Design case studies A:
Electric vans and Docklands Light Railway

Engr 514:2014 Design of safety-critical systems

Roger Kemp, January 2014

Historic EV

2

The project – to move EVs from a "tree-huggers' car" to a commercial vehicle

3

Lead-acid traction battery

Key parameters

- 6 V
- 180 Ah
- 32 kg
- ~ 34 Wh/kg

$Pb + SO_4^{2-} \longrightarrow PbSO_4 + 2e^-$

$PbO_2 + SO_4^{2-} + 4H^+ + 2e^- \longrightarrow PbSO_4 + 2H_2O$

4

Types of secondary battery

	Wh/kg	W/kg	Cycle life	€/kWh
Lead-acid	35	200	600-1000	150
Nickel-cadmium	50	175	1500 - 2000	600
Nickel-metal hydride	70	200	1500 ?	250 ?
Sodium-sulphur	150	200	600 ?	250 ?
Sodium-nickel chloride	90	110	1000 ?	250 ?
Zinc-bromine	70	100	1000 ?	250 ?
Zinc-air	180	125	400 ?	125 ?
Lithium	200 ?	400 ?	1000 ?	100 ?

Look at: http://www.powerstream.com

5

Installing batteries

6

Low energy density (compared with petrol)

7

Safety risks in the EV programme

Hazard	Risk level
Fault in structure of van, steering, etc.	UNLIKELY
Fault in control system, resulting in runaway	MODERATE
Explosion caused by battery (and/or hydrogen)	MODERATE
Electrocution of maintenance or servicing personnel	POSSIBLE
Leaking acid caused by accident	MODERATE
Fire caused by short-circuit battery	MODERATE
etc.	

Crash testing

Overturning test

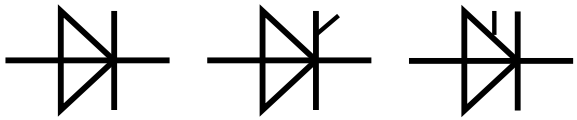
Low temperature operation

11

Rectifier diodes

Diode

Thyristor (2 options)

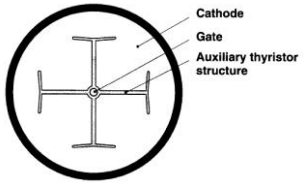


Direction of current flow

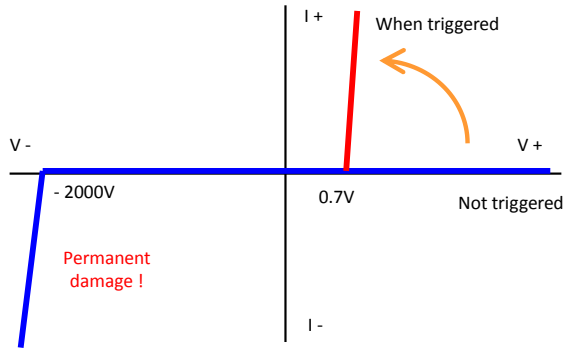
12

Thyristor conduction

- Devices only conduct when there are adequate carriers (electrons or holes)
- Diode always has enough carriers to get it going and then "avalanches"
- Thyristor needs injection of carriers to get it going
- Device continues to conduct until current drops to zero

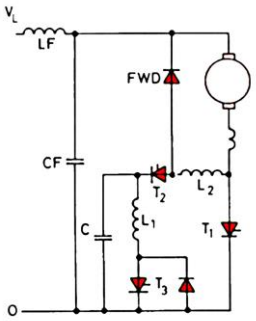


Typical thyristor characteristic



14

Traditional 3-thyristor chopper



T_1 is fired to start conduction

T_2 is fired to divert current into commutation capacitor, which switches off T_1

With T_1 off and C charged, motor current decays through FWD

What happens if T_1 doesn't turn off?

T_1 main thyristor
T_2 commutation thyristor
L_2 commutation inductor
C commutation capacitor
FWD free-wheel diode

This is actually the circuit of trains for Seoul subway L3 and L4

Battery charger (10 kW)

Failure of battery ventilation

- Hydrogen generated by charging process
- Insufficient ventilation to dissipate the gas
- Explosive mixture ignited by spark

This raised battery ventilation to the status of a safety-critical system

17

Explosion test

18

Evening News fire

This raised charger management to the status of a safety-critical system

- Battery charger "on" all long weekend
- Plates distorted
- Short circuit leading to thermal runaway
- Battery discharged very quickly
- Molten lead formed pool under vehicle

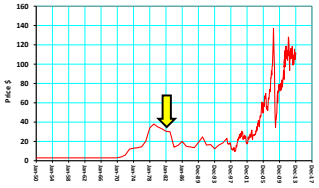
19

The problem – economics

- What constitutes suitable EV operation?

$$\frac{Daily\ mileage}{Maximum\ range} \approx 1$$

- No safety issues prevented introduction of electric vans

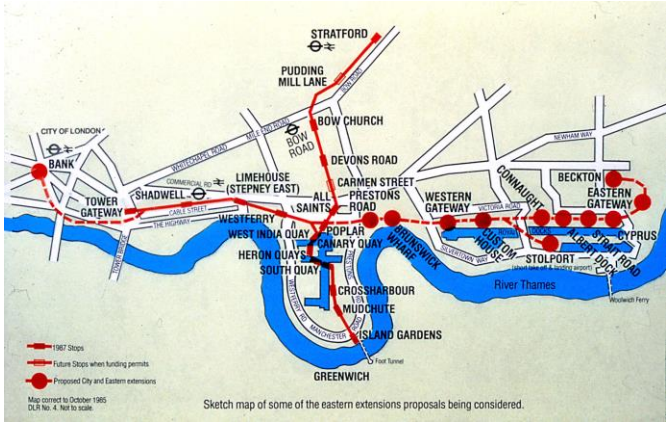


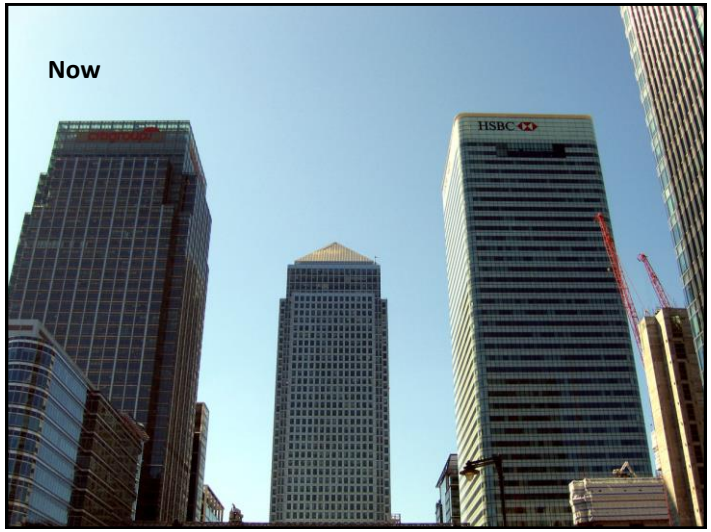
Price of Brent crude

Docklands Light Railway (DLR) Initial system

Initial system opened 20 years ago – since expanded ten-fold

Docklands Initial System – the route





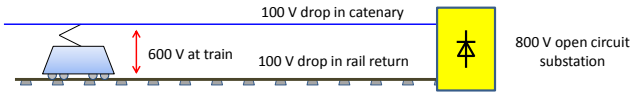
Possible safety risks in the DLR development

Bearing in mind, this was the first automatic metro in the UK

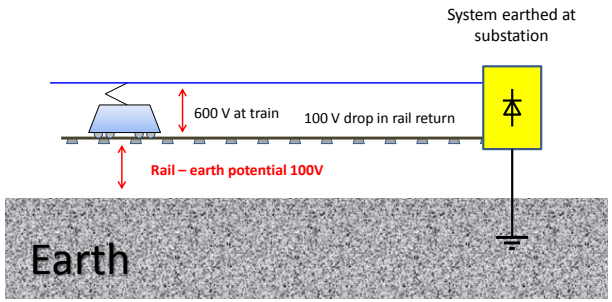
Hazard	Risk level
Development “teething problems”	High
Control system failure causes dangerous train operation	Possible
Passenger falls in front of train that can’t “see” him/her	Moderate
Electrocution from conductor rail	Possible
Step and touch potentials	Moderate
Inadequate crisis management ability with so few staff	Moderate
Vehicle mechanical problems	Low
System “freezing” and resultant passenger behaviour	High
etc.	

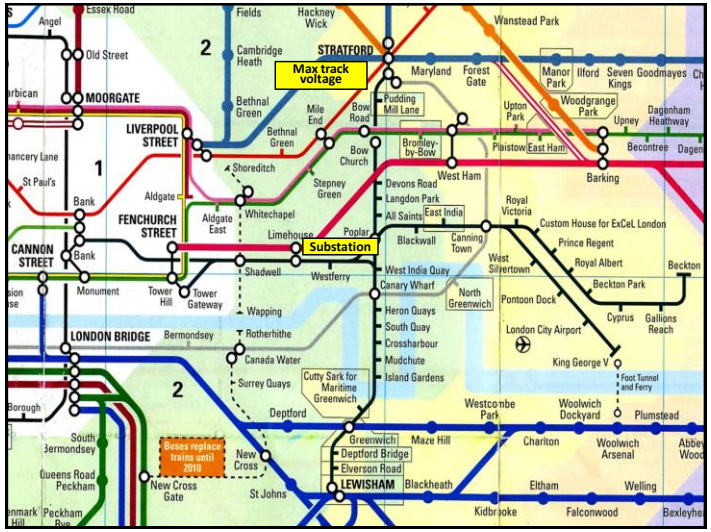
Step and touch potential (1)

Voltage drops in normal operation (simplified)



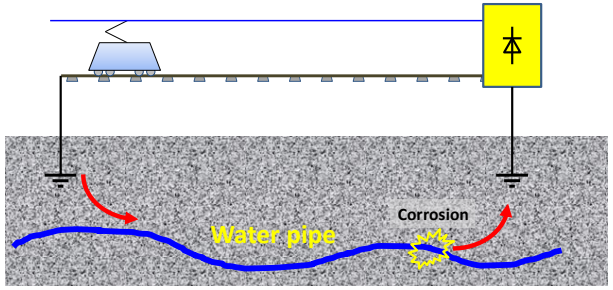
Step and touch potential (2)





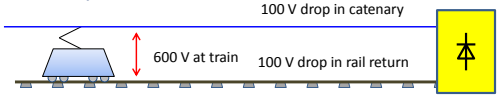
Multiple system earths

Current shared between rail and other earth paths.
Water and electricity companies object to stray currents in their services due to electrolytic corrosion.

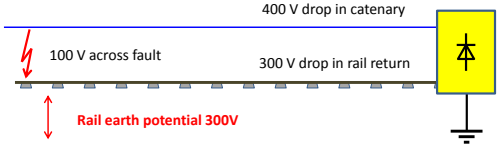


Step and touch potential (3)

Normal operation



Fault conditions



Managing potentials on other UK rail systems

London Underground

4-rail system, 300-0-300 V return current does not use running rails

Network Rail (south of the Thames)

Continuous earthing
"We were here first"

Note also lack of protection for conductor rails

Other metro system practice

Atlanta

San Francisco

Both these systems use a third rail with good insulation between rail and earth and ensure that passengers cannot touch "real earth" at the same time as a train.

Insulating the trackbed

Re-bar at N Quay junction

Testing effect of re-bar design on transmission of train control signals

Longitudinal re-bars connected back to substation via earthing cable and "drainage diode"

Stratford station

- No earthed metalwork (including vending machines) within reach of platform edge
- Insulating layer below paved surface

Protecting the 3rd rail (discovering best practice?)

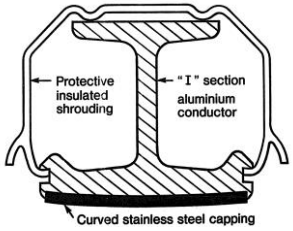
Atlanta Rapid Transit

Chicago people-mover

Detroit people-mover

Lyon Line D

DLR 3rd rail cross section



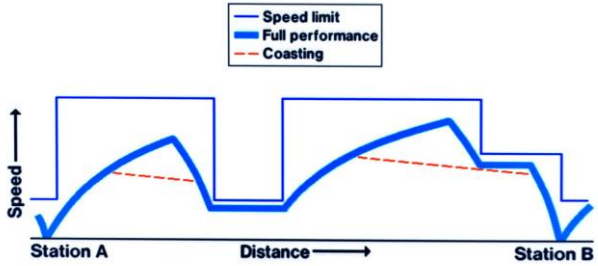
DLR conductor rail

Note also ATP track loops

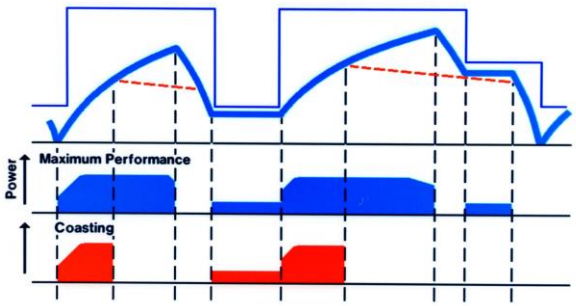
DLR – Automatic control systems

- Constraints
  - Client requirement for no drivers
  - 3 years from contract to passenger operation
- Decision to separate ATO and ATP systems, rather than design a SIL4 ATO
  - **Automatic train operation (ATO)** can be SIL0
  - **Automatic train protection (ATP)** must be SIL4

ATO trajectories

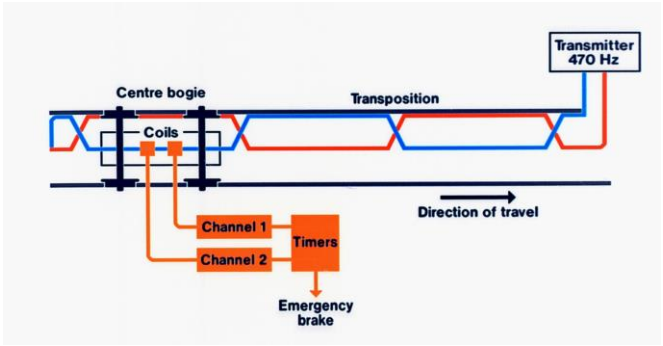


Coasting and timetable correction

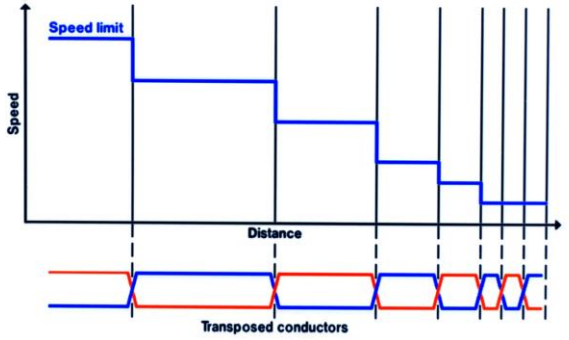


ATP transposed conductors

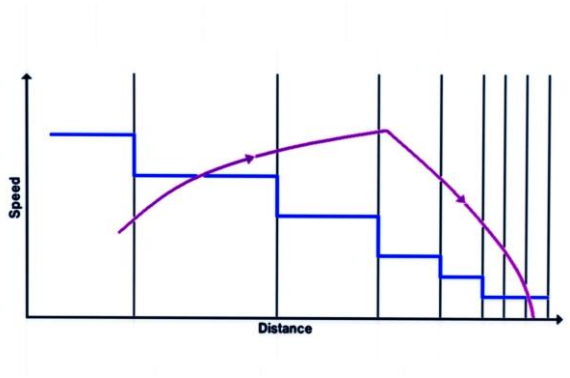
Principle of ATP operation



Speed limit into station



Design case for overspeed



Testing the ATP


PRICE 10p LONDON MIDDAY SPECIAL

DAILY NEWS

Inquiry after test-run crash on new Dockland railway

Train takes strain

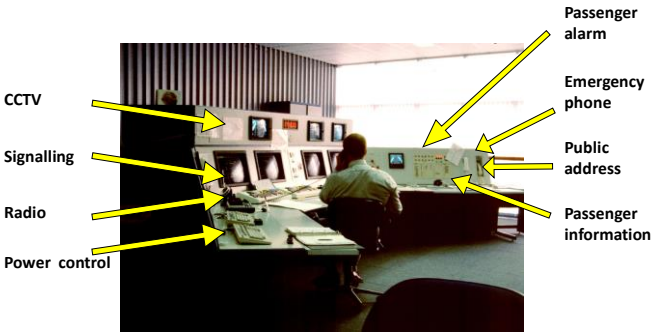
- Test not adequately planned
- Inadequate risk assessment
- Phase of adjacent loops not synchronised
- Train driven manually by graduate trainee

Requirements for control room operation

- One person operation
  - with assistant at busy times
- Signs-on train captains
  - allocates duties and radios
- Manually controls trains from depot to system
- Manages possessions
- Responds to passenger alarms, observes CCTV
- Supervises automatic systems

The control room

(Discussed in more detail in Engr 516)



HMRI criticisms

- Low refresh rate of screens so controller did not know what was happening
- Highly variable workload resulting in controller overload
- Too many controller distractions
  e.g. signing-on train crew, possessions, passenger queries, radio to train crew, …
- Poor alarm rationalisation
- No planned emergency actions

Redesigned interface

(Discussed in more detail in Engr 516)

Manual driving

- Used when there is an equipment fault
- Train manager can override automatic systems
- No trackside signals
- Permission to proceed given over radio link

The only accident in passenger service was caused by the controller giving permission for a train to proceed over a junction without cancelling automatic operation on all conflicting routes.

Main issues

- Project safety must consider all hazards – not just those that are easy to analyse or that correspond to a team's competences or preconceptions.
- Safety management must be embedded in the project structure – not seen as a separate deliverable managed by a remote team
- Imagination to ensure all hazards are covered is more important than the detail of how each is analysed.