YEAR 2000 EMBEDDED SYSTEMS SAFETY IMPLICATIONS

G R Brell BEng – Electrical
A J Napton BEng (hons), MBA
Shell Coal Pty Ltd

1. INTRODUCTION

The Year 2000 problem is a fundamental design flaw that may manifest itself in all aspects of electronics based systems. The essence of Year 2000 Compliance or Readiness is that irrespective of the century in which any dates fall, the electronic system will continue to function and will correctly interpret the dates being processed.

Shell Coal has conducted a centrally coordinated Year 2000 Programme for the seven coal mines that are managed by companies in the Shell Coal Group. Garry Brell – Embedded Systems Team Leader (Shell Coal) and Tony Napton – Embedded Systems Resource Manager & Strategist (Nuiec Projects) managed the Year 2000 Embedded Systems Programme for the Shell Coal Group.

The open cut mines in the Shell Coal Group include Callide, Drayton and German Creek at Capcoal. The underground mines include Central Colliery at Capcoal, Southern Colliery at Capcoal, Dartbrook Colliery and Moranbah North Colliery, the newest of Shell Coal's underground mines that was officially opened on the 23rd of June 1999 by the Queensland Premier, the Honourable Peter Beattie.

The Year 2000 Programme included the following project streams:

- IT and Business Systems
- **Embedded Systems (Automation and Process Control)**
- **Year 2000 Contingency Planning**
- Business Continuity
- Supply Chain including Customers and major utilities

2. OVERVIEW

2.1 Year 2000 Programme

The focus of this paper is on the Embedded Systems (Automation and Control) and Year 2000 Contingency Planning as it relates to Embedded Systems equipment and software. This paper outlines the Embedded Systems programme's objectives and methodology which were used in addressing the relevant issues and their risk/consequence effect on the safety, environmental and operational integrity of Shell Coal's businesses, assets and employees.

The methodology used involves Inventory, Risk & Compliance Assessment, Solution Plans & Remediation, Testing, Year 2000 Contingency Plans and Change Control. The Year 2000 risks identified were managed down to a level that, as a minimum, satisfied all safety, environmental and operational requirements of Shell Coal's Health, Safety and Environmental Policy.

The Embedded Systems Programme objectives were:

- to increase confidence and minimise operational risk by a 'triage' process, such that the level of Year 2000 Readiness assessment and testing is sufficient to address the assessed risk of that equipment's failure,

- to ensure a due diligence process has been implemented, such that documentation is available to satisfy insurance claim requirements if required for use in the year 2000.

The triage process, used as part of the methodology, achieved the equipment close out requirements summarised in Section 3.9.

The risk rating given to an equipment item determined the level of Year 2000 Compliance or Readiness that was sought – the higher the risk to the business if the item fails, the more critically the item was scrutinised in terms of it's compliance assessment.

Equipment items were also considered collectively when they formed part of a larger system. If the importance of the larger system warranted a higher risk rating than the components then the system was scheduled for full testing from an early stage of the programme.

The likely interaction between equipment items within systems was considered and taken into account when designing the higher level testing of the systems concerned.

2.2 Project Management

2.2.1 Quality Control

Procedures for each stream phase/activity were formulated from the Shell International Survival Guide and the ICS consultancy group's methodologies by the Embedded Systems team. Shell Coal engaged Nulec Projects Pty Ltd to provide the skilled personnel and technical resources to carry out Embedded Systems stream activities in Brisbane and coordination of the Embedded Systems stream activities with the site based Year 2000 Focal Points and Engineers.

The Embedded Systems team maintained a database of all inventory items with descriptive and assessment details. Documents and activities for each inventory item were also recorded. In addition, paper copies of all assessments and testing were kept in an hierarchical filing system, which is maintained at Shell Coal's Brisbane Office.

The Embedded Systems team reported monthly to a Senior Management Steering Committee chaired by Shell Coal's CEO.

Programme progress presentations were given to Year 2000 Focal Points and Engineers in July and October 1998 and January and May 1999. Further progress reports were provided. ie. inventory analysis and final close out reports, summary reports as requested during the course of the programme.

2.2.2 Planning

The target completion date for all activities (with the exception of Embedded Systems contingency and/or recovery plans) for high and significant risk items was 30th June 1999. This was achieved with some exceptions that were dealt with in July and August 1999 as resources and opportunities allowed.

The contingency and/or recovery plans for those items or systems requiring them, were formulated from June 1999 onwards and will continue to be developed, tested and implemented up to year 2000.

3. METHODOLOGY

All Embedded System stream activities were supported by entries in a Year 2000 Inventory Database and hard copy documentation in the programme's filing system.

Refer to Figure 1 '*Year 2000 Programme Embedded Systems Methodology Flow Diagram*' for an overview of the relationships between Embedded Systems programme activities. The final approach taken in each activity was the result of a review with mine site representatives, the Embedded Systems team and Shell Coal management.

Change Control was applied to new, replaced or modified equipment items or software after the initial inventory was recorded. Changes were recorded and appropriate stream activities undertaken to ensure that the equipment and software remained Year 2000 Ready.

3.1 Inventory

A Year 2000 Inventory was undertaken to identify all 'At Risk' equipment. 'At Risk' equipment was equipment that contains or may contain a 'time function'. This includes equipment that contains microchips and/or firmware; process monitoring, control and data acquisition systems; IT systems; or any other electrical equipment and/or operating system.

All inventory items were allocated a unique Shell Coal Year 2000 Project tag number. Relevant details were logged against each item and entered into the Year 2000 Inventory Database. Each site received a comprehensive inventory report on specific inventory collection activities.

3.2 Risk Assessment

Risk Assessment was the process of determining the risk to the business of all items identified during inventory collection. The risk of an item was determined by the greatest of its safety, environmental or operational consequence. The appropriate user or owner of the inventory item for each site performed the risk assessment.

Each item of equipment or custom software was assigned a risk class against the categories of safety, environment and operations (financial implications).

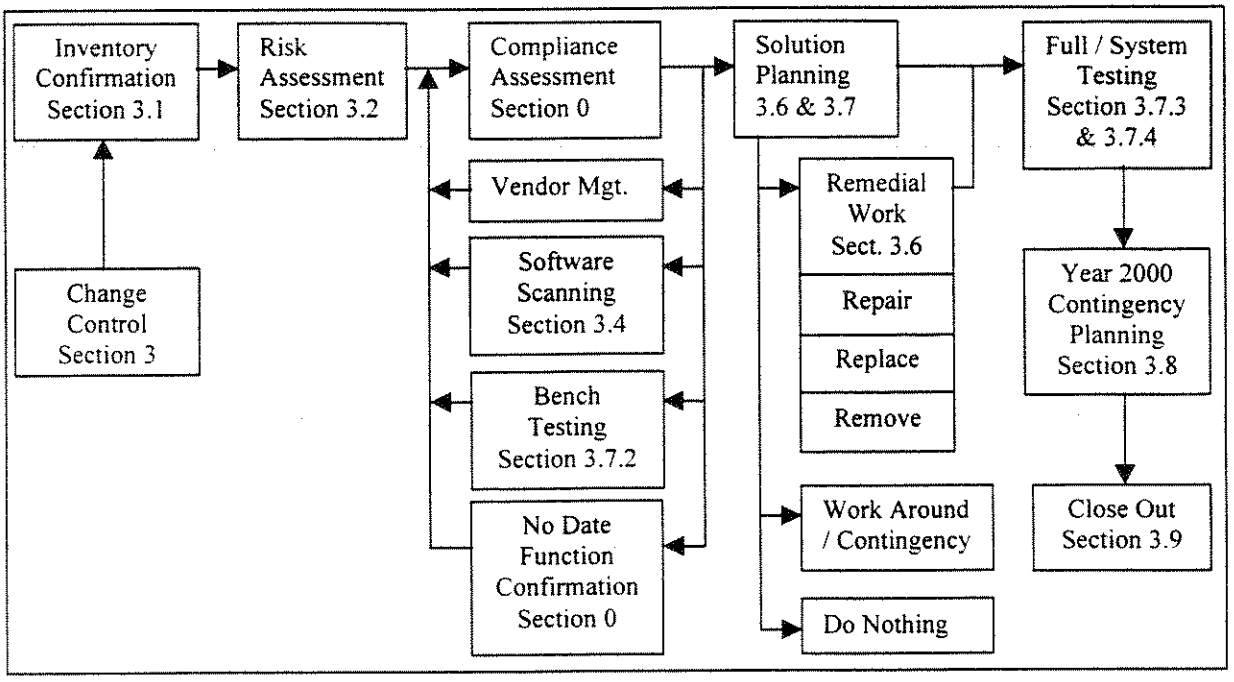

Figure 1 - Year 2000 Programme Embedded Systems - Methodology Flow Diagram

Risk Class	Risk Category		
	Safety	Environ-ment	Financial Loss
High	Severe Injury, 1 Death without Other Failure	Permanent Major Damage, Beyond Fence	>$1m
Significant	Severe Injury, 1 Death with Other Failure	Temporary Major Damage, Beyond Fence	<$1m
Medium	Slight Injury	Temporary Major Damage, Within Fence	<$100k
Low	No Injury	Minor or No Damage	<$10k

3.3 Compliance Assessment

Compliance Assessment was performed on each Inventory item. This process involved obtaining Year 2000 Compliance or Year 2000 Readiness statements from the manufacturers or vendors of the inventoried equipment. Year 2000 Ready is equivalent to Year 2000 Compliant or Year 2000 Compliant with acceptable work around.

Each item of equipment was assigned one of the following Compliance codes:

Code No	Compliance Description
0	Contains no date function (NDF)
1	Unconditionally passed tests
2	Conditionally passed tests
3	Vendor states compliance to British Standards PD2000 or equivalent
4	Vendor states compliance, but standards not clear
5	Believed to have a date related problem
6	Possibly not compliant, not enough information
7	Is expected to fail in 2000

In broad terms, after Compliance Assessment each item was identified for reporting purposes as one of the following:

- Year 2000 Compliant
- Year 2000 Compliant with minor issues
- Not Year 2000 Compliant

Definitive compliance information from manufacturers was requested in writing, addressed to Shell Coal to provide confirmation of the assessed equipment compliance.

3.4 Software Scanning

Software Scanning was the process of determining whether an item of custom software (ie software controlled and maintained by Shell Coal) was Year 2000 Ready. The software was scanned to find all instances of date sensitive code and an

assessment was made on each instance of code as to its Year 2000 Readiness. Each item of custom software was given a Compliance Code. Remediation was carried out on all non-Year 2000 compliant code (assigned a Compliance Code 7).

Each item of custom software was assigned one of the following Compliance Codes:

Code No	Compliance Description
0	Contains **no** date function (**NDF**)
4	Contains date sensitive code that is Year 2000 Compliant
7	Contains date sensitive code that is **not** Year 2000 Compliant

3.5 No Date Function (NDF) Assessment

All items that have been declared as having no date function and have been assessed as high or significant risk have had a 'No Date Function' assessment. This required confirmation of the 'no date function' by a thorough method, such as sighting of the circuit boards, reviewing manuals, or similar.

3.6 Remediation

All items that have primary functions that were non-compliant and have been evaluated as high or significant risk have been remediated. Items that have non-primary functions that were non-compliant were not remediated if site decided that work-around-contingency plans were sufficient or that sites did not use the non-compliant function.

3.7 Testing

All equipment identified as a high or significant risk required testing to confirm their Year 2000 Readiness. Exceptions or limitations were stated and justified in Close Out Reports, (refer section 3.9.)

These tests produce one of the of the following pass or fail criteria:

- Unconditional pass - Fully passed all functional tests at each test date. (Compliance Code 1)
- Conditional Pass - Fully passed all primary functional tests, but failed tests of unused or non-primary function of the equipment. (Compliance Code 2)
- Fail - Failed primary functional test. (Compliance Code 7)

3.7.1 Contingency/Recovery Plans

Contingency/Recovery plans were formulated for all situations where full or system tests were to be carried out on 'live' equipment at site and there existed a risk that the equipment or system being tested might be made inoperable. The Contingency/Recovery plans were established as a means of maintaining the equipment or systems' function regardless of the outcome of tests.

The existence of these measures reduced the risk to operations to an acceptable level to allow testing to proceed.

3.7.2 Bench Testing

Bench testing involves testing one or more of each type of item to confirm Year 2000 Readiness. The Year 2000 Readiness tests included Power On & Power Off date rollovers, manual date set and back-up recovery for a selection of 'at risk' dates.

Power On and Power Off roll over tests were undertaken for the following dates:

- 31/12/1999 – 01/01/2000
- 28/02/2000 – 29/02/2000
- 29/02/2000 – 01/03/2000
- 31/12/2000 – 01/01/2001
- 28/02/2004 – 29/02/2004
- 29/02/2004 – 01/03/2004
- Manual Date Set – 01/01/2000 & 29/02/2000
- Back-up recovery - 31/12/1999 – 01/01/2000

Unix based equipment was also tested for a number of dates containing '9's and '99's. PC based systems were tested for 9/9/99.

Items were considered as successfully bench tested, if similar items have been full or system tested successfully.

3.7.3 Full Testing

Full tests were either on-line or off-line on the equipment at site. The equipment underwent functional tests sufficient to confirm correct operation for the tested dates. The tests were similar to the bench tests, but may have been limited to the more critical dates due to production constraints.

3.7.4 System Tests

System tests were undertaken when a number of items of equipment formed an operational process. The systems underwent functional

tests sufficient to confirm correct operation for the tested dates. The tested dates may have been limited to the more critical dates due to production and access constraints.

3.8 Year 2000 Contingency Planning

Contingency plans have been developed and will be maintained for Embedded Systems of High and Significant Risk or for items which have known non-remediated problems. Individual items of Medium or Low Risk when combined as part of a larger system or assessed because of quantity to be of a higher overall risk were included in contingency or recovery plans.

3.9 Close Out Requirements and Reports

Each inventory item was 'Closed Out' on a grouped basis. The Close Out Requirements were:

- All items that have been assessed as High or Significant risk required successful testing or completion of a 'No Date Function' assessment.
- All items that have been assessed as Medium or Low risk required confirmation from the vendor or manufacturer that they are Year 2000 Compliant or Ready.
- All items where the Year 2000 Readiness status was not established also required testing, even if they are Medium or Low Risk.
- Trade-offs were made to lessen these requirements. The trade-offs required justifications based on the equipment's usage, known limitations and operational constraints. The trade-off justifications were considered by Shell Coal and site management for approval.

The Close Out Requirements are as detailed in the matrix and notes below:

Risk Class Consequence	Requirements:	
	Compliance Code	Additional requirements
High	≤ 2	Full tests recommended or NDF, refer to Notes 2 & 3
Significant	≤ 3	Full tests preferred or NDF, refer to Notes 2 & 3
Medium	≤ 4	Refer to Note 4
Low	≤ 5	Refer to Note 4

Notes:

1. Refer to previous sections for further descriptions of risk class, compliance code and remediation requirements.

2. All high and significant risk items were subject to system and/or full on-line tests. Exceptions or limitations were stated and justified.

3. All high and significant items that have no date function were confirmed by the satisfactory completion of a 'No Date Function' (NDF) assessment form.

4. Medium & Low risk items were closed out provided that:

   - the quantity of items was not significant, or
   - the proportion of this equipment to similar equipment on site was sufficiently low, such that the similar equipment may be used upon failure of the equipment covered under review,
   - known upgrades of the equipment were complete or were decided as unnecessary,
   - no other foreseen implications to site operations.

5. '≤' in the above table indicates 'equal to or better than' ie. a higher level of compliance.

4. ASSESSMENT SUMMARY

4.1 Equipment Groups

Figure 2 '*Year 2000 Programme - Embedded Systems Inventory Breakdown*' provides a summary of the quantity of inventory items broken into types of equipment and associated risk. 4470 items were tagged, of which 1/3 (1490 items) were assessed as high or significant risk in terms of safety, environment or financial consequence. Of these 772 were high or significant risk in terms of safety consequence.

Examples of Programmable Devices include special function cards in PLCs (Programmable Logic Controllers) used for data communications, programmable instrumentation and measurement devices (Gas Analysers). Examples of configurable Devices are Protection Relays, Gas Monitors and most instrumentation. Examples of Non-Configurable Devices are simple Protection Relays, Fire Panels, Earth Leakage Relays, PLC Input/Output Cards and Battery Chargers.

4.2 Key Functional Areas

The following is a breakdown summary of mine site key functional areas where equipment and software that may contain a date function were investigated.

4.2.1 Underground Mining

4.2.1.1 Development

Continuous Miners, Shuttle and Ram Cars were checked and none were found to have date functions on board.

Remote monitoring and control systems using high voltage modems were examined and found not to contain date functions. These systems were used on some mobile equipment for remote indication of equipment status and in some cases control.

Feeder Breakers were found to contain PLCs which were assessed and found generally not to contain date functions.

Similarly Substations and Distributed Control Boxes (DCBs) in some cases used PLCs for control and monitoring which were found not to contain date functions.

Protection relays for both high and medium voltage applications were found to contain date functions but none were inoperative due to Year 2000 problems. Some protection relays were found to be conditionally Year 2000 Ready with minor problems encountered with trip date logging during testing.

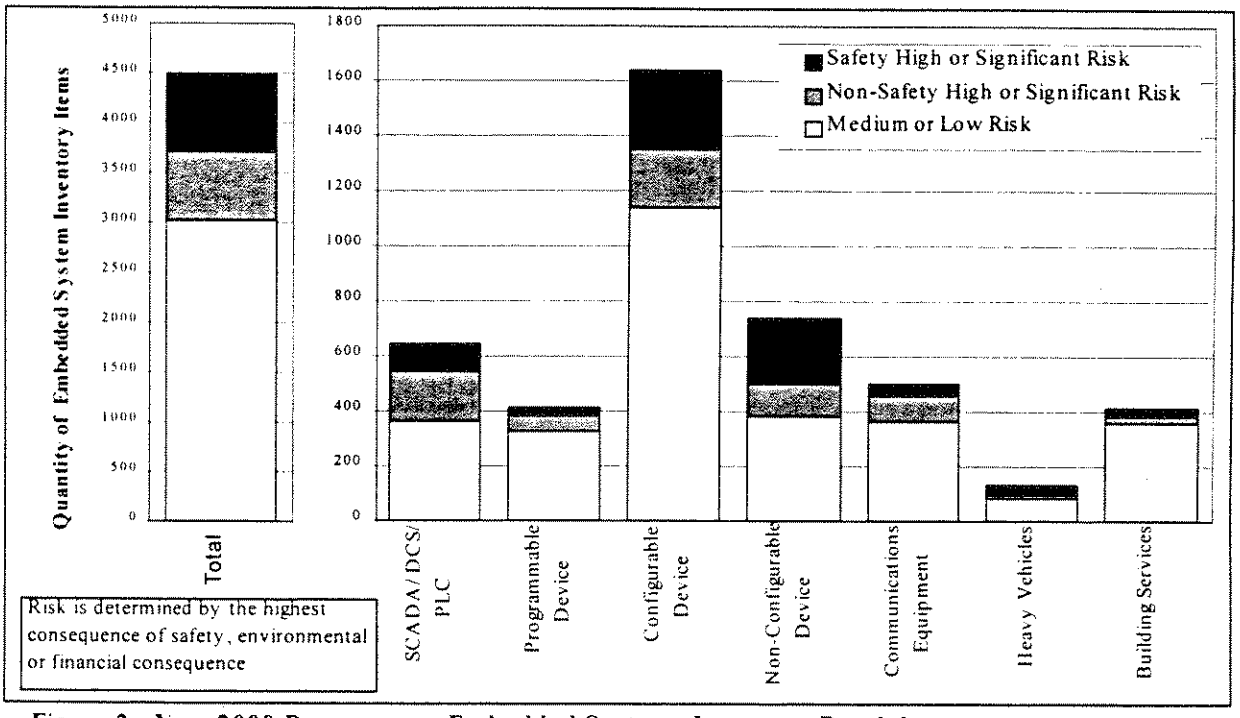

Figure 2 - Year 2000 Programme - Embedded Systems Inventory Breakdown

4.2.1.2 Longwall and Conveyor Operations

The longwall systems assessed comprised Shearers, Armoured Face Conveyors (AFCs), Beam Staged Loaders (BSLs), Roof Supports, Pump Stations, Panel, Trunk and Drift Conveyors, Substations and DCBs.

The safety implications of gas detection and equipment operational trips placed most equipment and software in this functional area into a high or significant safety risk category.

The systems contained PLCs, PCs, Operator Interface proprietary and custom software, PLC proprietary and custom software, earth leakage and overload protection relays, various smart instruments, high voltage modems, local area network equipment, intrinsically safe power supplies and voice communications equipment.

The equipment items found were all assessed for risk and compliance. The items were tested individually and collectively as part of their system to confirm Year 2000 Readiness.

All custom software was scanned and any instances of date functions checked, in a few cases date functions were found requiring remediation.

The system testing was carried out on simulated systems or 'off line' before live testing was carried out. The software scanning and testing revealed that most systems were not affected by date functions and were mostly Year 2000 Ready. The few problems encountered were remediated. There were several cases where equipment or software was upgraded. In a few instances equipment was replaced outright.

4.2.2 Open Cut Mining

4.2.2.1 Draglines and Shovels

Supervisory Control and Data Acquisition systems (SCADA), PLC and PC Based Operator Interfaces were found to contain date functions and required assessment, remediation and testing.

The safety implications of tight line protection and equipment operational trips placed the control equipment and software into a high or significant safety risk category.

Dragline tight line protection systems were found to have date functions and required assessment, remediation and testing. These systems were considered a high safety risk.

There were some non-compliant operator interface displays on draglines that required software upgrades.

The variable speed drives found were assessed and none were found to be affected by Year 2000 problems.

PLCs were bench tested and software scanned. None were found on to have any significant Year 2000 problems. Some had minor issues that were solved with work-arounds.

Various instruments were also assessed for compliance and found to be Year 2000 Ready.

Electrical protection relays were also assessed as Year 2000 Ready.

Air conditioning units were found with date functions.

4.2.2.2 Drill Operations

Most drill equipment did not contain devices that could be affected by Year 2000 problems. Some drills contained PLCs and instrumentation but none were assessed as high or significant risk.

4.2.2.3 Coal Haulage – Mobile Equipment

Some of the large mobile equipment was found to contain electronic control management systems. These systems were used for engine, transmission, brake and load management.

The safety implications of braking management systems placed this equipment into a high or significant safety risk category.

Generally detailed compliance information for these items was hard to obtain and not conclusive in nature. Consequently individual units were tested and shown to have minor Year 2000 non-compliances. The non-compliances were assessed as Year 2000 Ready with minor work-arounds.

4.2.3 Coal Processing

4.2.3.1 Surface Conveyors

Surface conveyors examined covered a variety of drive types from variable speed drives to scoop fluid couplings to direct on line (DOL) starts. The majority of conveyors were protected by overload and earth leakage protection relays, underspeed relays, lanyards, belt drift switches, various drive train instruments and overload devices.

The safety implications of operational trips such as conveyor lanyards placed the control equipment and software into a high or significant safety risk category.

The majority were PLC or DCS (Distributed Control System) controlled and monitored, reporting to Operator Interfaces running on PCs. All were found to be Year 2000 Ready.

4.2.3.2 Stockpile Machines (Stackers & Reclaimers)

The stockpile machines were similar in most cases to land based installations with a few exceptions.

The safety implications of operational trips on the stockpile machines such as conveyor lanyards and travel stops placed the control

equipment and software into a high or significant safety risk category.

Anti-collision systems relied on a variety of sophisticated inputs from tag readers, proximity sensors, multi turn potentiometers, laser distance measuring, ultrasonic distance probes and lanyards.

There were several instances of date functionality that required testing but none were found to be non-Year 2000 Ready.

Most switch rooms were fitted with fire detection and sometimes with fire suppression systems. The fire systems assessed were found to be Year 2000 Ready.

4.2.3.3 Coal Processing Plant (CPP))

Three CPPs are controlled and monitored by DCS and SCADA/PLC systems. All of these systems were software scanned and upgraded/remediated/tested as necessary to ensure that they were Year 2000 Ready.

The work involved extensive bench and simulation testing, contingency/recovery planning to ensure that the full system testing created the minimum disruption to production activity.

The plants contained a variety of instruments for measuring density, weight, pressure, flow, temperature, level and vibration. The equipment was found to be Year 2000 Ready with only minor non-compliances not significant enough to stop the processes.

4.2.3.4 Train Loading

The train loading systems were similar to the CPPs in that they used SCADA/PLCs and a variety of instruments with the addition of rail weighbridges and sensors for train speed. All testing indicated that train loading systems were Year 2000 Ready with only minor exceptions on some date displays.

4.2.4 Surface, Open Cut and Underground Services

4.2.4.1 Gas Detectors

One type of hand held gas detector failed certain tests and required a software upgrade. Larger PC and PLC based gas monitoring systems were found to be Year 2000 Ready except for minor date display problems that did not affect the systems functioning.

The safety implications of gas monitoring placed this equipment and software into a high or significant safety risk category.

4.2.4.2 Weighing

There were a number of different weighing devices recorded. They included conveyor belt weighers, load cell systems for bins, rail track and strain links, some of which were found to contain date functions but none required remediation or replacement. All were found to Year 2000 Ready.

4.2.4.3 Ventilation

There were a variety of systems and equipment supporting the ventilation fans of the underground mines. PLCs and Variable Speed Drives were commonly used for control and most were connected to a higher level monitoring system such as a SCADA running on PCs and reporting fan status to a remote control room.

The safety implications of ventilation placed the control equipment and software into a high or significant safety risk category.

The other devices found included protection relays, overload relays, vibration sensing systems, various instruments for measuring pressure, flow, vane angles and temperature. Most of these systems did not contain any date functions and were classified as NDFs, therefore Year 2000 Ready.

4.2.4.4 Water Pumping

Most water pumping was PLC controlled with some VSDs used for certain applications.

The same devices as supported in the ventilation installations were typically found in pumping installations.

4.2.4.5 Power Distribution

Power distribution uses specialised protection relays and transformer protection devices. Some of the latest protection relays contained date functions and required testing. To date all relays tested have been Year 2000 Ready.

The safety implications of the protection devices placed this equipment and software into a high or significant safety risk category.

A variety of UPS devices supporting the power protection equipment were checked and found not to contain date functions.

Later installations contain PLCs and communications devices. These possessed date functions and were checked as part of the overall SCADA systems.

4.2.4.6 Communications

There are usually several forms of voice communications available including intercoms, radios and telephones which have all been found not to have date functions affecting their operation.

The safety implications of communications in the mining environment placed this equipment into a high or significant safety risk category.

The data communications networks use a variety of technologies including fibre optic and copper based modems, local area networks (both switched and non-switched), radio data links and PLC networks. Predominantly there were only a few devices with date functions, they included the switched network components and smarter modems for the DCS, PLC and SCADA networks.

4.2.4.7 Gas and Goaf Drainage Plants

The equipment used at these installations is similar to the ventilation sites. The addition of specialised gas pumping equipment and associated instrumentation was the main difference. Gas level monitoring, pressure, temperature and flow measurement devices were accounted for and all were found to be Year 2000 Ready.

The safety implications of gas and goaf drainage placed the instruments, control equipment and software into a high or significant safety risk category.

PLCs and SCADA systems were commonly used to control and monitor the installations. These installations were typically tested as part of the system tests for the associated mine monitoring and control systems.

4.2.4.8 Water Reticulation

Surface and underground water reticulation was generally carried out using PLC control and simple instruments. These were connected to larger SCADA systems and monitored centrally. There were no instances of non-Year 2000 Ready equipment interfering with water reticulation.

4.2.4.9 Compressed Air Reticulation

The mine supplies of compressed air were typically derived from surface based compressor facilities. Most compressors were fitted with self-contained control and standby units which had to be tested. There were examples of units with date functions but none required remediation.

The support equipment included protection relays, PLC monitoring to SCADA systems and various instruments that were mostly classified as NDFs.

4.2.4.10 Fire Detection and Suppression

All sites had fire detection and suppression systems at most critical substation locations on the surface. These systems were tested and to date, all were found to be Year 2000 Ready. They are typically fitted with instruments that are classified as NDFs.

4.2.4.11 Mobile Equipment

The smaller mobile equipment used underground and service vehicles on the surface were found not to contain date functions. Some underground mobile equipment contained sophisticated shut down devices triggered by gas levels that were classified as NDFs.

To date no light vehicles have been found to contain date functions that will affect the vehicles operation.

4.2.4.12 Quality Monitoring

Most plants had several sample points for quality measurement either by discreet samples or by continuous measurement using gamma ray sources.

One of the gamma ray measurement systems required significant remediation, upgrades and testing to bring it to Year 2000 Readiness.

4.2.4.13 Potable Water

Potable water plants were sometimes PLC controlled and used configurable instruments for dosing and quality measurement. All plants assessed were found to be Year 2000 Ready.

4.2.4.14 Mines Rescue Facilities

The items and equipment used for Mines Rescue included the specialised vehicles, medical instruments, communications equipment, and computers for records and

mine layouts. All systems tested were found to be Year 2000 Ready.

The safety implications of this equipment placed it all into a high or significant safety risk category.

4.2.5 Building and Security Services

The surface infrastructure was examined in as much detail as other facilities and all relevant equipment and services were investigated. These included office equipment like photocopiers, facsimile machines, PABXs, air conditioning, UPSs, security systems, camera surveillance, computers, networks and printers to name a few. As the majority of this equipment was assessed as low risk, in most cases the manufacturers' Year 2000 Compliance statements were considered sufficient to meet the Embedded Systems Methodology readiness requirements.

Where the system was of a high risk such as the PABX, the system was tested as well as seeking Year 2000 Compliance information. The greater the number of similar items, the higher the possible risk to operations. When this was the case the decision to test was made as required by the methodology. The testing carried out increased Shell Coal's confidence that the group's infrastructure was Year 2000 Ready.

5. CONCLUSIONS

Shell Coal's Year 2000 Embedded Systems Programme examined 4,470 items comprising 1293 different models from 417 manufacturers across the seven mine sites and two offices during a period of two years. The bulk of the work was carried out over the last eighteen months and achieved a high level of readiness for the Shell Coal Group's entire Embedded Systems infrastructure.

The risk and compliance assessment along with the various levels of testing and contingency planning carried out have provided Shell Coal with a high level of confidence that its mines will be able to operate given sufficient levels of infrastructure services from power, water, transportation and telecoms.

Shell Coal is confident that the implementation of the overall Year 2000 Programme including the Embedded Systems work described has significantly reduced the risks to the organisation from safety, environmental and operational (financial) impacts of Year 2000 related problems.

The level of Year 2000 non-compliances found was relatively low and remediation formed only a small percentage of the total work. Until the level of equipment and software compliance was determined, there was no other effective alternative but to thoroughly examine the Embedded Systems without exposing the organisation to an unacceptable risk.

The testing of more complex systems such as SCADA, DCS and PLCs provided confidence that the critical mining and processing functions could operate safely without risk of injury to personnel or infrastructure.

6. RECOMMENDATIONS

One recommendation at this late stage on Year 2000 Embedded Systems or any other potentially Year 2000 impacted systems would be to consider implementing equipment contingency and business continuity plans in conjunction with system testing of high risk processes.

A principle that could be adopted is that it may be better to experience breakdowns now under controlled conditions than to leave systems to fail when resources and spare parts are difficult to obtain after January 2000.

Shell Coal would strongly recommend that organisations determine equipment and software that have a high safety risk and at least obtain definitive compliance information from the manufacturer or vendor. A number of each item should be fully tested providing a 'statistical' confidence that the equipment is Year 2000 Ready.

Although not a thorough approach the recommendations provide an alternative with the limited time available to the extended process carried out by Shell Coal and most other mining companies. The ability to recover systems and equipment in the event of Year 2000 failures and/or failures of external infrastructure would greatly improve a company's ability of surviving the potential interruptions that the Year 2000 Date Processing Problems may bring.

Shell Coal is carrying out both equipment Contingency Planning and Business Continuity Planning as vital components of their Year 2000 Programme. There are a number of organisations that can assist in these processes. As time is quickly running out, the entire process would need to be greatly compressed. Even at this point in time it is not too late to take action to improve an organisation's ability to survive the known

effects of Year 2000 Date Processing Problems.

7. ACKNOWLEDGMENTS

7.1 Shell Coal Embedded Systems Programme Team Members

The following people were critical to the implementation of the Shell Coal Year 2000 Embedded Systems Programme:

Garry Brell Team Leader/Shell Coal
Tony Napton Resource Manager/Strategist
Emma Bromley Administration/Organisation
John Edwards Y2K Engineer - Callide
Mark Jacobson Y2K Engineer - Capcoal
David Paige Y2K Engineer - Dartbrook
Kieran Nolan Y2K Engineer - Drayton
Giulian Fava Y2K Engineer - Moranbah
Kingsley Plows Y2K Engineer - Compliance Assessment, Brisbane and Sydney Coal Offices

The Brisbane based Embedded Systems team peaked at up to 15 members. The Brisbane based Embedded Systems Engineers were provided through Tim Haight of Nulec Projects Pty Ltd, Brisbane.

7.2 Infrastructure Control Services (ICS) Pty Ltd, Brisbane.

ICS, Brisbane provided both methodology and a knowledge base that was combined with Shell International's methodology to seed the Shell Coal Year 2000 Embedded Systems Programme.

7.3 Shell Coal Year 2000 Programme Site Focal Points and Engineers

The Site Year 2000 Engineers and Focal Points were essential to the successful implementation of the Shell Coal Year 2000 Embedded Systems Programme and methodology.

8. SHELL COAL Y2K EMBEDDED SYSTEMS PROGRAMME DISCLOSURE STATEMENT

This document contains Year 2000 related information about Shell Coal Pty Ltd and companies in the Shell Coal Group and is a Year 2000 disclosure statement for the purposes of the Year 2000 Information Disclosure Act 1999. A person may be protected by that Act from liability for disclosing information in certain circumstances.

Shell Coal Pty Ltd and its group of companies make no guarantees or warranties with respect to the information provided in this document and take no responsibility for its use under any circumstances.

9. AUTHORISATION AND COPYRIGHT

This paper is authorised by Shell Coal Pty Ltd for presentation at the Queensland Mining Industry Health and Safety Conference, on the 23rd of August 1999 at Yeppoon, Queensland.