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

- Safety
- De-energise to Trip (DT)
- Operation
- Availability
- Energise to Trip (ET)
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?

- Inadequate specification
- Inadequate design and implementation
- Inadequate installation and commissioning
- Inadequate operation and maintenance
- Inadequate modification

Source: Out of Control 2003
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?

![Diagram showing process units and emergency feed systems.]

- Surge Drum
- Process unit consumers
- Emergency Feed
- OAF
- LSZ
- SIF
Addition of Reactor Inhibitor Options

Energise to Trip

De-energise to Trip

HP N2

Inhibitor

Feed A

Feed B

HW In

CW Out

CW In

HW Out

TT 1

PT 1

BD1

Dump tank

Vent

N2 In

Product Out

Slide DT/ET - 11

Inhibitor

Energise to Trip

De-energise to Trip
Architecture and Spurious Trip Frequency

Frequency
Valve failure modes ~ 80% open

<table>
<thead>
<tr>
<th>Failure mode</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking</td>
<td>5</td>
</tr>
<tr>
<td>External leak</td>
<td>15</td>
</tr>
<tr>
<td>Passing</td>
<td>60</td>
</tr>
<tr>
<td>Sticking</td>
<td>20</td>
</tr>
</tbody>
</table>

Data source: Smith: Reliability, Maintainability and Risk
Relay failure modes ~ 90% open

<table>
<thead>
<tr>
<th>Failure mode</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts short circuit</td>
<td>10</td>
</tr>
<tr>
<td>Contacts open circuit</td>
<td>80</td>
</tr>
<tr>
<td>Coil</td>
<td>10</td>
</tr>
</tbody>
</table>

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


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)


References - 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