Where are we?

- We have addressed each of the aspects of LOPA to establish consensus among the group which includes industry, the regulator (Health and Safety Executive and Health and Safety Laboratory), consultants and human factors specialists about the rules we would apply. These have been tested in real life by the group to make sure that the methods and rules did result in sensible outcomes. This supports the guidance which will be completed by June 2009. – published December 2009

Now for a typical study

- Excel workbook run in ESRA session
  - Consideration of ALARP
  - Cost Benefit Analysis
  - Example only – uses optimistic statements on Probability of Ignition
- Ca be obtained from Rtgowland@aol.com

- Typical result for filling from pipeline we need SIL1 for pool fire cases and SIL 2 for VCE.
- Run down from refinery or fill from ships and tank cars gives less complex results

And the real world at Buncefield!

- Tank level measurement failed 14 times in 4 months
- Operators brought in an alarm clock from home to tell when tanks were full
- Maintenance group did not understand the LSHH instrumentation operation mode
- Emergency stop switch on panel was not wired up
- Read on…..
  www.hse.gov.uk/comah/**buncefield/buncefield**-report.pdf
  - and ask control operators if these practices exist in your plant

Thank you