Safety regulation of new nuclear power stations built for private operators

What can we learn from the railways?

Electricity Policy Research Group
Winter Research Seminar 8-9 December 2005

Professor Roger Kemp FREng
Lancaster University

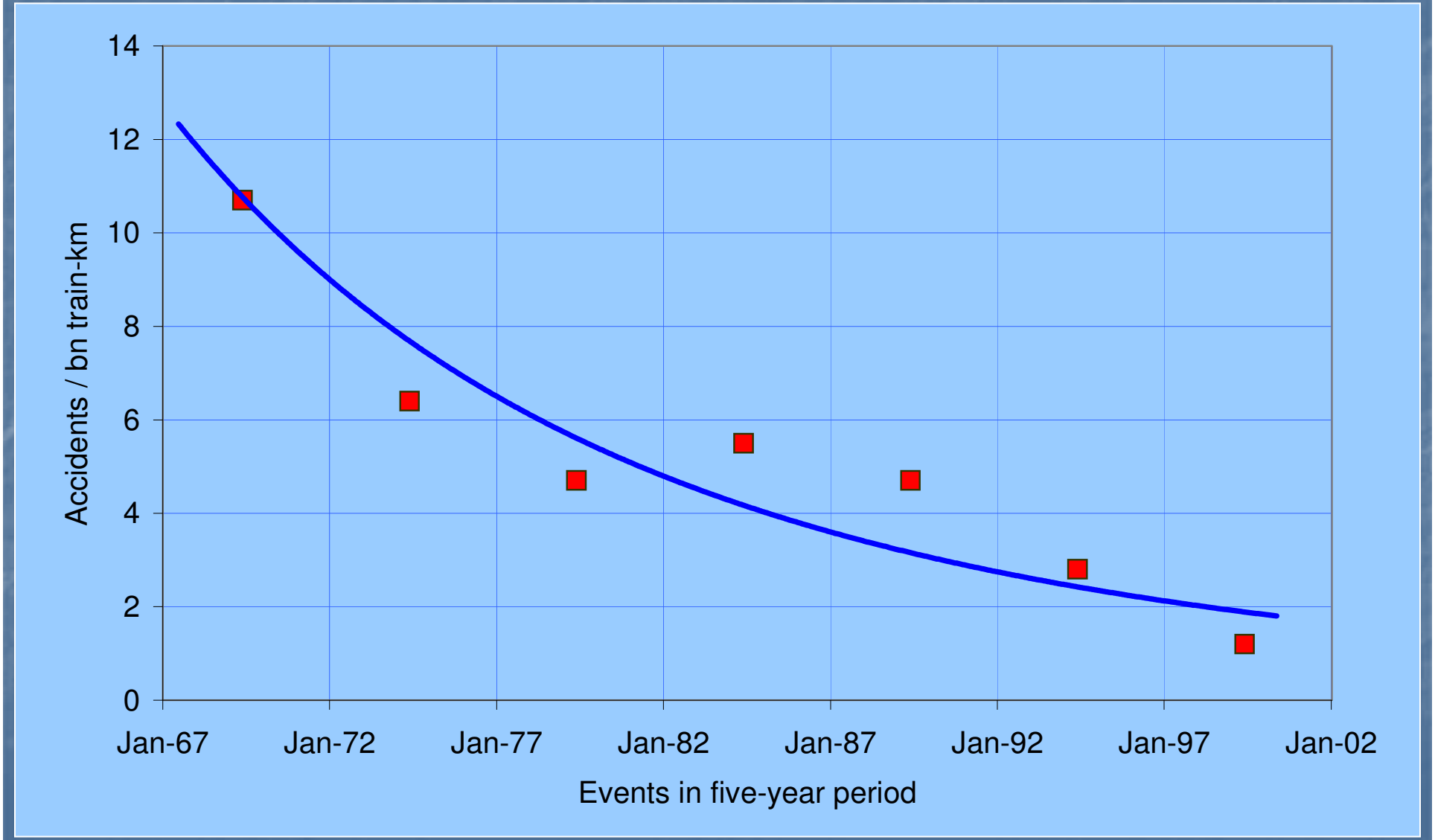
Nuclear new build

- This lecture does not attempt to justify the building of new nuclear power stations
- It discusses two questions:
  - How does the new structure of the industry change requirements for safety regulation?
  - Can we learn from the rail industry which went through a similar industry restructuring?

Safety regulation of the privatised rail industry

- Safety not compromised
  - Despite what one hears about Southall, Ladbroke Grove, Hatfield, Potters' Bar, etc.
- Regulatory burden increased by an order of magnitude
  - All industry players (except financial leasing companies) lost money
  - Overseas manufacturers badly hit and some left the UK market

Fatal train collisions, etc.



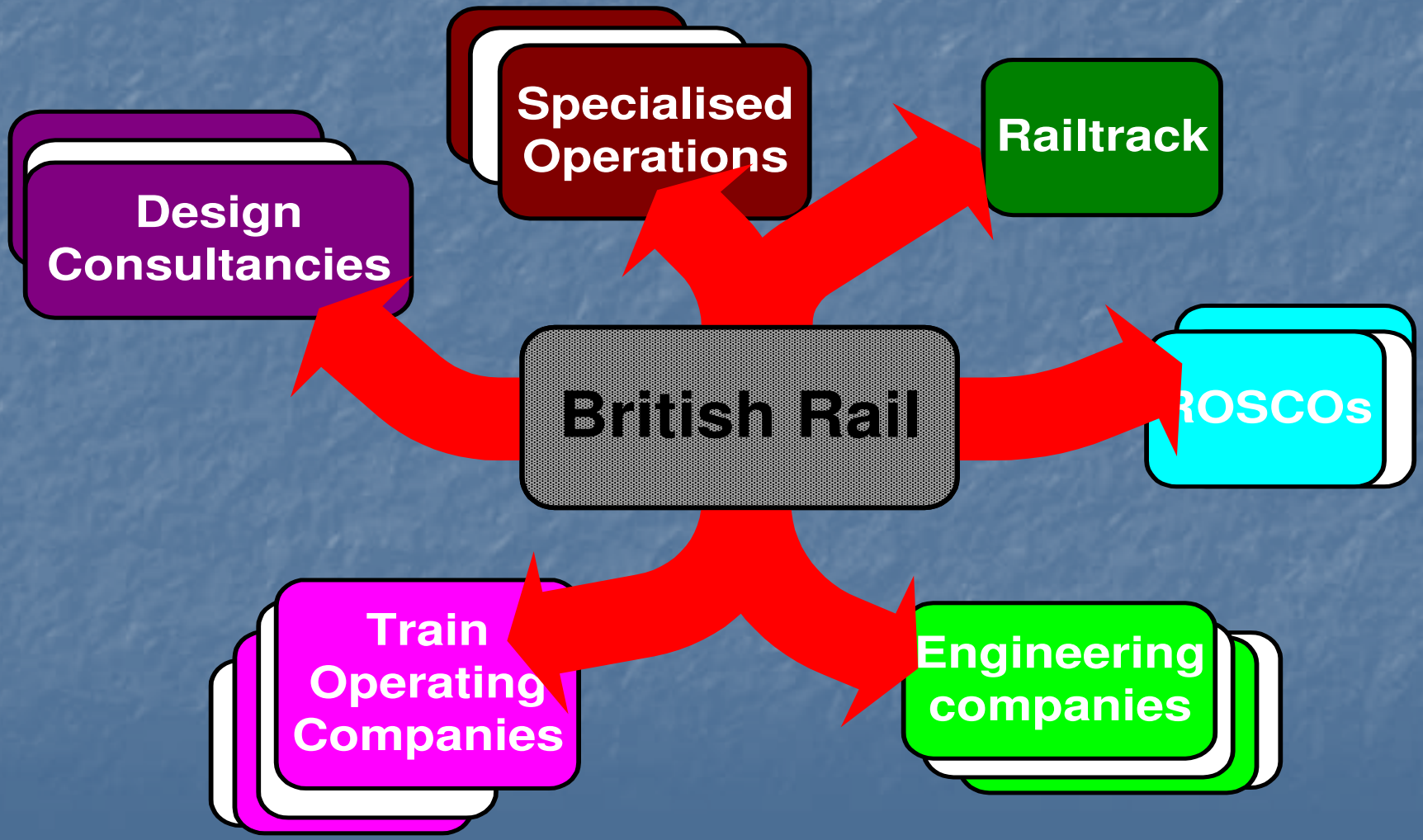
Source - Prof. Andrew Evans, Imperial College, March 2002

Structural changes in the industry

Structural change in nuclear generation and rail industries

- Past – monolithic state operator owning the design of the plant
  - CEGB or British Rail
- Future – several operators buying "proven" designs from overseas
  - Nuclear plant operators or Train Operating Companies (TOCs)

Impact of Privatisation



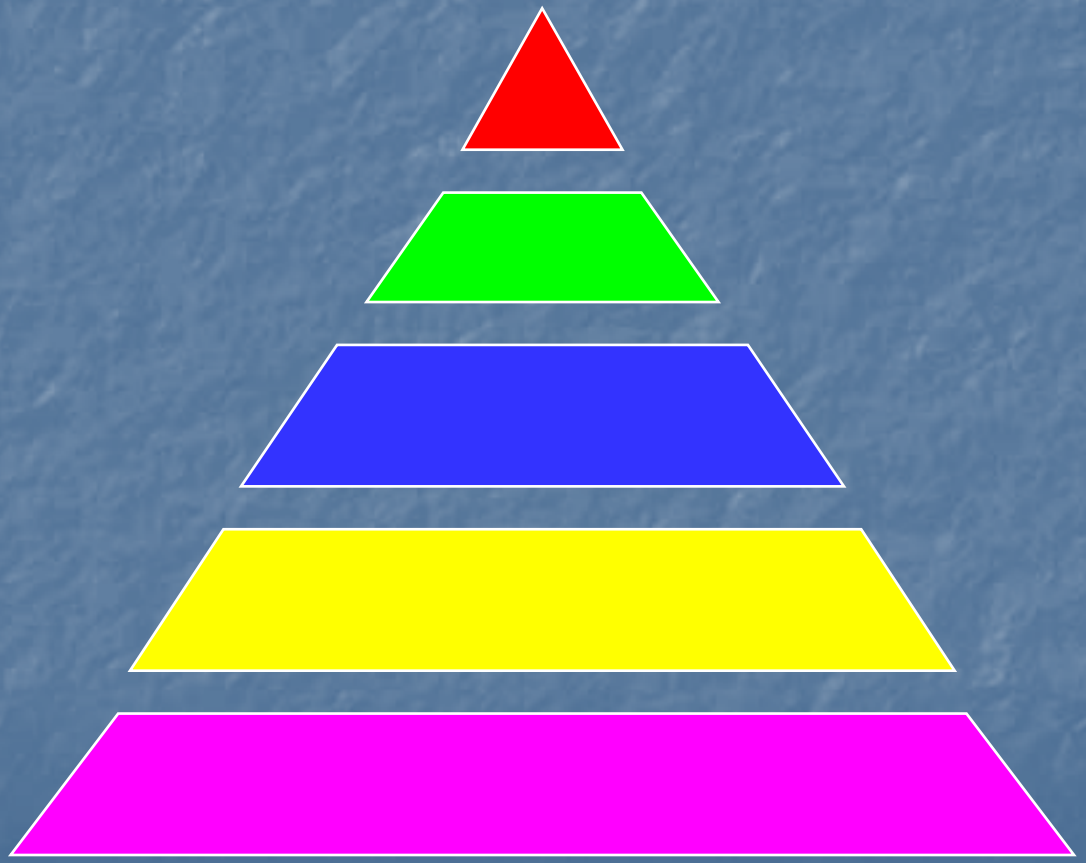
Parallels between Rail and Electricity Industries

- Before
  - British Rail
- After
  - Railtrack
  - Train operators
  - Overseas train builders
  - Consultancies

- Before
  - CEGB
- After
  - National Grid
  - Generators
  - Overseas power station builders
  - Consultancies

Design Authority

Specification Hierarchy



Business Specification

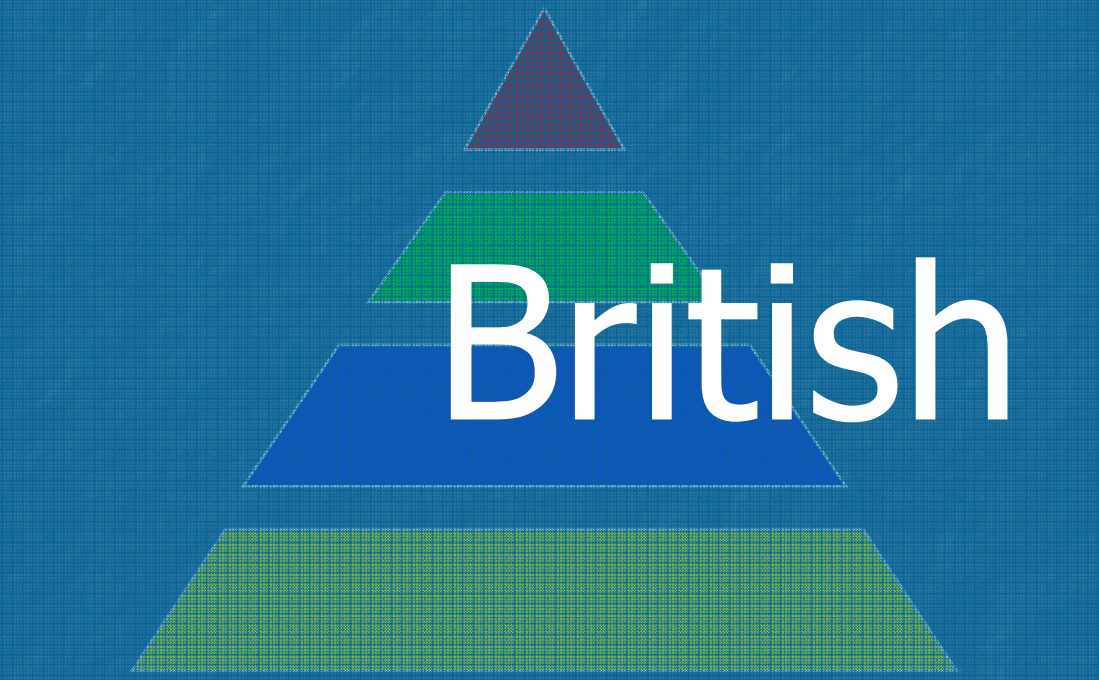
Functional Specifications

System Specifications

Detailed Requirements Specifications

Manufacturing drawings

Pre-privatisation



British Rail

Business Specification

Functional Specifications

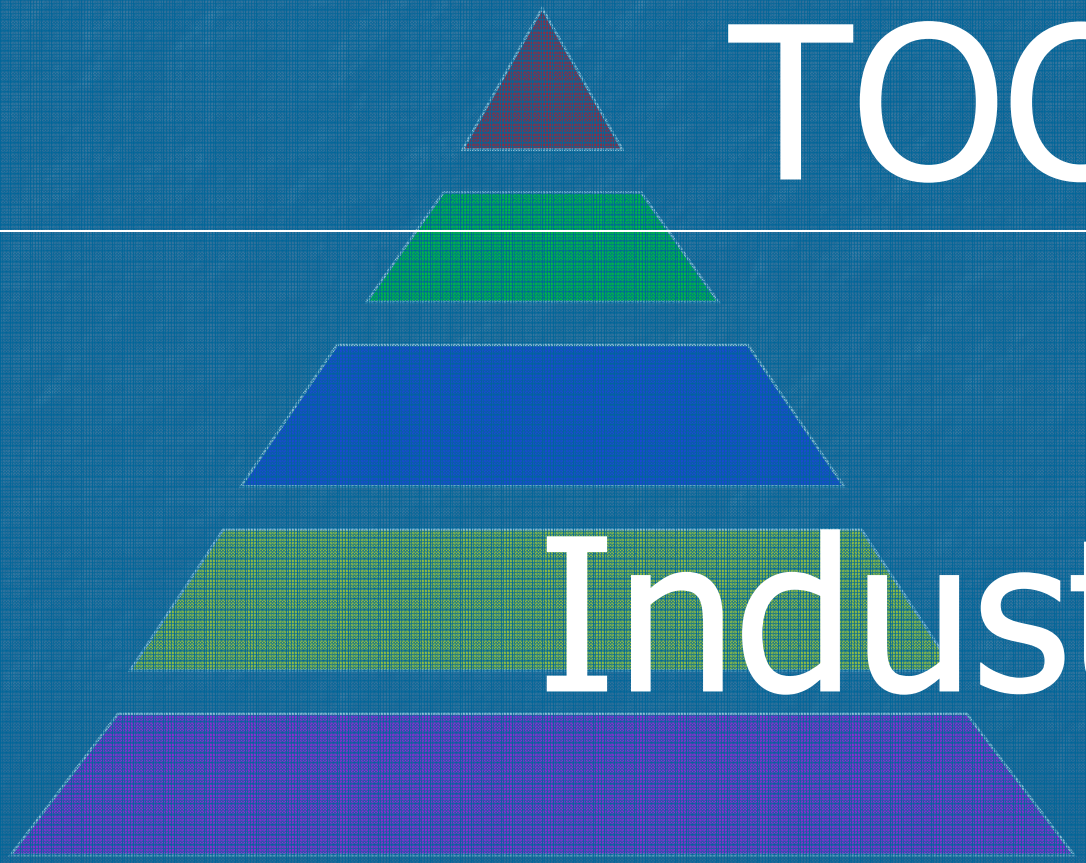
System Specifications

Detailed Requirements Specifications

Industry

Manufacturing drawings

Post-privatisation



TOC

Business Specification

Functional Specifications

System Specifications

Detailed Requirements Specifications

Manufacturing drawings

Industry

A Design Authority (DA)

- The DA for a system is the body that understands both the technical and operational requirements and the design of the system.
  - The "know why", not just the "know how"
- The DA has the authority, competence and responsibility for confirming that the system meets its technical requirements and is safe for use.
  - The DA "carries the can"
- The DA retains the design information so that, if 30 years after the plant enters service there is an accident, the original design calculations can be recalled.

A Design Authority (DA) contd.

- The DA may be called on to make an informed judgement on the suitability of the system for a particular application or to assess the technical, operational and safety implications of any proposed modifications to an existing system.

- The DA is responsible for establishing the configuration status of the design, for maintaining it throughout the product life and thus for confirming that any particular modification is compatible, not only with the original design, but also with any subsequent approved modifications.

Two options for Design Authority

- The CDM* model (e.g. chemical plant or infrastructure)
  - Contractor produces a safety file including all relevant calculations, drawings, etc.
  - Owner retains the safety file and gives it to anyone contracted to make changes to the plant
- The OEM* model (e.g. road vehicles & aircraft)
  - Manufacturer retains the design information, monitors safety performance, issues safety bulletins, recall notices, etc. as necessary
  - Manufacturer approves any significant post-delivery modifications to the equipment
  - Manufacturer retains configuration information

•The Construction (Design and Management) Regulations 1994
•Original Equipment Manufacturer

Design Authority in the nuclear and rail industries

- Traditionally in the UK both follow the CDM model
- The CDM model failed the rail industry when several different operators bought similar trains
- Directive 96/48/EC envisages moving the European rail industry to the OEM model
- If several different operators are planning to use the same design of reactor, which is the more appropriate for the nuclear industry?

Design Authorities – who pays to retain information?

Safety regulation

Risk management policy

- Goal-setting philosophy
- Control of risks remains the responsibility of those who create them - not the legislator
- Legislation can withstand rapid technological advancement and societal change

Robens Committee 1972

- But the Robens committee specifically excluded transport operators and state enterprises

Victorian values

"Once a railway is opened the State now holds the company responsible to maintain it and to work the traffic in a manner compatible with public safety.

Any change that would relieve railway companies from the responsibilities which now rest upon them to provide for the safety of that traffic would be undesirable."

Royal Commission 1884

Docklands Light Railway

DLR safety certification

1.5 CERTIFICATION

With the qualifications in section 1.4 above I certify that, to the best of my knowledge and belief, the Docklands Light Railway is safe for operation in passenger service.

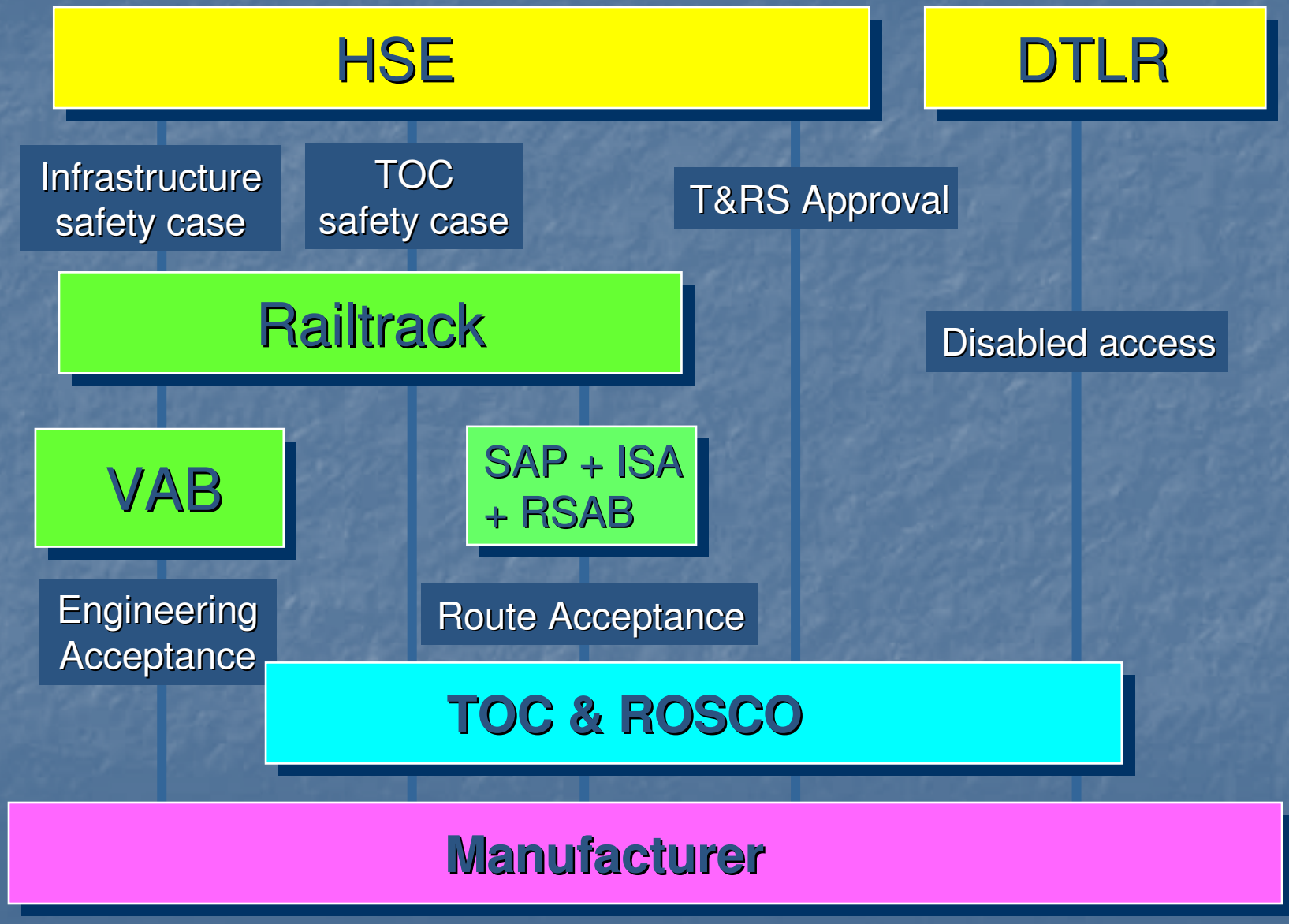
R J KEMP B.Sc. C.Eng. F.I.E.E.
ENGINEERING DIRECTOR,
GEC TRANSPORTATION PROJECTS LTD
RK0797

Mismatched safety responsibilities

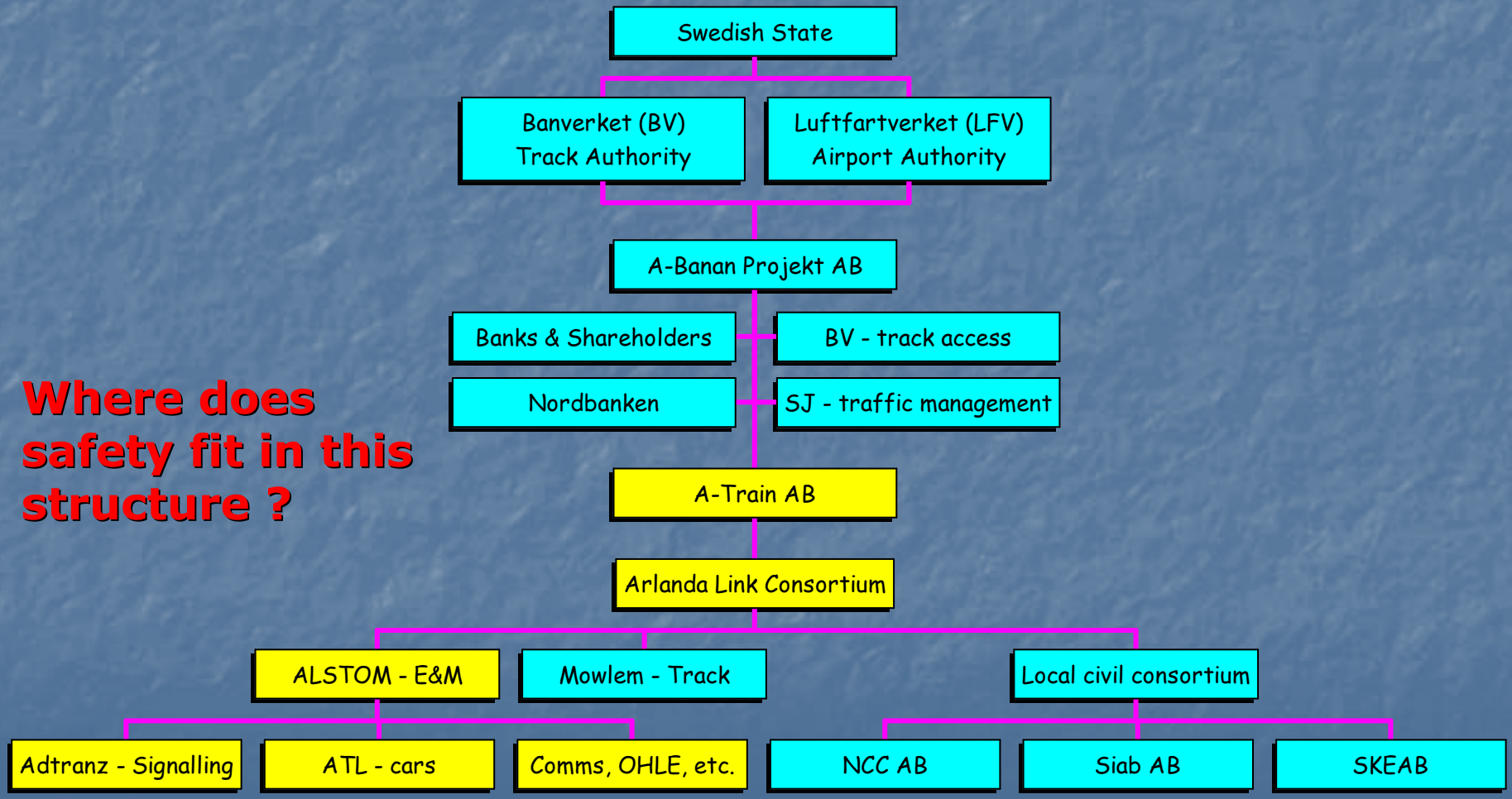
- Railways (Safety Case) Regulations 1994
  - Railtrack responsible for safety of the network
  - TOCs produced safety cases for train design and operation
  - TOC assumed to be an informed customer for the trains

It didn't work like this – the manufacturer was the only person to understand the product

Train approval structure (1994-2000)



Concession project (Arlanda)



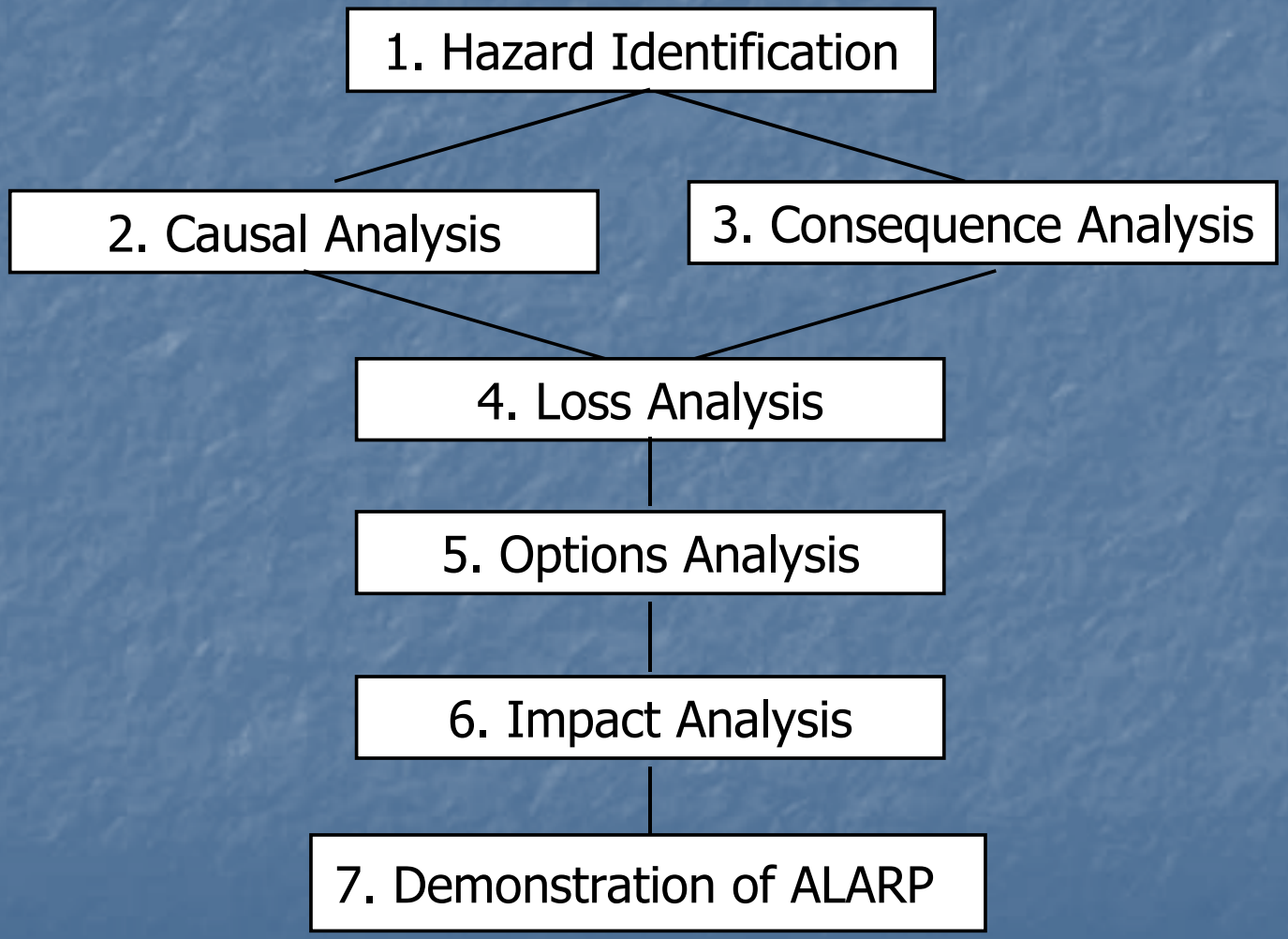
Where does safety fit in this structure ?

Power stations are more difficult than trains

- A nuclear power station is more complicated than even a very sophisticated train.
- An incident in a power station has much greater repercussions than a train crash – hence greater regulatory attention.
- A power station is less self-contained than a train.
- There is less recent UK experience of building – and regulating – power stations than trains.
- There are factions in the population opposed to a nuclear new build and thus one can expect the regulator to take more notice of societal concern.

Demonstrating ALARP

The 7-step risk reduction process



Managing societal concern

The Guardian

How widely accepted is the concept of ALARP?

Absolutely safe!

Cordelia Gummer during the BSE crisis

How widely is ALARP accepted ?

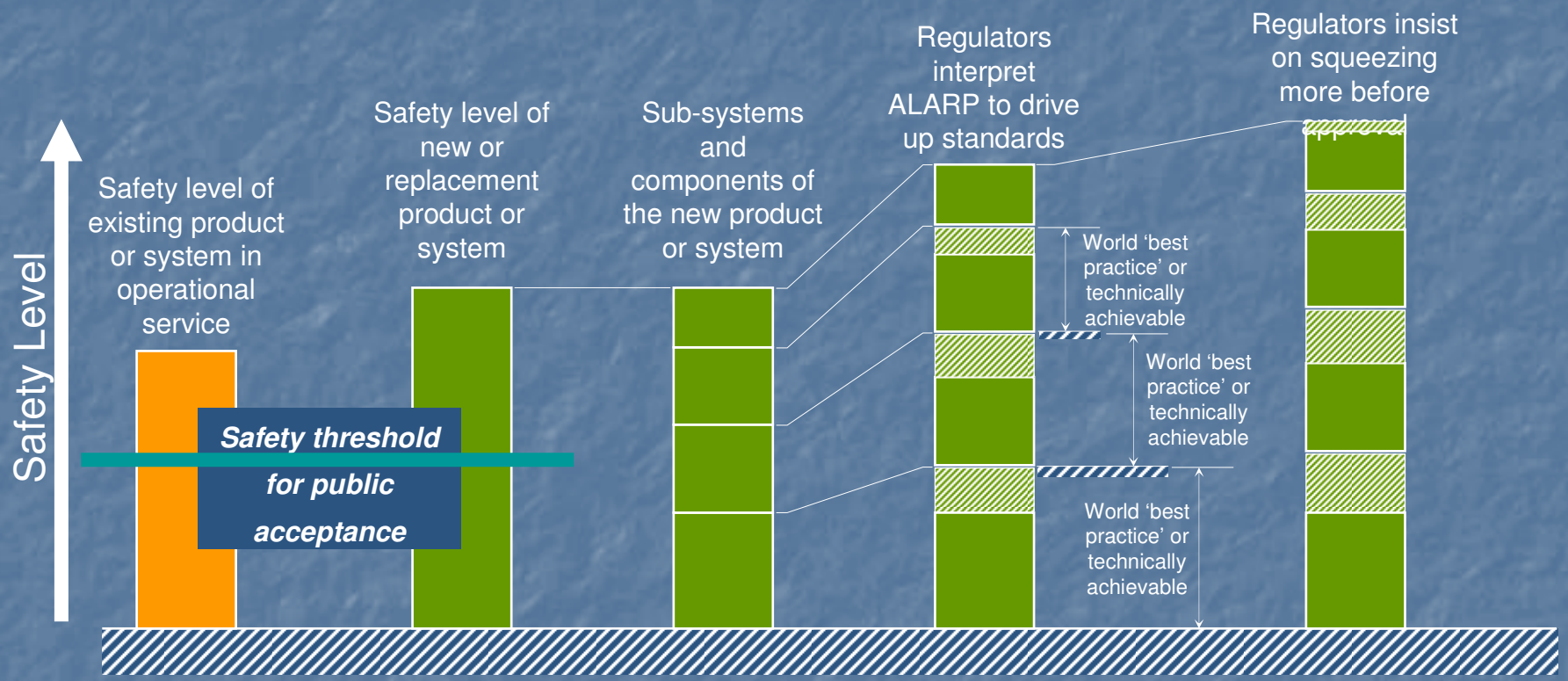
- France uses GAME (Globalement au moins équivalent)
- To most Southern Europeans the concept of ALARP is not accepted.

	ALARP	GAME
Reference system	☑	☑
Statistics & probability	☑	☒ ?
Consideration of costs	☑	☒
Value on "a life"	☑	☒

- The ALARP concept is not accepted by e.g. Louise Christian, the solicitor acting for the victims of Ladbroke Grove, Potters Bar, etc.

PA Consulting Group

Safety in UK's Railways – the vagaries of applying ALARP



Public and Government Response

COST DRIVERS and DELAY

'Agreed' level of safety between regulator and supplier / service provider at the start of the improvement work

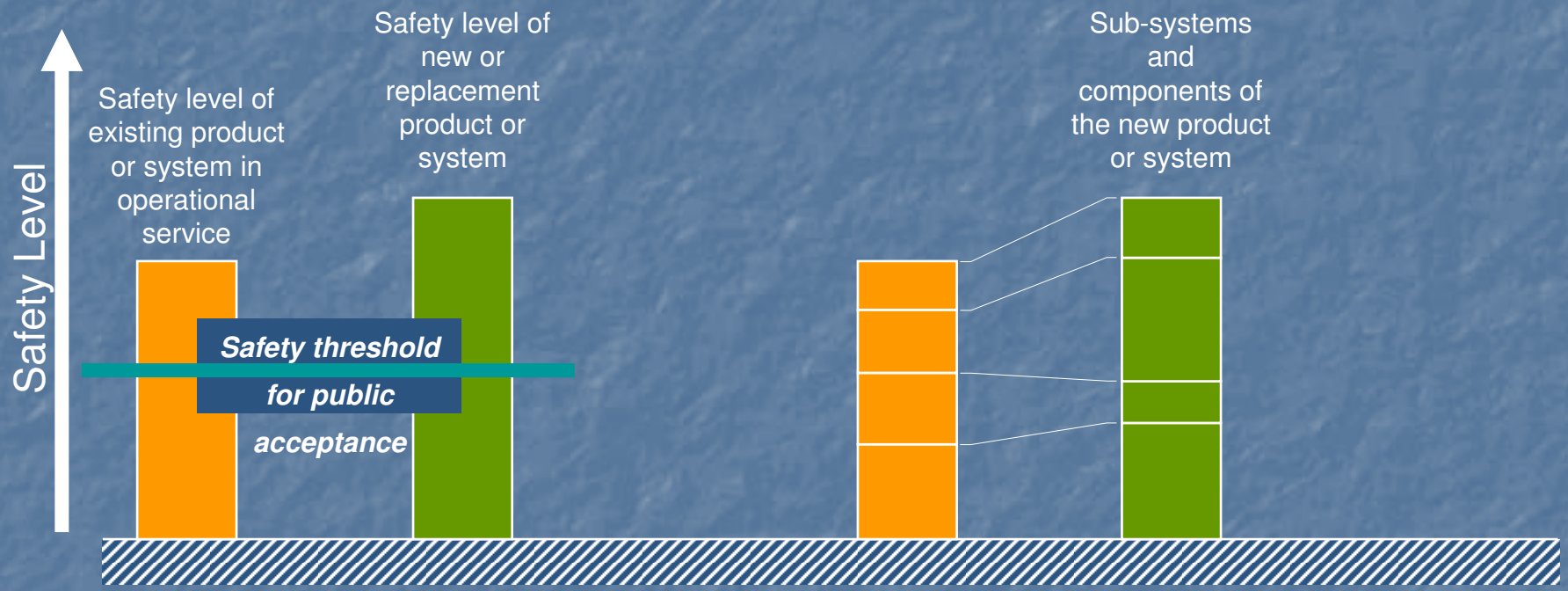
Unnecessary scope increase (Big)

Required level of safety before regulator is prepared to approve the new product or system for service

Major late scope change (Massive)

PA Consulting Group

The value of GAMAB is that there is a clear baseline that is not open for interpretation



Public and Government Response

Safety Case built on fixed indisputable baseline where new or replacement system is, in its totality, at least as good as the existing system

Fixed scope from start to finish

PA Consulting Group

The regulatory bodies apply the ALARP principle onerously, inflexibly and inconsistently

- The UK regulatory requirements place a huge burden on the industry:
  - By applying ALARP for each component of the system, and applying it at the time of commissioning, the overall effect is to add much more delay, cost and uncertainty than would result from a GAMAB approach applied at the overall system level and mainly at the design stage
  - ALARP is appropriate for improving safety performance that is near the intolerable level, but GAMAB is more appropriate where the risk is at least in the middle of the tolerable range, (as it is for rail)
- We don't achieve a balance between the workload and the available effort. We are chasing perfection at the expense of pragmatism

Are the concepts of ALARP and VPF accepted by the public?

'Arrogance and negligence'

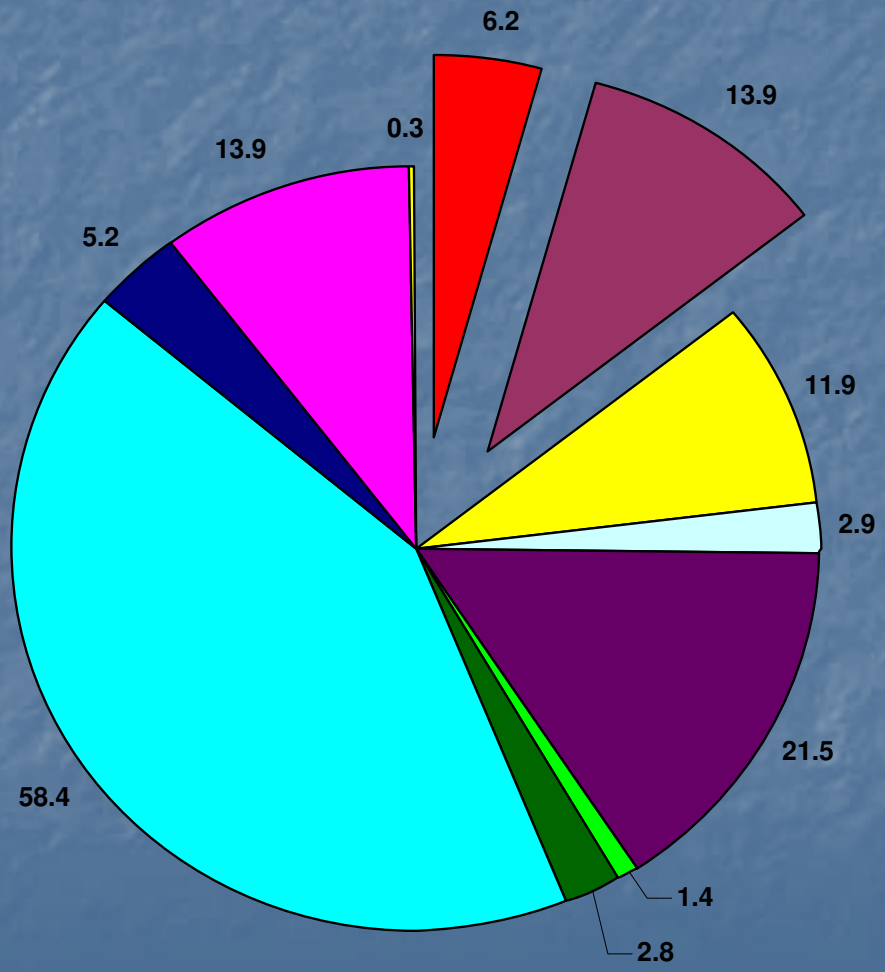
Mr Knox held up a poster featuring Mr Corbett with the words 'Wanted for serial killings on British railways'.

He said Mr Corbett should be prosecuted for arrogance, negligence and allegedly manslaughter.

BBC News Online

Railway risk (excluding suicides)

(equivalent fatalities)



The problem for the contractor

- How much work is involved in proving risks are ALARP for every sub-system?
- How do I demonstrate risks are ALARP for societal concerns where there is no quantifiable risk?
- Does societal concern allow the regulator to impose arbitrary regulations against scientifically implausible risks? If so, who pays?

The new European rail safety regime

- Objectives
  - Single European Railway
  - One specification for all suppliers
- Four Directives
  - High Speed Interoperability (implemented in UK in 2002)
  - Conventional Interoperability (implemented for freight 2003)
  - Safety (implementation 2005)
  - Amendment Directive (implementation 2005)
    - Brings HS in line with Conventional, extends geographical scope
    - Reduces the let-outs for not complying
- A new set of standards
  - TSIs for equipment
  - Common Safety Methods for organisations

Directive 96/48/EC

Interoperability of the trans-European high-speed rail system

- To ensure that high-speed trains can run freely across the European high-speed network and that railway products can be traded without restrictions.
- Implemented in the UK by the Railway (Interoperability) (High-speed) Regulations 2003.

Directive 96/48/EC

- Applies to the routes identified on the trans-European Transport Network (TEN) map as:
  - built for high-speed travel
  - upgraded for high-speed travel
- In the UK:
  - ECML, WCML, GWML and CTRL

    including connecting lines into stations

TSI compliance = ALARP (or does it?)

"Technical Specifications for Interoperability (TSIs) take precedence over all national legislation. In practice, this means that if there is any direct conflict between the requirements of the Health and Safety at Work Act etc 1974, (HSWA) to reduce risk to the lowest reasonably practicable level and the level of safety required by the TSI, the level of safety required by the TSI will be considered to meet the requirements of the HSWA. This is the case even if the level of safety imposed by the TSI is lower than that which had been previously applied under HSWA. Given that this is so, the level of safety imposed by the TSI must be considered to be the level which is 'as low as is reasonably practicable' where this is required under HSWA."

Simon d'Albertanson, Railway Sector Strategy Unit, HMRI, 26-07-02

Conclusions

Initial questions:

Can we learn from the rail industry which went through a similar industry restructuring?

How does the new structure of the industry change requirements for safety regulation?

Can we learn from the rail industry which went through a similar industry restructuring?

- The rail industry adopted many safety procedures from the civil nuclear industry.
- The procedures made little difference to the overall safety of the network, in comparison to the previous prescriptive regulations.
- Many suppliers lost money due to the regulatory burden and some got out of the UK market.
- The response to Hatfield led to the near collapse of the industry and the bankruptcy of Railtrack.

How does the new structure of the industry change requirements for safety regulation?

- Private sector constructors and banks will be looking for certainty of process. It is not possible to guarantee this under an ALARP regime including "societal concern".
- The presumption of an "informed client" acting as the design authority worked with a monolithic and technically expert CEGB. It is not appropriate in a situation where several operating companies buy a common design of equipment from an expert supplier.
- A new build will use a reactor design already approved for operation overseas. The regulatory structure must be able to cope with the transfer from a prescriptive regime without complete reapproval.