

# Regulating safety in a disaggregated private sector: a challenge for new build

Westminster Energy Forum  
UK Nuclear Regulation & Policy Conference

19th January 2006

Roger Kemp  
Lancaster University

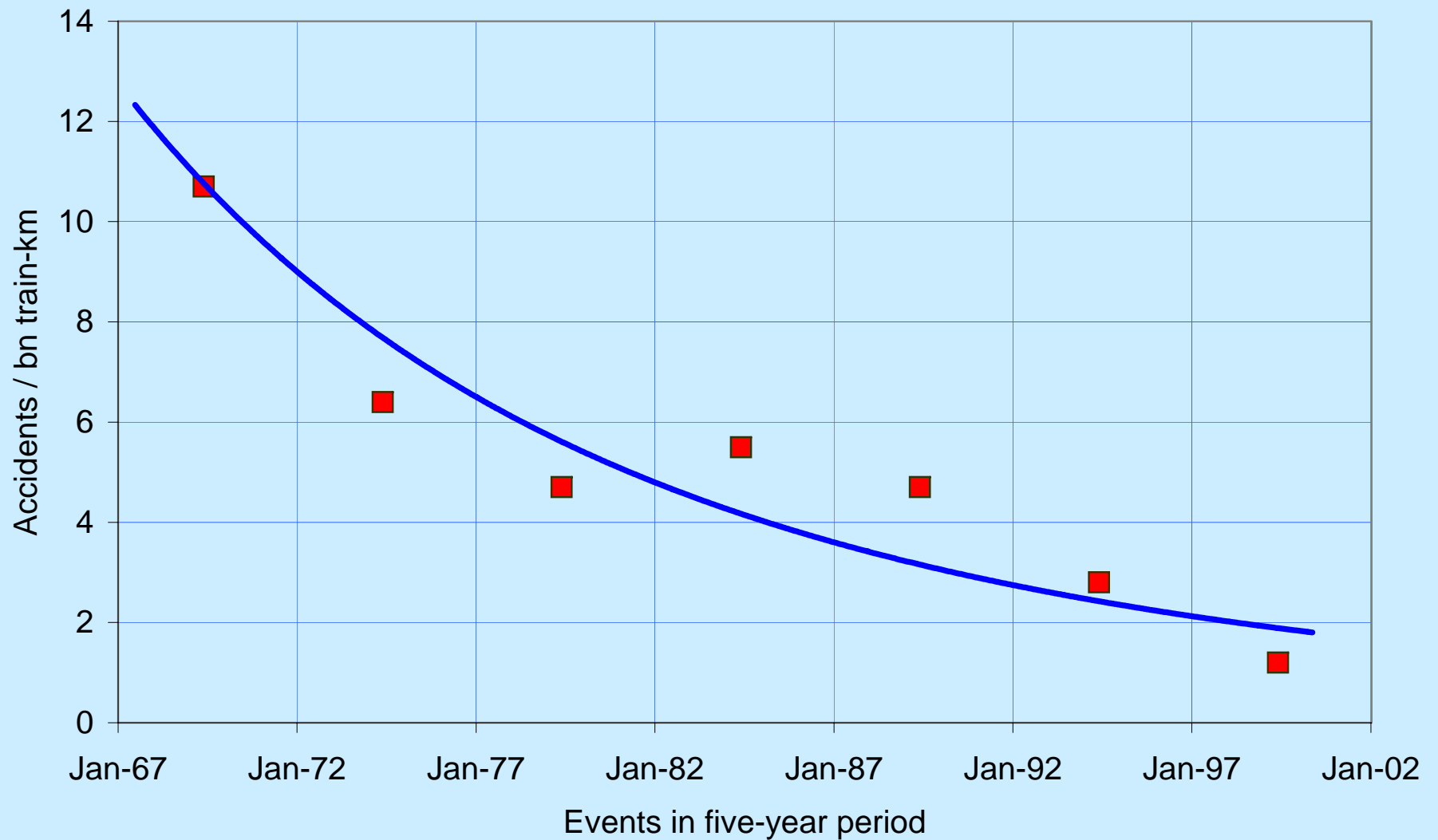
# Nuclear new build

- 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 by privatisation
  - 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.



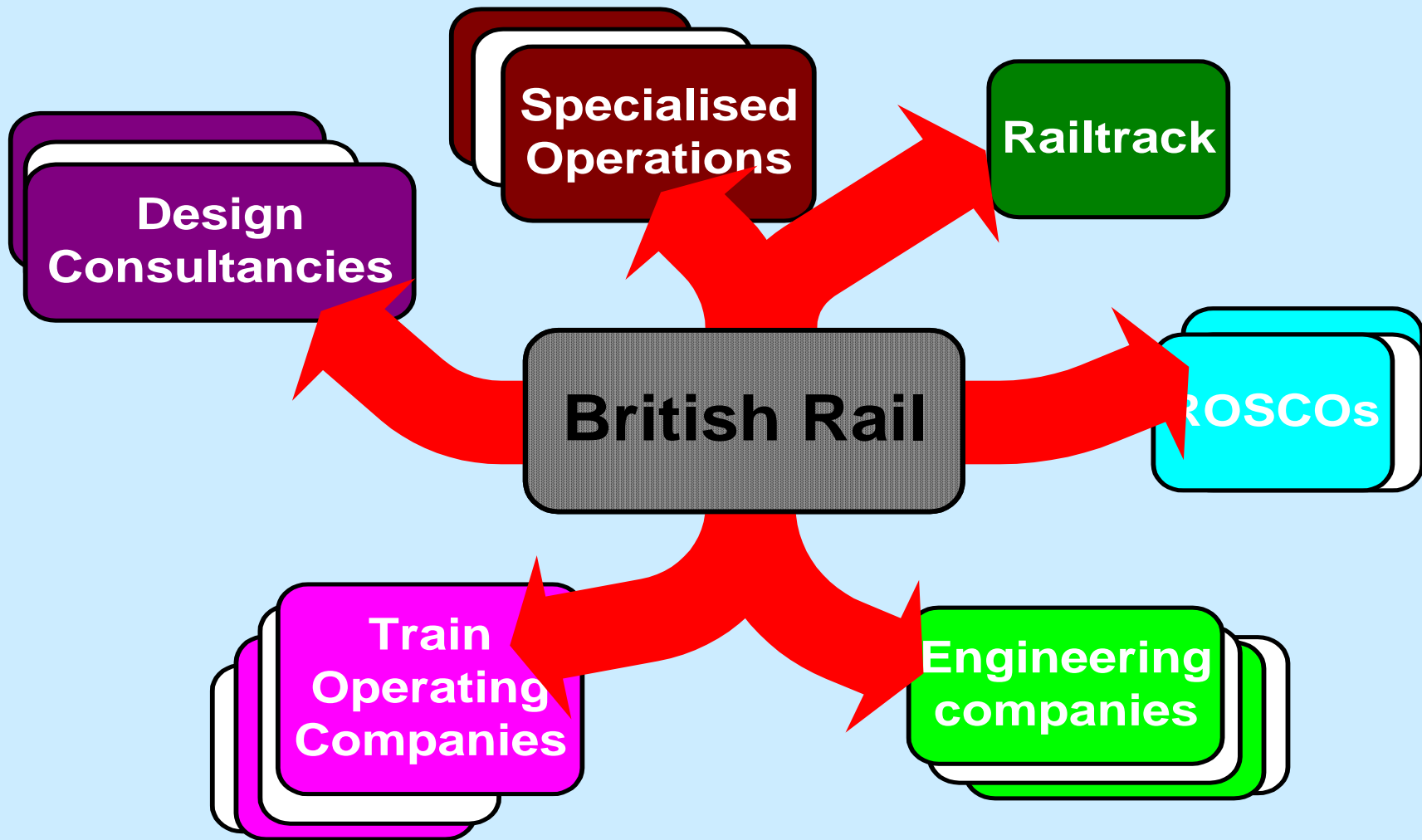
Source - Prof. Andrew Evans, Imperial College, March 2002

**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**

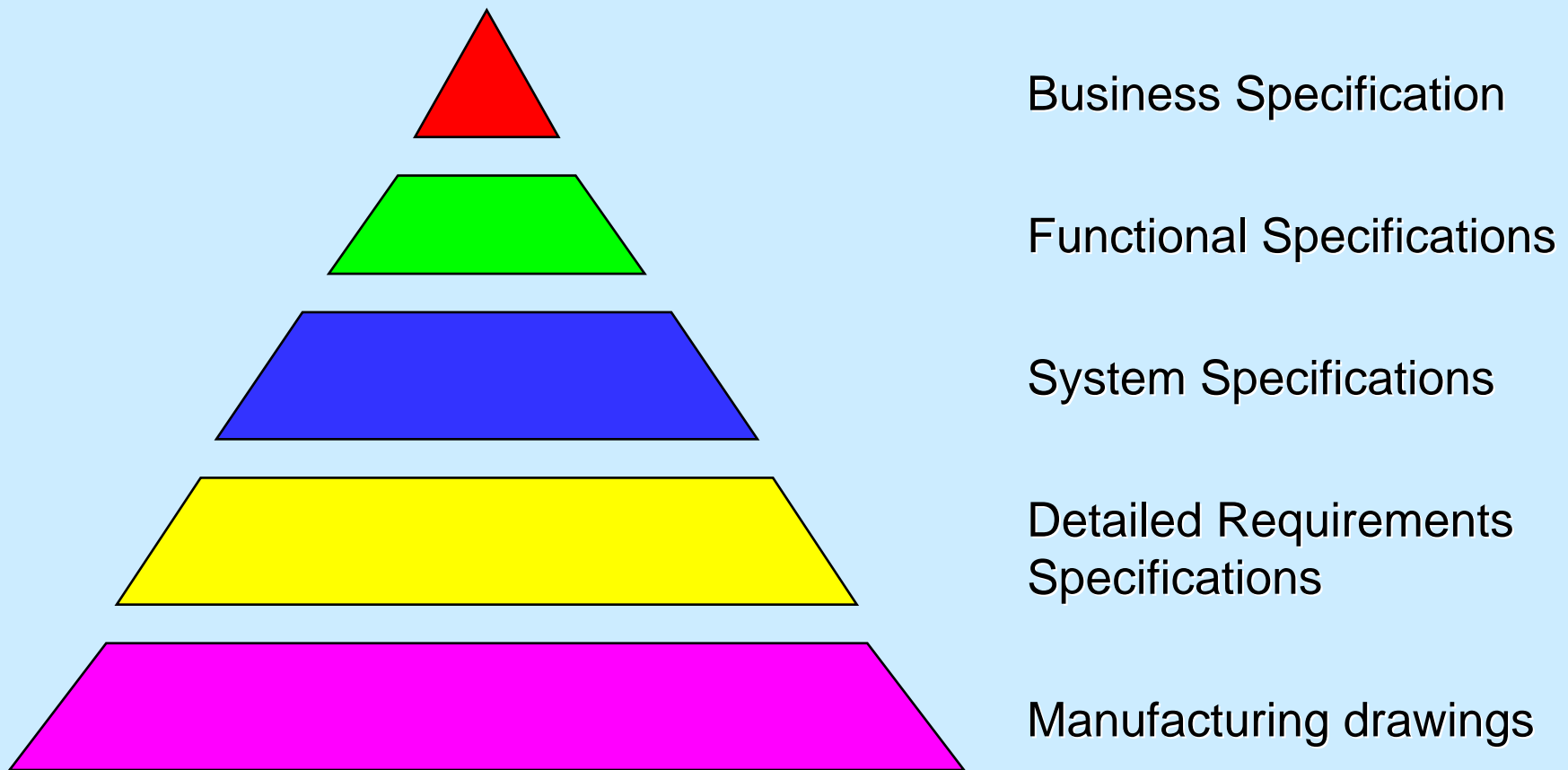
- CEGB

- **After**

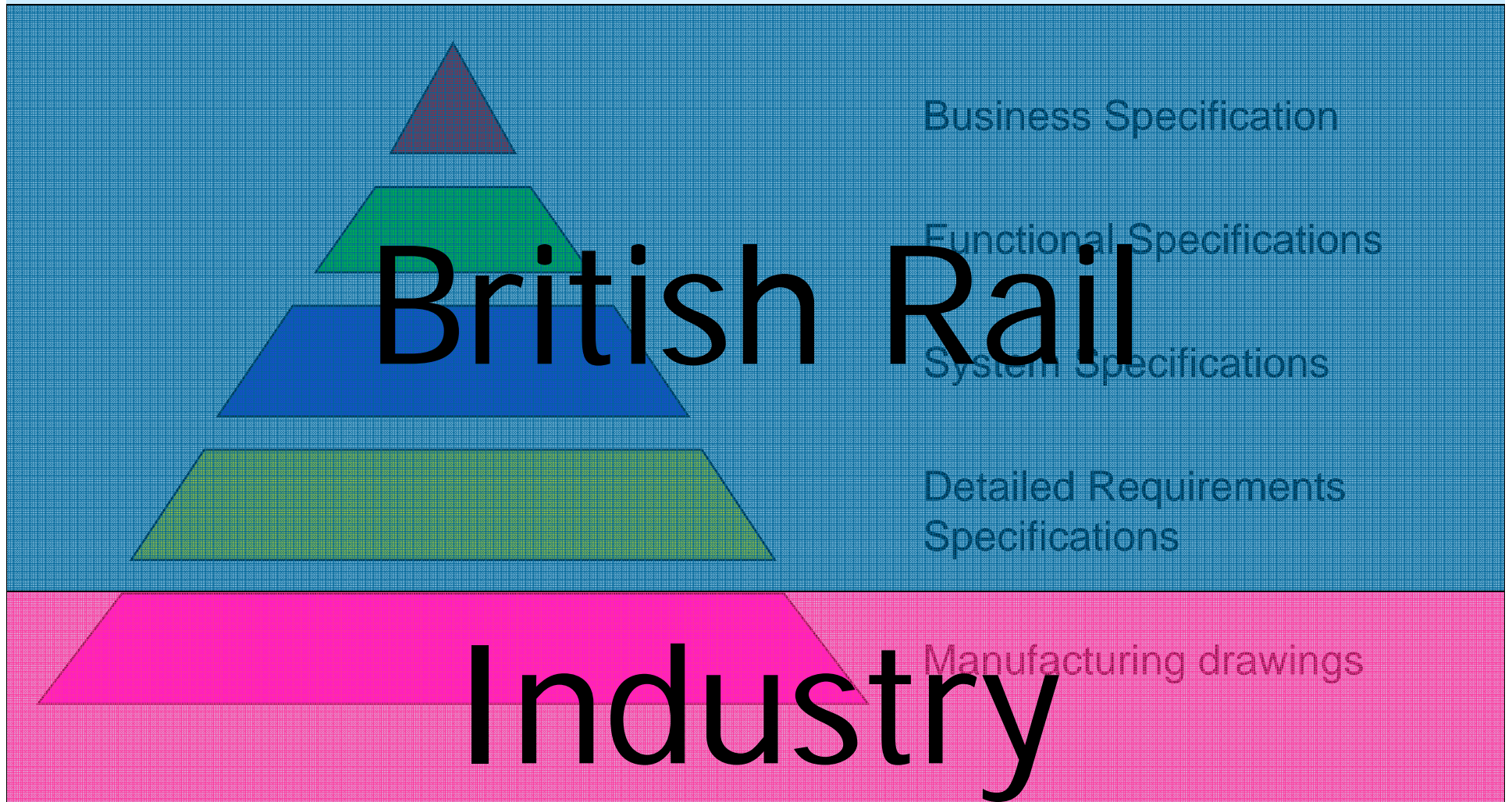
- National Grid
- Generators
- Overseas power station builders
- Consultancies

# Design Authority

# Specification Hierarchy



# Pre-privatisation



# Post-privatisation

# TOC

Business Specification

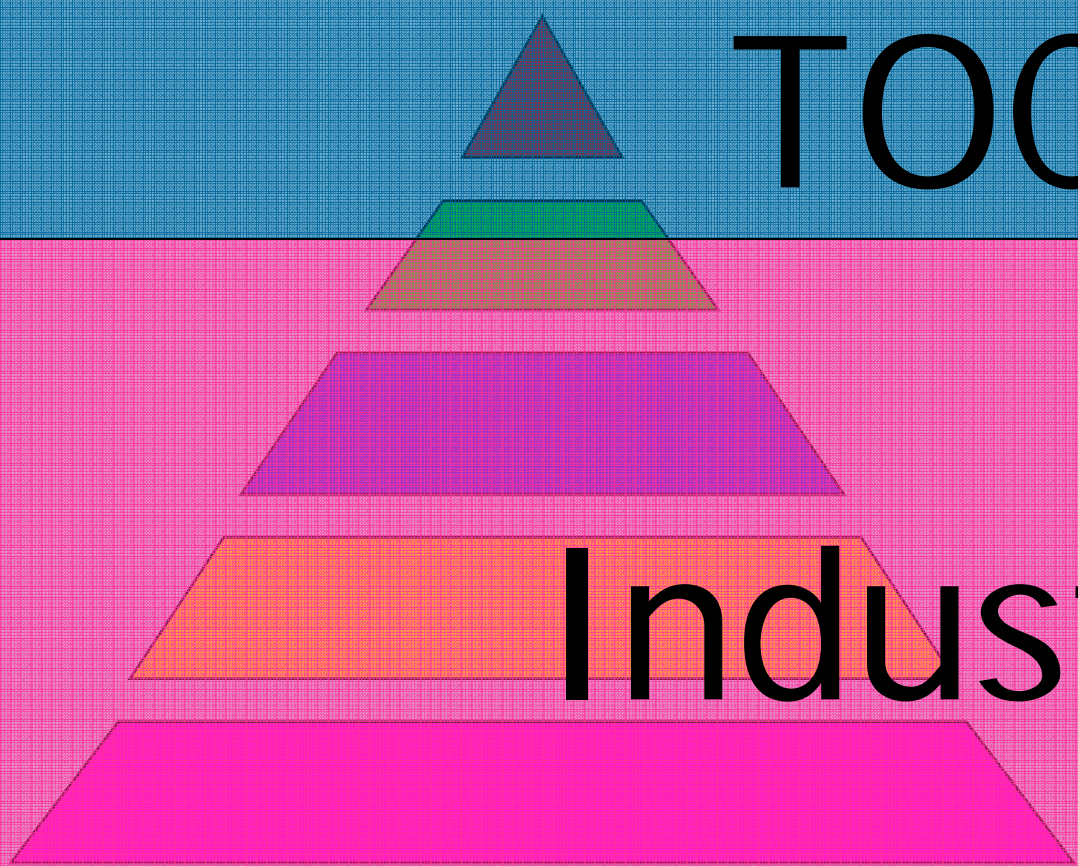
Functional Specifications

System Specifications

# Industry

Detailed Requirements Specifications

Manufacturing drawings



# 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 legislates to move 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?

# Retention of 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.



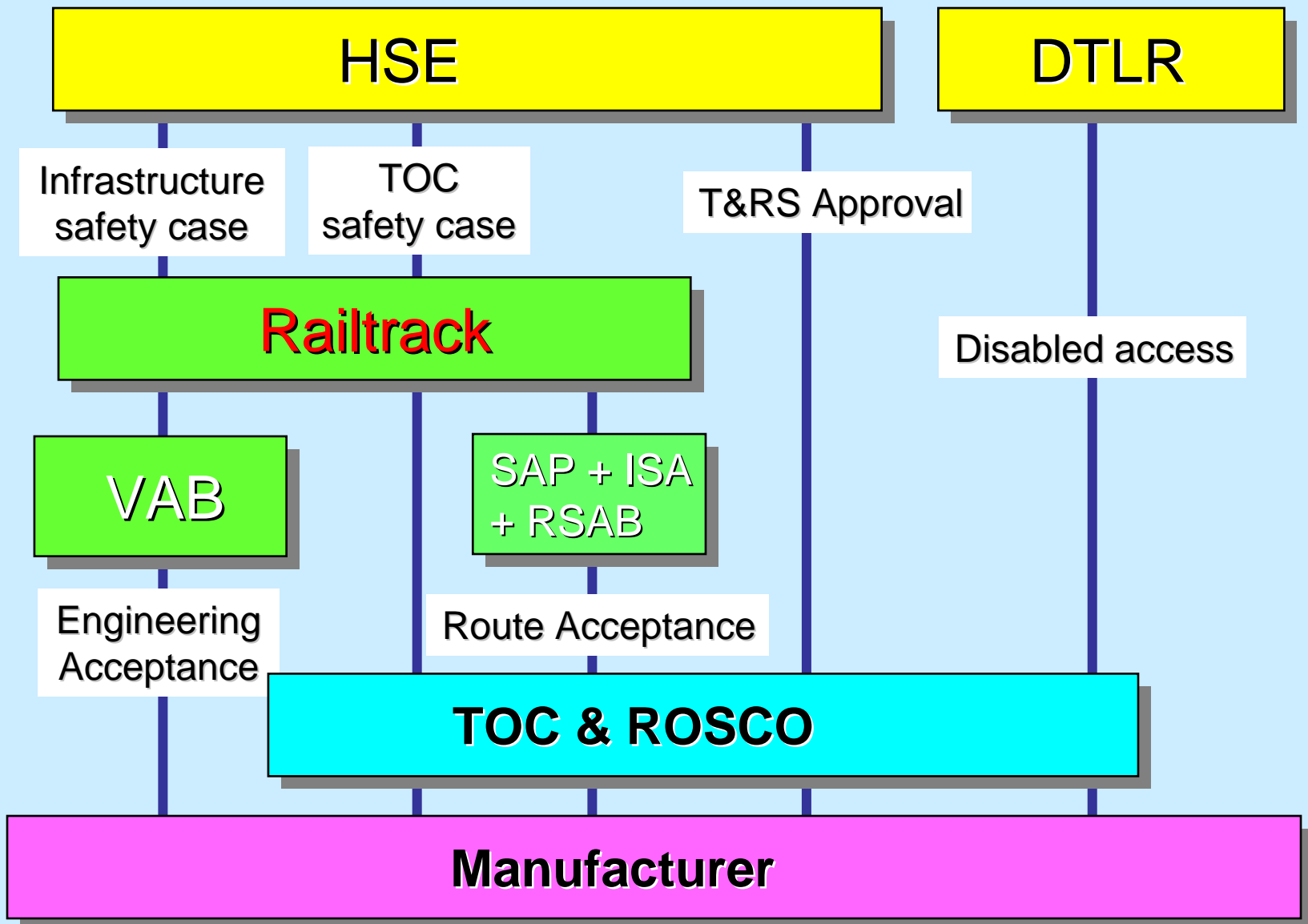
R J KEMP B.Sc. C.Eng. F.I.E.E.  
ENGINEERING DIRECTOR,  
GEC TRANSPORTATION PROJECTS LTD  
RK0797

# Mismatched safety responsibilities

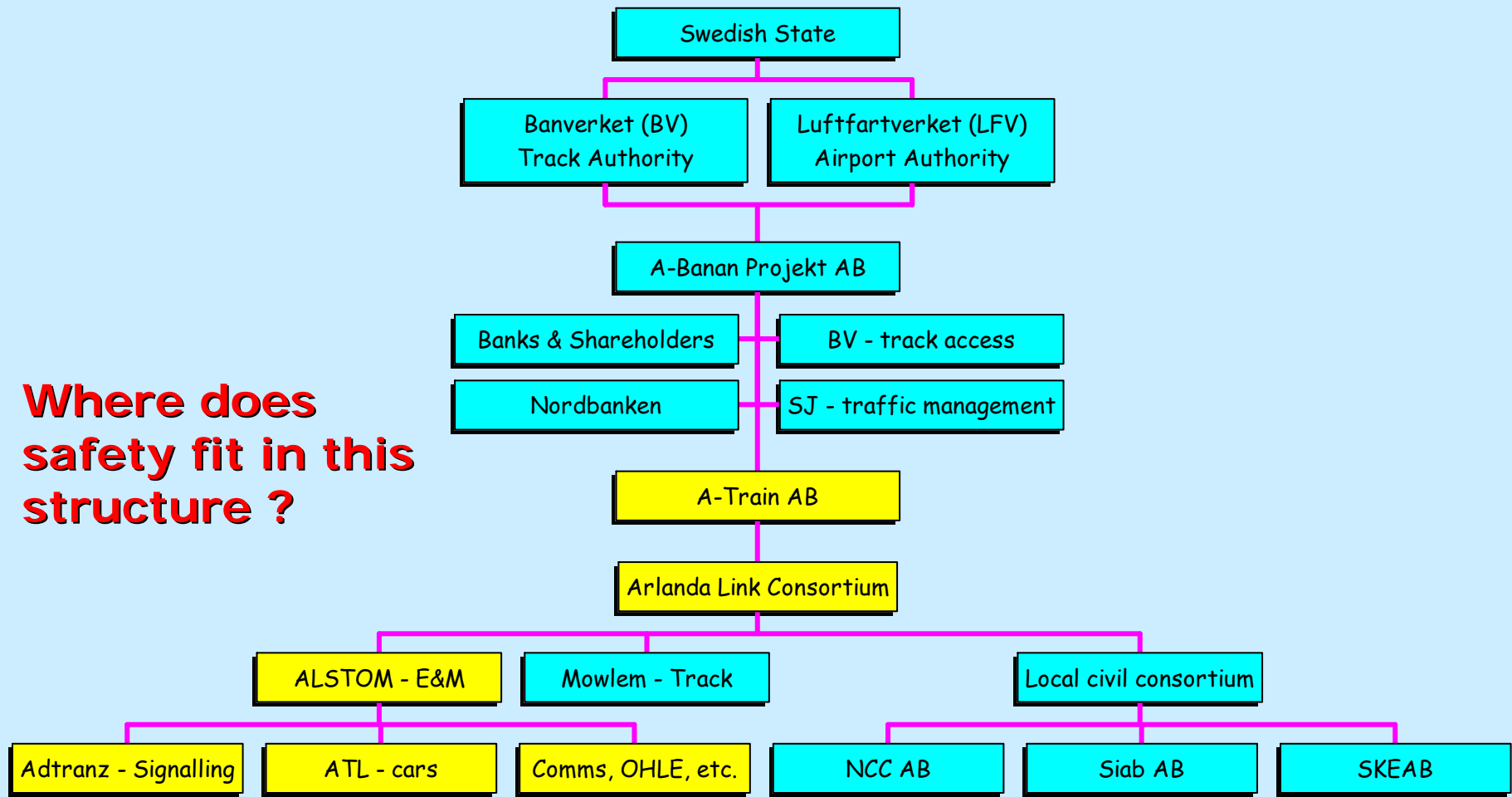
- Railways (Safety Case) Regulations 1994
  - Railtrack responsible for safety of the network
  - TOCs produced safety cases for train design and operation
  - TOC assumed to be an informed customer for the trains

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

# Train approval structure (1994-2000)



# Concession project (Arlanda)

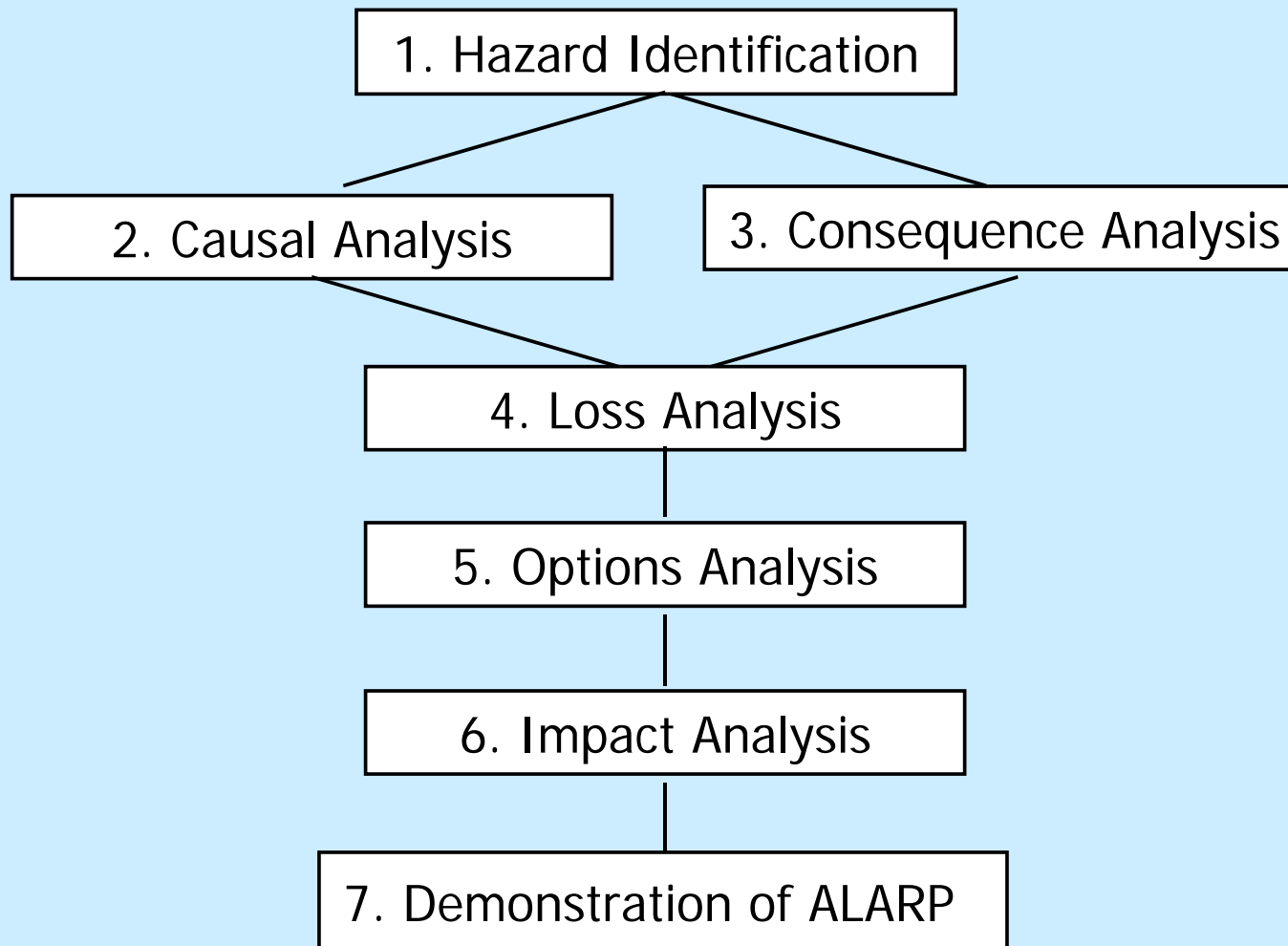


# Power stations are more difficult than trains

- 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 ALARP?

Absolutely safe!



Cordelia Gummer  
during the  
BSE crisis

## Are 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'.



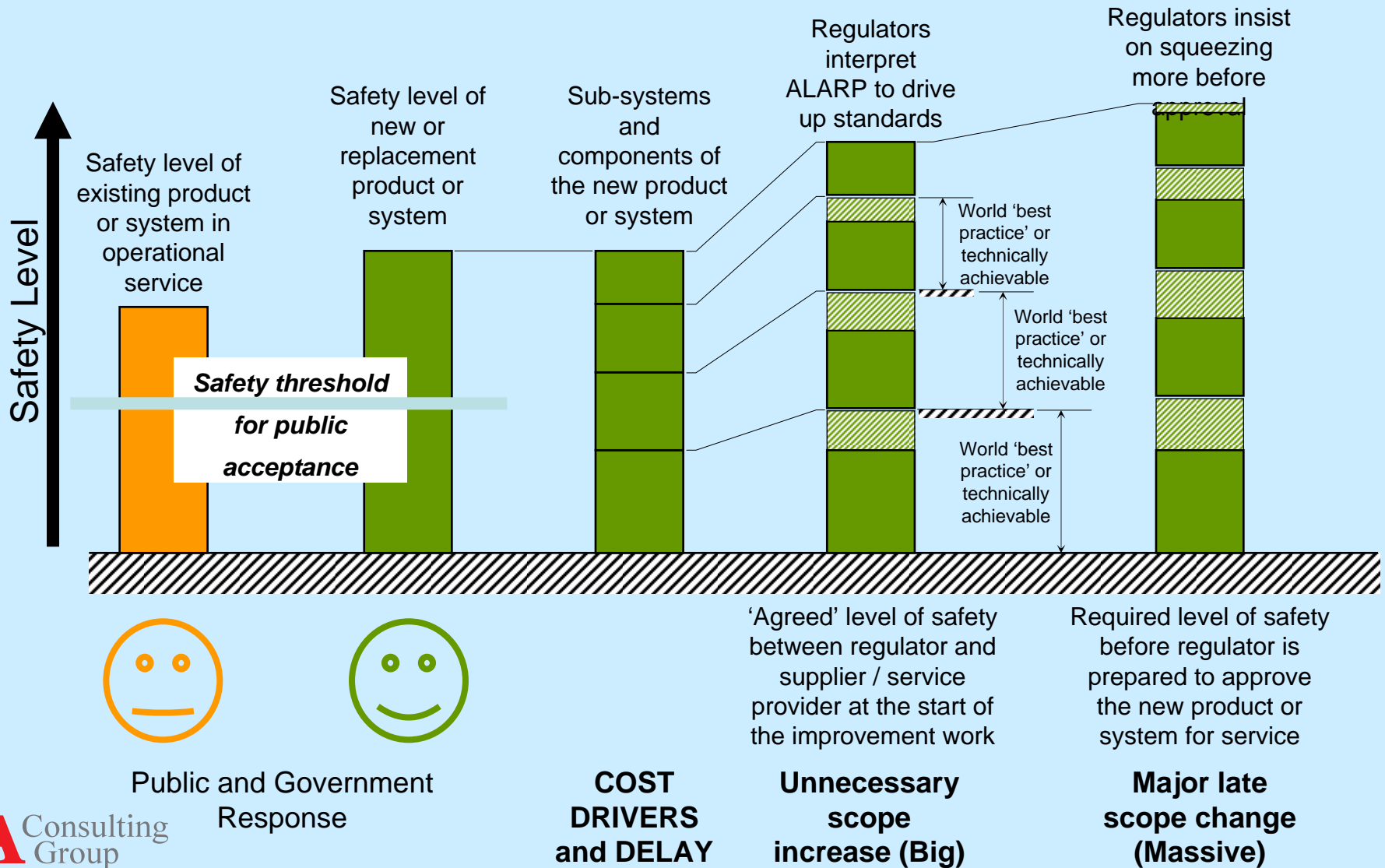
He said Mr Corbett should be prosecuted for arrogance, negligence and allegedly manslaughter.

# How widely is ALARP accepted ?

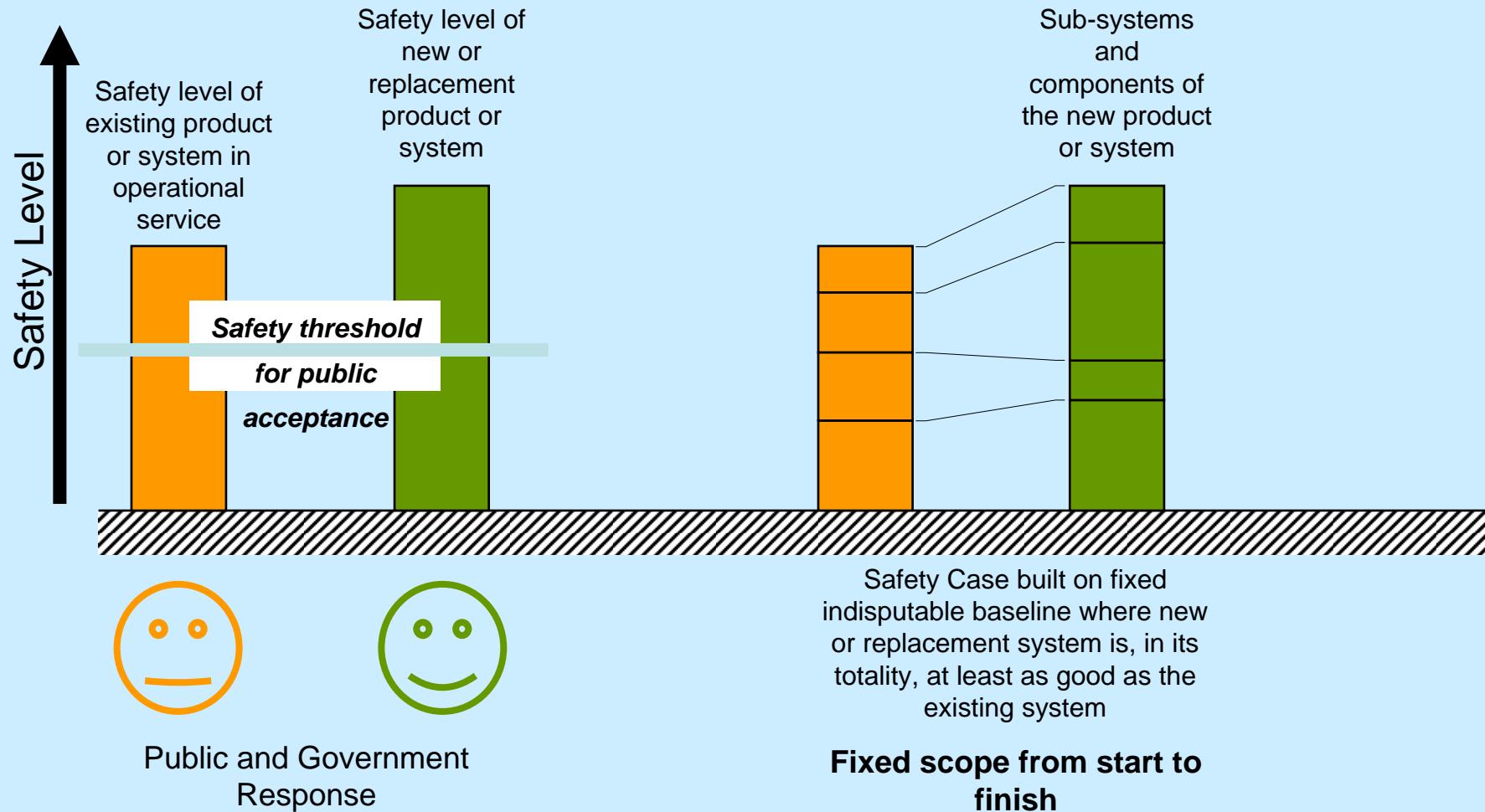
- France uses GAME (*Globalement au moins équivalent*)
- To most Southern Europeans the concept of ALARP is not accepted.

	ALARP	GAME
Reference system	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Statistics & probability	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ?
Consideration of costs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Value on "a life"	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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



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

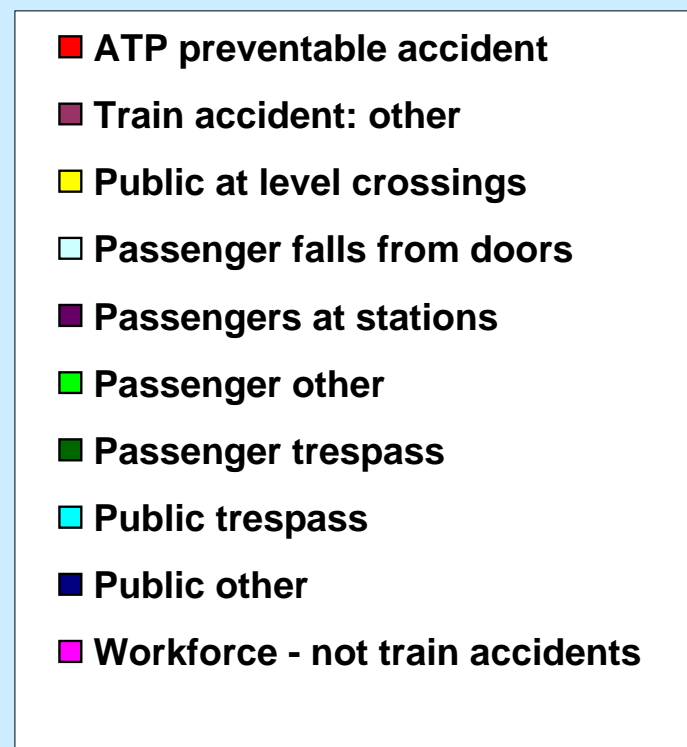
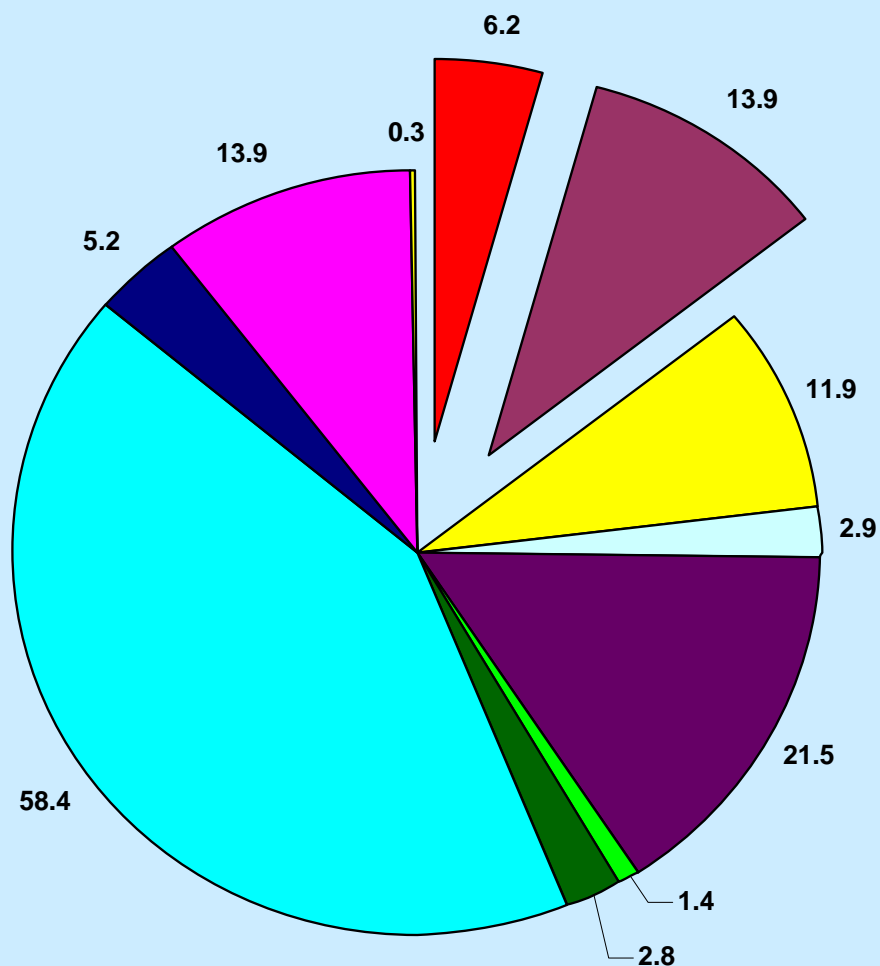


## The regulatory bodies apply the ALARP principle onerously, inflexibly and inconsistently

- 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 GAME 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 GAME 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

# Railway risk (excluding suicides)

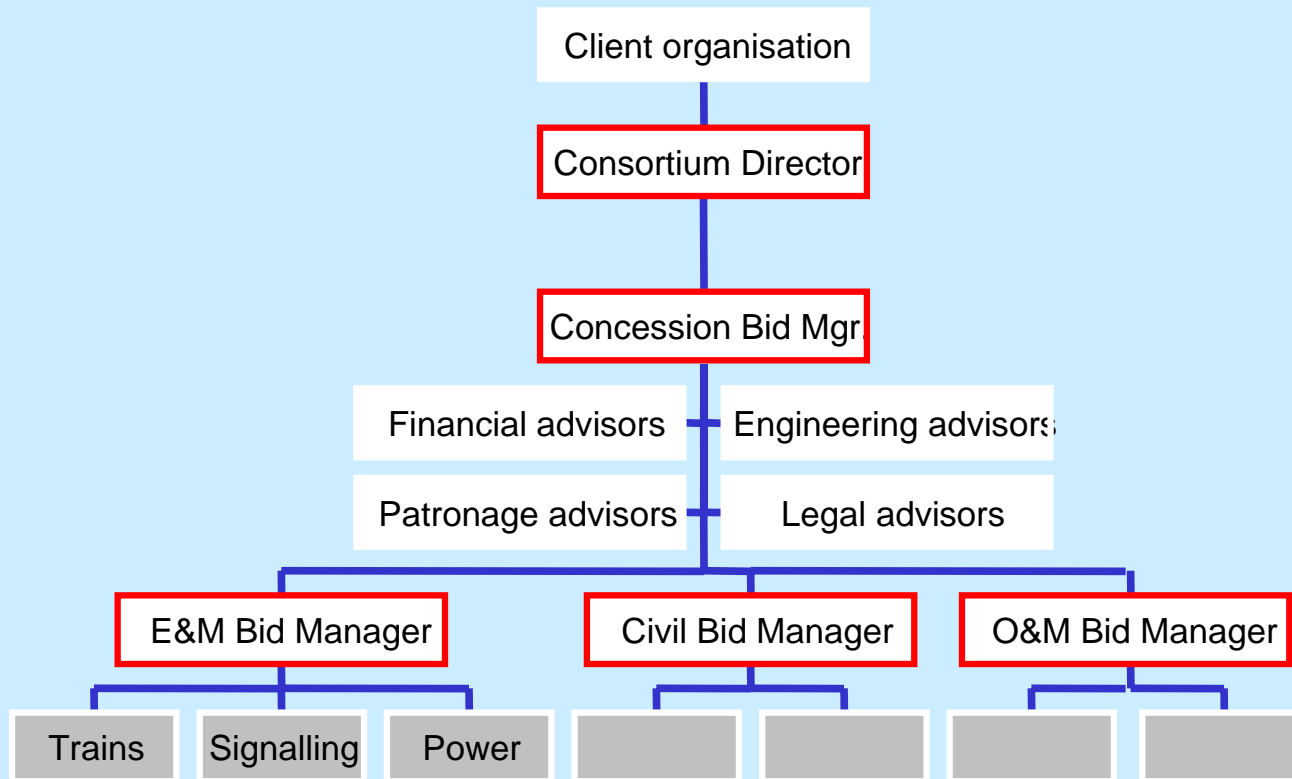
(equivalent fatalities)



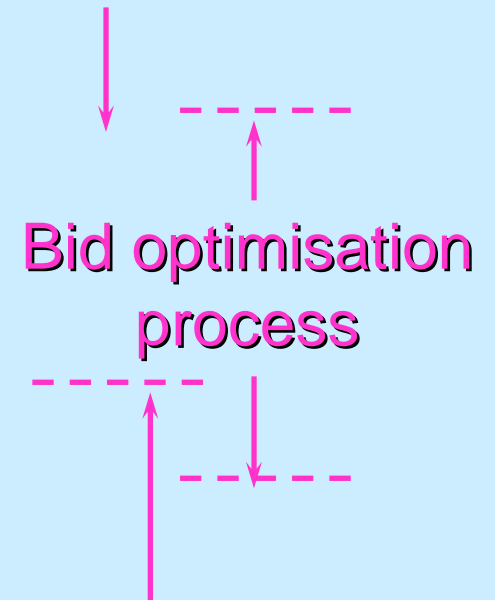
# Main contractor's risk categories

- Delivery risk
  - design more difficult than expected
  - build takes longer or is more expensive
  - delay to date project earns money
- Revenue risk
  - income per unit output (kWh delivered or train-km operated) less than predicted
- Regulatory risk
  - approval process increases costs, delays start-up or otherwise reduce profitability
- Financial risk
  - exchange rates, interest rates, etc.

# Rail concession project - bidding structure



Politics



Detailed offers

Regulatory uncertainty at this level feeds up the structure

## The problem for the bidder

- How much work is involved in proving risks are ALARP for every sub-system?
- Where can I find statistics for the MTBF of highly improbable events?
- 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?

Questions

# Design Authority

- If there are to be several power stations of basically the same design, run by different operators, is it appropriate for each operator to be treated as the Design Authority for that station?
- If not, how is an overseas constructor brought into the safety process?

# ALARP

- How does a contractor demonstrate ALARP in a complicated project where there may be thousands of ways of reducing risk?
- How do we bring into an ALARP regime designs that have been produced under a prescriptive or GAME safety regime?
- Is an ALARP regime suitable for dealing with societal concern?

# The regulatory challenge

- How do we construct a safety regulatory system that allows new power stations to be built by the private sector without huge financial provisions for regulatory risk?