Using software development standards to analyse incidents involving E/E/PE systems: The blade mill PLC case study

Mark Bowell
Health and Safety Executive

Chris Johnson
University of Glasgow

IRIA 03  17 September 2003
Overview

- Background and objectives
- PARCEL
- Case study
- Way forward
UK Health and Safety Executive
Mission statement

To ensure that risks to people’s health and safety from work activities is properly controlled
The Approved Code of Practice requires that employers:

*Adequately investigate the immediate and underlying causes of incidents and accidents to ensure that remedial action is taken, lessons are learnt and longer-term objectives are introduced.*

*It may be appropriate to record and analyse the results of monitoring activity, to identify any underlying themes or trends, which may not be apparent from looking at events in isolation.*
Industry today

- Fragmentation – impedes holistic root cause analysis and information sharing
- Contractors – lack of competence and experience
- Standards – main technical influence
- Existing systems – little knowledge of design history
- E/E/E/PES involvement – difficult for users to determine
- "Openness" culture – non-confidential reporting
Industry today

• Causal analysis techniques
  – Timelines, event trees and checklists
  – Accident trees plus structured checklists
  – Event chain modelling
  – Textual elaboration by experts

• Formal classification of causes is rare
• Focus on necessary immediate changes
• Good tracking of safety recommendations
Objectives

• To analyse the cause of E/E/PES incidents
• Incremental adoption
• Proportionality
• Trend analysis
• Information sharing
• Collation
• Match existing standards/guidance – IEC 61508
• Inform standard revision
Participants

• Adelard
• Glasgow Accident Analysis Group
• Blacksafe Consulting
• UK Health and Safety Executive
Industry sectors

- Onshore and offshore oil and gas
- Chemical plant
- Nuclear installations
- Railways
- Mines and quarries
- Factories
- Pharmaceuticals
- Marine
- Aviation
Roles

- End users
- Designers
- System suppliers/integrators
- Maintainers
Programmable electronic systems
Analysis of
Root
Causes for
Experience-based
Learning
<table>
<thead>
<tr>
<th>IEC 61508 lifecycle phase</th>
<th>Elicitation and analysis techniques</th>
<th>Event based techniques</th>
<th>Flowcharts and taxonomies</th>
<th>PRISMA</th>
<th>MORT</th>
<th>STAMP</th>
<th>TRIPOD</th>
<th>Argumentation techniques</th>
<th>CAE diagrams</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>S S</td>
<td>- - s</td>
<td>S s</td>
<td>S S</td>
<td></td>
<td>S</td>
<td></td>
<td>- S</td>
<td>S</td>
</tr>
<tr>
<td>Overall scope</td>
<td>S S</td>
<td>- - s</td>
<td>S S</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td></td>
<td>- S</td>
<td>S</td>
</tr>
<tr>
<td>Hazard and risk assessment</td>
<td>S S</td>
<td>s s s s</td>
<td>S S</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td></td>
<td>- S</td>
<td>S</td>
</tr>
<tr>
<td>Overall safety requirements</td>
<td>S S</td>
<td>- - s</td>
<td>s s</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td></td>
<td>- S</td>
<td>S</td>
</tr>
<tr>
<td>Allocation</td>
<td>S s</td>
<td>s - s</td>
<td>S S</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td></td>
<td>- S</td>
<td>S</td>
</tr>
<tr>
<td>Planning of I &amp; C, V and O &amp; M</td>
<td>- s</td>
<td>S s s S</td>
<td>S S</td>
<td>S S</td>
<td></td>
<td>S</td>
<td></td>
<td>- S</td>
<td>S</td>
</tr>
<tr>
<td>Realisation</td>
<td>- s</td>
<td>S s s S</td>
<td>S S</td>
<td>S s</td>
<td>-</td>
<td>S</td>
<td></td>
<td>S -</td>
<td>S</td>
</tr>
<tr>
<td>Installation and commissioning</td>
<td>- s</td>
<td>S S s S</td>
<td>S s s S</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S s -</td>
<td>S</td>
</tr>
<tr>
<td>Validation</td>
<td>s s</td>
<td>S s s S</td>
<td>S s s S</td>
<td>S s</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S s -</td>
<td>S</td>
</tr>
<tr>
<td>Operation and maintenance</td>
<td>s S</td>
<td>S s s S</td>
<td>S s s S</td>
<td>S s</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S s -</td>
<td>S</td>
</tr>
<tr>
<td>Modification</td>
<td>- S</td>
<td>S s s S</td>
<td>S s s S</td>
<td>S s</td>
<td></td>
<td>S</td>
<td>S</td>
<td>S s -</td>
<td>S</td>
</tr>
<tr>
<td>IEC 61508 common requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competence</td>
<td>s s</td>
<td>s s s S</td>
<td>S s s S</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>s s -</td>
<td>S</td>
</tr>
<tr>
<td>Lifecycle</td>
<td>- s</td>
<td>s s s S</td>
<td>S s s S</td>
<td>S S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>s s -</td>
<td>S</td>
</tr>
<tr>
<td>Verification</td>
<td>s s</td>
<td>s s s S</td>
<td>s s s S</td>
<td>S s</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>s s -</td>
<td>S</td>
</tr>
<tr>
<td>Safety management</td>
<td>s s</td>
<td>s s s S</td>
<td>s s s S</td>
<td>S s</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>s s -</td>
<td>S</td>
</tr>
<tr>
<td>Documentation</td>
<td>s s</td>
<td>s s s S</td>
<td>s s s S</td>
<td>S s</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>s s -</td>
<td>S</td>
</tr>
<tr>
<td>Functional safety assessment</td>
<td>s s</td>
<td>s s s S</td>
<td>s s s S</td>
<td>S s</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>s s -</td>
<td>S</td>
</tr>
</tbody>
</table>
A: Information elicitation
(Standard report forms)

B: Causal analysis

Simplified flowcharting
(Using preset questions leading to IEC 61508 lifecycle and common requirements)

Reconstruct incident
(ECF modelling)

Distinguish causal factors
(Counterfactual reasoning)

Root cause classification
(Using IEC 61508 lifecycle and common requirements)

C: Generation of recommendations

Simpler/lower risk mishaps

More complex/higher risk mishaps
## End user classification

<table>
<thead>
<tr>
<th>IEC 61508 lifecycle reference</th>
<th>IEC 61508 common requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>System assessment</td>
<td>Safety management</td>
</tr>
<tr>
<td>Safety requirements and allocation</td>
<td>Lifecycle</td>
</tr>
<tr>
<td>E/E/PES installation and commissioning planning</td>
<td>Competence</td>
</tr>
<tr>
<td>E/E/PES validation planning</td>
<td>Verification</td>
</tr>
<tr>
<td>E/E/PES operation and maintenance planning</td>
<td>Documentation</td>
</tr>
<tr>
<td>E/E/PES realisation</td>
<td>Functional safety assessment</td>
</tr>
<tr>
<td>E/E/PES installation and commissioning</td>
<td></td>
</tr>
<tr>
<td>E/E/PES validation</td>
<td></td>
</tr>
<tr>
<td>E/E/PES operation and maintenance</td>
<td></td>
</tr>
<tr>
<td>E/E/PES modification</td>
<td></td>
</tr>
<tr>
<td>IEC 61508 lifecycle phase</td>
<td>Classification</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System assessment</td>
<td>1 LTA hazard and risk assessment</td>
</tr>
<tr>
<td>E/E/PES operation and</td>
<td>1 LTA operation procedures</td>
</tr>
<tr>
<td>maintenance</td>
<td>2 Operation procedures not impact assessed</td>
</tr>
<tr>
<td></td>
<td>3 Operation procedures not applied</td>
</tr>
<tr>
<td></td>
<td>4 LTA maintenance procedures</td>
</tr>
<tr>
<td></td>
<td>5 Maintenance procedures not impact assessed</td>
</tr>
<tr>
<td></td>
<td>6 Maintenance procedures not applied</td>
</tr>
<tr>
<td></td>
<td>7 No routine operation or maintenance audits</td>
</tr>
<tr>
<td></td>
<td>8 Test interval not sufficient</td>
</tr>
<tr>
<td></td>
<td>9 LTA permit/hand over procedures</td>
</tr>
<tr>
<td></td>
<td>10 LTA procedures to monitor system performance</td>
</tr>
<tr>
<td></td>
<td>11 Tools incorrectly selected or applied</td>
</tr>
<tr>
<td>E/E/PES modification</td>
<td>1 LTA procedures applied to initiate modification in the event of systematic</td>
</tr>
<tr>
<td></td>
<td>failures or vendor notification of faults</td>
</tr>
<tr>
<td></td>
<td>2 LTA authorisation procedure</td>
</tr>
<tr>
<td></td>
<td>3 LTA impact analysis</td>
</tr>
<tr>
<td></td>
<td>4 LTA modification plan (including sufficient lifecycle activities)</td>
</tr>
<tr>
<td></td>
<td>5 LTA implementation of modification plan</td>
</tr>
<tr>
<td></td>
<td>6 LTA manufacturers information</td>
</tr>
<tr>
<td></td>
<td>7 LTA verification and validation</td>
</tr>
</tbody>
</table>
Blade Mill PLC case study

- Details from http://www.msha.gov/fatals/1997/ftl97m01.htm

- Gravel wash plant
- Blade mill to ‘precondition’ aggregates prior to wet screening
- Mill consisted of two interlocking screws driven by two 40-horse power motors
- Motors operated from a control center in a trailer 30 metres away
Blade Mill PLC case study

- At the start of this day, material was frozen inside mill and broken paddle tips and wearing shoes needed replacing.
- Material thawed using a propane burner, mechanic signalled to foreman to start motors to check that blades are free.
- Foreman switches buttons to ‘off’ and moves to another task elsewhere.
- Foreman returns to help carry out repairs, but is then called to assist an electrician working on a faulty circuit breaker.
- Circuit breaker in control center had been tripping out after 10-15 minutes of operation, resulting in loss of control power to the wash plant components.
Blade Mill PLC case study

- The electrician switched the breaker on and together with the foreman watched it for several minutes without observing a trip.
- The electrician then switched it off and began diagnosing the problem.
- Meanwhile the foreman returned to check on the mechanic.
- As he was leaving the control center, he noticed that the blade mill buttons were in the ‘run’ position.
- He pushed them off and continued to the mill where he found the mechanic entangled in the blades.
- Paramedics later pronounced the mechanic dead at the scene.
Blade Mill PLC case study

- A modification to the PLC three months earlier had resulted in power being unintentionally returned to components following a power failure, if their switches had been left ‘on’.

Investigators concluded:
- The mechanic turned the mill back on to clear some remaining frozen material while the foreman was away the first time
- The mill operated until the circuit breaker tripped out
- The mechanic went back to work on the mill without shutting off any switches
A: Information elicitation
(Standard report forms)

Reconstruct incident
(ECF modelling)

Distinguish causal factors
(Counterfactual reasoning)

Root cause classification
(Using IEC 61508 lifecycle and common requirements)

Simplified flowcharting
(Using preset questions leading to IEC 61508 lifecycle and common requirements)

C: Generation of recommendations

B: Causal analysis

Simpler/lower risk mishaps

More complex/higher risk mishaps

Reconstruct incident
(ECF modelling)

Distinguish causal factors
(Counterfactual reasoning)

Root cause classification
(Using IEC 61508 lifecycle and common requirements)
<table>
<thead>
<tr>
<th><strong>Initial incident report</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Your name</strong></td>
</tr>
<tr>
<td><strong>Date of report</strong></td>
</tr>
<tr>
<td><strong>Date of incident</strong></td>
</tr>
<tr>
<td><strong>Time of incident</strong></td>
</tr>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td><strong>Reference number</strong></td>
</tr>
<tr>
<td><strong>Location of Incident</strong></td>
</tr>
<tr>
<td><strong>Was any person hurt?</strong></td>
</tr>
<tr>
<td><strong>Did any damage or loss of production occur?</strong></td>
</tr>
<tr>
<td><strong>Could this have led to more serious consequences?</strong></td>
</tr>
<tr>
<td><strong>Has this problem occurred before?</strong></td>
</tr>
</tbody>
</table>
| **Electrical/electronic equipment involved** | Kolberg Products Model 6500 blade mill  
GE Fanuc 90-30 Programmable Logic Controller |
| **Electrical/electronic equipment cause or failure** | Unwarranted blade mill start-up |
| **Describe the incident** | Mechanic assigned to thaw frozen material inside the blade mill and then replace broken and worn paddle tips and wearing shoes. He was found entangled in the blades. Controls were found in ‘run’ position and circuit breaker had been reset after previously tripping out, so mill must have restarted while he was working. |
A: Information elicitation
(Standard report forms)

B: Causal analysis
- Simplified flowcharting
  (Using preset questions leading to IEC 61508 lifecycle and common requirements)

C: Generation of recommendations

- Reconstruct incident
  (ECF modelling)
- Distinguish causal factors
  (Counterfactual reasoning)
- Root cause classification
  (Using IEC 61508 lifecycle and common requirements)

Simpler/lower risk mishaps
More complex/higher risk mishaps
### Would the incident have been prevented if

<table>
<thead>
<tr>
<th>System concept</th>
<th>Design</th>
<th>Installation &amp; commissioning</th>
<th>Validation</th>
<th>Operation &amp; maintenance</th>
<th>Modification</th>
<th>Competence</th>
<th>Lifecycle</th>
<th>Verification</th>
<th>Safety management</th>
<th>Documentation</th>
<th>Safety assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>hazard and risk analysis had considered all modes of operation and causes</td>
<td>- operator facilities had been designed better - the installation design had been different</td>
<td>the equipment had been installed according to design</td>
<td>- operation facilities had been checked during validation</td>
<td>- operation procedures were applied - operation procedures were improved</td>
<td>- operation facilities had been reviewed during impact analysis</td>
<td>- operation or maintenance staff were more competent</td>
<td>- responsibilities were defined better</td>
<td>- a better verification scheme had been in place</td>
<td>- safety culture was improved - audits were more frequent</td>
<td>- documentation was clear and sufficient</td>
<td>- operation and maintenance phase had been assessed</td>
</tr>
<tr>
<td>hazard and risk analysis had considered all modes of operation and causes</td>
<td>additional actions had been specified - actions had been faster - final actuation device were improved</td>
<td>- the equipment had been installed according to design</td>
<td>- operation facilities had been fully checked</td>
<td>- correct maintenance procedure had been used - maintenance procedure was improved - proof testing was more frequent</td>
<td>- necessary system actions had been reviewed during impact analysis</td>
<td>- modification had been carried out by more competent staff</td>
<td>- modification lifecycle was better defined</td>
<td>- a better verification scheme had been in place</td>
<td>- accountabilities were better defined - suppliers had been reviewed</td>
<td>- documentation had been updated</td>
<td>- modification had been assessed</td>
</tr>
<tr>
<td>hazard and risk analysis had considered all modes of operation and causes</td>
<td>design requirements were better documented</td>
<td>- mitigation system had been installed according to design</td>
<td>- operation facilities had been fully checked</td>
<td>- correct operation procedure had been used - operation procedure was improved</td>
<td>- necessary system actions had been reviewed during impact analysis</td>
<td>- a better verification scheme had been in place</td>
<td>- responsibilities were defined better</td>
<td>- a better verification scheme had been in place</td>
<td>- documentation had been updated</td>
<td>- documentation had been assessed</td>
<td>- operation and maintenance phase had been assessed</td>
</tr>
<tr>
<td>hazard and risk analysis had considered all modes of operation and causes</td>
<td>mitigation system had been specified - mitigation system had been better designed</td>
<td>- the equipment had been installed according to design</td>
<td>- operation facilities had been fully checked</td>
<td>- mitigation procedures were applied - mitigation procedures were improved - mitigation system was proof tested more frequently</td>
<td>- need for mitigation had been reviewed during impact analysis</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- documentation had been updated</td>
<td>- documentation had been assessed</td>
<td>- operation and maintenance phase had been assessed</td>
</tr>
<tr>
<td>hazard and risk analysis had considered all modes of operation and causes</td>
<td>- operator facilities had been designed better - the installation design had been different</td>
<td>- the equipment had been installed according to design</td>
<td>- operation facilities had been fully checked</td>
<td>- operation procedures had been applied - operation facilities or procedures were improved</td>
<td>- need for mitigation had been reviewed during impact analysis</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- documentation had been updated</td>
<td>- documentation had been assessed</td>
<td>- operation and maintenance phase had been assessed</td>
</tr>
<tr>
<td>hazard and risk analysis had considered all modes of operation and causes</td>
<td>- Log failure and check - if dangerous failure rate is in line with design assumptions - all expected actions occurred and no unexpected actions occurred - if safe failure causes any unexpected actions occurred</td>
<td>- Log demand and check - if demand rate is in line with design assumptions - if demand cause was predicted in hazard and risk analysis</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- need for mitigation had been reviewed during impact analysis</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- a better verification scheme had been in place</td>
<td>- documentation had been updated</td>
<td>- documentation had been assessed</td>
<td>- operation and maintenance phase had been assessed</td>
</tr>
</tbody>
</table>
System operates correctly to prevent hazard

System fails on proof test

System fails to take action when required or takes action when not required

Setting is incorrect
Failure caused by maintenance

Yes

Would the incident have been prevented if

<table>
<thead>
<tr>
<th>System concept</th>
<th>– hazard and risk analysis had considered all modes of operation and causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>– maintenance facilities had been designed adequately</td>
</tr>
<tr>
<td>Installation &amp; commissioning</td>
<td>– the maintenance facilities had been installed according to design</td>
</tr>
<tr>
<td>Validation</td>
<td>– maintenance facilities had been fully checked</td>
</tr>
<tr>
<td>Operation &amp; maintenance</td>
<td>– correct maintenance procedure had been used</td>
</tr>
<tr>
<td></td>
<td>– maintenance procedure was improved</td>
</tr>
<tr>
<td></td>
<td>– permit procedures were improved</td>
</tr>
<tr>
<td>Modification</td>
<td>– maintenance facilities or procedures had been reviewed during impact analysis</td>
</tr>
<tr>
<td>Causal Event</td>
<td>IEC 61508 Classification</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>
| PLC allows automatic restart of equipment following power trip             | **Hazard and risk assessment**                | System fails to take required action ->                       | The reprogramming of the PLC allowed for a situation in which equipment was automatically restarted following a power trip. Reprogramming is likely to have prevented a restart without operator intervention had this potential hazard been recognised.  
(Note: if there were evidence that this hazard had been considered during the reprogramming then the causal analysis might have focussed more on validation to ensure that the PLC prevented the automated restart hazard.)                                                                                     |
| Failure to warn mechanic that power circuits not locked out during maintenance on circuit breaker. | **Operation and maintenance**                | System fails to take required action ->                       | On-site investigators argued that the foreman was aware of the relationship between the circuit breakers and the mill. The incident might have been avoided if they had followed a documented maintenance procedure or permission to work scheme that would have locked out all equipment affected by the maintenance on the circuit breakers.                                                                                                                                   |
|                                                                             |                                               | Failure caused by maintenance ->                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                                                             |                                               | Hazard and risk analysis had not considered all modes of operation. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                                                             |                                               | Accident would have been avoided if maintenance procedure were improved. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
Flow chart issues

- Need several passes for multiple causes
- Protocol can increase consistency
- Order bias
- User refinement necessary
- Complete for every scenario?
A: Information elicitation
   (Standard report forms)

B: Causal analysis
   - Simplified flowcharting
     (Using preset questions leading to IEC 61508 lifecycle and common requirements)

C: Generation of recommendations

Reconstruct incident
   (ECF modelling)

Distinguish causal factors
   (Counterfactual reasoning)

Root cause classification
   (Using IEC 61508 lifecycle and common requirements)

Simpler/lower risk mishaps

More complex/higher risk mishaps
Mechanic and foreman begin work on thawing the material in the blades.

Mechanic removes sheets on top of the mill and signals to foreman to start motors.

Motors start.

Foreman switched start/stop button to 'off' position and leaves for another task.

Foreman returns but is called away by the electrician.

PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position.

Mechanic is caught in the blades of the mill.
Mechanic and foreman begin work on thawing the material in the blades.

Mechanic removes sheets on top of mill and signals to foreman to start motors.

Motors start.

Foreman switched start/stop button to ‘off’ position and leaves for another task.

Foreman returns but is called away by the electrician.

PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position.

Mechanic is caught in the blades of the mill.
Mechanic and foreman begin work on thawing the material in the blades. Mechanic removes sheets on top of mill and signals to foreman to start motors. Motors start. Foreman switched start/stop button to 'off' position and leaves for another task. Foreman returns but is called away by the electrician. PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position. Circuit breaker trips. Electrician observes failure and calls foreman to help. Electrician resets circuit breaker. Foreman and electrician observe circuit breaker operation. Electrician turns off circuit breaker to diagnose problem. Foreman leaves control room and observes mechanic caught by the mill blades. Mechanic is caught in the blades of the mill.
Supposed: Mechanic observes additional frozen material in blades

Supposed: Mechanic clears material and restarts blades

Blades stopped by the loss of power to the circuit breaker

Supposed: Mechanic goes back to work on blade repair without shutting off motor switches

Mechanic is caught in the blades of the mill
Mechanic and foreman begin work on thawing the material in the blades

Mechanic removes sheets on top of mill and signals to foreman to start motors

Motors start

Supposed: Mechanic observes additional frozen material in blades

Supposed: Mechanic clears material and restarts blades

Blades stopped by the loss of power to the circuit breaker

Supposed: Mechanic goes back to work on blade repair without shutting off motor switches

Electrician observes failure and calls foreman to help

Electrician resets circuit breaker

Foreman and electrician observe circuit breaker operation

Electrician turns off circuit breaker to diagnose problem

Foreman leaves control room and observes mechanic caught by the mill blades

PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position

Foreman switched start/stop button to ‘off’ position and leaves for another task

Foreman returns but is called away by the electrician

Circuit breaker trips

Mechanic is caught in the blades of the mill

Foreman switched start/stop button to ‘off’ position and leaves for another task

Electrician observes failure and calls foreman to help

Electrician resets circuit breaker

Foreman and electrician observe circuit breaker operation

Electrician turns off circuit breaker to diagnose problem

Foreman leaves control room and observes mechanic caught by the mill blades
Supposed: Mechanic observes additional frozen material in blades.

Supposed: Mechanic clears material and restarts blades.

Blades stopped by the loss of power to the circuit breaker.

Supposed: Mechanic goes back to work on blade repair without shutting off motor switches.

Mechanic is caught in the blades of the mill.

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption.

Mechanic and foreman begin work on thawing the material in the blades.

Mechanic removes sheets on top of mill and signals to foreman to start motors.

Motors start.

Foreman switched start/stop button to 'off' position and leaves for another task.

Foreman returns but is called away by the electrician.

Circuit breaker trips.

Electrician observes failure and calls foreman to help.

Electrician resets circuit breaker.

Foreman and electrician observe circuit breaker operation.

Electrician turns off circuit breaker to diagnose problem.

Foreman leaves control room and observes mechanic caught by the mill blades.

PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position.
Mechanic and foreman begin work on thawing the material in the blades

Mechanic removes sheets on top of mill and signals to foreman to start motors

Motors start

Foreman switches start/stop button to ‘off’ position and leaves for another task

Circuit breaker trips

Electrician observes failure and calls foreman to help

Electrician resets circuit breaker

Foreman and electrician observe circuit breaker operation

Electrician turns off circuit breaker to diagnose problem

Foreman leaves control room and observes mechanic caught by the mill blades

Supposition: Mechanic observes additional frozen material in blades

Supposed: Mechanic clears material and restarts blades

Blades stopped by the loss of power to the circuit breaker

Supposed: Mechanic goes back to work on blade repair without shutting off motor switches

Mechanic and foreman begin work on thawing the material in the blades

Mechanic removes sheets on top of mill and signals to foreman to start motors

Motors start

Foreman switches start/stop button to ‘off’ position and leaves for another task

Circuit breaker trips

Electrician observes failure and calls foreman to help

Electrician resets circuit breaker

Foreman and electrician observe circuit breaker operation

Electrician turns off circuit breaker to diagnose problem

Foreman leaves control room and observes mechanic caught by the mill blades

PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption

Supposition: Need more risk assessment training material for PLC reprogramming in process industries

Mechanic is caught in the blades of the mill
Supposed: Mechanic observes additional frozen material in blades

Mechanic clears material and restarts blades

Blades stopped by the loss of power to the circuit breaker

Supposed: Mechanic goes back to work on blade repair without shutting off motor switches

Mechanic and foreman begin work on thawing the material in the blades

Mechanic removes sheets on top of mill and signals to foreman to start motors

Motors start

Foreman switched start/stop button to ‘off’ position and leaves for another task

Foreman returns but is called away by the electrician

PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position

Circuit breaker trips

Electrician observes failure and calls foreman to help

Electrician resets circuit breaker

Electrician turns off circuit breaker to diagnose problem

Foreman leaves control room and observes mechanic caught by the mill blades

Mechanic is caught in the blades of the mill

Supposition: Need more risk assessment training material for PLC reprogramming in process industries

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption

Supposition: Need more risk assessment training material for PLC reprogramming in process industries

Supposition: Need more risk assessment training material for PLC reprogramming in process industries

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption
Mechanic observes additional frozen material in blades

Mechanic clears material and restarts blades

Blades stopped by the loss of power to the circuit breaker

Mechanic goes back to work on blade repair without shutting off motor switches

Supposed: Mechanic stops work on blades due to loss of power.

Electrician observes failure and calls foreman to help.

Electrician resets circuit breaker

Foreman and electrician observe circuit breaker operation.

Electrician turns off circuit breaker to diagnose problem.

Foreman leaves control room and observes mechanic caught by the mill blades.

Mechanic is caught in the blades of the mill.

Supposition: Need more risk assessment training material for PLC reprogramming in process industries.

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption.
Supposition: Mechanic may have known about intended operation of the PLC and assumed that it would not allow restart after circuit breaker trip.

Foreman fails to alert mechanic that mill power supply is not disconnected while they work on the circuit breaker.

Supposition: Blade motor control settings could not be observed at the mill hence mechanic may have assumed foreman has shut down the mill as before.

Supposition: Mechanic observes additional frozen material in blades.

Mechanic clears material and restarts blades.

Blades stopped by the loss of power to the circuit breaker.

Supposed: Mechanic goes back to work on blade repair without shutting off motor switches.

Supposition: Need more risk assessment training material for PLC reprogramming in process industries.

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption.

Mechanic and foreman begin work on thawing the material in the blades.

Mechanic removes sheets on top of mill and signals to foreman to start motors.

Motors start.

Foreman switched start/stop button to 'off' position and leaves for another task.

Foreman returns but is called away by the electrician.

PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position.

Circuit breaker trips.

Electrician observes failure and calls foreman to help.

Electrician resets circuit breaker.

Foreman and electrician observe circuit breaker operation.

Electrician turns off circuit breaker to diagnose problem.

Foreman leaves control room and observes mechanic caught by the mill blades.

Mechanic is caught in the blades of the mill.
<table>
<thead>
<tr>
<th>Causal event</th>
<th>Associated conditions</th>
<th>Lifecycle classification</th>
<th>Justification</th>
<th>Common reqs classification</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position</td>
<td>Supposition: Need more risk assessment training material for PLC reprogramming in process industries.</td>
<td>Modification 6 LTA manufacturers information 7 LTA verification and validation</td>
<td>The company responsible for the PLC update arguably did not appreciate the need to formally consider the implications of the changes on the operation of the mill. Hence the potential restart hazard was not adequately tested for.</td>
<td>Safety Management 4 LTA safety management: external suppliers  Documentation 1 documentation absent/incomplete</td>
<td>The reprogramming of the PLC does not seem to have been supported by a detailed consequence assessment. Again, additional documentation may be required from regulatory organisations to guide E/E/PES suppliers about the best means of performing such a hazard assessment. The operators of the mill might also use such guidance to validate any maintenance activities by suppliers.</td>
</tr>
</tbody>
</table>

| Modification | 1 LTA modification plan (including sufficient lifecycle activities) 3 LTA impact analysis |  |  |  |  |
Develop training material for E/E/PES suppliers and for operators on necessary hazard identification during PLC programming

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Priority</th>
<th>Responsible authority</th>
<th>Deadline for response</th>
<th>Date accepted/rejected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop training material for E/E/PES suppliers and for operators on necessary hazard identification during PLC programming</td>
<td>Medium</td>
<td>Industry regulator</td>
<td>1 Sep 1997</td>
<td></td>
</tr>
<tr>
<td>Conduct formal hazard identification process to determine if there are any additional threats posed by reprogramming of PLC on this plant and supplier’s other installations</td>
<td>High</td>
<td>PLC supplier Safety manager</td>
<td>1 Jun 1997</td>
<td>Accepted 15 Feb 1997</td>
</tr>
</tbody>
</table>
PARCEL summary

- Two approaches depending on consequence and complexity
- IEC 61508 classification
- Supports end users, designers, suppliers/integrators, maintainers
- Several industry sectors
Next steps

- Publish HSE research reports
- Internal HSE consultation
- Published HSE guidance document
Further information

- [www.hse.gov.uk/research/rrhtm/index.htm](http://www.hse.gov.uk/research/rrhtm/index.htm)
- [www.dcs.gla.ac.uk/~johnson/hse](http://www.dcs.gla.ac.uk/~johnson/hse)
- mark.bowell@hse.gsi.gov.uk
- johnson@dcs.gla.ac.uk