5-7 Alexandra Road
Hemel Hempstead
Herts HP2 5BS. UK

Tel: 44 (0)1442 242200
Fax: 44 (0)1442 214077
business@bpa.co.uk
www.bpa.co.uk

# COPEX 2010 – When Things Go Wrong!

Peter Davis – Director and General Manager BPA

# Aims of Presentation

- Share some aspects of Business Continuity Planning and Emergency Planning
- Challenge to plans and procedures based on real events
- Presentation is will not to explain how to develop a Business Continuity Plan (BCP) or Emergency Plan (EP)

# Development of Emergency Plans

- Consider the threats
  - Corrosion
  - Third party damage
  - Theft
  - Natural hazard
  - Operator error
  - Fire
  - Equipment failure
- Design it out
- Mitigate in operation e.g. Monitoring
- Consequence management plans (emergency plans)

# Pipeline Spillage

# Pipeline Damage

# Pipeline Repair

# Challenges to our procedures and plans

## Two events

- Buncefield Incident
- Major communications failure

# Buncefield Incident

- Major explosion and Fire in December 2005
- Explosion generated by failure on adjacent site

**Pipelines operations at Buncefield**

- 3 pipelines in and two pipelines out
- Key hub for SCADA system for all pipelines
- SCADA system back up location

**Immediate Issues**

- Pipelines shutdown effecting complete system operations and other terminals
- No site power
- No control and monitoring at site

# Investigation and Immediate Actions

- All computers ceased by investigators (including SCADA system, Flow computers, PC's)
- No access to control room due to investigation
- Limited access to control room due to damage
- Nothing could be disturbed or changed
- Nothing returned to Pipeline Operator for six months

**Immediate actions**

- Could not do anything on site so ultimately needed to bypass site for pipeline operation.
- Modify SCADA system – mainly alarms and automation

## Lessons and Questions?

- Following a major incident, could the impact go further than the incident site?
- Major equipment could be removed from site by Investigators?
- Consider where are back up systems located and back up software held?
- You may not be able to access site to repair equipment or by-pass equipment, do you have options?
- Should the main pipeline control room be located on an operating site?

# Major Communications Failure

- BPA rely on the national telephone/broadband network for SCADA and voice communications.
- The SCADA system has various levels of redundancy (back-up) in the event of a failure
- Ultimately the SCADA system is design to run in manual from each site in the event of a major failure.

# The Incident

**The event**

- 900m of 400 core cable and 900m of 500 core cable was stolen.
- Cable were underground and needed to be pulled out of the ducts.
- Cable provided SCADA and voice communications to main pumpstation plus 2 refinery feed stations.

**The Consequences**

- No SCADA communications
- No remote monitoring and local SCADA only contained 24hrs of pumping schedule
- No voice communications

# What were the Actions?

- Unless systems operated manually the pipeline would have been shutdown for 5 days!
  - No other fall back systems were available
- We needed to utilise mobile phones
  - Needed to get formal dispensation from the Refineries.
- Lack of skills from maintenance staff to operate all functions in manual
  - Trained to operate for short periods
- Complicated product batching arrangements and interface cutting.
- Relocated a senior control centre operator to site to manage operations

# What were the lessons?

- Plans did not consider such a failure!
  - Repair time was 5 days, previous history worst case was less than 24 hours.
  - Is this a change in risk profile to the industry?
- Failure outside control of pipeline operator
  - But a single point failure for pipeline operator
- Planned fallback not exercised and thus staff not fully competent
  - Do we even have enough staff for a sustained failure.

# And Finally

- One week later a 400 core cable was stolen again in the same area!
- There must be a good market for copper!

# Summary Lessons

- Do Business continuity plans consider **all** risks
- Has the risk profile changed
- Have the consequences changes
  - More automation
  - Less staff
  - Different skill profile of staff
  - Greater system utilisation
- Are the back up systems robust

# Thanks You and Questions