Energise to trip?
De-energise to trip?

Simple Choice?

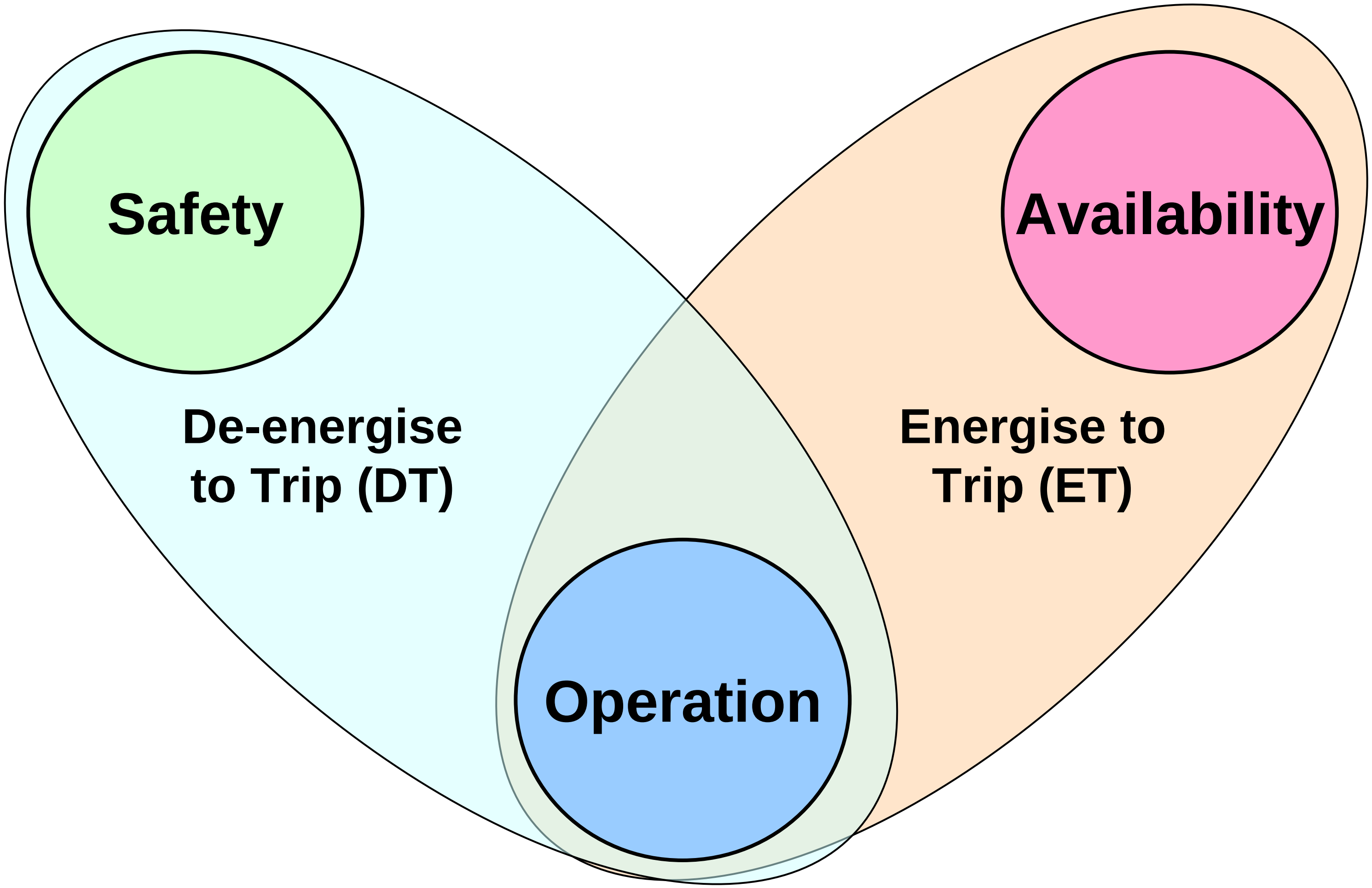
Tony Foord & Colin Howard
www.4-sightConsulting.co.uk
+44 (0)1 582 462 324

Examples

Overview

- Available guidance
- Why do trip systems fail?
- Trip system issues
- System failure modes
- 3 examples
- Architecture and Spurious trip frequency
- Diagnostics and Reverse acting transmitters
- References
- Conclusions

Traditional Choices



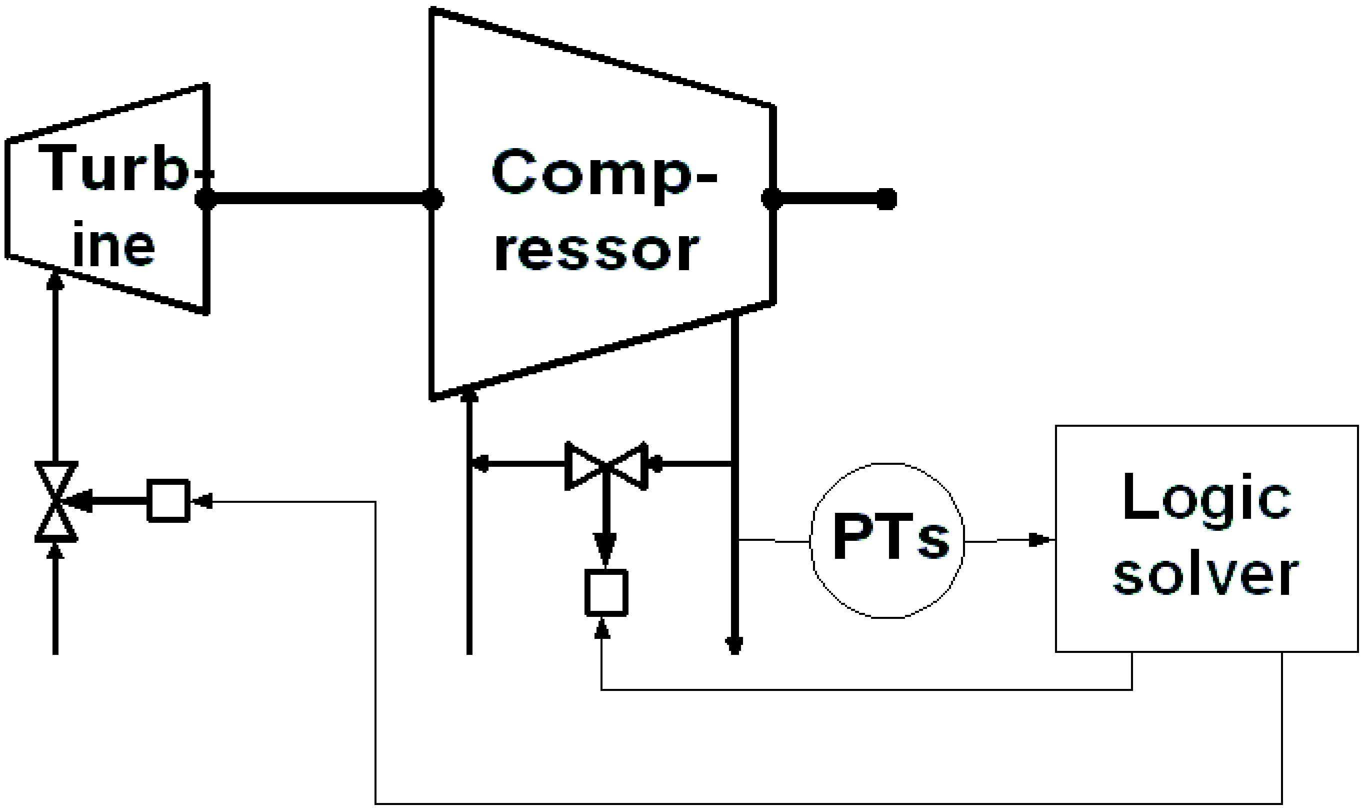
Available Guidance

- Very little specific guidance published
- One or two paragraphs only
    - Concentrate on “fail safe”

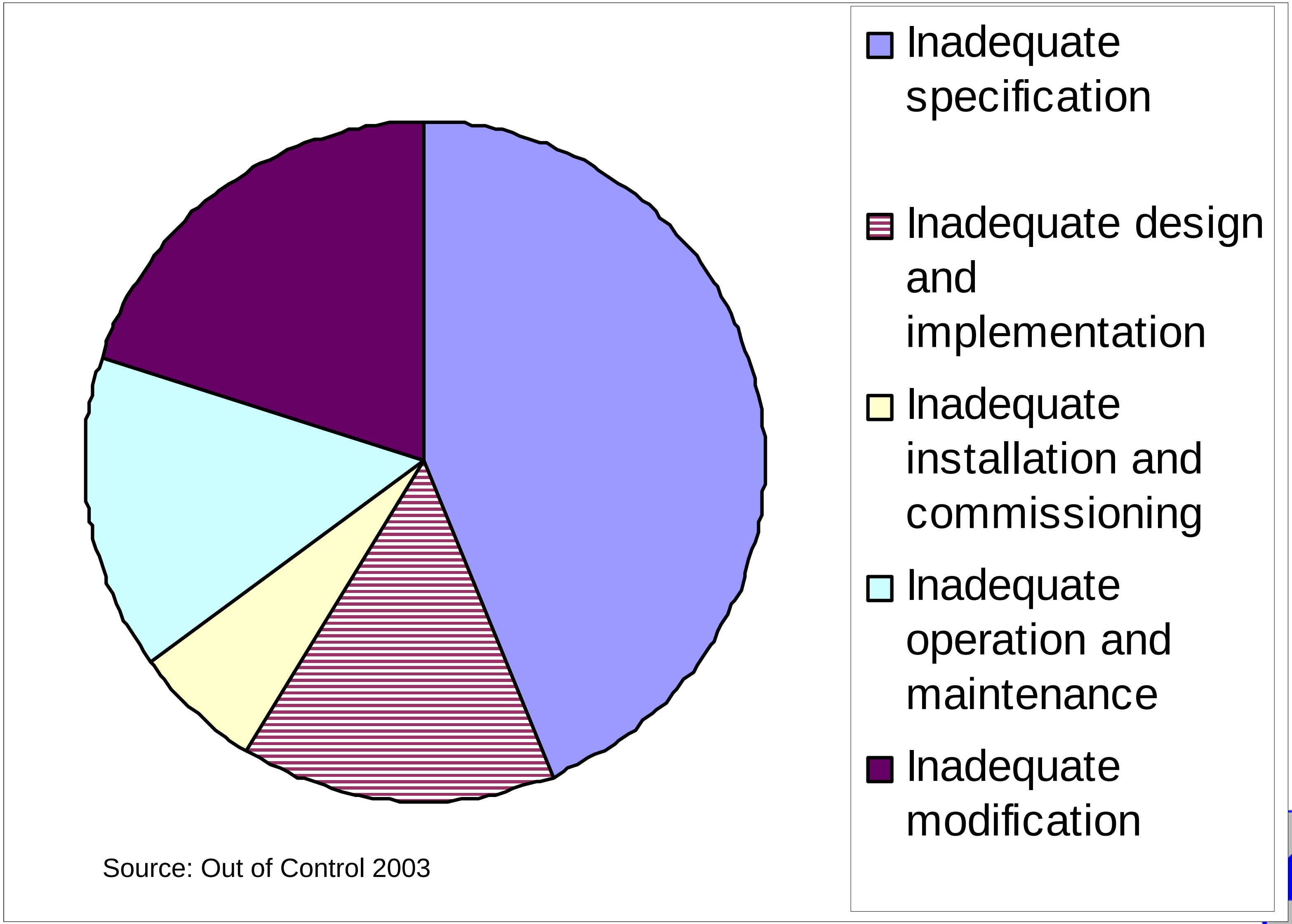
WHY?

- Custom and practice?
- Taken for granted?
- Principles assumed?

Overpressure protection for a turbine driven compressor



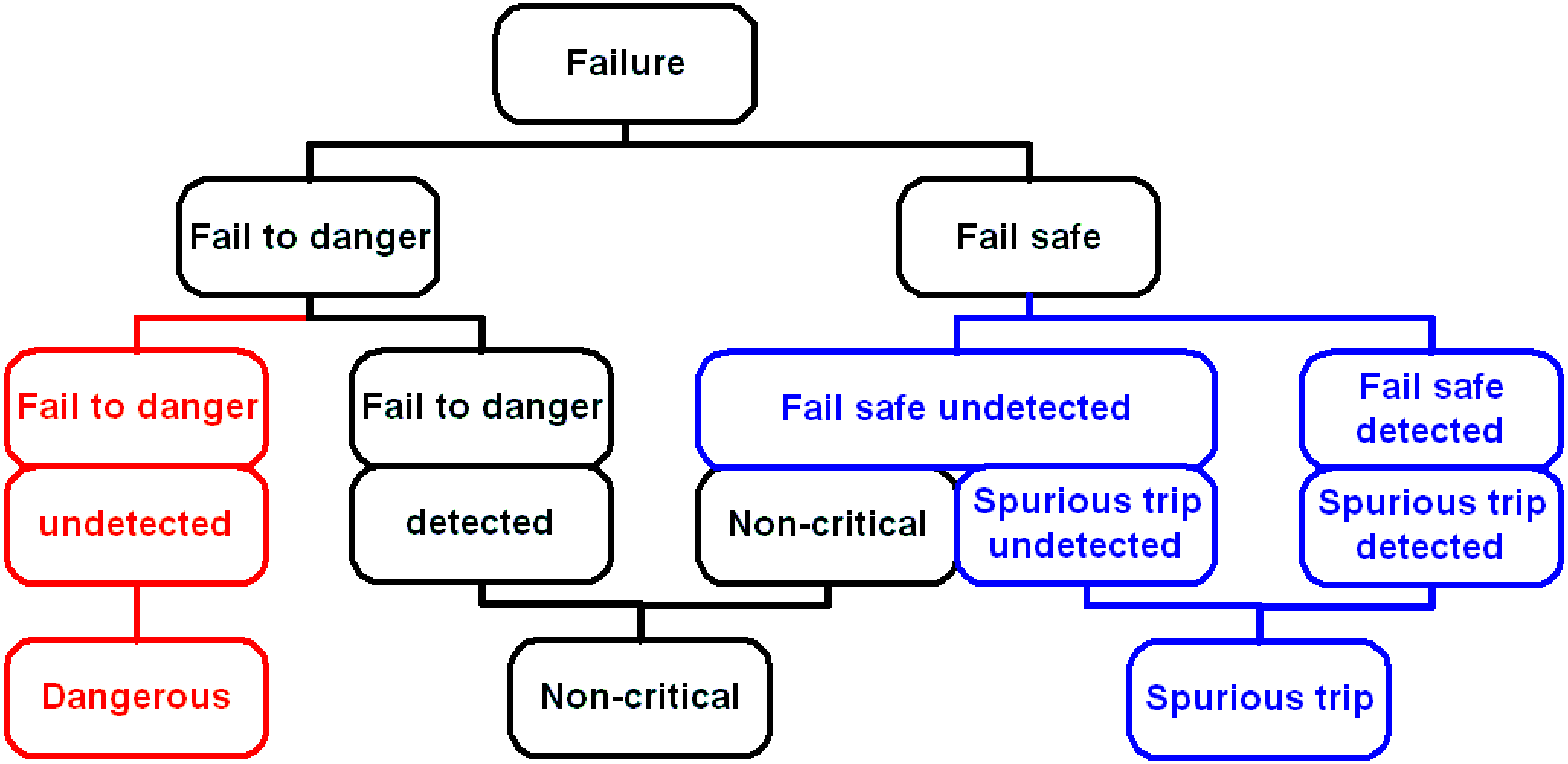
Why do trip systems fail?



Trip system issues

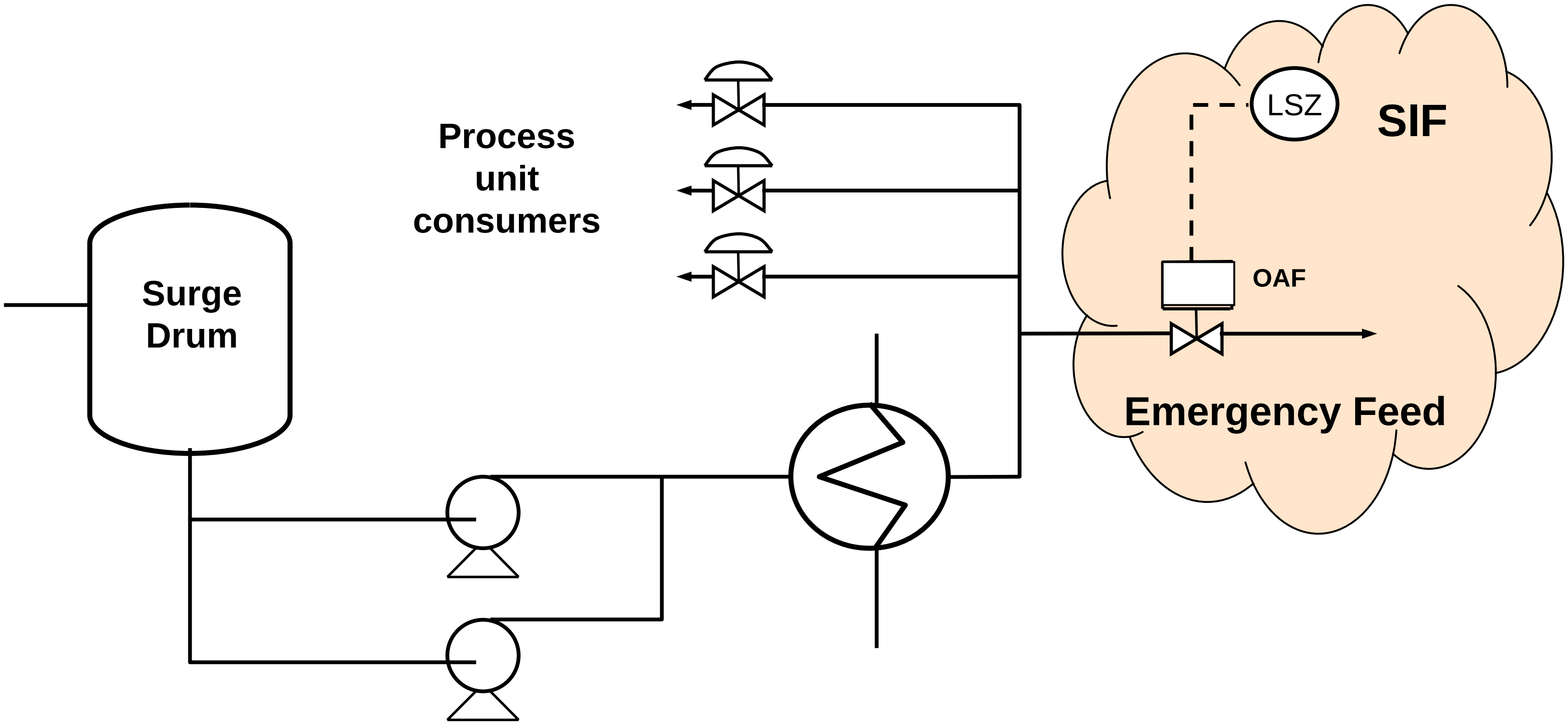
- SIF Requirements
- Passive / active systems
- Utility Requirements
- Effect on Fail to Danger and Spurious Trips
  - Design policy / Architecture / Overrides (defeats)
  - People issues
  - Operate / Test / Repair policies
  - Component reliability
  - Diagnostics

System failure modes

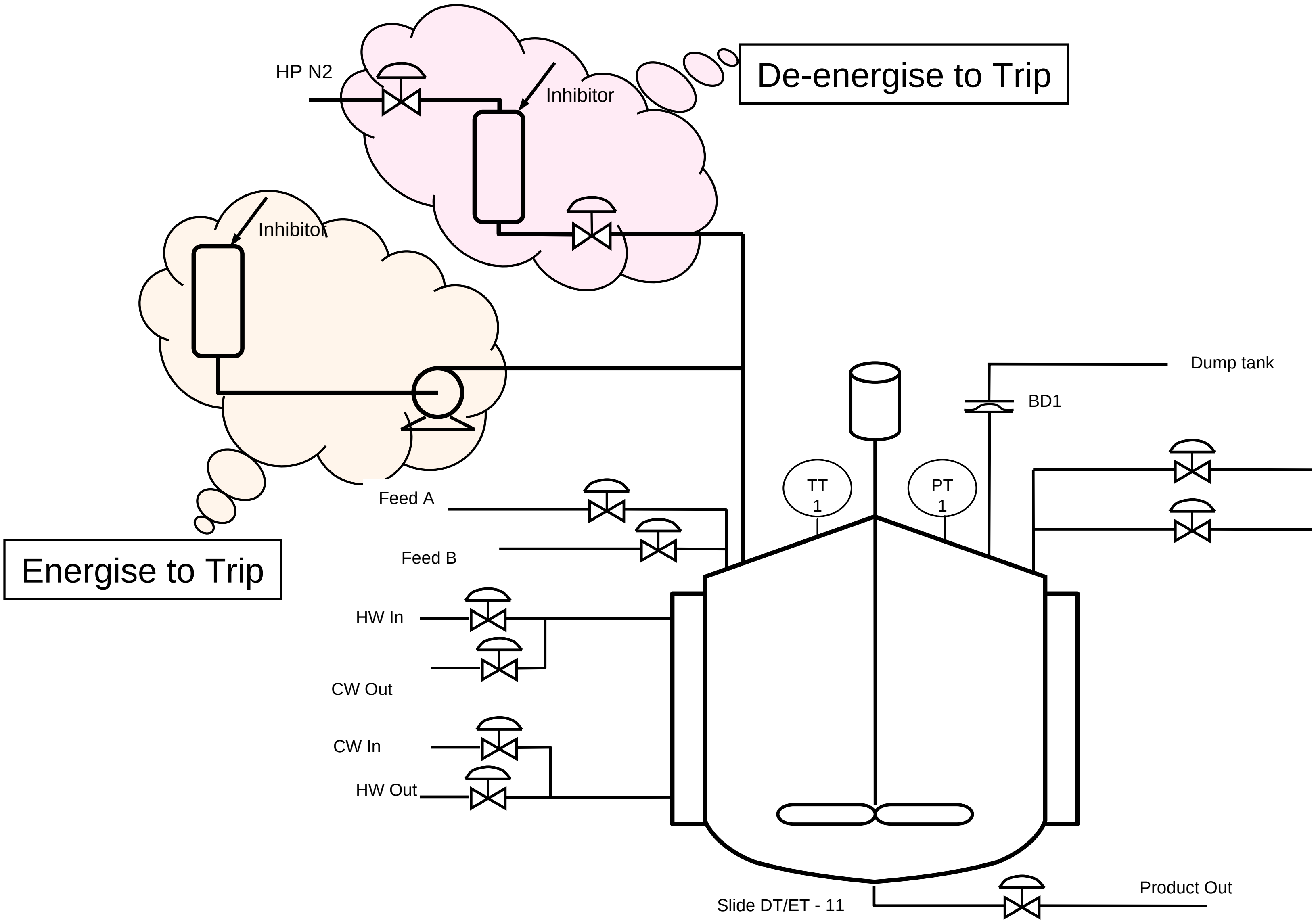


Source: Sintef PDS Method Handbook 2006

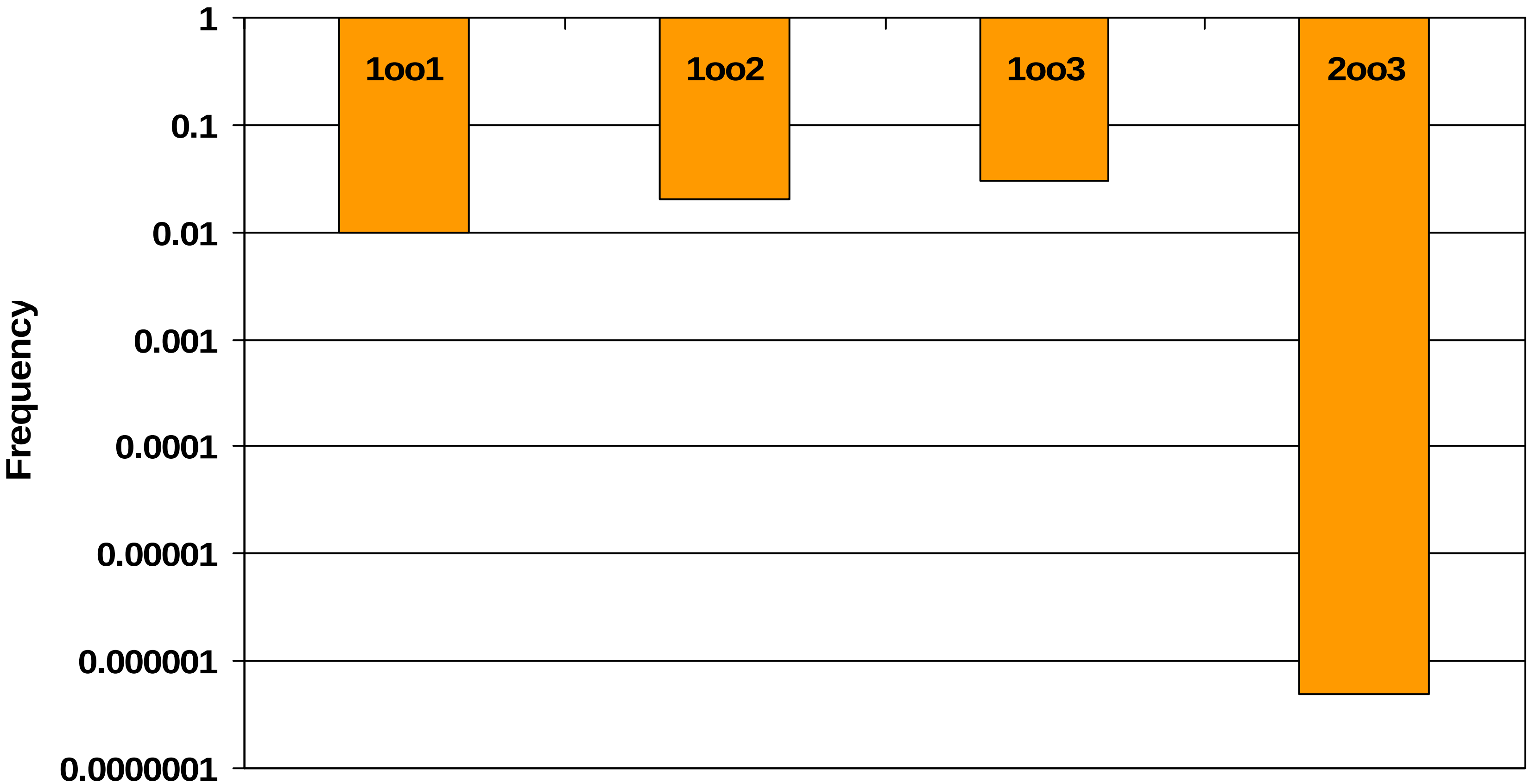
Energise or De-energise to Trip?



Addition of Reactor Inhibitor Options

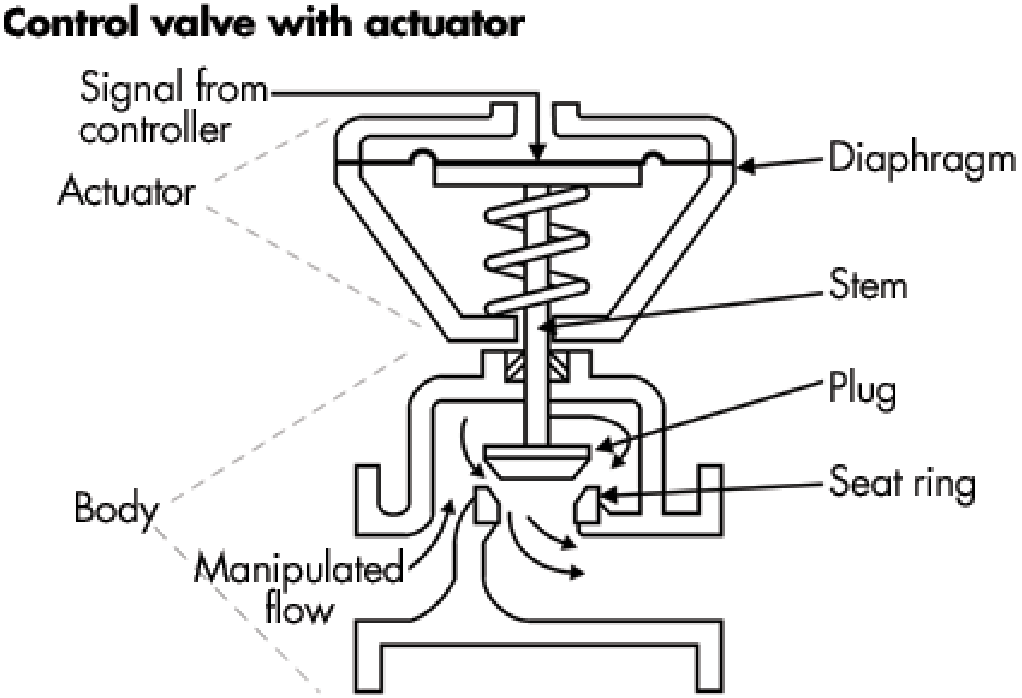


Architecture and Spurious Trip Frequency



Valve failure modes ~ 80% open

Failure mode	%
Blocking	5
External leak	15
Passing	60
Sticking	20



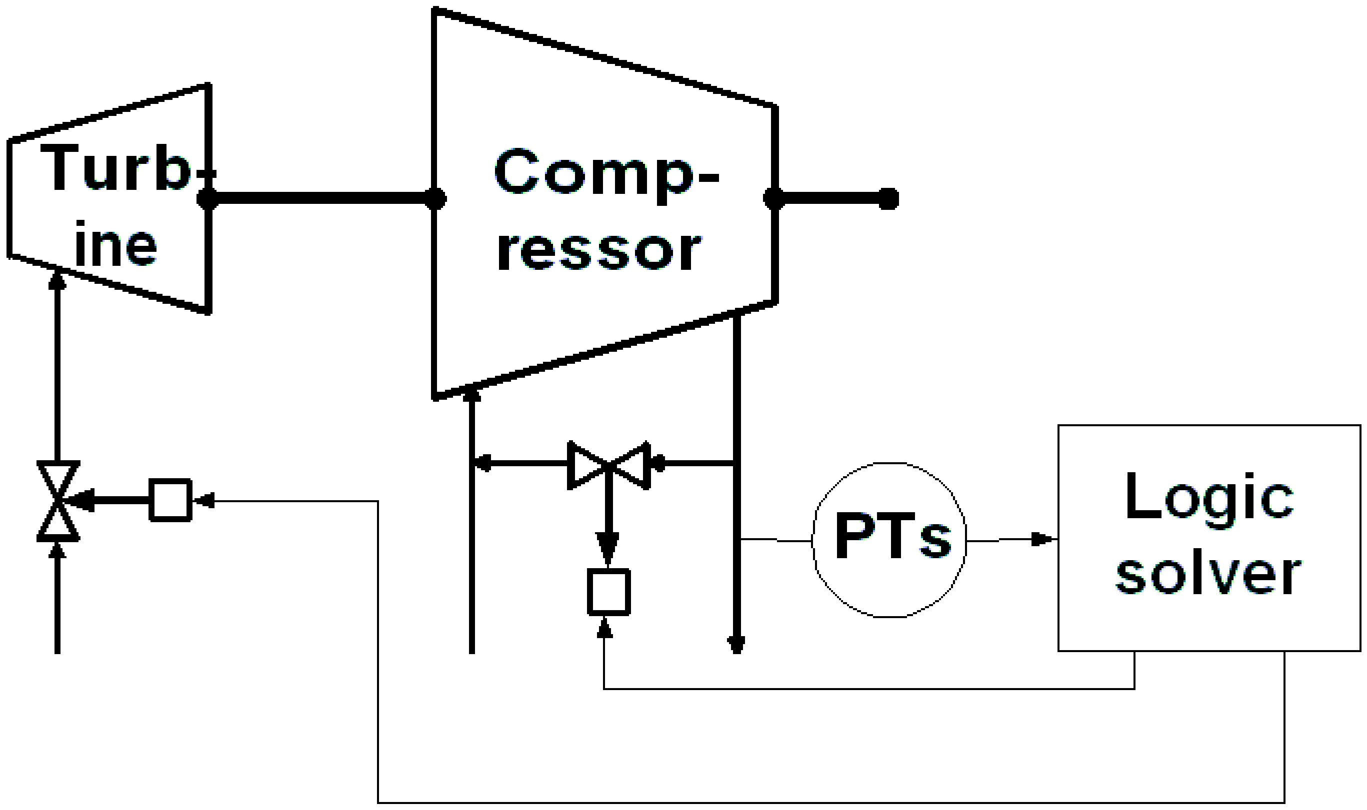
Data source: Smith: Reliability, Maintainability and Risk

Relay failure modes ~ 90% open

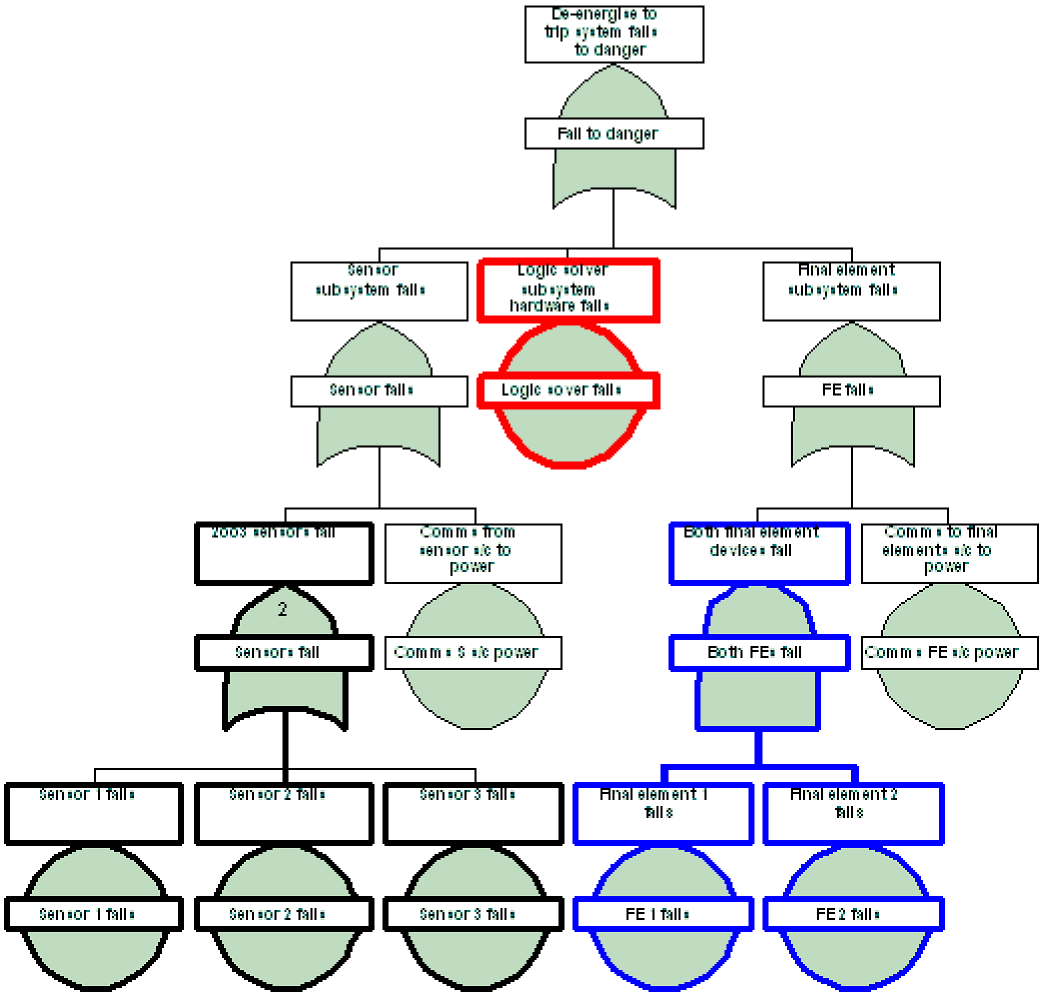
Failure mode	%
Contacts short circuit	10
Contacts open circuit	80
Coil	10

Data source: Smith: Reliability, Maintainability and Risk

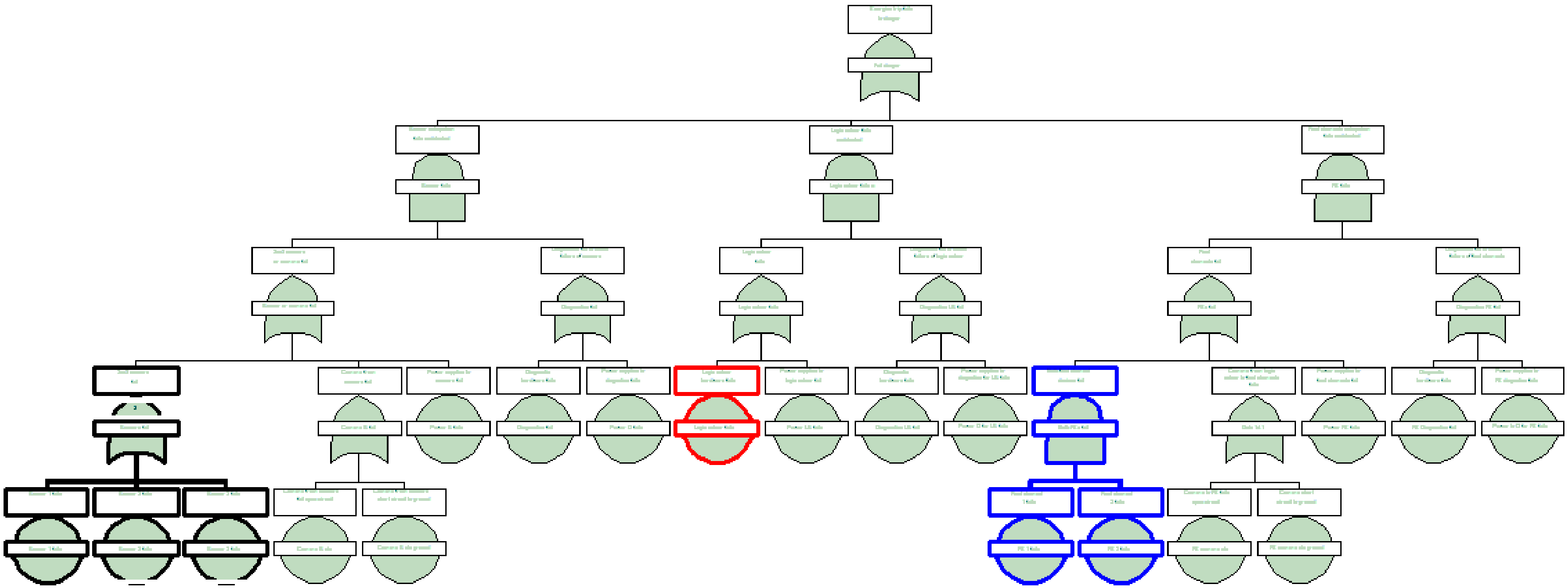
Overpressure protection for a turbine driven compressor



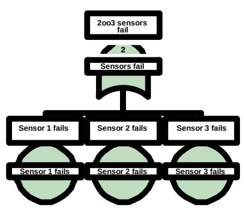
DT fails to danger



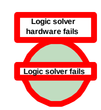
ET fails to danger



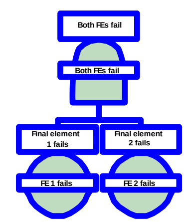
Key to Fault Trees



Sensors

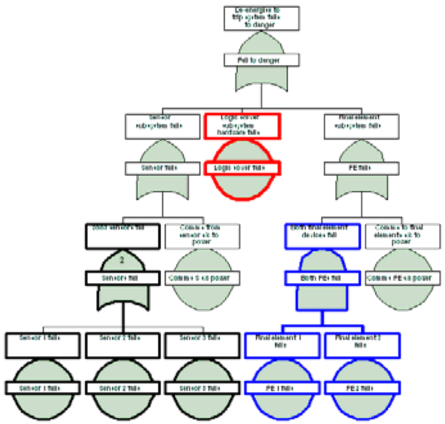


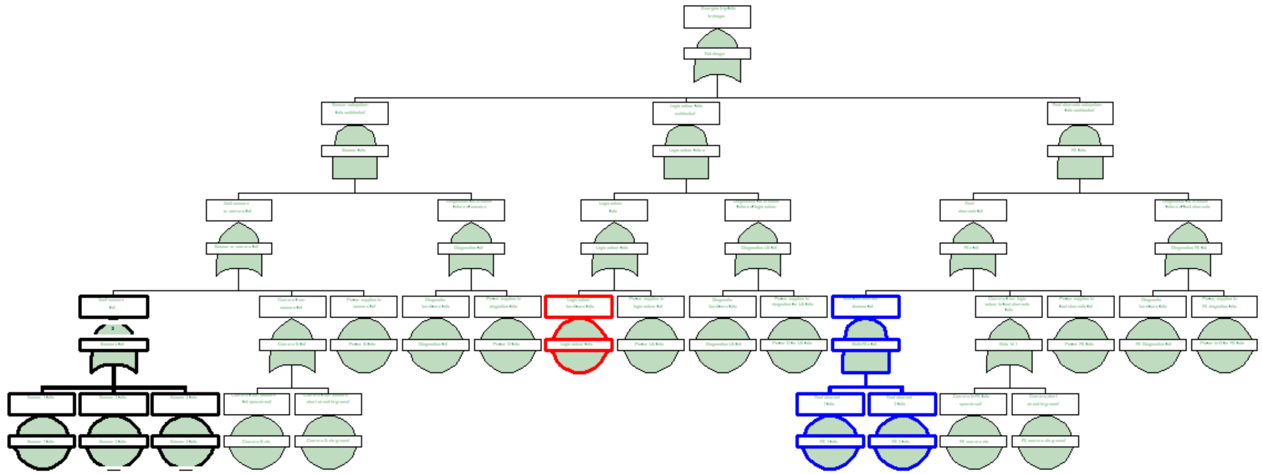
Logic solver



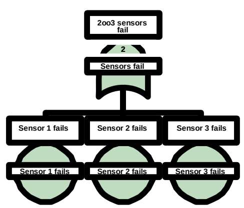
Final elements

DT (left) and ET fails to danger

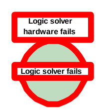




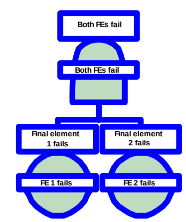
Key to Fault Trees



Sensors

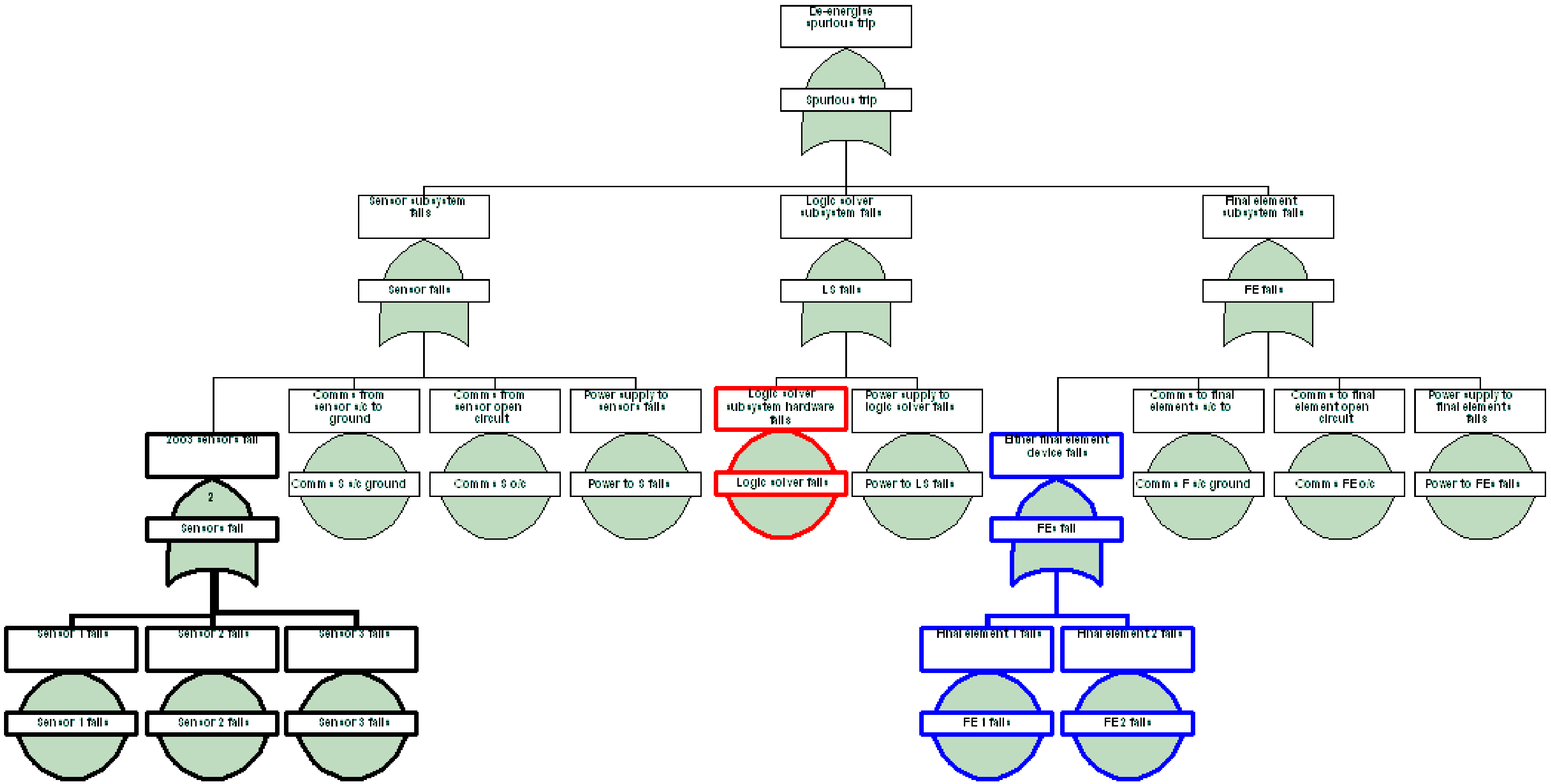


Logic solver

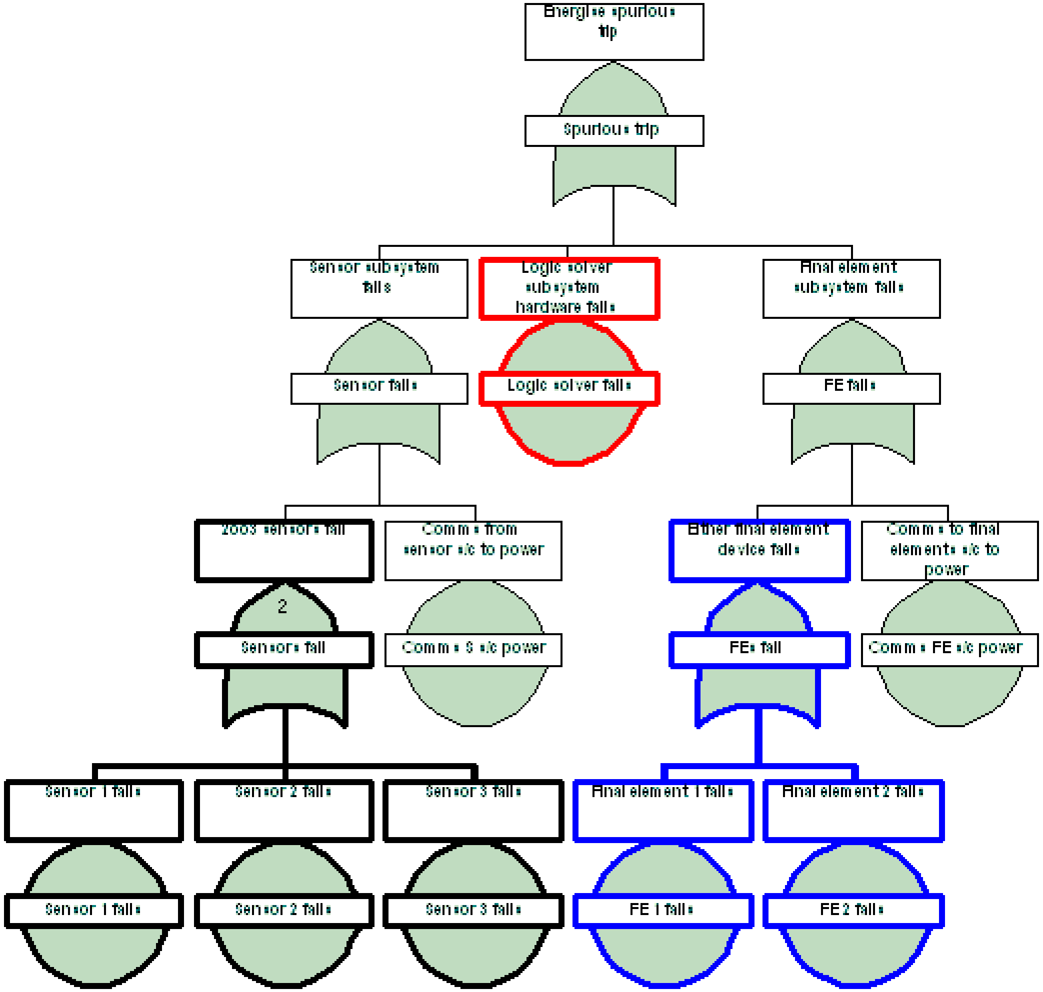


Final elements

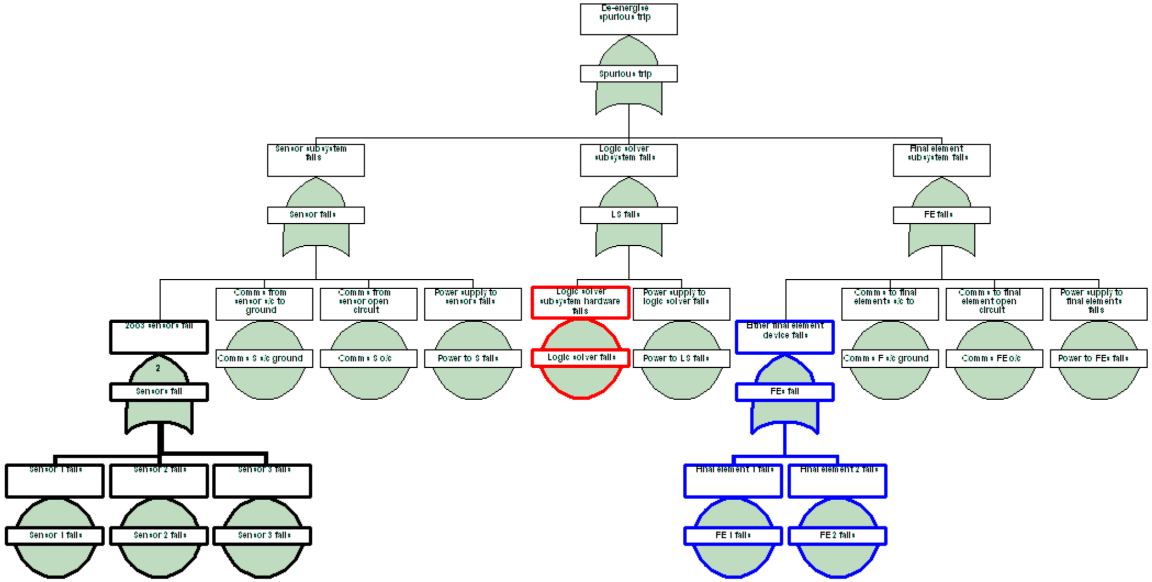
DT spurious trips

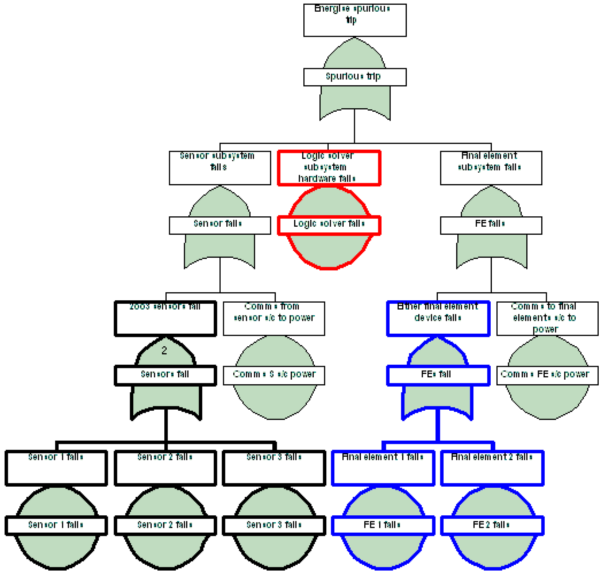


ET spurious trips

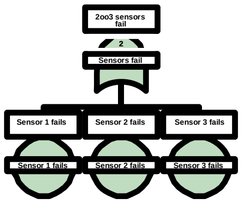


DT (left) and ET spurious trips

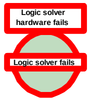




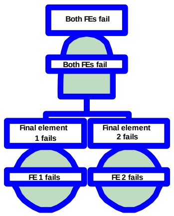
Key to Fault Trees



Sensors



Logic solver



Final elements

Diagnostics and Reverse Acting Transmitters

- Safety Function operates on “high” signals
- Transmitter failure leads to low signal
- ↓ Diagnostics require separate input
- ↑ Reverse acting transmitter provides automatic protection
  - Avoids technical complexity BUT introduces human factors and management complexity

References - 1

- http://www.hse.gov.uk/comah/sragtech/index.htm

  which includes links to Case Studies illustrating the importance of Control and Protection Systems, for example
  - Texaco Refinery - Milford Haven - Explosion and Fires (24/7/1994)
  - International Biosynthetics Ltd (7/12/1991)
  - BP Oil (Grangemouth) Refinery Ltd (22/3/1987)
  - Seveso - Icmesa Chemical Company (9/7/1976)

- Out of Control (2003), Second edition, HSE Books, ISBN 0-7176-2192-8
- IEC 61508 (1998 & 2000), Functional safety of electrical/electronic/programmable electronic safety-related systems Parts 1-7

References - 2

- Reliability Prediction Method For Safety Instrumented Systems. PDS Method Handbook (2006) SINTEF
- ISA-TR84.00.02 (2002) - Safety Instrumented Function (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 1: Introduction – page 57
- Reliability Maintainability and Risk (2001) David J Smith ISBN 0-7506-5168-7
- Safety Shutdown Systems Design, Analysis and Justification (1998) Paul Gruhn and Harry Cheddie ISBN1-55617-665-1
- Safety-Critical Computer Systems (1996), Neil Storey, ISBN 0-201-42787-7
- Safeware: system safety and computers (1995), Nancy Leveson, ISBN 0-201-11972-2

Available Guidance on ET

Is there anything else out there?

Conclusions

- Choice less clear-cut than at first sight
  – Need to look holistically
  – Wider than simply the core SIF
- ET can be made to work – possibilities of getting it wrong are greater
- ET inherently more complex
  – Does everyone understand the complexity?
- Some DT systems have ET elements