

**PARCEL:  
Learning from incidents  
involving E/E/PES**

Peter Bishop



# Background

---

- HSE sponsored project
- Wanted a scheme to learn from incidents involving E/E/PES
- Wanted it to be consistent with IEC 61508
- Adelard, Glasgow Univ. and Black Consulting commissioned to develop the scheme
- Scheme now called PARCEL
- PES Analysis of Root Cause and Experience-based Learning

# Why Investigate Incidents?

---

- Mandatory requirements to record an investigate incidents and accidents,
  - H&S at Work, Control of Major Hazards, 1999
- Required for E/E/PES in IEC 61508
  - Part 1, incident investigation
  - Part 2, defect reporting and correction
- Learning opportunity for stakeholders
  - fewer injuries
  - improved production
  - E/E/PES product improvement

# Development of PARCEL scheme

---

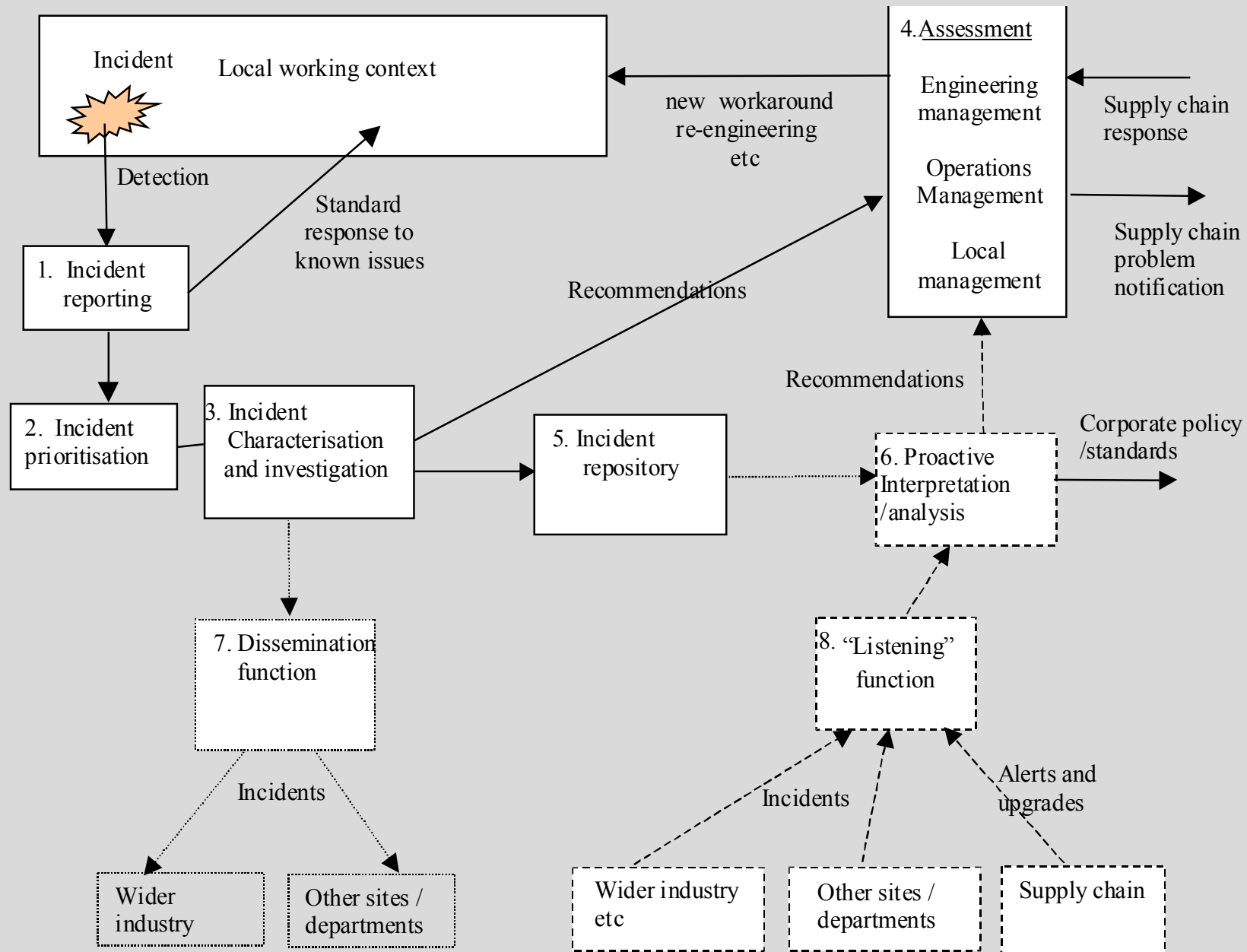
- Review of current schemes and industry practice
  - Process, Offshore, Machinery, Nuclear, Rail
  - Marine, Medical, Aviation
  - E/E/PES Supply chain (systems suppliers, product suppliers)
- Initial Scheme Design
- Scheme Evaluation (with industry)
- Final Scheme

# PARCEL scheme approach

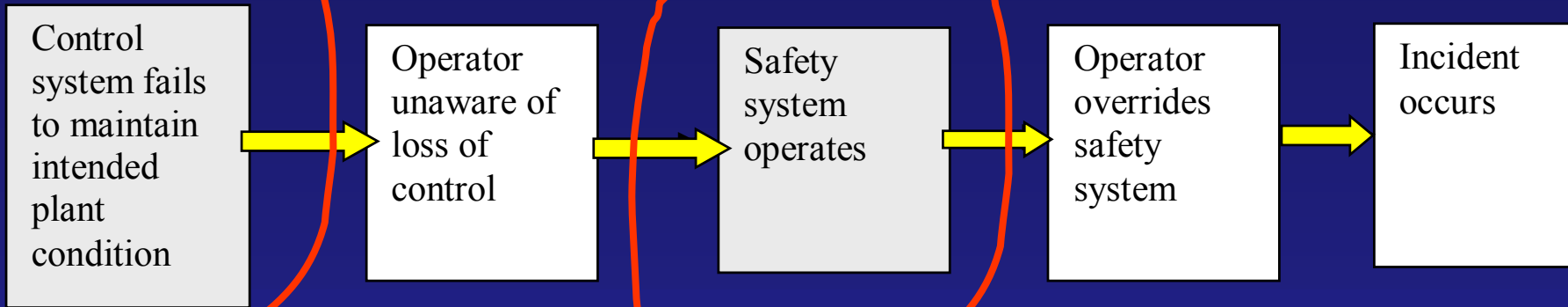
---

- Focusing on the *additional* information / activities needed for handling E/E/PES incidents
- Supports process improvement - identify changes needed
- Practical
  - Current best practice in industry
  - Example forms
  - Intended to fit into existing infrastructure
  - Adaptable to different scales and maturity levels

# Learning feedback loops

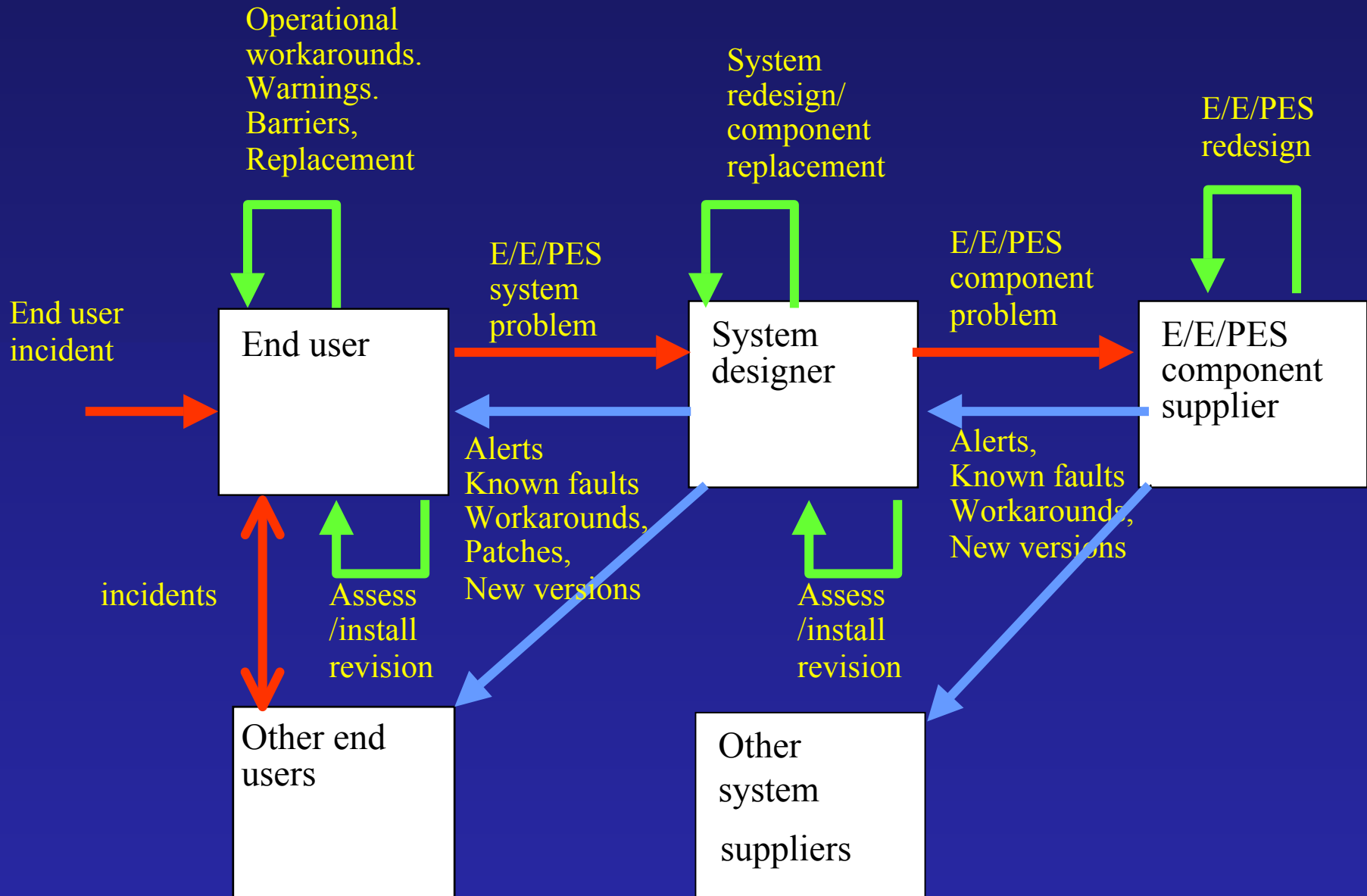


# E/E/PES elements of incident



- Overall incident identifies technical equipment problem
- Results in “equipment problem report”
  - Problem here: control deviation? Or safety system?
- Technical investigation performed to find cause
  - Can involve supply chain if an equipment problem
- Reports back to main incident investigation

# Reporting through the supply chain



# Classification Scheme

---

- Classification used to facilitate appropriate process change i.e. how to prevent problem
- Classification taxonomy based on IEC 61508
  - specific phase
  - common “through-life” elements (competency, doc, V&V..)
- Less detailed taxonomy if stakeholder not involved
  - no knowledge of cause
  - sufficient to identify who to report problem to

# Aids to causal identification (E/E/PES)

---

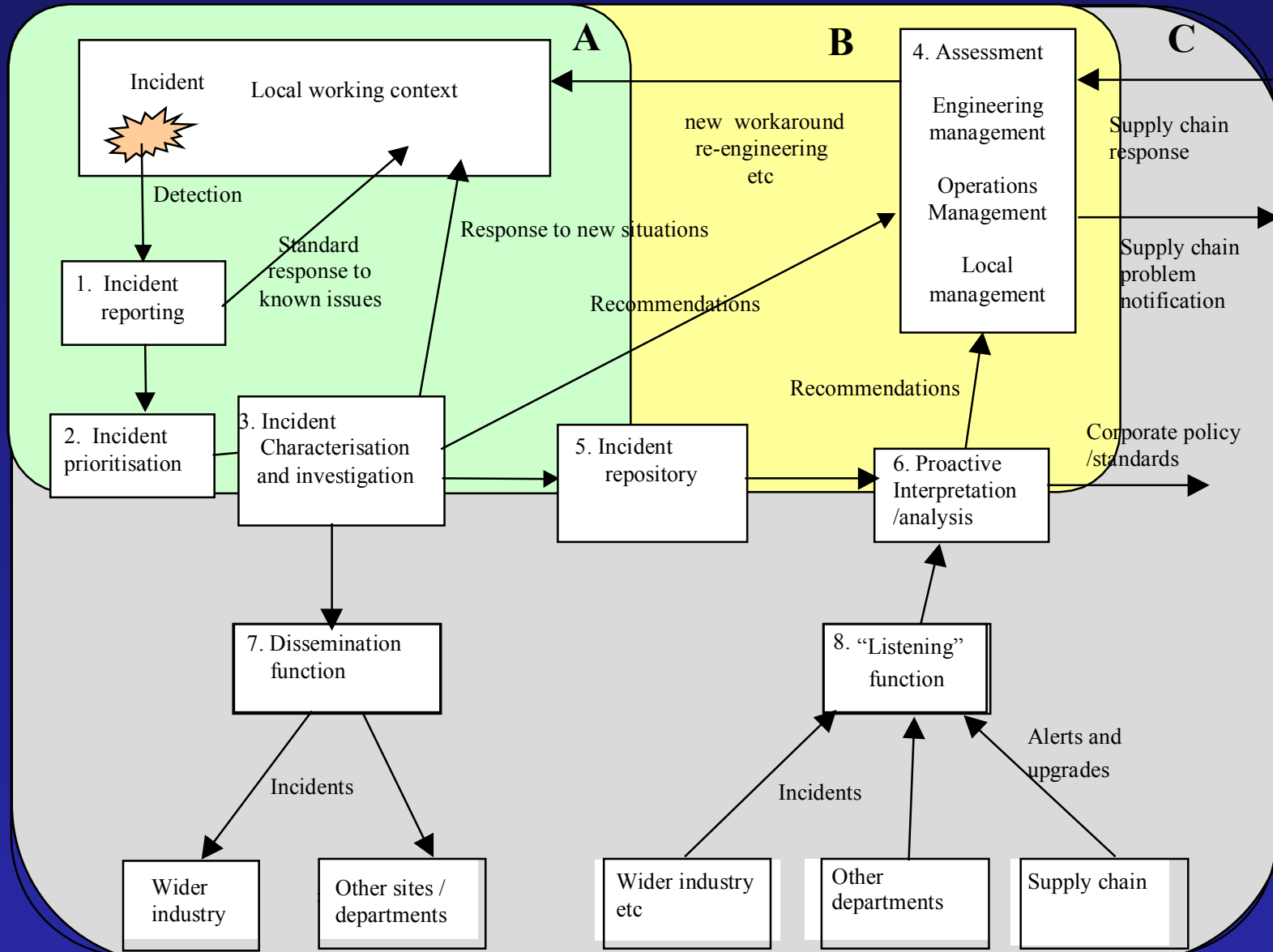
- Problem prevention checklist (based on taxonomy)
  - example checklists for end-user
  - system integrator
  - E/E/PES component supplier
- PARC (PES Analysis of Root Cause)
  - Simple causal analysis scheme for E/E/PES (end user)
  - Decision flowchart
  - Leads to sequence of IEC 61508 based questions
    - “could the problem be prevented if”
- Both methods designed to ways of preventing a recurrence of the problem
  - + Consistent classification for E/E/PES problems

# Implementation of scheme

---

- Characterise the organisation's current incident investigation capability
- Decide what any new scheme is intended to achieve
- Characterise available resources in the organisation
- Customise the scheme to take account of the organisation's capabilities, objectives and infrastructure
- Progressively implement further phases of the "learning from incidents" structure (see next slide)

# Learning maturity levels



- Starting point depends on current maturity
- incident reporting process
- QMS process
- IT infrastructure
- etc

# Decide on scheme aims

---

Possible objectives (depends on company role):

- Reduce work place injuries
- Reduce production losses
- Reduce environmental damage
- Improve product quality
- Reduce project cost and time overruns

# Implementation approach

---

- Map LFI “boxes” and “arrows” on to company infrastructure
  - roles, documents ...
- Keep it simple
  - don't overload staff with paperwork
- Focus on aspects that give an early payback
  - important to keep staff motivated
  - let them know the reports have some effect
- Only collect what you need
  - no information “black holes”
  - consider what can realistically be changed
- Evolve to more complex levels later

# Example: Chemco (Level A)

---

- Objectives

1. Reduce injuries in the local workplace
2. Reduce production losses in the local workplace

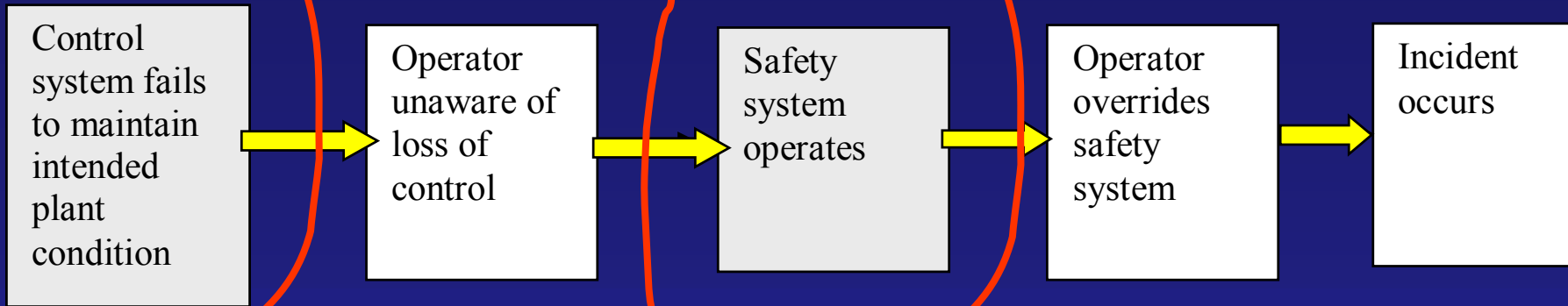
- Relevant incidents

- RIDDOR reportable injuries
- "Near misses" of reportable injuries
- Production and asset losses

- Roles implemented by local workplace staff

- Reporter Workplace staff, first aider
- Prioritiser Supervisor
- Investigator Supervisor
- Decision maker Supervisor (+ workplace staff )
- Implementer Supervisor (+ workplace staff )
- Archiver Supervisor

# Example incident



- Batch vessel overfilled
- Level trip + alarm bell + "Vessel Full" light on vessel
- Control panel shows vessel empty
- Operator uses standby pump to fill vessel
- Chemicals overflow vessel

# Chemco incident report

Incident Report	
Your name	<i>John Scripps</i>
Date of incident	<i>12 Jun 2003</i>
Time of incident	<i>15:30</i>
Location of Incident	<i>Building A12, Batch vessel #4</i>
Title	<i>Batch Vessel #4 overflow</i>
Describe the incident	<p><i>“Autofill” sequence initiated on control panel, but control system stopped.</i></p> <p><i>I heard an alarm, but we have had a lot of those recently.</i></p> <p><i>As the console display showed that the vessel was empty, I used the manual override to operate the standby pump.</i></p> <p><i>Vessel overflowed</i></p>
<b>For completion by the supervisor</b>	
Incident reference number	<i>A12/45</i>
Was any person hurt?	<i>No</i>
Did any damage to property occur?	<i>No, excess fluids went into drain</i>
Was there a loss of production or materials? If so how much?	<i>Production delay of 20 minutes. Loss of 500 litres of feedstock</i>
In your view could this have led to more serious consequences? If so, what could have occurred?	<i>No</i>
What short term fixes or work-arounds have been applied?	<i>Manually opened the drain valves, drained vessel ..</i>
To your knowledge, has this problem occurred before?	<i>Yes (see incident A12/16)</i>
Any electrical or electronic control equipment involved?	<i>Block A12 Batch controller</i>

- Simple paper form
- keep first part short
- Supervisor gives details,
- + any E/E/PES involved

# Chemco incident analysis

Incident analysis	
<b>Immediate Cause(s)</b> <input checked="" type="checkbox"/> Operational <input type="checkbox"/> Maintenance <input checked="" type="checkbox"/> Equipment	<b>Details</b>  <i>Engineering department tell me there is a level trip on Vessel #4 that is supposed to stop filling if the level gets too high and sounds an alarm. The level trip also activates the indicator light on the batch vessel wall.</i> <i>John Scripps thinks that the batch controller did not work correctly. The level display stayed at zero when autofill was initiated (just like in A12/16).</i> <i>The spill could have been avoided if the alarm had been understood.</i>
<b>Actions</b> <input checked="" type="checkbox"/> Log problem <input checked="" type="checkbox"/> Operational change <input type="checkbox"/> Maintenance change <input checked="" type="checkbox"/> Copy to engineering dept	
<b>To:</b> <i>Operations Supervisor</i>	<b>Recommendations</b> <i>The Operations Supervisor should make changes to procedures and conduct training so that:</i> 1) <i>Operations staff always manually check the overflow indicator light on the batch vessel wall if filling stops for no apparent reason</i> 2) <i>If the vessel does overflow, use the level indicator on the wall to restore the level rather than draining completely then refilling</i> 3) <i>A list of audio alarms is available on the operator's desk, for reference if an audio alarm heard.</i>

## Changes

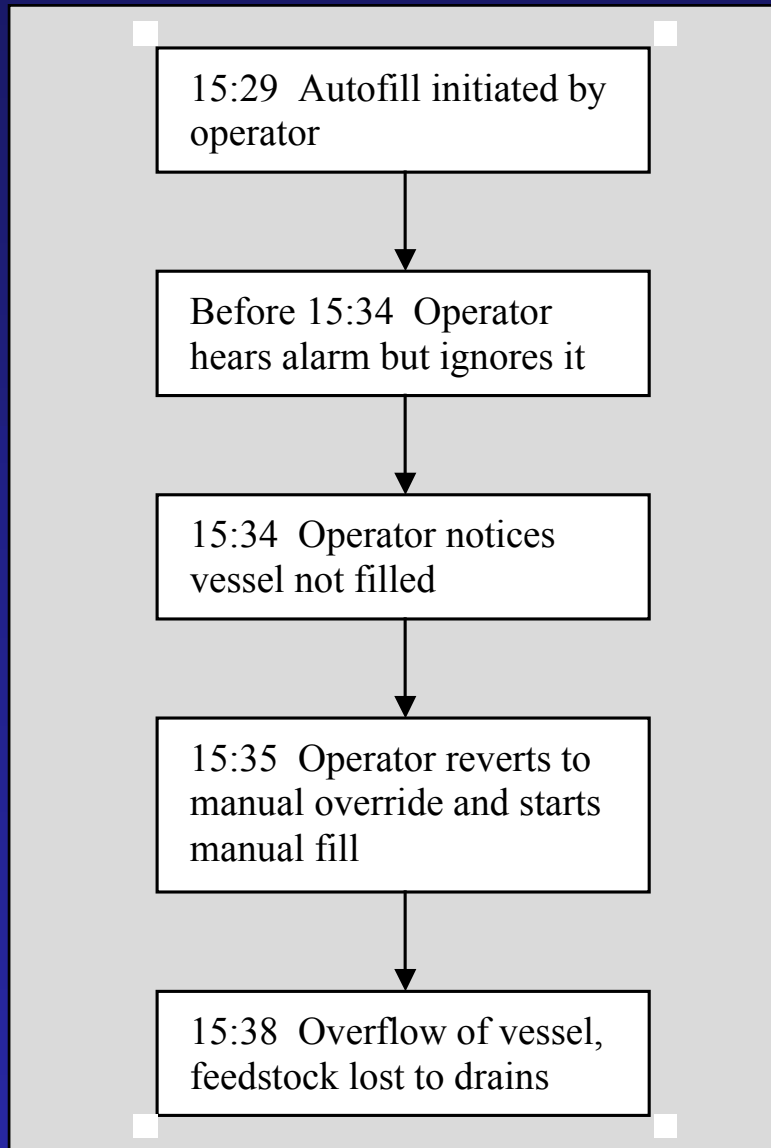
- if unsure about level use lamp on vessel wall
- brief staff about audio alarms

# Capturing experience

<b>Situation</b>	<b>Batch vessel #4 overflow</b>
<b>How to recognise</b>	<i>Filling stops unexpectedly, audio alarm sounds about the same time.</i>
<b>How to fix</b>	<i>Send maintenance engineer out to batch vessel #4, with radio microphone to monitor the level fill indicator light.</i>  <i>Revert to manual control and open drain valve V6.</i>  <i>Allow draining for 10 seconds after the warning indicator light goes out.</i>  <i>Perform mixing manually.</i>

Simple  
"How-to"  
records to  
deal with  
known  
problems

# Level B Incident investigation



- Formal incident analysis methods
  - incident reconstruction time-line
  - barrier analysis

# Barrier analysis

---

Hazard                      Control system malfunction results in vessel overflow  
Targets                     Production delay, loss of feedstock, workplace staff

<b>Barrier</b>	<b>Reason(s) for failure</b>
Independent level trip	Trip on feed pump can be bypassed by using the standby pump
Level monitoring by operator	Level displayed by batch controller incorrect Operator unaware that the level trip had operated

# E/E/PES Problem prevention checklist

<b>E/E/PES Problem Prevention Checklist – Incident would have been avoided if:</b>	
<input type="checkbox"/> <b>System assessment</b>	<input checked="" type="checkbox"/> hazard and risk assessment applied/improved <input type="checkbox"/> better allocation of functions to people and equipment
<input type="checkbox"/> <b>System design</b>	<input type="checkbox"/> better specification of system functions <input type="checkbox"/> better design and development <input checked="" type="checkbox"/> improved operation facilities <input type="checkbox"/> improved maintenance facilities
<input type="checkbox"/> <b>Installation and commissioning</b>	<input type="checkbox"/> improved installation plan/procedures <input type="checkbox"/> improved commissioning plan/procedures
<input type="checkbox"/> <b>Validation</b>	<input type="checkbox"/> better validation techniques/plan <input type="checkbox"/> fully implement validation plan <input type="checkbox"/> better validation equipment <input type="checkbox"/> better analysis/resolution of discrepancies <input checked="" type="checkbox"/> usability assessment
<input type="checkbox"/> <b>Operation and maintenance</b>	<input type="checkbox"/> operation procedures improved <input type="checkbox"/> impact assessment of operation procedures <input type="checkbox"/> operation procedures properly applied <input type="checkbox"/> maintenance procedures improved <input type="checkbox"/> impact assessment of maintenance procedures <input type="checkbox"/> maintenance procedures properly applied <input type="checkbox"/> routine operation and maintenance audits <input type="checkbox"/> test interval changed <input type="checkbox"/> permit/hand over procedures <input type="checkbox"/> procedures to monitor system performance <input type="checkbox"/> selection/application of tools
<input type="checkbox"/> <b>Modification</b>	<input type="checkbox"/> procedures applied to initiate modification in the event of systematic failures or vendor notification of faults <input type="checkbox"/> modification authorisation procedures <input type="checkbox"/> impact analysis of modification <input type="checkbox"/> improve modification planning (including following appropriate lifecycle) <input type="checkbox"/> improve implementation of modification plan <input type="checkbox"/> better manufacturers information <input type="checkbox"/> improve verification and validation of modification

Identifies potential process improvements  
 Checklist also includes:  
 safety man  
 lifecycle def  
 competencies  
 documentat'n  
 FSA

# Incident analysis report

Incident Analysis Report	
Investigation report ref:	<i>INV/AI2/2</i>
Incident report ref:	<i>INC/AI2/45</i>
Incident reconstruction	<i>See time line reconstruction</i>
Analysis of causal factors	<i>See barrier analysis</i>
Investigation details	<i>See attached analysis reports</i> <i>See technical investigation of the batch controller</i>
Causal factors	<p><i>Batch control malfunction</i></p> <ul style="list-style-type: none"> <li>• <i>Lack of awareness of batch control failure</i></li> <li>• <i>Lack of awareness of current level in vessel</i></li> <li>• <i>Lack of awareness of operation of trip</i></li> <li>• <i>Standby pump can still operate even if there is a level trip on the main pump</i></li> </ul>
Problem prevention classification	<p><i>1) Assessment: hazard and risk assessment</i> <i>Capability to bypass overflow trip by using the standby pump should have been identified</i></p> <p><i>2) Design: operation facilities</i> <i>Design should ensure operator is aware of equipment failure</i> <i>Design should ensure important plant status information is available to the operator</i></p> <p><i>2) Validation: usability assessment</i> <i>Chance of operator error increased due to lack of information – audio alarm not specific</i></p> <p><i>4) Operation competence: Training</i> <i>Operator should be made aware of the currently available alarms</i></p>

# Recommendations

Ref	Recommendation	Department role	Priority	Response deadline
1	Brief operators to assume overflow has occurred when audio alarm heard during fill operations	Operations manager	1	30 Jun 2003
2	Change operational procedures to get permit from supervisor before using the standby feed pump	Operations manager	1	30 Jun 2003
3	Ensure operating staff are briefed about the change in procedure	Operations manager	1	30 Jun 2003
4	Request engineering change to place a visible alarm on the control desk to indicate the vessel is full. Should be applied to all vessels in Block A12	Engineering manager	2	25 Jul 2003
5	Investigate why the batch controller malfunctioned and failed to indicate level to the operator	Engineering manager	3	8 Aug 2003
6	Ensure engineering standards require that all trip status signals be presented to the operator.	Engineering standards manager	3	8 Aug 2003

● E/E/PES technical investigation

# Equipment problem report

Equipment Problem Sheet	
Supplier	ACME corp
Product name	CONPAC 800-
Serial no.	AC-b72-1289
Configuration/version information	Hardware Rev 8.12, SW rev A12 v3
Location	Block A12
Date	12 Jun 2001
Incident reference (if applicable)	INC/PROD A12/45
Used for: <input type="checkbox"/> protection <input checked="" type="checkbox"/> control <input type="checkbox"/> monitoring <input type="checkbox"/> alarm/direction <input type="checkbox"/> safety-classified	
<b>Problem Description</b> <input type="checkbox"/> failed to act when needed <input type="checkbox"/> acted when not needed <input checked="" type="checkbox"/> acted in unexpected way <input type="checkbox"/> failed completely <input type="checkbox"/> failed during test <input type="checkbox"/> maloperation of equipment by staff <input type="checkbox"/> other <input type="checkbox"/> <b>dangerous/potentially dangerous</b>	<b>Details</b> <i>Controller overfilled vessel #4                      Displayed level on the console did not change</i>
<b>Immediate Cause</b> <b>Operational</b> <input type="checkbox"/> operator action <input type="checkbox"/> operator inaction <b>Maintenance</b> <input type="checkbox"/> fault diagnosis <input type="checkbox"/> fault correction <input type="checkbox"/> left in wrong mode <input type="checkbox"/> configuration <input type="checkbox"/> calibration <b>Environment problem</b> <input type="checkbox"/> condensation <input type="checkbox"/> contamination <input type="checkbox"/> temperature <input type="checkbox"/> vibration <input type="checkbox"/> EMI <b>Equipment functionality</b> <input type="checkbox"/> user interface <input type="checkbox"/> operational func <input type="checkbox"/> maintenance func <input checked="" type="checkbox"/> resp to comp failure <input type="checkbox"/> performance <input type="checkbox"/> hardware failure <b>Equipment integration/installation</b> <input type="checkbox"/> power supplies <input type="checkbox"/> wiring <input type="checkbox"/> connections <input type="checkbox"/> incompatible i/o <input type="checkbox"/> incompatible suby <input type="checkbox"/> configuration	<b>Details</b> <i>Diagnostic tests showed that the 4-20MA level sensor had failed and was reading low</i>  <i>Disconnecting the sensor resulted in a low displayed level, but otherwise appears normal.</i>  <i>Suspect the controller kept pumping to increase the level until there was an overflow trip.</i>
<b>Actions</b> <input checked="" type="checkbox"/> log problem <input checked="" type="checkbox"/> repair/reconfigure equipment <input checked="" type="checkbox"/> report to supplier <input checked="" type="checkbox"/> problem prevention review	<b>Details</b> <i>4-20 mA level sensor replaced</i> <b>Contact supplier to ask if the control system can warn of sensor failure</b>

- Equipment problem sheet (Eng. Dept)
- Triggered by:
  - incident report
  - problems in test/maint (unsafe state of protection eqt (excessive failure rate))

# ACME problem report

Problem Report	
From	<i>Bill Smith</i>
Company	<i>Chemco</i>
Location	<i>Widnes, Lancs</i>
Date	<i>15 Jun 2001</i>
Details	
<p><i>CONPAC 800 Rev 8.12, SW A12 Rev 3.</i></p> <p><i>Chemco have complained that the Batch controller in Block A12 failed to inform the operator that the level sensor was suspect. See attached problem report.</i></p> <p><i>Maybe we should also disable auto-control if this is detected?</i></p> <p><i>Chris Curry</i></p>	
From: Mark Hughes, Software Development	
Have checked the software A12 Rev 3, and it <b>does</b> check for sensor failure. If a failure is detected the level indicators go to flash mode, and auto-control is disabled for that loop,	
Have talked to CONPAC system support and apparently there is a known problem with Rev 8.12 firmware. The 4-20mA fails to set the fail-flag (or DBI "don't believe it") indicator.	
As our application software relies on the DBI flag this did not work either.	
I think our application software testing used a DC volt interface configuration as that is what our test environment uses so we did not spot it during testing.	
CONPAC suggest the following workaround:	
<ul style="list-style-type: none"><li>• Configure the level input as a raw signal.</li><li>• Implement a test in the application software for a low raw ADC (below 819).</li><li>• Perform the conversion from the raw ADC value to the level value in the application software.</li></ul>	
CONPAC says the fail flag problem will be addressed in a later version of the CONPAC 800 software.	

- Chemco reports problem by email
- ACME is the system designer
- Problem is due to known fault in CONPAC 800 rev 8.12
- Suggest work-around or wait for new release

# ACME problem prevention checklist

- Focus on system development lifecycle phases
- More detail factors (based on groups of clauses in IEC 61508)

<b>Validation</b> <ul style="list-style-type: none"><li><input type="checkbox"/> Better implementation of validation plan</li><li><input checked="" type="checkbox"/> Better validation equipment</li><li><input type="checkbox"/> Better analysis/resolution of discrepancies</li><li><input type="checkbox"/> Better usability assessment</li></ul>	<i>Factory test equipment should be able to replicate all inputs.</i>
<b>Safety management</b> <ul style="list-style-type: none"><li><input type="checkbox"/> specification of necessary management and technical activities</li><li><input type="checkbox"/> define accountability for all activities</li><li><input type="checkbox"/> check activities are implemented and monitored</li><li><input type="checkbox"/> check activities are formally reviewed by all organisations</li><li><input type="checkbox"/> ensure all organisations are informed of responsibilities</li><li><input checked="" type="checkbox"/> review suppliers for appropriate quality management system</li></ul>	<i>CONPAC did not alert us about the fail flag issue. Need to ensure that all component suppliers will inform us of known problems.</i>

# CHEMCO change recommendations

## Recommendations

### Policy change

- procurement procedures
- supplier approval
  - engineering standards
- acceptance procedures

### Equipment change

- warning/advisory labelling
- equipment relocation
- environmental protection
- hardware repair
- upgrade to new version
- equipment replacement
- reprogramming

### Operational change

- procedures
- support documentation
- access controls
- warnings
- staff training
- staff briefing
- staff supervision

### Maintenance change

- procedures
- support documentation
- access controls
- warnings
- staff training
- staff briefing
- staff supervision

## Recommendations

- *Change system acceptance procedures to require that site and factory tests include tests for sensor failure and appropriate notification of failures are given to the operator.*
  - *We discussed the option of getting ACME to reprogram the application to detect sensor failure but would recommend that we wait for an upgrade to the CONPAC firmware that resolves the issue.*
- In the mean time, as this failure has happened more than once, we would recommend that operations staff request a sensor test if they suspect the displayed level is incorrect.*

# Summary

---

- Have developed developed the PARCEL scheme for E/E/PES
- Designed to be a modular addition to general incident investigation
- Causal classification based on IEC 61508 life-cycle phases
  - granularity depends on viewpoint (user, system, component)
- Causal analysis checklists and flowchart method (PARC)
- Example forms
- Adaptation of scheme according to company maturity and size
- Now publicly available from the HSE
  - <http://www.hse.gov.uk/>