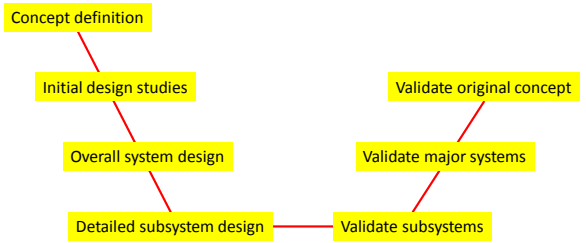
# Tools and techniques for designing safe systems

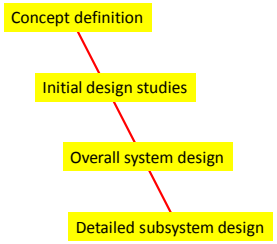
**Engr 514:2014 Design of safety-critical systems**

**Roger Kemp, January 2014**

## The design process




## The design process




- It is essential that safety assessment is not left until the validation process
- As the design progresses through these 4 steps, decisions must factor-in system safety

## Consider safety from the beginning

**Concept definition**

- Optioneering to choose best concept – intrinsic safety to be an important selection criterion.
- Confirm concept only after ensuring it is (or can be made) adequately safe.

**Initial design studies**

Safety to be an explicit objective, priority to be:

- Eliminate hazard
- Control hazard by technical means
- Control hazard by operational procedures
- Provide operators with PPE

## Safety management tools

- Identifying hazards
  - Previous experience (including check lists)
  - Brainstorming
  - Hazard and Operability Analysis (HAZOP)
  - Fault Tree Analysis (FTA)
- Listing and classifying hazards
  - Hazard log
  - Risk matrix
- Managing risks
  - Stress analysis and other deterministic tools
  - Probabilistic risk assessment (PRA)
  - Quantified risk assessment (QRA)
  - Failure Mode, Effect and Criticality Analysis (FMECA)

## Tools

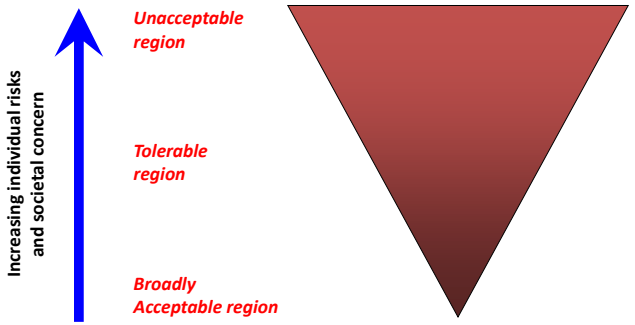
## Techniques

- There is no “right” way to analyse safety or environmental impact

- The important thing is that the analysis should:
  - be clear and understandable
  - define exactly what is ***in*** and what is ***out***
  - be relevant
  - not give a false impression of accuracy or completeness

## CLASSIFYING RISKS

## HSE framework for tolerability of risk




*Environmental risks can be similarly classified*

## Risk matrix

*from EN 50126:1999*

Consequence

| Likelihood | Catastrophic | Critical | Marginal | Insignificant |
|---|---|---|---|---|
| Frequent | A | A | A | B |
| Probable | A | A | B | C |
| Occasional | A | B | C | C |
| Remote | B | C | C | D |
| Improbable | C | C | D | D |
| Incredible | C | D | D | D |

**Risk categories:**

- A Intolerable
- B Undesirable
- C Tolerable
- D Negligible

*Risk = Fn (consequence, likelihood)*

## Hazard log

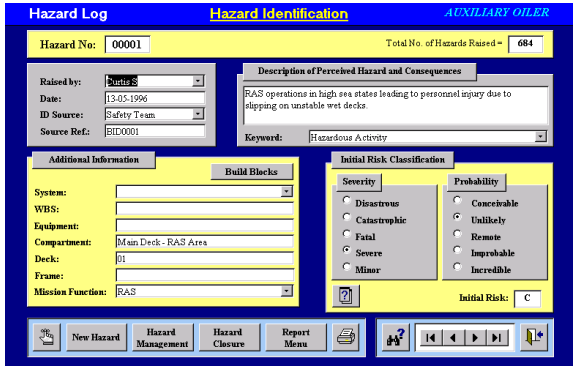
**A hazard log is:**

- A complete list of identified hazards
- A means of classifying risks into broad categories
- A statement of who is charged with finding a solution
- A record of the action taken to resolve the hazard

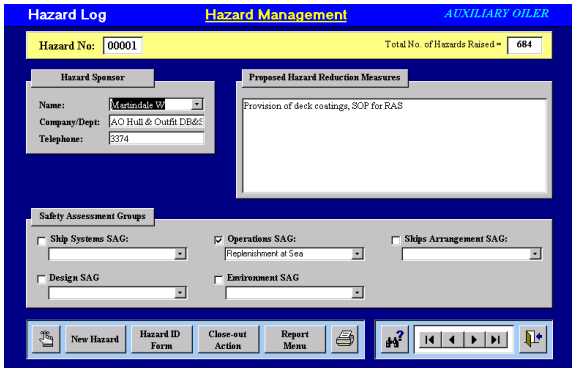
**A hazard log is not:**

- A way of identifying hazards
- A detailed calculation of risk
- A safety justification for a project
- A calculation of reliability
- A means for demonstrating contractual targets are met

## "Hazard Identification" Screen

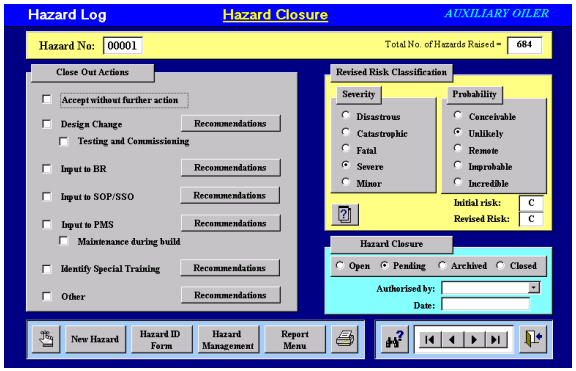


## "Hazard Management" Screen



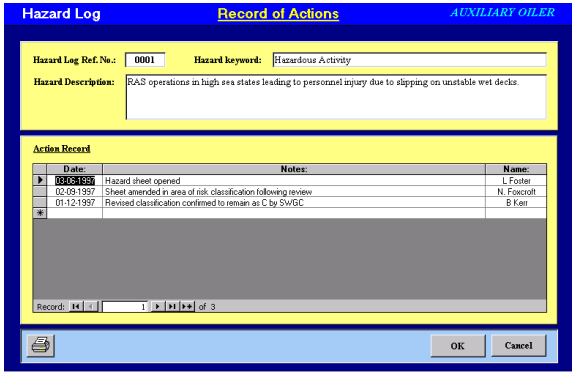



## "Hazard Closure" Screen






## "Record of Actions" Screen



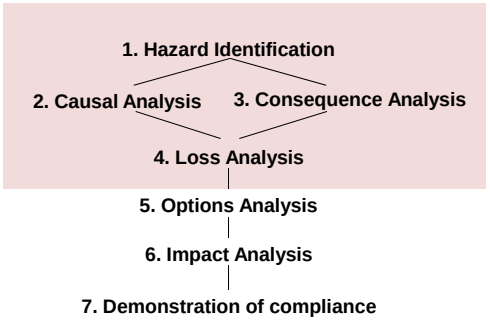



## IDENTIFYING HAZARDS

## Hazard identification

- Previous experience
  - What went wrong last time?
  - Service and maintenance records
  - Information on competitors' failures
- Brainstorming
- Hazard and Operability Analysis (HAZOP)
- Fault Tree Analysis (FTA)

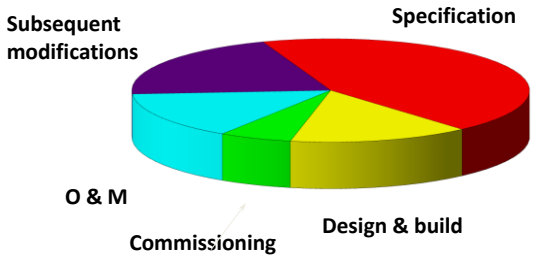
## Where does HAZOP fit?




***NB: Not everyone would agree with this definition – Trevor Kletz uses HAZOP for stages 1 to 5 – risk management, not just hazard identification***

## Why use a HAZOP?

***Reasons for unsafe failures of electronic systems***




*Source: S. Brown HSE*

## Why use a HAZOP?

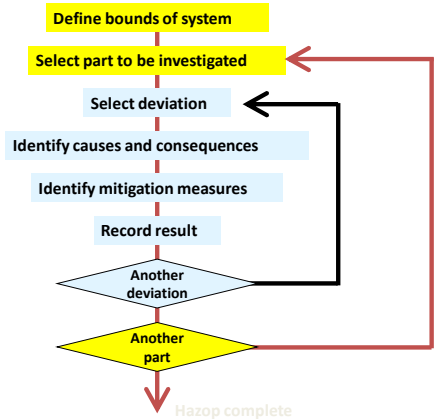
- Most accidents are caused by people doing the wrong thing, not technical failures
- HAZOP allows interactions of people and equipment to be investigated
- HAZOP identifies possible failures that "technical" analysis cannot see

## What is a HAZOP?

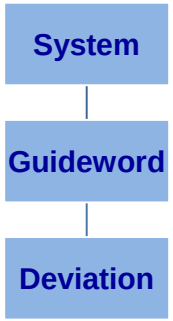
"HAZOP is a technique which provides opportunities for people to let their imaginations go free and think of all possible ways in which hazards or operating problems might arise, but – to reduce the chance that something is missed – it is done in a systematic way. . . The study is carried out by a team so that members can stimulate each other and build upon each other's ideas."

Trevor Kletz

## Structure of a HAZOP




## How to define a deviation ?




- Typical guidewords
- None
- More of
- Less of
- Part of
- More than
- Other than

## Example from chemical industry

| Guideword | Deviation | Possible causes |
|---|---|---|
| None | No flow | No hydrocarbon available from previous stage |
| | | Pump fails |
| | | Line blockage, valve closed in error |
| | | Line fracture |
| More of | More flow | Valve fails open |
| | More pressure | Valve closes with pump running |
| | | Thermal expansion due to solar gain with valves closed |

From Trevor Kletz, *Hazop and Hazan*, 1999

## Other possible guidewords / deviations

- Speed
  - Too fast
  - Too slow
  - Does not move
- Position
  - Too low
  - Too high
  - Wrong bearing
  - Off course laterally
- Weight
  - Too heavy
  - Too light
  - Unbalanced L-R
  - Unbalanced fore-aft
  - CG too high

## Who should be involved ?

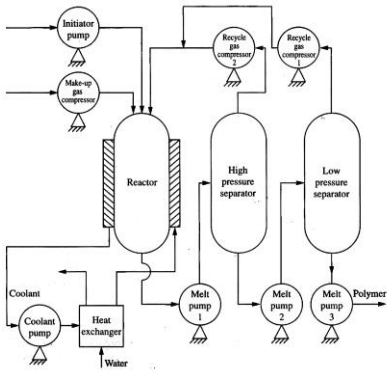
- Independent team leader
  - Understands HAZOP process
- Customer's chief engineer
  - Understands what was intended
- Operator
  - Can predict how operators might respond to system
- Supplier's project engineer
  - Understands what has been built
- Experts – if relevant *(see next slide)*
- Independent person who understands the technology

## Experts

- For process plant, do you need a chemist to predict what could happen when the reaction chamber is too hot, too cold, contaminated, etc.?
- For a power station control room, do you need an HF expert who could give a view on how the operators might respond to particular crises?
- For a process involving plasma or arcing, do you need a health physicist to identify hazards such as the emission of soft X-rays by a plasma or toxic decomposition products?

**A HAZOP is only as good as the people involved**

## Example of coarse scale Hazop: Polythene plant




Source NIOSH

## Part of coarse-scale HAZOP

- Guide word: HIGHER
- Deviation: Higher reactor temperature
- Consequences: Runaway reaction in reactor
- Causes:
  - Coolant pump to reactor fails
  - Coolant temperature too high
- Recommended actions:
  - Reactor temperature control
  - Reactor high temp. alarm
  - Pressure relief valve
  - Spare coolant pump
  - Alarm on coolant temp.

Source NIOSH

## When to programme a HAZOP

- Coarse scale
  - When an outline design exists and can be discussed
  - When it is reasonably clear what staffing / management processes will exist
  - When changes are possible without prohibitive cost
    - *"Design-stage gate review" ?*
- Detailed HAZOP
  - When the design is largely complete
  - Before "design freeze"
  - When drafts of the operating instructions are available

## Running a HAZOP

- There is no cast-iron rule on how to prepare a HAZOP
  - Choose suitable guidewords for the application
  - Decide on a coarse-scale or normal analysis
  - The important thing is "to provide opportunities for people to let their imaginations go free and think of all possible ways in which hazards or operating problems might arise - in a systematic way"*
- Make sure the team is competent but not overcommitted to the design (or intrinsically hostile!)
- Decide whether the HAZOP is to identify hazards or to come up with recommendations on how to resolve them
- Decide how HAZOP fits in to the other risk identification and management processes

* T Kletz

## Exercise – making a cup of tea

**Instructions (from packet)**

- Use only fresh water (do not reboil water)
- Use one teabag per cup
- Pour water onto tea as soon as it has boiled
- Stir immediately
- Leave for 3 – 5 minutes depending on preference
- Press bag against side of cup and remove

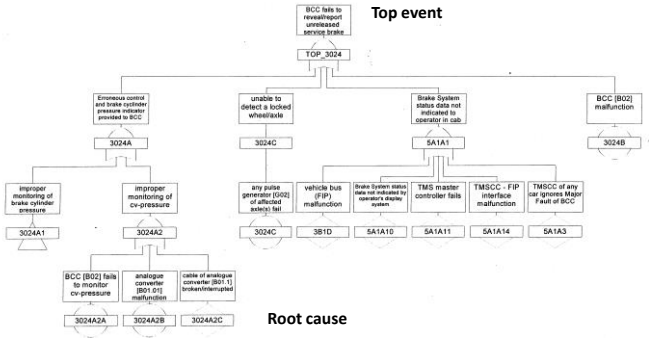
From Trevor Kletz, Hazop and Hazan, 1999

## Hazop results

| Step | Guide word | Deviation | Possible causes | Result | Action required |
|---|---|---|---|---|---|
| 1 | Non | No water kettle | No water supply | No tea | Keep bottle of water |
| | | | fails | | |
| | | | | | |

Please work in groups for 10 minutes to complete table

## Fault tree




If probabilities are associated with the root causes, combinational maths can be used to analyse the probability of a "top event"

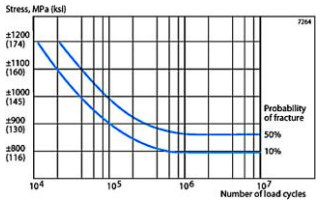
## When to use a fault tree

- Top down – only analyses what is important
- Reasonably easy to understand
- Identifies single-point failures
- Identifies possibility of double failures
  - and thus identifies maintenance requirements
- Can be used either for identification of hazardous failures or for quantitative analysis of failure modes

**NB: Fault tree concentrates on technical failures, not human factors**

# MANAGING RISKS

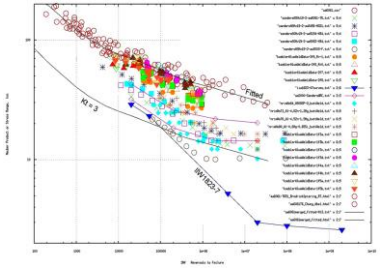
## Deterministic tools – fatigue stress




*The diagram shows a Wöhler S-N curve for Sandvik Chromflex (strip steel) type 7C27Mo2 under reverse bending stress*

- Calculate fatigue stresses in components
- Select materials so that probability of fracture is acceptably low

## Weld fatigue calculations for aluminium alloy



*Aluminium Weld Fatigue Calculation Curve, F A Conle, University of Waterloo, January 2012*

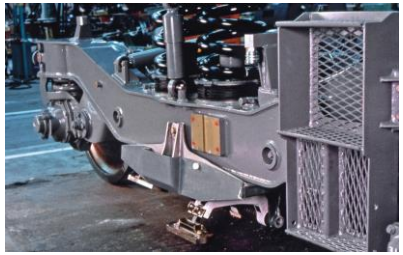
"In the ground vehicle industry much of the local stress analysis is done using elastic finite element (or simple stress*Kt) type calculations.

These elastic stresses are then transformed into local stresses and strains using some form of plasticity correction tool which requires a definition of the cyclic stress-strain curve along with the fatigue life curve.

The analysis method proposed here allows this type of correction to be made for aluminium weld data sets, and thus will conform to the standard methods presently applied in the ground vehicle industry."

## Stress calculations on Eurostar power bogie

- Calculated accelerations at axlebox up to 30g
- Computer modelling used to predict stresses in bogie frame
- Pessimistic weld fatigue characteristics assumed
- Designed for infinite fatigue life



## Example of FMECA (Pendolino auxiliary system)

| ID1 | Dwg. No | Ref | Item | Component | SFAS | Car type |
|---|---|---|---|---|---|---|
| 11676 | ZM5.IC1.Iss 6. | | BZ-SSK | Bell/buzzer | No | A |

| Function | Failure Mode | Fail rate fpmh | Fail mode ratio |
|---|---|---|---|
| Smoke siren kitchen | Buzzer O/C | 9.90E-02 | 1 |

| Fail mode fpmh | No off | Total fpmh | System effect | Train level effect |
|---|---|---|---|---|
| 1.00E+00 | 1 | 1.00E+00 | Smoke siren in kitchen permanently disabled | Siren will not sound in kitchen. Reduced diagnostic facility |

| Railway effect | HSC | Detection | Mitigating effects? | Dormant failure? | Remarks |
|---|---|---|---|---|---|
| Minor | 2 | Operator | None | Yes | Audible alarm on detector may provide some back up |

## When to use FMECA (or FEMA)

- Use other tools to identify critical subsystems or components, then use FMECA to analyse these areas in detail
- Typical areas where FMECA could be used:
  - Track circuit receiver
  - Ejector seat firing circuit
  - Control rod lowering system
- Do not attempt to do a FMECA on a whole project as you risk drowning in paper!

## Track circuits – part of the railway system

- Electric trains are part of a railway system
- The system consists of the major sub-systems:
  - A power supply – the energy source
  - A distribution and return current network
  - An electric train – the energy consumer
  - A safety system – "signalling"
  - A communication system – "command & control"
- Outside the railway system – neighbours
- In or out? – passengers

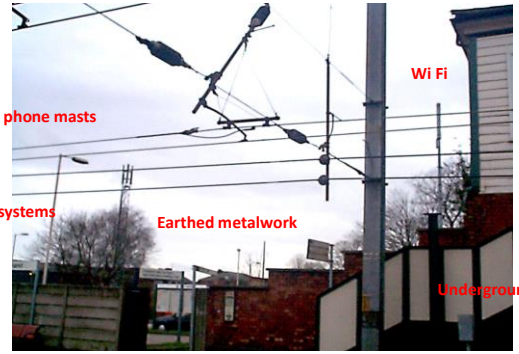


## The ideal railway environment

- Track not near other electrical systems
- Stone bridges (not steel)
- No near neighbours
- Clean ballast on consistent soil



## What normally happens



## Interference & susceptibility

- Each of these sub-systems contributes to the overall tendency to interference
- "Interference" is defined as "unwanted effects due to one system acting on another, causing malfunctions"
- Interference can affect safety and/or functionality
- The most desirable situation is that system components neither emit interference, nor are susceptible to it!
- Reality means interference is inevitable!



## Signalling Interference

- Signalling is obviously a safety-critical system
- The "**Train detection**" function is probably the most important part of it
- In UK generally we are concerned with the block system of signalling, where the track is divided into sections and only one train is allowed to be in each section at any one time, under the control of lineside colour-light signals
- A failure to detect that a train is on the track section is a **wrong-side safety failure** as it may lead to a second train being allowed into the section
- A failure to detect that a track section is clear is a **right-side failure** – a reliability problem – as it will normally prevent a train from being allowed to enter a section
- Signalling is often referred to as a "**fail-safe**" system



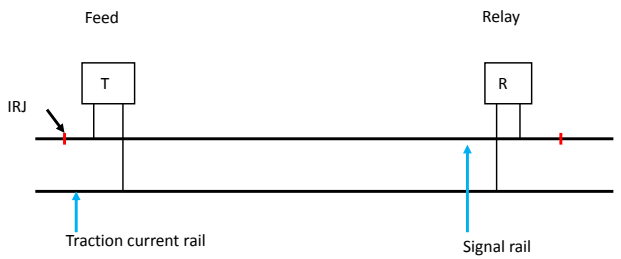
## Track Circuits & traction

- "Track circuits" use the track, either 1 or 2 rails with IRJs (insulated rail joints), as their circuit conductors to detect trains
- The voltage and current levels of a TC are typically a few volts and amps in the DC to low AF band
- The return traction current in the rails from a train can be up to 300A at 50Hz or 6800A at DC with high harmonic levels
- Modern TCs use modulated currents – an anti-mimicking technique – but there are plenty of old ones in service!

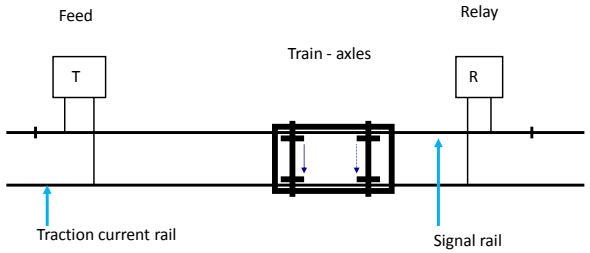


## Track Circuit Operation

Discussed in more detail in Engr 529



## Track circuit operation






## Longitudinal voltage

Apart from traction currents, there are other sources of track voltages:

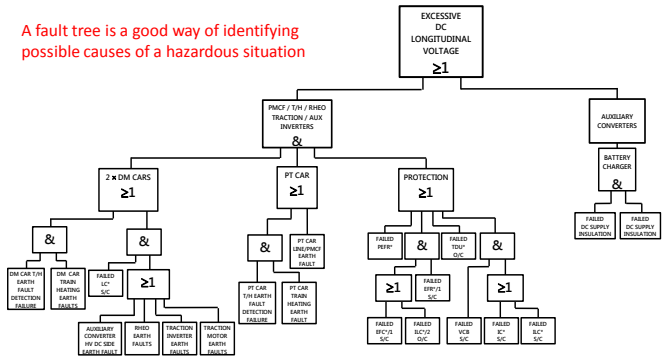
- Primarily from "earth faults" giving longitudinal currents in the vehicle body shell
- Protection against interference therefore involves prevention of such currents, by design, and detection of such currents in the event of a fault
- The reliability of the design is required to be high to give a low probability of interference

- The LV problem also occurs with non-electric trains & vehicles



## Class 334 DC Longitudinal Voltage Fault Tree

A fault tree is a good way of identifying possible causes of a hazardous situation

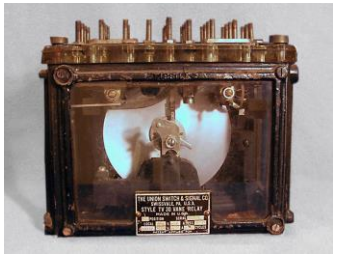


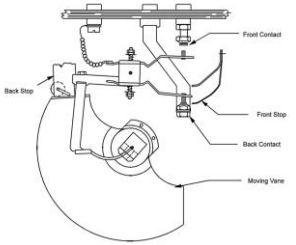



## Vane relay

A frequency and phase-sensitive detector for track circuit currents

Use FTA to identify potential hazards – FMECA to drill-down into the design





## IGBT drive on Pendolino

FMECA is a suitable tool for determining what faults are likely to cause interference

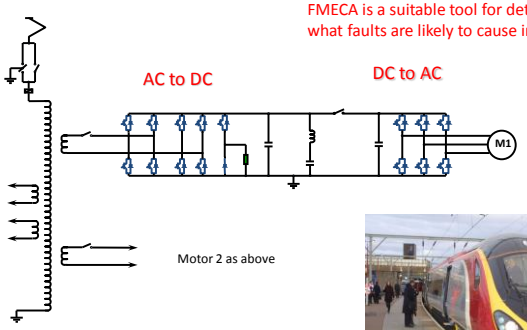



Photo: Alstom

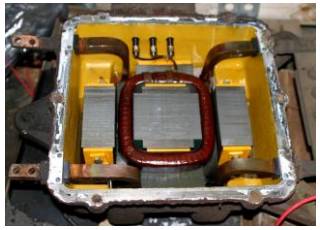
## Risk assessment - dealing with "defences"

- A traction converter could, theoretically, create currents that cause a signal to show a more permissive aspect.
- But, what is the probability of the fault occurring:
  - over a susceptible track circuit?
  - at the worst point on that track circuit?
  - on more than one motor?
  - at exactly the "right" train speed?
  - with the fault current exactly in-phase with the reference?

Use **quantitative risk assessment** – e.g. Monte Carlo technique – to assess likelihood of risk (see Engr 529)

## What assumptions do you make?

***New impedance bond***



***As found on track***

## Using the right tools

- **Hazard Log** – classifies hazards
- **Risk matrix** – assesses risk caused by hazards
- **Fault trees** – link components to hazards
- **Deterministic tools** – to ensure design can cope with stresses to which it will be subjected
- **FMECA** – drills down into critical components
- **HAZOP** – investigates human interaction