How the design process can fail

- and what this might mean for safety

Engr 514:2014 Design of safety-critical systems

Roger Kemp, January 2014

Three projects

1. Advanced Passenger Train (APT)
2. European overnight stock (EONS)
3. Intercity Express (ICE)

Each of these projects suffered a design/development failure. Not all resulted in a safety hazard but the failure processes were ones that might have had this effect.

All examples are "historic" to avoid discussing current projects but the process failings are equally relevant today!

Project 1 – Advanced Passenger Train

Advanced Passenger Train

- Technology-led project
- Public sector design/project team
- In BR Research Department 1967 – 1974
- Transferred to BR Engineering Department 1974
- Scrapped by incoming government – 1981

APT objectives

- Euston - Glasgow in 4 hours
- No changes to fixed infrastructure
- Full operational flexibility (e.g. Holyhead)

Unwritten objectives

- State-of-the-art technology
- Maintain differentiation vis-à-vis the "competition" – IC225

Internal politics

HST vs. APT

Central power cars

- Overhead line characteristics make two pantographs "impossible"
- Railway Inspector "bans" 25kV line along the train for "safety" reasons
- Maths "prove" pushing a train with 6MW causes derailment on curve - also a "safety" issue

Driving van trailers

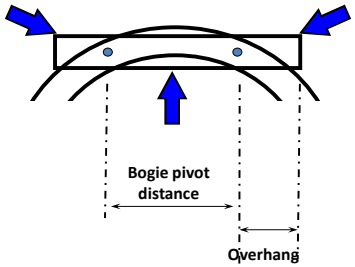
- Railway Inspector "bans" passengers in end car at >200 km/h for "safety"
  - an ALARP issue?
- Commercial spec "requires" diesel haulage to Holyhead by loco not fitted with auxiliary supply

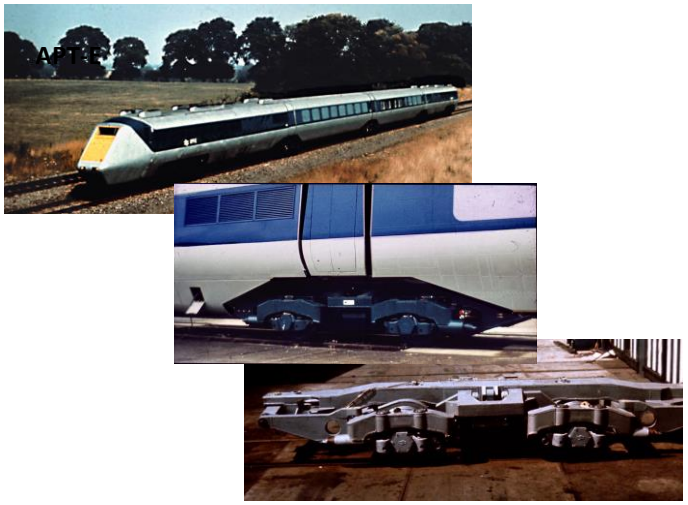
Resulting train formation

Motored axles

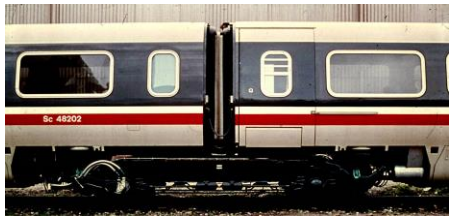
- Platforms limit length to 14 cars
- Wasted space:
  - 2 cars in centre for power equipment
  - End cars for generators and baggage
- 4/14ths of train (30%) not available for passengers

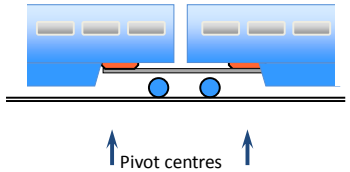
Limit on vehicle length



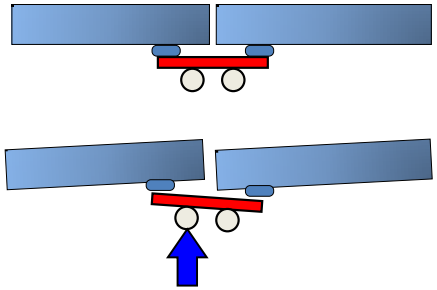


APT-P articulation





Vertical discontinuity



APT-P bogie geometry

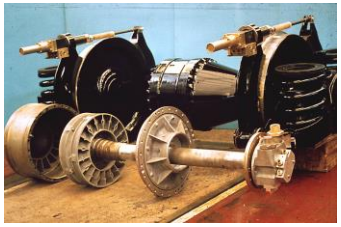
Maximises vehicle length

BUT

At the expense of ride comfort

It just makes the design more challenging

New technology



HK brake

Inadequate manufacturing standards resulted in a derailment that could have been very serious.

Final drive

Every system new !

- Welded aluminium body
- Articulated bogies
- Hydrokinetic brakes
- Tilt system
- Air conditioning
- Thyristor-controlled drives
- External plug doors

Aircraft engines

40 years steady development

- **1971** First RB211 for L1011
- **1996** RB211-524Gs for 747-400
- 2002 - Trent based on RB211

Development - the ideal

- Break task into manageable chunks
- Initial R&D in the lab
- Test prototypes in environmental chamber and on test bed
- Fit pre-production equipment to service trains and flog to death
- Production

What often happens

"During the development of a product, when a design has been produced and prototypes built and tested for function, there is often such a state of euphoria that the product works at all, that questions of reliability take a back seat."

APT Conclusions

- No-one questioned the stone tablets
- Safety used (spuriously) as a reason for stupid decisions
- Too much innovation; expected to fly straight off the drawing board
- Dysfunctional industry structure – project opposed by large sectors of BR
- Optimised for the wrong route

European overnight stock

Sleeping cars to run from UK to continental destinations

Nightstock

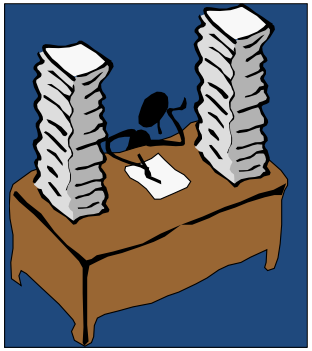
- Consortium of customers
  - BR, DB, SNCF, NS
- Overnight train services from UK to Continent
- Compatibility with many locos and systems
- Thick specification

The invitation to bid

"The specification is complete, except for the sections relating to catering and Control Authority requirements".

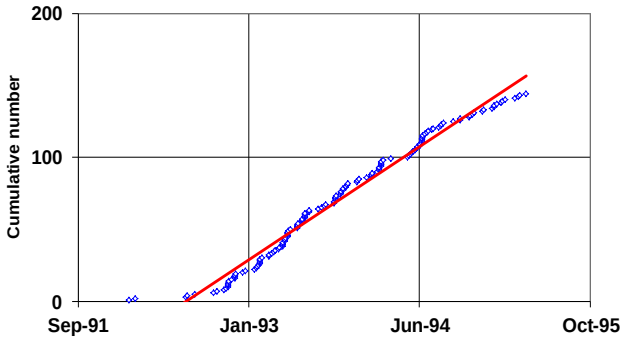
Letter dated 21 December 1990, from J. G. Palmer, BR Procurement Manager.

Specifications



- Main spec 2.5kg
- Calls up more than 200 other specs
- Completely rewritten by BR halfway through bid period

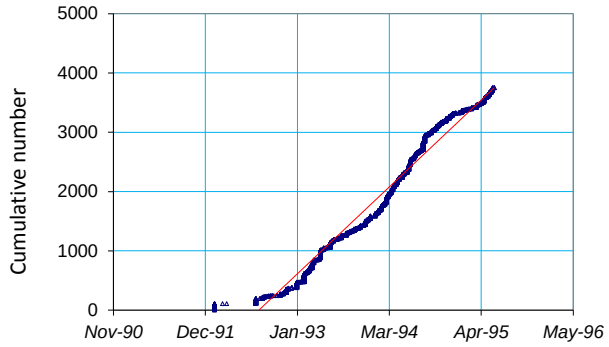
Variation orders



Approval vs. Scrutiny

Approval	Scrutiny
• User approves specifications and all main drawings	• User looks at designs and "comments" on them
• User can instruct supplier to make changes	• Supplier need not take action on comments, but must explain why not
• Subsequent problems only supplier's fault if not built to drawing	• Supplier fully responsible for performance of project

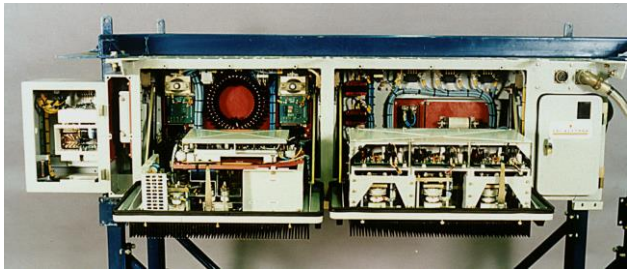
Submissions for "scrutiny"



European auxiliary power systems

• 1000V 50Hz 2-wire	UK
• 1000V 50Hz earth return	France
• 1000V 16.6Hz earth return	Germany
• 750V dc	UK (third rail)
• 800V dc 2-wire	UK diesel locos
• 1500V dc	Netherlands, France
• 3000V dc	Belgium

Auxiliary converter



Input: 600 - 3300Vdc 1000V 16.6/50Hz
Output: 415V 3-phase 50Hz 100kW

Coach auxiliary loading

- Air-conditioning (individually adjustable)
- Lights
- Showers, hand-driers, hair driers, water heaters
- Kettles, catering cars
- Losses in energy conversion

Max load c. 80kW/car

Auxiliary supply

Train loading

- Spec. requires 24-car trains
- Loading 80kW/car (max)
- Thus total load is up to 1.9MW
- When fed from 600V (750 x 0.8) current is 1900/0.6 = 3000A (peak)
- Diversity helps - but not much !

Supply jumper limited to 600A

Auxiliary power supply

"There is not, and never has been, the remotest chance of being able to supply sufficient auxiliary power to ENS to maintain specified vehicle temperatures in the worst case specified ambient temperature, particularly when the train is fed from one Class 92 locomotive on the 750V NSE portion of the route. [. . .] The shortfall in power available is significant, at least 50%."

M. P. Reece PhD, FREng, FIEE January 1994

Possible solutions

- Reduce max. train length
- Redesign the air-conditioning, showers, etc.
- Take power from loco at 1.8kV
- Use diesel generator vans
- . . . .

The chosen solution

A sophisticated computerised load control system to "time share" the different loads

e.g. this would reduce air-conditioning performance when showers were in use

How much does a sleeper cost ?

Sleeper from Lancaster to Paris

Amortisation of capital / car	£100,000 pa
Staff costs / car	80,000
Maintenance (7% capital)	70,000
Energy (traction + auxiliary)	50,000
Railtrack & ET charges / car	100,000
Share of loco and other costs	100,000
Total	500,000 pa

Spread over 10 berths, 300 nights pa, 75% full

Addition to ticket price = £500,000 / 2250 +20%

= £250 one way

Nightstock conclusions

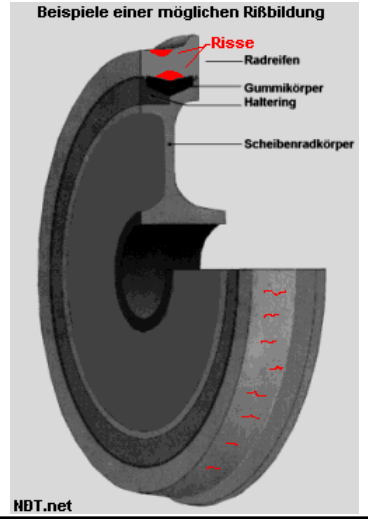
- The specification was impossible
  - No-one in authority would accept this
- Variation orders were out of control
  - The objective was never fixed
- Design approval muddied responsibility
- Technology used as a “cure all”
- The project economics were “dubious”

Intercity Express

Summary of the problem

- Unacceptable noise in passenger cars
- Root cause - hard trackbed
- Possible solutions:
  - Modify track
  - Extra vibration isolation in suspension
- Cost and timescale pressures and loss of face vis-à-vis TGV

The solution



Eschede accident

Important conclusions from these three projects

- The design/development process can fail if the specification is not clear, fixed – and technically possible.
- Late modifications can increase risk
- A failure of this process is likely to result in safety failings – and greatly increases the likelihood of accidents